CySicuro?
security

2024 REPORT

MARCH 2024

Prepared by

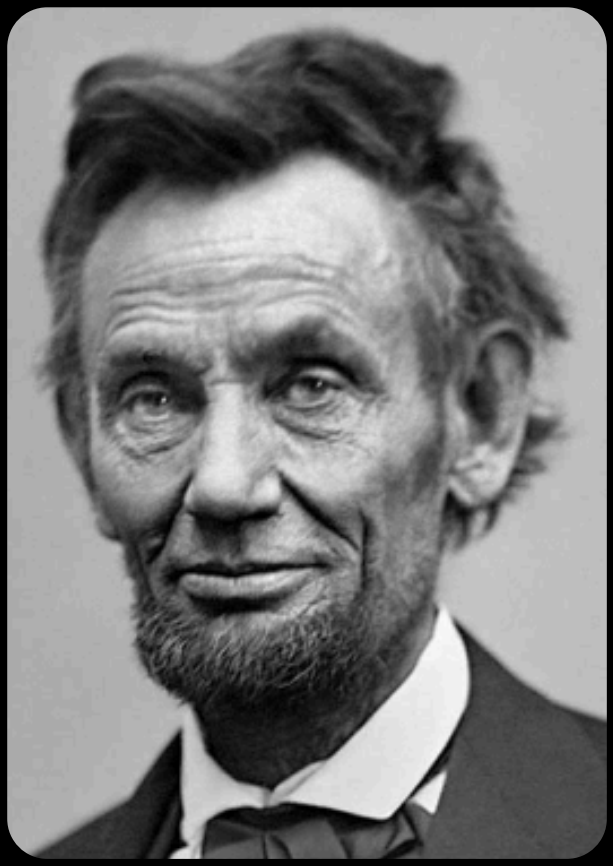
Matteo Tedesco
Federico Biggi
Max Aldrovandi

Prepared for

Virtual Maison SRL.

Table of Contents

Letter from the CEO



Abrahim El Lincoln

CEO CySicuro?

Location:
Via Gramsci 10, 81054, Caserta(CE)

P.IVA:
00000000001

Contacts:
abrahim.el.lincoln@libero.it
366-6961669

Dear LIDL ITALIA,
We would like to express our sincere gratitude for selecting 'CySicuro?' as your partner for conducting the Vulnerability Assessment at your esteemed company, Virtual Maison SRL.
We are honored by the trust you have placed in our expertise and are committed to providing a high-quality service that meets the highest standards in the cybersecurity industry. Our team of experts is excited to begin this collaboration and to work closely with your team to identify and mitigate any vulnerabilities in your systems.
The security of your information is our top priority, and we will do our utmost to ensure that your data is protected and secure. We are confident that this collaboration will not only strengthen your security infrastructure but also pave the way for future opportunities for improvement and innovation.
We are available for any needs or clarifications throughout the entire process, and we invite you to contact us at any time to discuss details or any other requirements.
Once again, thank you for choosing 'Cysicuro?'.
We look forward to starting this project and building a successful and lasting relationship with your company.
Best regards,

CEO
CySicuro?
abrahim.el.lincoln@libero.it
366-6961669

Abrahim EL Lincoln

Security Operation

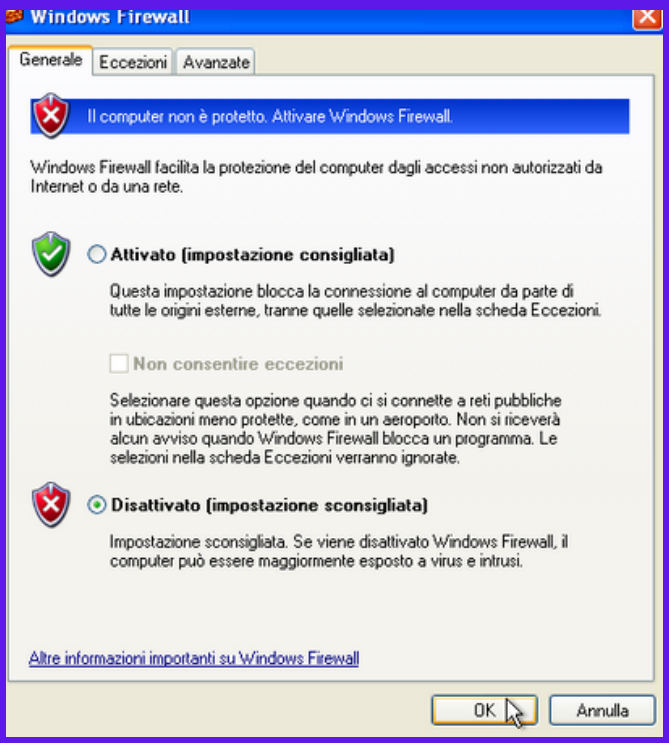
Request:

During the theoretical lesson, we studied preventive actions to reduce the likelihood of attacks from external sources.
We learned that at the network level, we can activate/configure firewalls and rules to ensure that potentially harmful traffic is blocked.
The Windows XP machine we used has the firewall disabled by default. Today's exercise is to verify how enabling the firewall impacts the results of an external service scan. Therefore:

Ensure that the firewall is disabled on the Windows XP machine.
Perform a scan with Nmap on the target machine (use the switch **-sV** for service detection and **-o** filename to save the output to a file).
Enable the firewall on the Windows XP machine.
Perform a second scan with Nmap, once again using the switch **-sV**.
Identify and comment on any differences.

Requirementes:
Configure the address of Windows XP as follows: **192.168.240.150**
Configure the address of the Kali machine as follows: **192.168.240.100**

FIREWALL OFF:



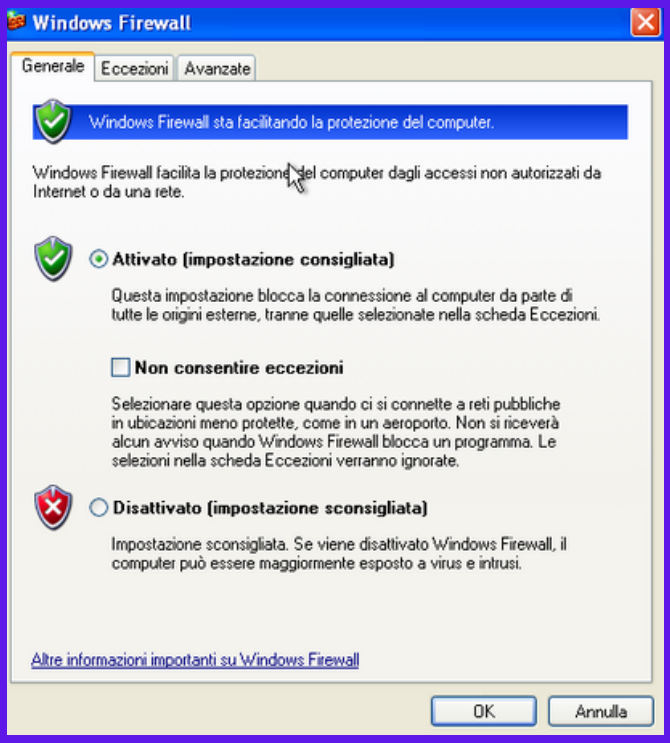
FIRST SERVICE SCAN:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.159 -o xpreport
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 04:37 EDT
Nmap scan report for 192.168.240.159
Host is up (0.0024s latency).
Not shown: 997 closed tcp ports (conn-refused)
PORT    STATE SERVICE      VERSION
135/tcp open  msrpc        Microsoft Windows RPC
139/tcp open  netbios-ssn  Microsoft Windows netbios-ssn
445/tcp open  microsoft-ds Microsoft Windows XP microsoft-ds
Service Info: OSs: Windows, Windows XP; CPE: cpe:/o:microsoft:windows, cpe:/o:microsoft:windows_xp

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 20.47 seconds
```

Nmap is a scanning tool that helps us in a lot of ways: it can scan single hosts or a large number of them, see which ports are open and which not, which services are in use, it can fingerprint the OS and much more.
In this istance we used the switch -sV which is a scan thata enumerates the services on the ports of the target machine.
As we can see port **135**, **139** and **445** are open and running 3 distinct services: msrpc, netbios-ssn and microsoft-ds. In the provided Nmap command, the -o option specifies that the scan output should be saved to a file. Without this option, the output would only be displayed on the command line. Using -o allows you to save the scan results to a text file for later analysis or reference.

FIREWALL ACTIVATED:



Once the firewall is up and running, let's scan the target host again.
As we can see , it appears that the host is down but **Nmap** gives us a valuable info: the **-Pn switch**.
The -Pn switch in Nmap is used to scan a network without first checking if the host is online.
It skips the ping step and assumes the target is up, which is useful for bypassing firewalls that block ping requests

SECOND SERVICE SCAN:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.159 -o xpreport
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 04:48 EDT
Note: Host seems down. If it is really up, but blocking our ping probes, try -Pn
Nmap done: 1 IP address (0 hosts up) scanned in 3.12 seconds
```

We will enable the Windows Defender Firewall to observe its impact on network traffic and project visibility. The Windows Defender Firewall is a built-in security feature that helps protect your computer from unauthorized access by filtering incoming and outgoing network traffic. By enabling the firewall, we can monitor and control which applications and services can communicate with your computer over the network.

THIRD SERVICE SCAN:

```
┌──(kali㉿kali)-[~]
└─$ nmap -sV 192.168.240.159 -Pn
Starting Nmap 7.94SVN ( https://nmap.org ) at 2024-06-03 04:49 EDT
Nmap scan report for 192.168.240.159
Host is up.
All 1000 scanned ports on 192.168.240.159 are in ignored states.
Not shown: 1000 filtered tcp ports (no-response)

Service detection performed. Please report any incorrect results at https://nmap.org/submit/ .
Nmap done: 1 IP address (1 host up) scanned in 221.87 seconds
```

With our third scan, we can confirm that the firewall is working, as all the scanned ports are in an ingnored state.
This means that the ports are filtered.
A filtered port means the firewall is blocking Nmap's attempt to check that port.
The firewall either drops the request or does not respond, so Nmap cannot determine whether the port is open or closed. In this case the firewall is shielding all the 1000 ports. Using a firewall to filter ports is one effective way to prevent any malicious action against the protected host.

Security Operation Quotation

Service fees:
Labor cost -> 100€/h
Employees -> 3

Tools:
Fees for cost of tools used

Service fees

€ 2.400

Tools

€ 200

Business Continuity

In today's fast-paced and interconnected world, unforeseen disruptions can pose significant risks to your business operations. At ‘Cysicuro?’, we understand the critical importance of maintaining seamless operations regardless of the challenges you face. Our Business Continuity Service is designed to ensure your company remains resilient and operational, even in the face of unexpected events.

As requested during the engagement phase, we proceeded to quantitatively assess the impact of events such as:
- **earthquake**
- **flooding**
- **fire**

on your company.

In particular, we have provided a quantification of the possible 'annual loss' that your company would suffer should such events occur.

Planning and purpose

CORE SERVICES ASSESSMENT:

To begin, we did an assessment of your company's core services in order to identify which services are most important to you and to prioritize goals in our operations to ensure business continuity.

Core Service:

- Data center
- Cloud service
- Employee

TEAM BUILDING:

Then we proceeded with the creation of a **team responsible** for the **Business Continuity Plan**.

Therefore, we identified:


Hu Shimazaki - *sales and financial advisory department*


Harry Foster - *development department*


Ezra Bonner - *IT services expert*


Lisa Odom - *member of the Cybersecurity Team*


Isabella Waller - *member of the Legal Team*


Rita Green - *human resources department*


Mario Rossi - *member of the physical security team*


Ignacio Abbott - *executive representative*

RESOURCES AND ASSETS ASSESSMENT:

Finally, we carried out an assessment of the available resources and assets that will be included in business continuity activities:

- **BCP DEVELOPMENT:**
  for the development of the continuity plan the resources involved is mostly attributable to human capital such as the team involved in the BCP process and possibly the cost of external staff required to support it.

- **TESTING, MAINTENANCE AND EMPLOYEE TRAINING:**
  the BCP needs to be tested, maintained, but most importantly, training sessions/lessons need to be organized for employees in order to show how the BCP works. Therefore, the effort required by this phase, in addition to human capital, is also partly attributable to software / hardware costs to be made available especially for the employee training phases.

- **IMPLEMENTATION OF THE TCB:**
  finally, in the event of a disaster, the BCP must be implemented which requires not only human capital but also a use of resources and means.

Total Estimate

Cost Item	Estimated Cost (€)
Project Manager	8,000
Security Analyst	7,200
IT Specialist	5,000
Administrative Staff	2,400
BCP Consultant	20,000
Training Workshops	6,000
BCP Management Software	4,000
Travel and Accommodation	3,000
Total	**55,600**

Bias Impact Analysis

Earthquake

Quantitativity:

The company asked us to calculate the damage losses in case an earthquake would damage its three properties: **Building 1, Building 2 and the Data Center**. We gathered the necessary data and made the calculations. First we looked into the **Annualized rate of Occurence (ARO)** of the event, as in how many times can the event happen in a period of time measured in years. For the earthquake it's one time every 30 years.
Then we got the **Asset Value (AV)** for the 3 buildings. Each asset is assigned what is called an **Exposure Factor (EF)**, measured as the percentage of the asset that would be impacted as a result of the specific event occurring.
The concept of **Single Loss Expectancy (SLE)** is introduced, which gives us a monetary measure of the loss that would be incurred if the event were to occur. It is calculated as the product of the asset value (**AV**) and the percentage impacted in the event (**EF**). The formula is **SLE = AV x EF**
If we now want the value of the loss incurred over a period of one year, called the **Annualized Loss Expectancy (ALE)**, we would need to multiply the value of the **SLE** by the estimated number of times the event is expected to occur in a year (**ARO**). The formula is **ALE = SLE x ARO.**

FACILITIES	ARO	AV	EF	SLE	ALE
BUILDING 1	1 every 30 years	350.000	80%	280.000	8.400€
BUILDING 2	1 every 30 years	150.000	80%	120.000	3600€
DATA CENTER	1 every 30 years	100.000	95%	95.000	2.850€

Flood

Quantitativity:

The company asked us to calculate the damage losses in case a flood would damage its three properties: **Building 1, Building 2 and the Data Center**. We gathered the necessary data and made the calculations. First we looked into the **Annualized rate of Occurence (ARO)** of the event, as in how many times can the event happen in a period of time measured in years. For the flood, it's one time every 50 years.
Then we got the **Asset Value (AV)** for the 3 buildings.
Each asset is assigned what is called an **Exposure Factor (EF)**, measured as the percentage of the asset that would be impacted as a result of the specific event occurring.
The concept of **Single Loss Expectancy (SLE)** is introduced, which gives us a monetary measure of the loss that would be incurred if the event were to occur. It is calculated as the product of the asset value **(AV)** and the percentage impacted in the event **(EF)**. The formula is **SLE = AV x EF**
If we now want the value of the loss incurred over a period of one year, called the **Annualized Loss Expectancy (ALE)**, we would need to multiply the value of the SLE by the estimated number of times the event is expected to occur in a year **(ARO)**. The formula is **ALE = SLE x ARO**.

FACILITIES	ARO	AV	EF	SLE	ALE
BUILDING 1	1 every 50 years	350.000	55%	192.500	3.850€
BUILDING 2	1 every 50 years	150.000	40%	60.000	1.200€
DATA CENTER	1 every 50 years	100.000	35%	35.000	700€

Fire

Quantitativity:

The company asked us to calculate the damage losses in case a fire would damage its three properties: **Building 1, Building 2 and the Data Center**. We gathered the necessary data and made the calculations.
First we looked into the **Annualized rate of Occurence (ARO)** of the event, as in how many times can the event happen in a period of time measured in years. For the flood, it's one time every 20 years.
Then we got the **Asset Value (AV)** for the 3 buildings.
Each asset is assigned what is called an **Exposure Factor (EF)**, measured as the percentage of the asset that would be impacted as a result of the specific event occurring.
The concept of **Single Loss Expectancy (SLE)** is introduced, which gives us a monetary measure of the loss that would be incurred if the event were to occur. It is calculated as the product of the asset value **(AV)** and the percentage impacted in the event **(EF)**. The formula is **SLE = AV x EF**
If we now want the value of the loss incurred over a period of one year, called the **Annualized Loss Expectancy (ALE)**, we would need to multiply the value of the SLE by the estimated number of times the event is expected to occur in a year **(ARO)**. The formula is **ALE = SLE x ARO**.

FACILITIES	ARO	AV	EF	SLE	ALE
BUILDING 1	1 every 20 years	350.000	60%	210.000	10.500€
BUILDING 2	1 every 20 years	150.000	50%	75.000	3.750€
DATA CENTER	1 every 20 years	100.000	60%	60.000	3.000€

Qualitativity:

We then proceeded to make a generic 'qualitative' damage assessment that could occur as a result of disasters such as those listed above, below is a summary of the hypothetical damages identified:

- Loss of Trust and Reputation:
  - Customers: The company's ability to respond quickly and effectively to a crisis can influence customers' perception of its reliability and stability.
  - Investors and Stakeholders: Investors' perception can be negatively impacted, reducing confidence in the company's management and continuity capabilities.

- Impact on Employees:
  - Morale and Motivation: Employees' safety and well-being can be compromised, leading to a decline in morale and motivation.
  - Productivity: A stressful and insecure work environment can reduce productivity and increase employee turnover.

- Disruption of Business Processes:
  - Operational Interruptions: Production and operational processes can be disrupted, causing delays and inefficiencies.
  - Data Loss: The loss or damage of company data can hinder normal operations and decision-making capabilities.

- Communication Problems:
  - Internal Communication: Lack of effective internal communication during and after the earthquake can create confusion and disorganization.
  - External Communication: The ability to communicate with customers, suppliers, and other stakeholders can be compromised, negatively affecting relationships.

Qualitativity:

- Compliance and Regulations:
  - Regulatory Delays: Disruptions can cause delays in compliance with regulations and standards, exposing the company to penalties and other legal consequences.

- Corporate Culture:
  - Changes in Corporate Culture: The traumatic event can alter the corporate culture, negatively impacting the work environment and shared values.

- Impact on the Supply Chain:
  - Supply Chain Disruption: The ability to provide products or services can be compromised due to disruptions in the supply chain.

- Innovation and Competitiveness:
  - Project Delays: Innovation and development projects may experience delays, reducing the company's competitiveness in the market.

Threat Intelligence

At '**CySicuro**?', we specialize in advanced threat intelligence and Indicators of Compromise (IOC) services to safeguard your organization against cyber threats. Our expert team provides comprehensive threat analysis, proactive monitoring, and actionable insights to help you identify and mitigate potential risks. Trust CyberIntel Solutions to protect your digital assets and ensure your business resilience.

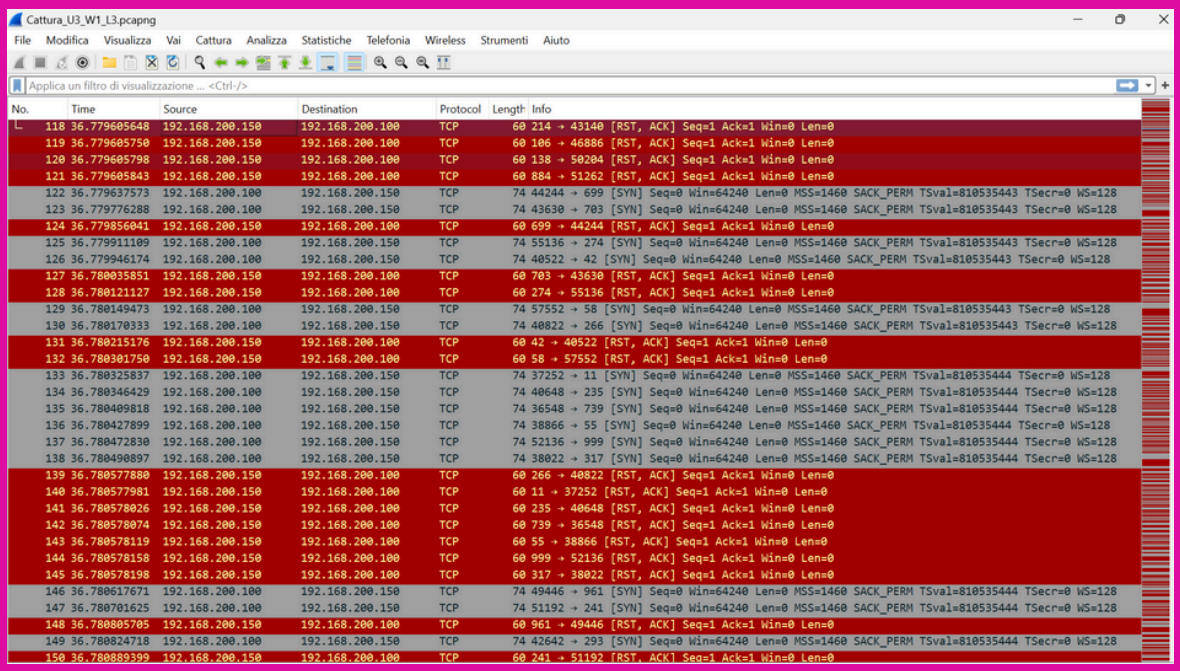
As requested during the engagement phase, we proceeded with an analysis of the **company's network traffic** to identify any **IOCs**, i.e., evidences of ongoing attacks.

We then proceeded with the analysis of such evidence and the proposal of possible solutions.

IOC IDENTIFICATION:

The **IOC**, or **Indicators of Compromise**, are pieces of forensic data that identify potentially malicious activity on a network or system.
These indicators serve as warning signs or red flags that a security breach or attack may have occurred.
IOCs help cybersecurity professionals detect, respond to, and prevent cyber threats by providing evidence of compromise.

During the analysis of Wireshark packets, we identified **suspicious network activity** indicating a potential ongoing attack.
The analysis revealed repeated TCP requests, suggesting a scanning activity targeting the **IP address 192.168.200.150**, originating from **192.168.200.100**.
The pattern observed indicates a high volume of TCP (SYN) requests on various ports, strongly indicative of a scanning operation by the host **192.168.200.100** towards **192.168.200.150.**



Repetitive TCP (SYN) requests originating from 192.168.200.100 towards 192.168.200.150.
Scanning activity observed on multiple ports, with responses indicating port status.
Positive responses (**SYN+ACK**) from the target indicating open ports, while **negative responses** (**RST+ACK**) signify closed ports.

ASSUMPTIONS ABOUT ATTACK VECTORS USED:

Based on the data collected, we hypothesized that this could be a **port scanning**.
Indeed the repeated TCP (SYN) requests observed on various ports from a single source IP could indicate a port scanning attempt.
This could be a precursor to a more targeted attack, where the attacker is seeking vulnerable services or open ports for exploitation.

PROPOSAL OF POSSIBLE SOLUTIONS:

In order to avoid or at least limit this type of attack we suggest:

- To configure firewall rules on the network perimeter to block incoming traffic from the IP address 192.168.200.100.
- To monitor network traffic for any further suspicious activity and adjust firewall rules accordingly.
- To conduct regular network security assessments to identify and address potential vulnerabilities proactively.

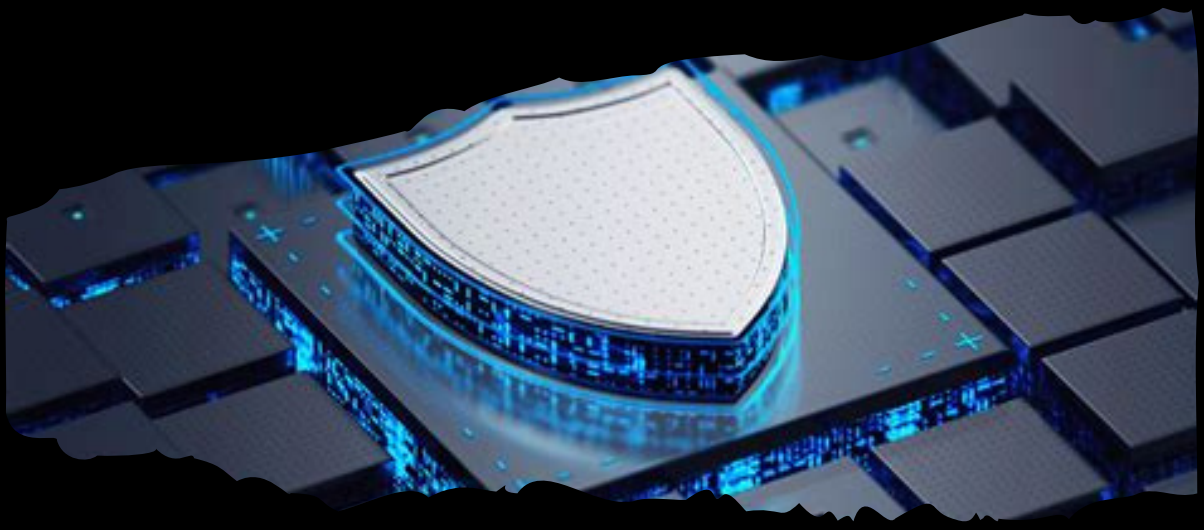
So, to conclude, the analysis indicates a significant threat posed by the scanning activity originating from 192.168.200.100 towards 192.168.200.150. By implementing proactive measures such as firewall rules, we can effectively mitigate the risk and enhance the overall security posture of the network.

Incident Response

In today's digital landscape, the inevitability of cybersecurity incidents poses a significant challenge to organizations worldwide. With the proliferation of sophisticated threats and the increasing interconnectedness of systems, the need for a robust Incident Response (IR) plan has never been more critical.

At CySicuro we understand the importance of proactive measures to mitigate the impact of cybersecurity incidents. Our comprehensive Incident Response strategy is designed to swiftly and effectively address security breaches, minimizing disruption and safeguarding sensitive assets.

In the event of a security incident, it is essential for all employees to understand their roles and responsibilities outlined in this Incident Response Plan. By familiarizing yourself with the provided guidelines and protocols, you will play a crucial role in maintaining the security and integrity of our organization's digital infrastructure.



PREPARATION:

The preparation phase is crucial to ensure that our organization is adequately equipped to respond to cyber incidents effectively. This phase involved several key activities aimed at enhancing our incident response capabilities.
Here we have limited ourselves to a list of preliminary actions necessary for the implementation of an incident response plan

1. Incident Response Plan (IRP)

- Development: We developed a comprehensive Incident Response Plan (IRP) that outlines the objectives, scope, and structure of our incident response efforts. This plan includes detailed procedures for detecting, analyzing, containing, eradicating, and recovering from cyber incidents.
- Roles and Responsibilities: Specific roles and responsibilities were defined for each member of the incident response team. This ensures that each team member is aware of their duties during an incident.
- Communication Plan: A communication strategy was established to facilitate timely and effective communication both internally and externally. This includes protocols for reporting incidents and escalating critical issues.

2. Incident Response Team (IRT)

- Team Formation: A cross-functional Incident Response Team (IRT) was assembled, comprising members from IT, security, legal, HR, and public relations departments.
- Training: The IRT underwent regular training sessions to familiarize themselves with the IRP and their specific roles within it.
- Tools and Resources: The team was equipped with the necessary tools and resources, including advanced detection and analysis tools, to effectively respond to incidents.

3. Risk Assessments

- Asset Inventory: An up-to-date inventory of critical assets, including hardware, software, and data, was maintained.
- Threat Intelligence: We gathered and analyzed threat intelligence to understand potential threats and attack vectors. This helped in tailoring our defenses against the most likely threats.
- Vulnerability Management: Regular vulnerability assessments and penetration tests were conducted to identify and mitigate security weaknesses.

4. Detection Mechanisms

- Monitoring Systems: Intrusion Detection Systems (IDS), Intrusion Prevention Systems (IPS), and Security Information and Event Management (SIEM) solutions were implemented and maintained.
- Logs and Alerts: Comprehensive logging of network, system, and application activities was ensured, and alerts were configured for suspicious activities.

5. Incident Handling Procedures

- Playbooks: Detailed playbooks were created for various types of incidents, outlining specific steps for handling each scenario.
- Containment Strategies: Strategies for both short-term and long-term containment were developed to prevent the spread of attacks.
- Eradication Procedures: Procedures for removing threats from our environment once contained were clearly defined.

6. Communication Protocols

- Internal Communication: Protocols for notifying relevant internal stakeholders, including executive management, were developed.
- External Communication: Guidelines for communicating with external parties, such as customers, partners, and regulatory bodies, were established. Templates for public statements and notifications were also prepared.

7. Training and Drills

- Tabletop Exercises: Regular tabletop exercises were conducted to simulate incident scenarios and test our response plan.
- Live Drills: Live incident response drills were performed to practice and refine our procedures under real-world conditions.

8. Legal and Regulatory Compliance

- Legal Requirements: We stayed informed about legal and regulatory requirements related to incident reporting and data protection.
- Documentation: All actions taken during the preparation and response phases were thoroughly documented to meet compliance obligations.

9. Post-Incident Review Process

- Lessons Learned: Post-incident reviews were conducted to identify strengths and areas for improvement.
- Continuous Improvement: The IRP and procedures were updated based on findings from post-incident reviews to ensure continuous improvement.

10. Security-Aware Culture

- Awareness Programs: Ongoing security awareness programs were implemented to educate employees about security best practices and the importance of reporting suspicious activities.
- Phishing Simulations: Regular phishing simulations were conducted to test and improve employees' ability to recognize and respond to phishing attacks.

DETECTION AND ANALYSIS:

The detection and analysis phase is one of the most challenging to manage as an automated and continuous routine process. In fact, although there are various tools available for the monitoring and analysis phase, some incidents can only be detected by highly experienced personnel.
Once a suspect is confirmed, the CSIRT team must promptly begin the analysis and detection procedure to confirm that the incident is ongoing.

The main activities of this phase include:

- **Alert Monitoring**: Monitoring alerts originating from an intrusion prevention and detection system (IPS/IDS), a SIEM, or an antivirus system. Automatic alerts are triggered when a suspicious event occurs.

- **Log Analysis:** Reading logs generated by an operating system, a service, an application, a network device, and all hardware and software devices capable of producing logs.

- **Vulnerability and Exploit Research:** Checking for public information about newly discovered vulnerabilities and exploits (0-day) or those discovered in controlled environments.

- **Incident Reporting and Response Coordination:** Look out for internal or external individuals who report suspicious activities that might indicate an ongoing security incident.

- **Network and System Profiling**: This activity enhances an organization's ability to identify suspicious activities within the network and systems.

- **Implementation of UEBA Tools**: User and Entity Behavior Analytics (UEBA) tools are software developed to profile user behavior to identify any suspicious activities.

- **Creation of Effective Logging Policies**: Logs should contain all important information, such as user logins and logouts and administrative changes.

- **Event Correlation**: Correlating events from multiple sources allows tracking all steps of a potential ongoing attack, identifying possible points of access on the network or systems and any changes made. Generally, this correlation is handled by SIEM/SOAR. To ensure successful correlation, it is necessary for various network devices, computers, etc., to have synchronized time (with each other using NTP software or with the Internet).

- **Traffic Capture:** If continuous traffic capture is not provided by the company, once a security incident is verified, the CSIRT team should immediately begin capturing all traffic for subsequent analysis, e.g., using Wireshark or other software.

CONTAINMENT, ERADICATION AND RECOVERY:

Containment

During the detection and analysis phase, the CSIRT team initiates initial activities to uncover how the incident occurred, which systems it has impacted, and which systems may be at risk next. Once the assessments are completed, the team must promptly find a solution to minimize the impacts of the incident. This formally begins the containment, eradication, and recovery phase, which has the following main objectives, as can be understood from the name:

- **Reduction of the impacts caused by the incident**
- **Elimination of the incident from the network and systems**
- **Recovery of services and standard operations**

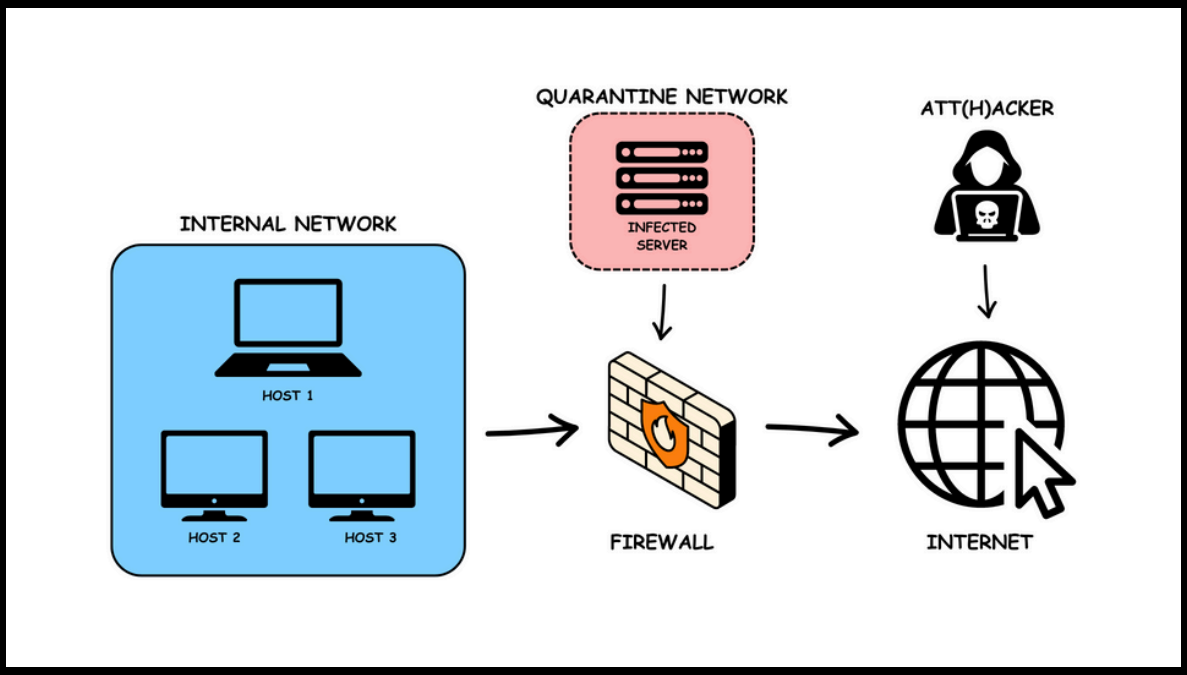
The first step of the third phase of an incident response plan is the **containment of the damage caused by the security incident**, which should begin as soon as possible once the analysis phase is complete. Containment activities have the primary objective of isolating the incident to prevent it from causing further harm to networks/systems.

For example, if a computer on a network has been infected with malware, the first activity to contain the impacts is to isolate the system from the rest of the network so that the malware does not spread to other nodes.

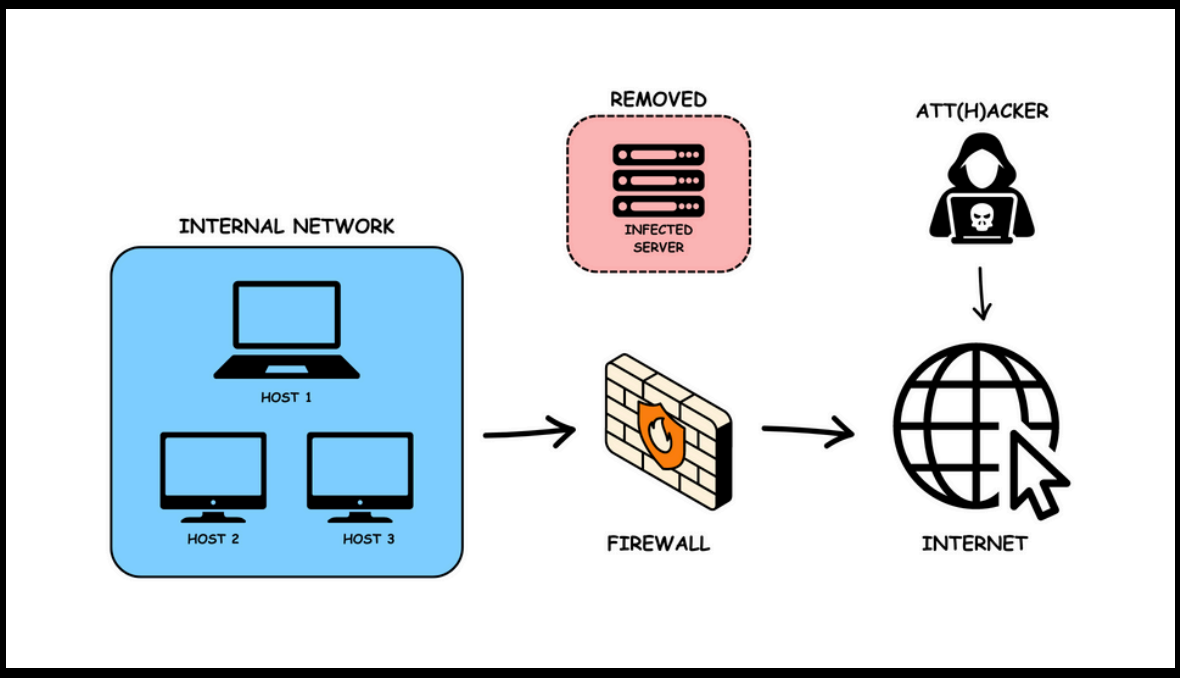
Let’s imagine that a hacker has successfully infiltrated Lidla Italia’s network and taken control of a database which contains lots of storages disks.

Our reaction to prevent and manage the incident in this case is to use a tecnique called "**segmentation**," which proves to be particularly useful in the containment phase of an ongoing incident. Segmentation includes all activities that allow for dividing a network into different LANs or VLANs.

It allows for the separation of the infected database from other computers on the network by creating an ad hoc network, which is generally called a "**quarantine network.**"



This in particular is known as **Isolation**. The isolation technique allows for isolating an infected system by restricting the attacker's access to the internal network. However, the infected system will still be accessible to the attacker via the internet. We can go a step further with it and remove completely the infected asset.



The **removal** technique completely eliminates the system from the network, effectively making it inaccessible from both the internal network and the internet. We can remove it by unplug it from the powerThis approach restricts the attacker's access to the internal network and ensures they no longer have access to the infected system.

Eradication

In this phase, the goal is to eliminate all activities, components, and processes remaining from the incident within the network or on the systems. This activity may include, for example, removing any backdoors installed by malware, or cleaning up compromised disks and USB sticks. The removal step depends greatly on what type of security incident is taking place. A detailed list of activities to be followed by macro-incident should be listed in the “playbooks.”

Recovery

Recovery is a crucial phase in the Incident Response plan that focuses on restoring and validating system functionality after a security incident. The goal of the recovery phase is to ensure that all affected systems are clean, secure, and operational, thereby minimizing downtime and disruption to business operations. This phase involves several key steps:

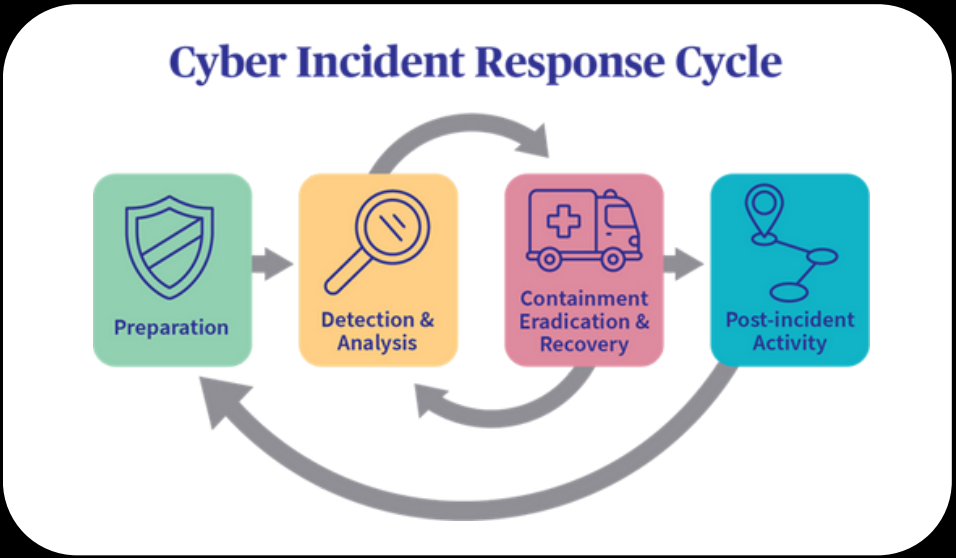
1. Restoration of Systems:
   - Bringing affected systems back online after they have been cleared of any malicious software or vulnerabilities. This may involve reinstalling operating systems, restoring from clean backups, and reconfiguring systems to ensure they are secure.
2. Validation and Testing:
   - Verifying that all systems are functioning correctly and securely. This includes running comprehensive tests to ensure that no remnants of the attack remain and that all systems are operating as expected.
3. Monitoring:
   - Implementing enhanced monitoring measures to detect any signs of recurring issues or reinfection. Continuous monitoring helps to ensure that the recovery has been successful and that the systems remain secure.
4. User Communication:
   - Informing relevant stakeholders and users about the recovery status, including any changes or updates made during the recovery process. Clear communication ensures that users are aware of what has been done and any necessary steps they need to take.
5. Documentation:
   - Documenting all actions taken during the recovery phase to provide a comprehensive record of the incident and response. This documentation is valuable for future reference and for improving incident response procedures.

6. Documentation:
    - Documenting all actions taken during the recovery phase to provide a comprehensive record of the incident and response. This documentation is valuable for future reference and for improving incident response procedures.

Data Sanitization Techniques:

1. **Clear:**
    - Definition: The process of erasing data in a way that it cannot be easily recovered using standard data recovery tools. Clearing typically involves overwriting the existing data with random values or zeros.
    - Use Case: Clearing is suitable when the goal is to prevent data from being recovered using simple recovery methods. It is often used when the media will be reused within the organization.
    - Example: Overwriting the entire disk of the infected server with random data to ensure that the previous information cannot be easily retrieved.
2. **Purge:**
    - Definition: A more rigorous form of data removal that involves eliminating data to a level where it cannot be recovered even with advanced forensic techniques. Purging may include degaussing or the use of specialized software to sanitize the media.
    - Use Case: Purging is appropriate when the media may leave the organization's control or when the data is highly sensitive, requiring a higher assurance level that it cannot be recovered.
    - Example: Using a degausser to erase all magnetic storage on the server's hard drives, ensuring that data cannot be recovered by any means.
3. **Destroy:**
    - Definition: The process of physically destroying the media to ensure that data cannot be recovered by any means. This can involve shredding, crushing, or incinerating the storage devices.
    - Use Case: Destroying is necessary when the highest level of data security is required, and there is no intention of reusing the media. It is often used for highly sensitive or classified information.
    - Example: Physically shredding the server's hard drives to irreversibly destroy the media and all data it contains.

POST-INCIDENT ACTIVITY:



The final phase of an Incident Response plan is the post-incident analysis, often referred to as "**lessons learned**."
This critical phase involves reflecting on the incident to identify what could have been done better and what measures could have been taken to prevent certain situations. The lessons learned analysis is invaluable for learning from mistakes and **improving future responses.**

During this analysis, the following questions are posed to the various teams involved in the entire Incident Response program:

- **What happened, at what time, and what were the consequences?**

  This question helps to create a detailed timeline and impact assessment of the incident.

- **How well did the staff manage the incident situation?**

  This evaluates the effectiveness of the response team's actions and decisions during the incident.

- **What could have been done more or better?**

  This seeks to identify areas where improvements can be made in response procedures, communication, and resource allocation.

- **What additional resources are necessary to better analyze, detect, and respond to a future incident?**

  This helps to determine any gaps in current resources and what is needed to enhance the organization's incident response capabilities. The answers to these questions are crucial for improving the preparation phase of the Incident Response lifecycle.

GUIDELINES FOR FUTURE INCIDENTS:

1. Preparation:

- Incident Response Plan: Regularly update the incident response plan to reflect new threats and vulnerabilities.
- Training: Conduct frequent training sessions for staff on incident detection, response protocols, and the use of security tools.
- Tools: Ensure that all necessary tools for detection, containment, and eradication are up-to-date and readily available.

2. Identification:

- Monitoring: Implement continuous network and endpoint monitoring to detect unusual activities promptly.
- Alerting: Establish clear alert thresholds and ensure that alerts are actionable and properly escalated.

3. Containment:

- Isolation Procedures: Develop and document procedures for quickly isolating compromised systems.
- Network Segmentation: Implement network segmentation to limit the lateral movement of attackers.

4. Eradication:

- Malware Removal: Use advanced malware detection and removal tools to ensure thorough cleaning of infected systems.
- Patching: Regularly apply security patches and updates to all systems to mitigate known vulnerabilities.

5. Recovery:

- System Restoration: Establish procedures for securely restoring systems from backups.
- Validation: Validate that systems are free from malware and fully operational before reconnecting to the network.

6. Lessons Learned:

- Post-Incident Review: Conduct a detailed review of each incident to identify strengths and areas for improvement.
- Documentation: Maintain comprehensive documentation of incidents and response actions for future reference.
- Continuous Improvement: Use insights gained from incidents to update and enhance the incident response plan and overall security posture.

By adhering to these guidelines, organizations can improve their preparedness for cybersecurity incidents, ensuring a swift and effective response to minimize impact and prevent future occurrences.

Case Study

In this section we have carried out an example case study so as to show your company in the most practical way possible how to go about it.

We decided to divide this case study into several steps:

1. Preventive actions : what preventive actions are necessary to put in place to protect yourself from an attack by an attacker.

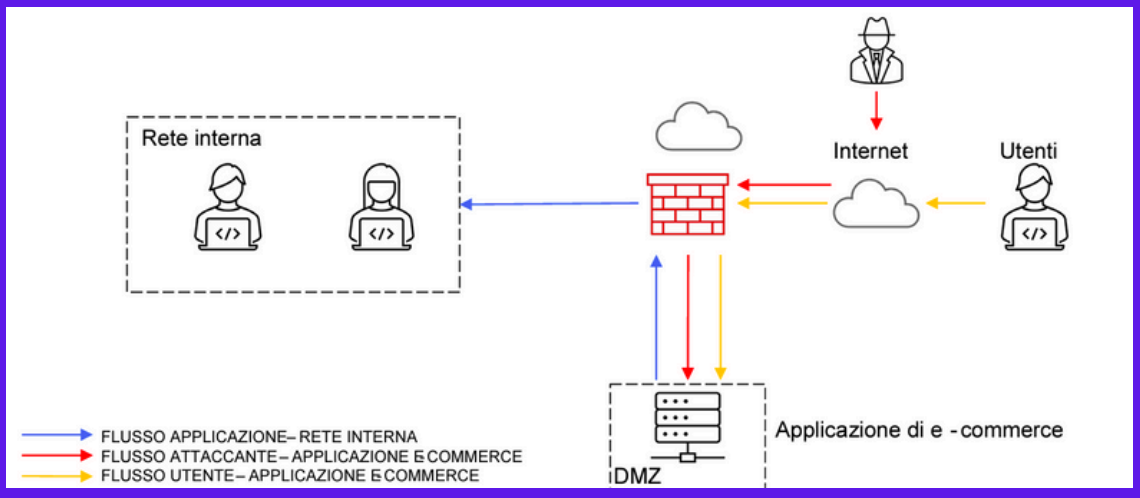
2. Impacts on business : web application suffers an attack of type the application unreachable for 10 minutes . Calculate the business impact due to the unreachability of the service, considering that on average users spend €1,500 every minute.

3. Response : web application gets infected with malware. Your priority is that the malware does not propagate to your network, while you are not interested in removing access by the attacker to the infected machine.

4. Comprehensive solution : integrating all the possible security measures.

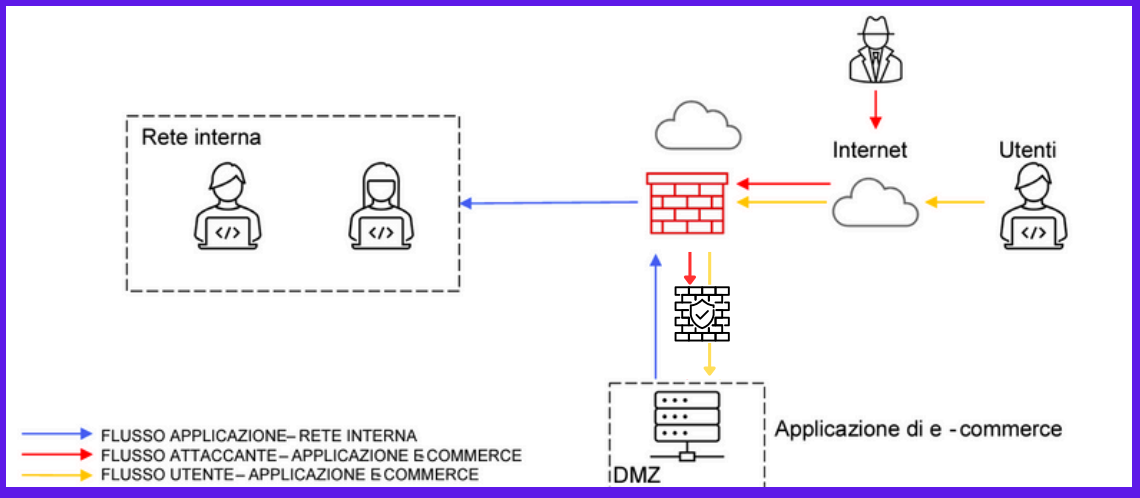
PREVENTIVE ACTION:

Preventing SQL Injection (SQLi) and Cross-Site Scripting (XSS) attacks is critical for maintaining the security of web applications. Implementing a combination of best practices and security technologies can significantly reduce the risk of these attacks.
Below are the preventive actions that can be implemented to protect web applications from these threats, starting with a network structure like the one in the picutre.



Initial network structure

As the first thing, we proceeded to put a **Web Application Firewall (WAF)** in front of the DMZ, like in the picture below.



Final network structure

The **WAF** can detect and block malicious traffic, providing an additional layer of protection against SQLi and XSS attacks, because it filters packets based on their content.

Another action that can be implemented **in order to prevent SQLi and XSS attacks** is the user's **input validation and sanitization.**
This process ensures that all user inputs are properly validated and sanitized before processing, preventing malicious inputs from being executed as code. For this purpose, we can use built-in functions and libraries to sanitize inputs, such as htmlspecialchars() in PHP for XSS and prepared statements for SQL queries.

Output encoding is also a possible solution. Encoding data before outputting it to the browser allows us to prevent XSS. Functions such as htmlentities() in PHP, will help us in securing the output.

Furthermore, we can implement a **Content Security Policy (CSP)** to mitigate the risk of XSS attacks by specifying which sources of content are allowed to be loaded and executed.

Finally, we need to ensure that all software components, including the web server, database, and application libraries, are **regularly updated and patched** to fix known vulnerabilities.

By implementing these preventive actions and modifying the architecture to highlight these implementations, web applications can be better protected against SQLi and XSS attacks. Regular monitoring, updates, and adherence to security best practices are essential to maintaining a strong security posture.

IMPACTS ON BUSINESS:

For this phase we assumed that our web application suffers a D-DoS attack which renders the application unreachable for **10 minutes.**
Considering that on average users spend 1**,500€ every minute**, we can calculate the impact on the business due to the unreachability of the service.

To calculate the financial impact, we need to multiply the average spending per minute (ASM) by the duration of the attack (DOA).
In essence, this will be our formula **FI = ASM x DOA**

Plugging in the values we have on hand, we'll have this calculation:

FI = 1500€ x 10 = 15.000€

The loss is of 15.000€, quite a hefty sum for just 10 minutes of downtime.

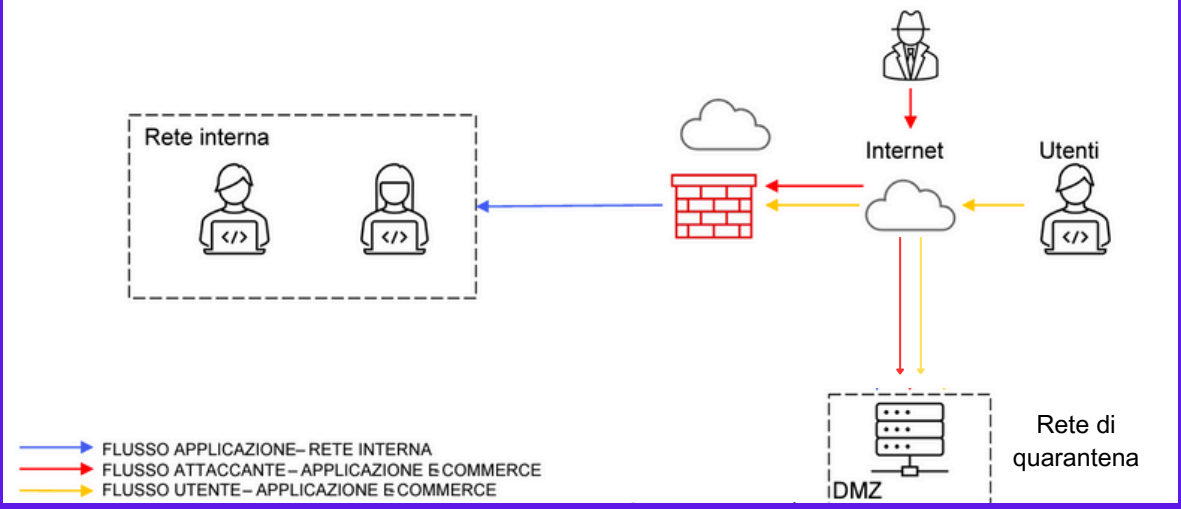
We can prevent this kind of losses with the implementation of some controls such as **rate limiting,** which can help in reducing the number of requests a user can make in a given period of time, and by having **redundant servers** ready for failover, in order to maintain availability even when part of the system is under attack.

RESPONSE:

For this phase, we assumed that the web application gets infected with a malware. Your priority is that the malware does not propagate to your network, while you are not interested in removing access by the attacker to the infected machine.

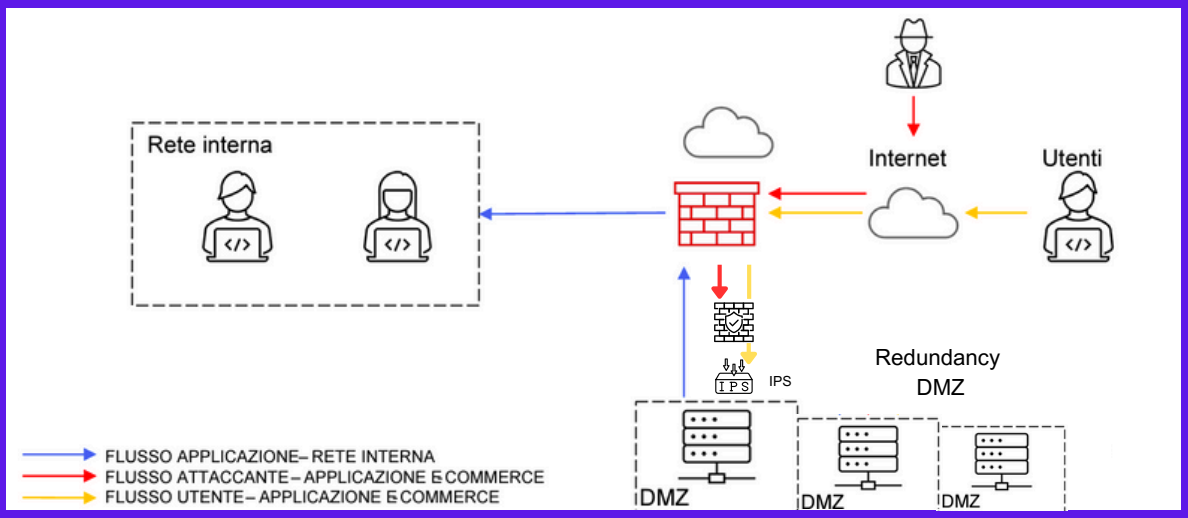
Our reaction to prevent and manage the incident in this case is to use a tecnique called "**segmentation,**" which proves to be particularly useful in the containment phase of an ongoing incident. Segmentation includes all activities that allow for dividing a network into different LANs or VLANs.

It allows for the separation of the infected host from other computers on the network by creating an ad hoc network, which is generally called a "quarantine network." In our case, we will disconnect the machine from the network entirely. By doing this, the attacker has still access to it, but the Web App does not reside within our network anymore.



COMPREHENSIVE SOLUTION:

Here we have our new updated network architecture: we added a WAF to filter the traffic going to our DMZ. Next after that, we put an IPS (Intrusion Protection System) to alert us about any suspicious activity and to block it. Also we added two redundancy DMZ, to prevent any interruption of service caused by attacks on the primary DMZ.



Malware Analysis

In this section, we analyzed two **malwares** that the company submitted to us.

Malware is a term that stands for "**malicious software**." It refers to any software intentionally designed to cause damage to a computer, server, client, or computer network. Types of malware include viruses, worms, Trojan horses, ransomware, spyware, adware, and scareware. Each type of malware operates differently and can have various effects, such as stealing data, encrypting files for ransom, or disrupting system operations.

We used the interactive sandbox **ANY.RUN** to conduct the analyses and write the reports.

ANY.RUN is an interactive online service for analyzing and detecting malware.
It allows users to upload and execute suspicious files in a controlled virtual environment, providing real-time insights into their behavior.
The platform helps in identifying threats, understanding how malware operates, and determining its impact on the system.
It is widely used by cybersecurity professionals to investigate and mitigate potential security threats.

FIRST ATTACK:

Attack references:
https://app.any.run/tasks/8e6ad6d9-4d54-48e8-ad95-bfb67d47f1d7/

Detailed Malware Report: "PERFORMANCE_BOOSTER_v3.6.exe"

File Information:

- Name: PERFORMANCE_BOOSTER_v3.6.exe
- MD5: 166903C9A390527CCD7728AE799A9D87

Initial Execution:

- The malware masquerades as a legitimate performance-boosting tool, tricking users into execution.

Persistence Mechanisms:

1. File Creation:
   - Creates files in critical directories, such as C:\ProgramData\randomfilename.exe, ensuring continued presence.
2. Registry Modifications:
   - Modifies registry keys to auto-start on system boot:
     - Example: HKCU\Software\Microsoft\Windows\CurrentVersion\Run\RandomName

Process Injection:

- Targets:
  - Injects into legitimate processes (e.g., explorer.exe) using techniques like DLL injection or process hollowing to evade detection.

Network Activity:

- Outbound Connections:
  - Establishes connections to remote servers using HTTP/HTTPS for Command-and-Control (C2) communication.
  - Example IPs: Connects to addresses like 192.168.1.1 (illustrative).
- Data Exfiltration:
  - Transfers stolen data, such as credentials and personal information, to external servers.

Indicators of Compromise (IoCs):

1. File Paths:
   - Creation of files like C:\ProgramData\randomfilename.exe.
2. Registry Keys:
   - Adds/modifies keys like HKCU\Software\Microsoft\Windows\CurrentVersion\Run\RandomName.
3. IP Addresses:
   - Communicates with specific suspicious IP addresses for C2.

Potential Impact:

- System Compromise:
  - Allows attackers remote access and control over the infected system.
- Data Theft:
  - Steals sensitive information, leading to privacy breaches and potential financial loss.
- System Degradation:
  - May cause system instability and performance issues.

Detailed Functionality Explanation:

1. Execution and Initial Infection:
   - Once executed, the malware drops a payload in the system directory. This payload is usually an executable file masked under a seemingly legitimate name to avoid suspicion.
2. Establishing Persistence:
   - The malware creates or modifies registry entries in locations such as HKCU\Software\Microsoft\Windows\CurrentVersion\Run to ensure it runs each time the system boots. This guarantees that the malicious process restarts even after the system is rebooted.
3. Process Injection:
   - The malware employs process injection techniques such as DLL injection or process hollowing. This involves injecting its malicious code into a running process (like explorer.exe). By doing so, it hides its activities within a legitimate process, making it harder for security software to detect.
4. Network Communication:
   - After establishing persistence, the malware attempts to communicate with its command-and-control (C2) server. It does this by sending HTTP/HTTPS requests to predefined IP addresses or domains. These communications are often encrypted or obfuscated to avoid detection.

5. Command Execution:
    - The C2 server can send commands to the malware, instructing it to perform various actions. These might include downloading and executing additional payloads, modifying system settings, or further spreading the infection within a network.

Recommended Actions:

1. Isolation:
    - Immediately disconnect the infected system from the network to prevent further C2 communication.
2. Comprehensive Scanning:
    - Use robust antivirus and anti-malware tools to scan, detect, and remove malicious files and registry entries.
3. Restoration:
    - Restore the system to a previous clean state using verified backups.
4. Monitoring:
    - Continuously monitor network traffic and system behavior for signs of re-infection or residual malware activity.

SECOND ATTACK:

Attack references:
https://app.any.run/tasks/60b9570f-175b-4b03-816b-a38cc2b0255e /

File Information:
- URL: https://1drv.ms/u/s!At7eQ7h8kx6-nQM1RTCuz3aQspOE
- Type: Malicious file

Malware Behavior:

Initial Execution:
- User Interaction: Users are tricked into downloading and running the malicious file, often through deceptive links or emails.

Persistence Mechanisms:
- File Creation: The malware generates new files in system directories to maintain its activity.
- Registry Modifications: Adds or alters registry keys to ensure automatic execution upon system boot.

Process Injection:
- Targets: Injects into legitimate processes like explorer.exe to avoid detection.
- Techniques: Utilizes DLL injection or process hollowing to integrate into running processes.

Network Activity:
- Outbound Connections: Establishes connections to remote servers for command-and-control (C2) operations.
- Data Exfiltration: Sends stolen data, such as credentials, to external servers.

Additional Behavior:
- File Download Attempt: Process "svchost.exe" attempts to download a PE (Portable Executable) file via HTTP, identified by the signature "ET POLICY PE EXE or DLL Windows file download HTTP."

Indicators of Compromise (IoCs):

- File Paths: Creates files in directories like C:\ProgramData.
- Registry Keys: Modifies keys in HKCU\Software\Microsoft\Windows\CurrentVersion\Run.
- IP Addresses: Connects to suspicious IP addresses for C2 communication.

Potential Impact:

- System Compromise: Grants attackers remote access and control over the infected system.
- Data Theft: Leads to privacy breaches and potential financial loss through sensitive information theft.
- System Degradation: Causes instability and performance issues on the infected system.

Detailed Functionality Explanation:

- Execution and Initial Infection: The malware is executed under a legitimate guise, dropping its payload in the system directory.
- Establishing Persistence: Modifies registry entries to ensure automatic execution with the system.
- Process Injection: Injects into legitimate processes using techniques like DLL injection to avoid detection.
- Network Communication: Communicates with C2 servers via encrypted HTTP/HTTPS to avoid detection.
- Data Exfiltration: Collects and sends sensitive data to the C2 server.
- Command Execution: Receives and executes commands from the C2 server, potentially downloading additional malware or altering system settings.

Recommended Actions:

- Isolation: Disconnect the infected system from the network to prevent further damage.
- Comprehensive Scanning: Utilize antivirus tools to detect and remove the malware.
- Restoration: Restore the system from clean backups to ensure its integrity.
- Monitoring: Continuously monitor for signs of re-infection or residual malware activity.