African Cyber Security

BEST PRACTICE GUIDELINES FOR WEBSITE OWNERS

For website security to be effective, it has to be implemented with care and attention and it has to be monitored and maintained continually.

While there are tools to help you keep your website ecosystem secure, it all starts with education. You've read about the risks—now find out what you can do about them.

Get in line with industry standards

- **Implement always-on SSL.** Implement SSL/TLS on every page of your website so that every interaction a visitor has with your site is encrypted. Switching to 'HTTPS everywhere', as it's also called, with OV or EV SSL/TLS certificates demonstrates your credibility and can also improve your search rankings and paves the way for an upgrade to HTTP/2, delivering better performance.
- **Migrate to SHA-2.** As discussed in the report, certificate authorities should have stopped issuing SHA-1 certificates as of 1 January 2016, but you need to ensure any legacy certificates are also upgraded and that any devices and applications that may not currently recognize SHA-2 are upgraded too.
- **Consider adopting ECC.** Symantec also offers the use of the ECC encryption algorithm. All major browsers, even mobile, support ECC certificates on all the latest platforms, and compared to an industry-standard 2048-bit RSA key, 256-bit ECC keys are 64,000 times harder to crack.

Use SSL/TLS Correctly

SSL/TLS is only as good as its implementation and maintenance. So be sure to:

- **Keep protocol libraries up to date.** SSL/TLS implementation is an on-going task and it's vital that any patches or updates to the software you use are implemented as soon as possible.
- **Don't let your certificates expire.** Keep track of what certificates you have, from which certificate authority, and when they are due to expire. Symantec offers a range of automation tools to help you do this, giving you more time for proactive security tasks.
- **Display recognized trust marks.** Display trust marks (such as the Norton Secured Seal) in highly visible locations on your website to show customers your commitment to their security.

Manage your SSL/TLS keys properly. Limit the number of people with access to them; have separate administrators for managing the passwords for the server where they're kept and for managing the systems they're actually stored in; and use automated certificate and key management systems to reduce human involvement.

Any breach affecting SSL keys should be notified to the CA quickly, so that corresponding certificates can be revoked.

Adopt Comprehensive Website Security

- **Scan regularly.** Keep an eye on your web servers and watch for vulnerabilities or malware. Automation tools can help with this.
- **Use antivirus.** Antivirus software isn't just for PCs and smartphones—it's for servers too and could help prevent a serious malware attack against your entire website infrastructure.
- **Be picky about your plugins.** The software you use to manage your website comes with vulnerabilities too. The more third-party software you use, the greater your attack surface; so only deploy what's absolutely necessary.
- **Consider the whole ecosystem.** Have you deployed a Web Application Firewall to defend against injection attacks? Is your code signing secure for your web apps? Do you have automated tools to detect and defend against the increasingly common problem of DDoS attacks?

Symantec offers a range of tools that makes maintaining complete website security a straightforward and efficient task.

Avoid Compromising Trusted Relationships with Customers by:

- Regularly assessing your website for any vulnerabilities.
- Scanning your website daily for malware.
- Setting the secure flag for all session cookies.
- Securing your websites against man-in-the-middle (MITM) attacks and malware infection.
- Choosing SSL Certificates with Extended Validation to display the green browser address bar to website users.
- Displaying recognized trust marks in highly visible locations on your website to show customers your commitment to their security.

There Is No 'I' in Team

Consumer confidence is built up over multiple interactions across numerous websites owned by countless different organizations. It only takes one bad experience to tarnish the reputation of every single one in the consumer's mind.

As we said in the report, there exists a real opportunity in the coming year to reduce the number of successful web attacks and limit the risks your website potentially poses to consumers, but it will take commitment and action from website owners for it to become a reality.

Adopt comprehensive website security in 2016 and, together with Symantec, make it a good year for cyber security and a very bad one for cyber criminals.