IT COMPANY
MANAGED SOLUTIONS PROVIDER

Case Study : WordPress Maintainance & Update

Client: Digital Marketing Agency
Industry: Digital Marketing and Web Design
Website: anonymous
Challenge: Security Vulnerabilities & Maintenance Issue Due to Outdated WordPress Core

Presented by
Neelam Khalid

BACKGROUND

INFORMATION

Agency is a growing digital marketing agency that serves multiple small and medium-sized businesses (SMBs) by providing web design and marketing solutions. The agency's website, built on WordPress, was a critical part of their operations, serving as both their portfolio and a hub for client interactions.

Despite the importance of their website, the agency had fallen behind on updating their WordPress core and plugins due to a focus on client projects and day-to-day operations. Their WordPress installation had not been updated in over 6 months.

Challenges Faced By

Digital Agency in WordPress Maintainance

In early 2023, the agency's website was targeted by cybercriminals exploiting a known vulnerability in an outdated version of WordPress. The WordPress core had not been updated to the latest stable release, which contained crucial security patches. The hackers were able to gain access to the website's admin panel by exploiting an existing vulnerability related to user authentication.
The breach went unnoticed for several days, but during this time, the attackers injected malicious code into several pages, which resulted in:

- A slowdown in website performance
- A temporary loss of search engine rankings due to Google flagging the website as unsafe
- A significant reduction in client trust, as some visitors encountered warning pages while browsing the site

IT COMPANY

SERVICES

Upon discovering the breach, the Creative Solutions Agency took immediate action to secure their site and restore trust. Their IT team followed these steps:

ACTION TAKEN

1. **Immediate WordPress Core Update:**

The first step was to update WordPress to the latest stable version. This update included critical security patches that resolved the vulnerability being exploited by the attackers.

2. Website Backups and Restoration:

The team restored the website from a recent, clean backup that was created before the breach occurred. This allowed them to recover the site without losing critical data or content.

ACTION TAKEN

3.Security Plugin Installation:

1. After the core update, they installed and configured the Wordfence Security Plugin to monitor for any suspicious activities in the future. This plugin also provided an added layer of protection by blocking IPs attempting brute force login attacks.

4.Ongoing Monitoring and Regular Updates:

The agency set up a schedule to ensure the WordPress core, themes, and plugins would be updated monthly. They also decided to enable automatic minor updates for WordPress to ensure security patches would be applied as soon as they were released.

OUR

SERVICES

- **RESTORED SECURITY:**

THE CORE UPDATE PATCHED THE VULNERABILITIES AND BLOCKED FUTURE ATTACKS, ENSURING THE WEBSITE WAS SECURE AGAIN.

- **FASTER WEBSITE PERFORMANCE:**

AFTER PERFORMING THE UPDATE, THE WEBSITE EXPERIENCED FASTER LOAD TIMES AND SMOOTHER PERFORMANCE DUE TO OPTIMIZATIONS MADE IN THE NEWER WORDPRESS VERSIONS.

- **SEO RECOVERY:**

GOOGLE SEARCH CONSOLE SHOWED A RECOVERY IN SEARCH RANKINGS, AS THE SITE WAS NO LONGER FLAGGED AS UNSAFE. WITHIN WEEKS, THE WEBSITE'S SEARCH VISIBILITY IMPROVED, AND TRAFFIC LEVELS RETURNED TO PRE-BREACH NUMBERS.

- **INCREASED TRUST:**

- CLIENTS AND VISITORS APPRECIATED THE IMPROVED SECURITY MEASURES, WHICH WERE COMMUNICATED THROUGH A BLOG POST AND EMAIL UPDATES ABOUT THE BREACH RESOLUTION AND NEW SECURITY PROTOCOLS IN PLACE.

KEY TAKE AWAYS

- **Timely WordPress Core Updates Are Crucial:**

The breach could have been avoided had the website been updated regularly. Timely updates, especially for WordPress core, are critical to securing a website against known vulnerabilities.

- **Security First:**

Regular core updates should be accompanied by robust security plugins and monitoring tools to protect against new and evolving threats.

- **Backups and Recovery Plans:**

Regular backups play a key role in quickly recovering from any breach or technical failure, minimizing downtime and data loss.

For further information **Click Here**