THE WALK AGENCY

Security matters in 6 steps

A quick guide to help you review and master your brands online security

We all know how important security is, especially when it comes to your customer data. A breach of trust there could ruin your brands reputation. That's why we spend so much effort on reviewing and optimising security for all our clients. Working at the coal face with state-of-the-art data platforms, new-age serverless programming solutions, decentralised networking (and on it goes...) means we get to see not only the opportunities available, but also the pitfalls of leveraging something you might not fully understand. And with the proliferation of technology and services, let's face it, not understanding something has become a part of life.

So, with that in mind, we've put together a simple guide to help you get on top of the security of your website and avoid being THAT brand who was in the news for all the wrong reasons. This guide has been designed to help you quickly identify possible gaps in the security of your brand website. Simply list your answers to each question and see if you have any items for attention when you're done.

Let's get started.

1) Backup and restore

Is there a backup process and does it include database backups?

Are the backups stored securely and independently of the primary server?

How quickly could you restore the site from backups if there was a need?

Is there a hardware failover process setup, i.e. what's the plan should there be a hardware issue?

Has anyone looked at load balancing, in order to handle high demand periods?

Is a bare-metal image available of the server?

The Walk Agency | ABN: 54 607 284 122
2/166 Wellington Street, Collingwood, VIC 3066 | +61 (3) 9973 0204

Is there a staging environment for managing more significant changes to the production environment?

---

2) Network monitoring

Is the network monitored for intrusions and unusual activity? If so, who does it and what do they look for? Who do they notify?

---

3) SSL, Firewalls and DDoS Preventions

Is there a firewall? If so, what kinds of controls are in place? Who manages this? Who do they notify of changes?

---

4) General security best practices

Access and user permissions

Who has physical access to the server?

Who has login access to the server?

Is SSH open to everyone? If so, do you use RSA keys to manage this?

Do you have a whitelist of accepted IP's which can access the server for maintenance?

Who is responsible for file permissions? Are all file permissions correct? See description under point 10 on this page:
https://blog.sucuri.net/2015/06/10-tips-to-improve-your-website-security.html

---

THE WALK AGENCY

File Management

Ensure FTP is secure (SFTP) and that a robust password is used for all file transfer and maintenance. Who is responsible for this? When was it last reviewed? Ensure other FTP best practices are observed too, per recommendations here:
https://www.helpsystems.com/blog/10-essential-tips-securing-ftp-and-sftp-servers

---

Applications and logins

Are passwords changed at regular intervals? Who is responsible for this?

Is there a policy for strong passwords? Who enforces this?

Remove any unused apps on the server to avoid being exploited via unused software. Who should review this?

Database protection

Harden your databases against attacks. A great guide on this can be found here:
https://security.berkeley.edu/resources/best-practices-how-articles/system-application-security/database-hardening-best-practices

Who would be best placed to review this?

---

5) CMS & Plugin updates

Who is responsible for updating the CMS? When was this last updated?

Who is responsible for updating plugins (if applicable)? When was this last done?

THE WALK AGENCY

6) Code review

Does anyone review the code used to ensure it's not creating any security vulnerabilities (like SQL injection)? If so, who and when was it last done? What were the results?

Linux users - review server config via .htaccess (and others) and ensure measures are in place to control access accordingly at this level.

That's it! We hope this guide has helped you to identify any security concerns and action them accordingly. Should you have any questions, feel free to reach out at any time.