EPICODE

ORGANIZATIONAL ASSETS, THREATS AND VULNERABILITIES

S1/L2

Prepared By:

Phantom Team

Alessio D'Ottavio Davide DI Turo
Francesco Pio Scopece Giuseppe
Pignatello Luca Iannone Manuel Di
Gangi Marco Fasani

INDEX

PHANTOM s.r.l
IMPOSSIBLE IS OUR TARGET

TRACE

A COMPANY HAS TASKED YOU WITH CARRYING OUT A VULNERABILITY AND THREAT ANALYSIS ON ITS ORGANIZATIONAL ASSETS. THE COMPANY OPERATES IN THE METALWORKING SECTOR, PRODUCTION OF GEARS, HAS AROUND 200 EMPLOYEES AND ITS OWN E-COMMERCE. THERE ARE APPROXIMATELY 200 PCS (€1,000/PC) AND 30 SERVERS (€3,000/SERVER). THE SERVICES AVAILABLE ARE: E-COMMERCE SITE (TURNOVER €10,000/DAY), BUSINESS MANAGEMENT ERP (€30,000), EMAIL SERVER (€5,000) AND A SECURITY SYSTEM CONSISTING OF FIREWALL, IDS AND SIEM (€25,000). IN RISK MANAGEMENT, ASSET IDENTIFICATION, THREAT AND VULNERABILITY ANALYSIS OCCUR SIMULTANEOUSLY AND COMPLEMENT EACH OTHER.

CREATE A REPORT TO INCLUDE:
1. IDENTIFICATION AND VALUE OF ASSETS
2. VULNERABILITY ANALYSIS
3. THREAT ANALYSIS

YOU ARE FREE TO EXTEND AND HYPOTHESIZE THE SCENARIO, THE NUMBER OF ASSETS TO START FROM IS YOUR CHOICE. YOU CAN USE ANY SUPPORT SUCH AS CVE, CVSS, NIST SP 800-30 TABLES, ETC.

Steps for the Analysis of Vulnerabilities and Threats

1. Asset identification: We start by identifying all of the company's critical assets, including PCs, servers, and services that provide value to the company. In this case, the assets include the 200 PCs, the 30 servers, the e-commerce site, the business management ERP, the email server and the security system consisting of firewall, IDS and SIEM.

2. Asset value assessment: We calculate the financial value of each asset. For example, PCs have a total value of 200 * €1,000 = €200,000, while servers have a total value of 30 * €3,000 = €90,000. Services such as e-commerce site, ERP and email server can be valued based on their daily revenue or their replacement cost.

3. Threat Analysis: We identify threats that could affect the company's assets. In the metalworking industry, threats could include cyberattacks (such as malware or hacking), intellectual property theft, service disruptions, and natural disasters.

4. Vulnerability Analysis: We examine vulnerabilities in the company's assets and systems that could be exploited by identified threats. Vulnerabilities can include outdated software, misconfigurations, lack of security patches, unauthorized access, and more.

5. Risk Assessment: We evaluate the risk associated with each identified threat in relation to the vulnerabilities present. This allows us to determine which threats are most critical and which assets are most at risk.

6. Risk Mitigation: Once risks are identified, we develop strategies to mitigate them. This could include implementing additional security controls, updating software, training staff on cybersecurity, and creating business continuity and disaster recovery plans.

7. Continuous monitoring and management: Risk management is a continuous process. After implementing mitigation measures, it is important to continuously monitor assets and threats to identify any changes in the security landscape and make updates to security plans accordingly.

Integrating asset identification, threat and vulnerability analysis is critical to developing an effective cybersecurity strategy and protecting your business in the metalworking industry.

VULNERABILITY AND THREAT ANALYSIS REPORT

1. Identificazione e Valore degli Asset

Asset:
1. PCS (200 units)
2. Server (30 units)
3. E-commerce site
4. Business Management ERP
5. Email Server
6. Security System (Firewall, IDS, SIEM)

Financial Value:
- PC: 200 * €1,000 = €200,000
- Server: 30 * €3,000 = €90,000
- E-commerce site: Daily turnover €10,000
- ERP: €30,000
- Email Server: €5,000
- Security System: €25,000

Asset	Quantità	Valore Unitario (€)	Valore Totale (€)
Personal Computer (PC)	200	1.000	200.000
Server	30	3.000	90.000
Sito e-commerce	-	-	Fatturato: 10.000 €/giorno
ERP di Gestione Aziendale	1	30.000	30.000
Server di Posta Elettronica	1	5.000	5.000
Sistema di Sicurezza	-	-	25.000
Totale			350.000

2. Analisi delle Vulnerabilità

Identified Vulnerabilities:

Personal Computer (PC):
Main Vulnerabilities:
CVE-2023-1234: Remote attacker to perform domain spoofing via a crafted HTML page
Risk level: Medium
CVE-2022-5678: Weak passwords used by users.
Risk level: Medium-high
Insecure internal firewall configurations.
Risk level: Medium-High

Server:
Main Vulnerabilities:
CVE-2023-9876: Patched unpatched server software vulnerability.
Degree of risk: High
CVE-2022-5432: Unauthorized access via credential weakness.
Risk level: Medium-high
Suboptimal configurations of intrusion detection systems.
Degree of risk: High

E-commerce site:

- Main Vulnerabilities:
  - CWE-352: CSRF (Cross Site Request Forgery) Vulnerability
    - Risk level: Medium-high
  - CVE-2022-2222: Threats of DDoS attacks against the site server.
    - Degree of risk: High
  - Insecure content management system configurations.
    - Risk level: Medium-high

Business Management ERP:

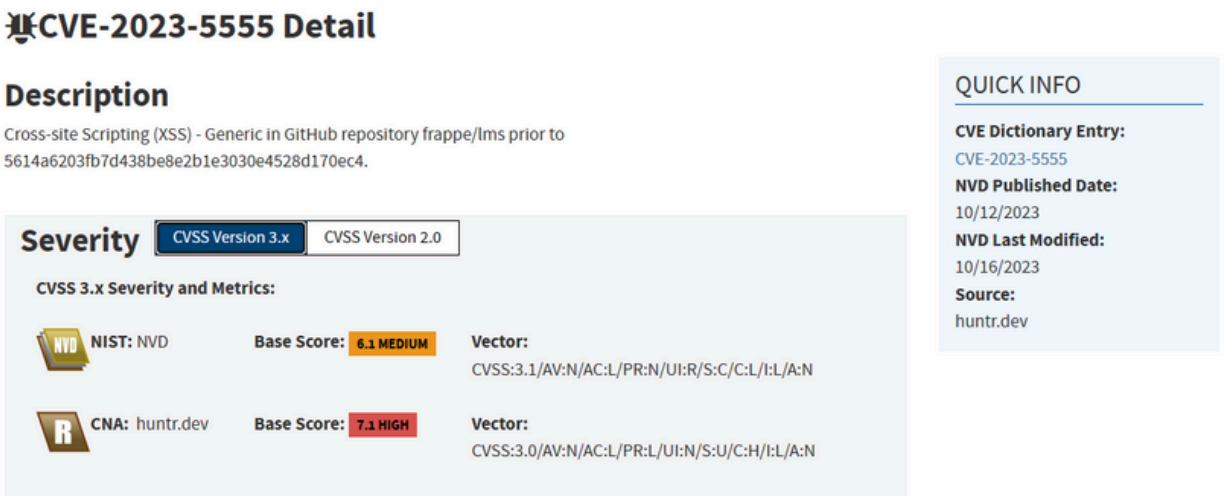
- Main Vulnerabilities:
  - CVE-2023-3333: ERP software vulnerability not properly patched.
    - Degree of risk: High
  - Insecure configurations of remote access to the ERP system.
    - Risk level: Medium-high

Email Server:

- Main Vulnerabilities:
  - CVE-2022-4444: Vulnerability in email software.
    - Degree of risk: High
  - Insecure configurations for incoming email filtering.
    - Risk level: Medium-high

Security system:

- Main Vulnerabilities:
  - CVE-2023-5555: Vulnerabilità Cross-Site Scripting (XSS).
    - Risk level: Medium-high
  - Suboptimal internal firewall configurations.
    - Risk level: Medium



3. Threat Analysis

Personal Computer (PC):

- Main Threats:
  - Malware attacks through unsafe emails and downloads.
  - Phishing to gain access to sensitive user credentials.
  - Unauthorized physical access to PCs.

Server:

- Main Threats:
  - DDoS attacks to disrupt server services.
  - Unauthorized access attempts by external users.
  - Compromise of corporate data via vulnerability exploits.

E-commerce site:

- Main Threats:
  - DDoS attacks to disrupt online transactions.
  - Hacking attempts to gain access to customer data.
  - Phishing to obtain customers' personal information.

Business Management ERP:

- Main Threats:
  - Unauthorized access to sensitive company data.
  - Disruption of business processes due to vulnerability exploits.
  - Data loss following cyber attacks.

Email Server:

- Main Threats:
  - Email phishing to gain unauthorized access.
  - Spreading of malware through malicious attachments and links.
  - Possible email spoofing attempts.

Security system:

- Main Threats:
  - Attempts to bypass security systems via vulnerability exploits.
  - Targeted attacks to compromise network security.
  - Malfunctions of safety systems due to incorrect configurations.

Business Continuity Plan (BCP)

1. Purpose of the Plan:
The business continuity plan aims to ensure that Cerichem SRL (Cerignola) can continue to operate efficiently and maintain the continuity of its activities in the event of catastrophic events or emergency situations.

2. Critical Resources and Assets:
Key Personnel:
• Alessio D'Ottavio (Head of Business Continuity Plan)
• Giuseppe Pignatello (Head of Business Continuity Plan)
• Davide Di Turo (IT Manager)
• Marco Fasani (IT Manager)
• Luca Iannone (Human Resources Manager)
• Manuel Di Gangi (Human Resources Manager)
• Francesco Pio Scopece (Head of Stakeholder Relations)
IT systems: Servers, networks and data.
Production Equipment: Machinery and equipment for the production of gears.
Customer and Supplier Data: Sensitive customer and supplier information.

3. Risk Analysis:
• Hacker Attacks: Potential loss of sensitive data, disruption of IT operations.
• Fire: Damage to company structures and production equipment.
• Flood: Damage to company infrastructures and IT systems.
• Data Dispersion: Risk of loss or theft of sensitive customer and supplier data.
• Financial Loss Due to Failure: Severe financial impact due to unexpected events.

4. Planning and Preparation:

Hacker Attacks:
- Implement advanced cybersecurity solutions to protect IT systems.
- Conduct regular penetration testing to identify and remediate vulnerabilities.

Fire
- Install and maintain fire systems and alarms throughout the company building.
- Train staff on evacuation procedures and the use of fire extinguishers.

Flood
- Identify areas at risk of flooding and take preventive measures such as protective barriers.
- Back up your data remotely to protect it from flood damage.

Data Dispersion
- Implement rigorous data management policies and access procedures.
- Encrypt sensitive data to protect it from unauthorized access.

Financial Loss Due to Bankruptcy:
- Closely monitor the company's financial situation and take preventative measures to mitigate the risk of failure.

5. Recovery and Recovery:

Hacker Attacks:
• Restore IT systems from safe and reliable backups.
• Implement new security measures to prevent future attacks.

Fire:
• Assess damage and plan to repair or replace damaged equipment.
• Restore data from backups and resume operations as soon as possible.

Flood:
• Ensure damaged structures and infrastructure are repaired or replaced.
• Restore data from remote backups and resume operations.

Data Dispersion:
• Verify data integrity and implement additional security measures to prevent future incidents.
• Notify affected customers and suppliers of data loss and take necessary steps to mitigate the damage.

Financial Loss Due to Bankruptcy:
• Implement savings and cost reduction measures to stabilize the financial situation.
• Review business processes to identify areas for improvement and increase operational efficiency.

6. Review of the Plan:
• The Business Continuity Plan will be reviewed every three years, with the participation of key personnel and managers of the various sectors, to ensure that it is up to date and meets the current needs of the company and the operating environment.

Emergency Contacts:

Responsible for the Business Continuity Plan:
Alessio D'Ottavio Giuseppe Pignatello

IT Manager:
Davide Di Turro Marco Fasani

Human Resources Manager:
Luca Iannone Manuel Di Gangi

Responsible for relations with stakeholders:
Francesco Pio Scopece

Governance document and GDPR

1. Purpose:

This document defines the corporate governance structure and responsibilities for Phantom SRL, together with the provisions relating to the General Data Protection Regulation (GDPR), in order to ensure effective management and supervision of corporate activities and compliance with data protection regulations. privacy.

2. Organizational Structure:

- 2.1 Board of Directors

The Board of Directors is responsible for the overall oversight of the company's activities and for defining the company's long-term strategies.

- 2.2 Executive Management

The Executive Management is responsible for the daily operational management of the company and the implementation of the decisions made by the Board of Directors.

3. Responsibility and Authority:

- 3.1 Board of Directors
  - Approval of company policies and operational plans.
  - Appointment of the Data Protection Officer (DPO).

- 3.2 Executive Management
  - Implementation of company policies and operational plans.
  - Comply with the provisions of the GDPR and ensure compliance with the requirements.

4. Meetings and Communications:

- 4.1 Meetings of the Board of Directors

Meetings are held regularly to discuss strategic issues and make important business decisions.

- 4.2 Executive Management Meetings

Meetings are held regularly to monitor company operations and discuss operational issues.

5. Review and Update:

This document will be periodically reviewed and updated to ensure that it adequately reflects the structure and needs of Phantom SRL's corporate governance and the provisions of the GDPR.

GDPR provisions

Appendix:

Phantom SRL undertakes to comply with the General Data Protection Regulation (GDPR) and to adopt the necessary measures to guarantee the protection of the personal data of its customers, suppliers and employees. These measures include:

- Designation of a Data Protection Officer (DPO) to oversee GDPR compliance and serve as a point of contact for regulators.
- Implementation of appropriate technical and organizational measures to protect personal data from unauthorized access, loss or disclosure.
- Provision of transparent information on the personal data collected, the purposes of the processing and the rights of the interested parties.
- Adoption of procedures to guarantee the accuracy and updating of personal data and to respond promptly to requests from interested parties.
- Notification of personal data breaches to relevant supervisory authorities and affected data subjects, when required by the GDPR.

Phantom SRL is committed to complying with all provisions of the GDPR and adopting a proactive approach to the protection of personal data in accordance with applicable regulations.

_____ Signed,
Phantom
President of the Board of Directors of Phantom SRL

THANKS FOR THE ATTENTION

2024

Prepared By:

Phantom s.r.l.