1 Executive Security Assessment Report

1.1 Introduction

The security assessment was conducted on the domain **cpaglobal.dk**. The analysis was initiated on **April 8th at 05:46** and completed in **00h:09m:34s**. The assessment was categorized as a “Basic” type scan. The evaluation focused on identifying High and Medium-risk vulnerabilities that could impact the organization’s security posture.

1.2 Short Summary of Main Issues

The security assessment identified a total of **18 issues**, categorized as **2 High-risk**, **1 Medium-risk**, **1 Low-risk**, and **14 informational**. The most critical findings include a High-risk shared hosting environment with over **262,000 shared domains**, posing significant exposure to potential attacks, and a Denial of Service (DoS) vulnerability on port **443** with a **96.24%** timeout rate, indicating severe service disruption risks. Additionally, a Medium-risk issue was detected with an open HTTP port lacking encryption, necessitating immediate review for HTTPS redirection or HSTS implementation. These vulnerabilities highlight the need for urgent remediation to mitigate potential business disruptions and data breaches. Prioritizing these High-risk areas will enhance the organization’s security posture and resilience against cyber threats.

1.3 Key Security Issues

Title	Risk
Shared Hosting Environment Analysis	High
Denial of Service (DoS) Assessment	High
Nmap Port Scan Results Analysis	Medium
Login Form Detection Analysis	Low

1.4 Shared Hosting Environment Analysis

Description:
The assessment revealed that the domain **cpaglobal.dk** is part of a High-risk shared hosting environment with **262,264** shared domains. This significantly increases the attack surface and potential for cross-site vulnerabilities.

Affected Assets:
- Hostname: **cpaglobal.dk**

Recommendations:
- Consider migrating to a dedicated hosting environment to reduce exposure. - Implement strict access controls and monitoring to detect unauthorized activities. - Regularly audit hosted domains for vulnerabilities.

1.5 Denial of Service (DoS) Assessment

Description:
A potential DoS vulnerability was identified on port **443 (HTTPS)**, with a timeout rate of **96.24%**, indicating a High risk of service disruption.

Affected Assets:
- Ports: **80 (HTTP)** and **443 (HTTPS)**

Recommendations:
- Enhance server capacity and optimize configurations to handle peak loads. - Implement rate limiting and traffic filtering to mitigate DoS attacks. - Continuously monitor server performance and adjust resources as needed.

1.6 Nmap Port Scan Results Analysis

Description:
Port **80** was found open, serving HTTP without encryption, which poses a Medium risk due to the lack of data protection.

Affected Assets:

- IP: **3.33.139.32** - Port: **80/tcp** - Service: **http** - Version: **awselb/2.0**

Recommendations:

- Implement HTTPS with a valid SSL certificate to encrypt data in transit. - Enable HTTP Strict Transport Security (HSTS) to enforce secure connections. - Regularly test for SSL/TLS vulnerabilities and update configurations accordingly.

1.7 Login Form Detection Analysis

Description:
One login form was detected on the domain, assessed as Low risk due to its normal interest level.

Affected Assets:

- URL: `http://cpaglobal.dk:80`

Recommendations:

- Ensure login forms are protected with HTTPS to secure credentials. - Implement multi-factor authentication (MFA) to enhance security. - Regularly review and update authentication mechanisms.

1.8 General Recommendations

To improve the overall security posture, it is recommended to prioritize remediation of High-risk vulnerabilities, particularly those related to shared hosting and DoS risks. Implementing robust encryption standards, enhancing server configurations, and adopting proactive monitoring and response strategies will significantly mitigate potential threats. Regular security audits and updates should be conducted to ensure ongoing protection against emerging vulnerabilities.