**Assessment 1: Case Study / Scenario**

**Submission date: 24th November 2023**

**Module: Securing Web Technologies**

CST2572

Secure Web Technologies CST2572

Secure Web Technologies CST2572

**Table of Contents**

[Context/Case Study: 3](#_Toc151776656)

[Describe/Questions: 3](#_Toc151776657)

[Introduction 3](#_Toc151776658)

[1.0 – Initial Reconnaissance and Discovery 4](#_Toc151776659)

[2.0 Remediating a Hacked Website for a Major National Health Conference 5](#_Toc151776660)

[3.0 Clean-up and Restoration 6](#_Toc151776661)

[4.0 Mitigation 8](#_Toc151776662)

[I 9](#_Toc151776663)

[Network server diagram 10](#_Toc151776664)

[Remediation flowchart 11](#_Toc151776665)

[11](#_Toc151776666)

[iii- Updates made - plug-ins and firewalls into the wordpress website. 12](#_Toc151776667)

[Reference list 12](#_Toc151776668)

# **Context/Case Study:**

A client calls you first thing on a Saturday morning, panicking as their website has been hacked. The website is for a major national health conference with NHS as a leading promotor. Other details:

* The server had auto-malware checks on it which shut the site down.
* The server is an Apache server setup in a VM by a host.
* The setup also contains the company’s main health website with a member’s database.
* All websites are designed and running WordPress.
* There is admin access via a username/password.
* The web developers have declared that what has happened is ‘out of their remit’.

# **Describe/Questions:**

1. How do you initially reconnaissance and discover what has occurred?
2. How do you remedy?
3. How do you clean-up and restore?
4. Mitigate?

Ensure you provide diagrams of the system and any upgrades or updates that are needed

# **Introduction**

This report details the initial reconnaissance, remedial steps, clean-up and restoration, and mitigation strategies employed in response to a website hack that targeted a major national health conference website. The affected Apache server, hosting WordPress-based sites, prompted an automatic shutdown due to malware detection. The incident involves sensitive data within the company's primary health website. While the web developers claim the issue is beyond their scope. To maintain long-term protection, this report will execute clean-up tasks, conduct regular vulnerability assessments, and develop comprehensive disaster recovery plans. Furthermore, it will offer suggestions to management for improving security posture and implementing measures to mitigate risks. The focus of this report is to analyse and provide solutions for a severe website hack.

## **– Initial Reconnaissance and Discovery**

When a client's website gets hacked, conducting initial reconnaissance and discovery is critical to determining the extent of the damage and developing an appropriate plan for addressing and fixing the issues (Cybersecurityexchange, 2022).

**Verify the reported issue & isolate the affected server**

Check to see if the auto-malware checks were responsible for the website's failure, and make sure the server is disconnected from the network to prevent future damage (Sharif, 2022).

**Analyse server logs**

Examine the server logs for any strange activity or error messages that happened during the incident. Look for unusual access patterns, brute-force attempts, or unauthorised modifications. The log management platform enables the IT team and security specialists to create a centralized location for all essential endpoint, network, and application data. This log file is typically completely indexed and searchable, allowing the log analyzer to quickly obtain the information needed to make network health, resource allocation, or security decisions (Sharif, 2022).

**Scan for malware**

Run a thorough malware scan on the server with reliable security solutions such as Wordfence or Sucuri. This will aid in the detection of infected or malicious files within the WordPress installation or other related files.

**Check file integrity**

To identify any modifications done by the attacker, compare the WordPress core files and plugins to their original versions. Pay close attention to files with out-of-the-ordinary timestamps or file extensions. Collaborate with the hosting provider

Report the situation to the hosting provider and request their aid in investigating the server breach. They may have other tools or logs that can help with the inquiry.

# **2.0** **Remediating a Hacked Website for a Major National Health Conference**

**Secure the Main Health Website**

Since the hacked website shares the server with the company's main health website, it's crucial to ensure the main website remains secure. This includes resetting all admin passwords, checking website security plugins, and screening for malware.

**Gather Information**

**Gather as much information about the hack as possible, including any error messages, logs, or notifications issued by the auto-malware scans. This information will help in determining the cause of the hack and the amount of the damage.**

**Identify the Attack Vector**

**Determine how the hackers got into the website. This could be due to weak passwords, obsolete software, or WordPress CMS vulnerabilities.**

**Scan for Malware**

Thoroughly scan the entire server, including all websites, for any remaining malware or malicious code. Use reputable antivirus and anti-malware tools to identify and remove any infected files.

**Restore from Backup**

**If a clean backup created before the attack is available, restore the conference website. This will restore the website to its pre-malware state, removing all harmful content.**

**Update Software**

Ensure that all software on the server, including WordPress, Apache, and any plugins, is up to date. Regular updates often include security patches that address known vulnerabilities.

**Implement Strong Passwords**

Enforce strong password policies for all admin accounts, including complex passwords, regular password changes, and avoiding using personal information.

**Enable Two-Factor Authentication**

Add an extra layer of security by enabling two-factor authentication (2FA) for all admin accounts. This requires both a password and a second verification factor, such as a code sent to a mobile phone, to access the account.

**Keep Software Updated**

Regularly check for and install updates for WordPress, Apache, and any plugins or themes used on the websites. Updates often include security patches and bug fixes.

**Regular Vulnerability Scans**

Schedule regular vulnerability scans to identify any potential weaknesses in the websites or server configuration. These scans can help detect vulnerabilities before they can be exploited by hackers.

**Consider Managed WordPress Hosting**

If technical expertise is limited, consider switching to a managed WordPress hosting provider. These providers handle server maintenance, security updates, and often include malware scanning and removal services

**Communicate with Stakeholders**

Keep the client and relevant stakeholders informed throughout the remediation process. Provide regular updates on the progress, the extent of the damage, and the estimated timeframe for recovery.

# **3.0 Clean-up and Restoration**

**Identify what was lost or stolen**

Given the urgency of the issue presented in the case study, in which a client's website for a major national health conference, in collaboration with the NHS, has been hacked, identifying the full extent of the damage is an important first step, as, by assessing the damage, time can be saved as it will give us to prioritise and treat the most essential issues first, lowering overall risk and potential future threats.

Identifying the corrupted data after the cyber-attack will enable us to properly manage resources by focusing on areas that require immediate attention while avoiding unnecessary efforts in insignificant areas (Managedmethods, 2023).

**Identify the source**

Tracing the origin of the cyber-threat activity will help in pinpointing the vulnerabilities being targeted and determining the subsequent steps to address and alleviate the situation. Examine the incident thoroughly and establish connections between its discovery and initiation. This process will aid in assessing the severity of the threat and deciding whether it is necessary to inform law enforcement authorities.

By successfully identifying the source, it will allow us to determine which vulnerabilities were targeted in the cyber assault. This information is critical for determining how the breach occurred and what flaws must be rectified to avoid similar instances. Moreover, examining the incident in depth allows for an in-depth understanding of the type and scope of the cyber threat (Managedmethods, 2023).

**Isolate and restrict the hacked website**

**The website for a major national health conference was hacked, so one of the first steps to take into consideration must be to** isolate the affected server immediately to prevent the threat from spreading to other systems. Take the hacked website down and unplug it from the network to isolate it. This will block access to the compromised site and prevent future damage.

Once the threat has been recognised, necessary steps should be taken promptly to keep it from spreading, like, isolate the affected system, alert the concerned stakeholders, blocking specific network traffic, disabling compromised accounts, or implementing security measures and use updated antivirus or anti-malware tools to scan and remove malicious software (Managedmethods, 2023).

**Analyse logs for more information**

After implementing containment measures, the specialists should conduct a thorough inspection of the infrastructure to ensure the complete removal of any remaining malware. This process is essential before restoring online operations to prevent the risk of the threat spreading and infecting additional resources (Managedmethods, 2023).

**Eradicate**

Restore the systems to their pre-incident condition. Gather as much evidence as possible while maintaining a strong chain of custody. All logs, memory dumps, audits, network traffic, and disc images should be gathered. Without appropriate evidence collecting, digital forensics cannot be performed.

Remove the security risk to prevent the attacker from regaining access. Patching systems, limiting network access, and changing passwords for hacked accounts are all part of this. Create a root cause identification during the eradication process to assist in determining the attack path utilised so that security controls can be changed to prevent similar attacks in the future (Carson, 2023).

**Restore data and Backup**

Recover the website and related systems by restoring them from a clean backup that was created before the security breach occurred. Verify Data Integrity by ensuring that the recovered data is free of errors and corresponds to the most recent clean state (Managedmethods, 2023).

# **4.0 Mitigation**

**Install SSL and Security Plugins**

Installing SSL and security plugins is a fundamental security measure to protect a website from hacking. This ensures that data submitted through your website is encrypted and securely transmitted to its intended recipients (Hacken, 2023).

**Have The Latest Security Software in Place**

It's crucial for website owners, especially those utilizing content management systems like WordPress with numerous plugins, to consistently install the latest security software. Updates not only bring specific security enhancements but also incorporate features to address evolving threats, effectively safeguarding websites from potential hacker attacks (Hacken, 2023).

**Use https Protocol**

Encrypting HTTPS enhances the security of data transfer, which is particularly crucial when users transmit sensitive information (Hacken, 2023).

**Implement firewall and other security solutions**

Utilizing a firewall is essential for warding off most cyber threats, though it may not thwart every possible attack. It serves as a crucial component for your network by adding an additional layer of protection between devices and the network. Essentially acting as a barrier between your organization's internal network and the external world, a firewall provides greater control. It has the capability to block both incoming and outgoing traffic, preventing harmful data packets from reaching your network (Cepero, 2021).

Antivirus software can help identify viruses on your employees' computers, and if they use mobile devices, it's advisable to install such software on those as well. Ensure that your IT department keeps all security solutions updated (Cepero, 2021).

**Utilising cloud-based security solutions that adhere to industry regulations**.

This not only enables businesses to optimize their processes and conserve valuable time and resources but also guarantees adherence to all pertinent compliance standards. Organizations can reduce the likelihood of cyberattacks and safeguard their sensitive data by adhering to these compliance requirements and others (Woodgate, 2023).

**Use Strong Password**

A strong password should be difficult to trace and include special characters, numbers, and upsize and small letters (Hacken, 2023).

**5.0 Diagram of the system**

## **I**

## **Network server diagram**

Bottom of Form

## **Remediation flowchart**

## 

## **iii- Updates made -** plug-ins and firewalls into the wordpress website.

* Firewall installed into the apache server.

# **Reference list**

Cybersecurity exchange. (2022) What Are Footprinting and Reconnaissance?. [Online]

Available at: <https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/basics-footprinting-reconnaissance/>

Sharif, A., 2022. WHAT IS LOG ANALYSIS?. [Online]

Available at: <https://www.crowdstrike.com/cybersecurity-101/observability/log-analysis/>

[Accessed 30 October 2023].

Joseph Carson. (2023) ‘Cyber incident response checklist and plan: Are you breach-ready?’, available at: <https://delinea.com/blog/cyber-incident-response-checklist> [Accessed 30 October 2023].

Managed Methods. (2023) ‘How to recover from Cybver attack’, available at: <https://managedmethods.com/blog/cyber-attack-recovery/> [Accessed 30 October 2023].

Exabeam. (2022) available at: <https://www.eccouncil.org/cybersecurity-exchange/ethical-hacking/basics-footprinting-reconnaissance/> (accessed at: 30 octobver 2023).