CYBERRISKS&LIABILITIES_

Website Security

Website security is more important than ever. Cyber-criminals are constantly looking for improperly secured websites to attack, while many customers say website security is a top consideration when they choose to shop online. As a result, it is essential to secure servers and the network infrastructure that supports them. The consequences of a security breach are substantial: loss of revenue, damage to credibility, legal liability and loss of customer trust.

Web servers, which host the data and other content available to your customers on the internet, are often the most targeted and attacked components of a company's network. By securing your web server, you protect customers and prospects that use your company website. The following are examples of specific security threats to web servers:

- Cyber-criminals may exploit software bugs in the web server, underlying operating system or active content to gain unauthorised access to the server.
- Denial-of-service attacks may be directed at the web server or its supporting network infrastructure to prevent or hinder your website users from making use of its services. Attacks can include preventing users from accessing email, websites, online accounts or other services. One of the most common attacks is flooding a network with information so that it can't process users' requests.
- Sensitive information on the web server may be read or modified without authorisation.
- Information on the web server may be changed for malicious purposes.
- Cyber-criminals may gain unauthorised access to resources elsewhere in the organisation's network with a successful attack on the web server.
- The server may be used as a distribution point for attack tools, pornography or illegally copied software.

Take the following five steps to protect your company from the threats listed above.

Step 1: Form a plan and utilise the right people.

Because it is much more difficult to address security once deployment and implementation have occurred, security should be considered from the initial planning stage.

Businesses are more likely to make decisions about configuring computers appropriately and consistently when they develop and use a detailed, well-designed deployment plan. Developing such a plan will support web server administrators in making the inevitable trade-off decisions between usability, performance and risk.

Make sure to define appropriate management security practices, such as identification of your company's information system assets and the development, documentation and implementation of policies, as well as guidelines to help ensure the confidentiality, integrity and availability of information system resources.

Businesses also need to consider the human resource requirements for the deployment and continued operation of the Web server and supporting infrastructure. Consider the personnel you will need on your team—for example, system and Web server administrators, webmasters, network administrators and information systems security personnel. Additionally, consider the level of training (initial and ongoing) that will be required to maintain this team.

Step 2: Ensure that web server operating systems and applications meet your security requirements.

When securing a web server, you must first secure the underlying operating system. Most web servers operate on a general-purpose operating system. Many security issues can be avoided if the operating systems underlying web

senti insurance brokers

servers are configured appropriately. Default hardware and software configurations are typically set by manufacturers to emphasise features, functions and ease of use at the expense of security. Because manufacturers are not aware of each organisation's security needs, web server administrators must configure new servers to reflect their business' security requirements and reconfigure them as those requirements change. Take the following steps as appropriate to your business:

- Patch and upgrade the operating system.
- Change all default passwords.
- Remove or disable unnecessary services and applications.
- Configure operating system user authentication.
- Configure resource controls.
- Install and configure additional security controls.
- Perform security testing of the operating system.

Step 3: Publish only appropriate information.

Company websites are often one of the first places cyber-criminals search for valuable information. Still, many businesses lack a web publishing process or policy that determines what type of information to publish openly, what information to publish with restricted access and what information should not be published to any publicly accessible repository. Some generally accepted examples of what should not be published or what should at least be carefully examined and reviewed before being published on a public website include the following:

- Classified or proprietary business information
- Sensitive information relating to your business' security
- Detailed physical and information security safeguards
- Details about the network and information system infrastructure—for example, address ranges, naming conventions and access numbers
- Information that specifies or implies physical security vulnerabilities
- Detailed plans, maps, diagrams, aerial photographs and architectural drawings of business buildings, properties or installations
- Any sensitive information about individuals that might be subject to privacy laws

Step 4: Prevent unauthorised access or modification on your site.

It is important to ensure that the information on your website cannot be modified without authorisation. Users of such information rely on its integrity. Content on publicly accessible web servers is inherently more vulnerable than information that is inaccessible from the internet, and this vulnerability means businesses need to protect public web content through the appropriate configuration of web server resource controls. Examples of resource control practices include the following:

- Install or enable only necessary services.
- Install web content on a dedicated hard drive or logical partition.
- Limit uploads to directories that are not readable by the web server.
- Define a single directory for all external scripts or programs executed as part of web content.
- Disable the use of hard or symbolic links.
- Define a complete web content access matrix identifying which folders and files in the web server document directory are restricted and which are accessible, and by whom.
- Disable directory listings.
- Deploy user authentication to identify approved users, digital signatures and other cryptographic mechanisms as appropriate.
- Use intrusion detection systems, intrusion prevention systems and file integrity checkers to spot intrusions and verify web content.
- Protect each backend server (database server or directory server) from command injection attacks.

Step 5: Protect and monitor web security.

Maintaining a secure web server requires constant effort, resources and vigilance. Securely administering a web server on a daily basis is essential. Maintaining the security of a web server will usually involve the following steps:

- Configuring, protecting and analysing log files
- Backing up critical information frequently
- Maintaining a protected authoritative copy of your organisation's web content
- Establishing and following procedures for recovering from compromise
- Testing and applying patches in a timely manner
- Testing security periodically

Taking proactive measures to secure your website by carefully setting up and maintaining your web server can save your business from experiencing crushing losses of revenue, customer loyalty and proprietary information. For more information about how to mitigate your cyber-risk, contact Sentio Insurance Brokers Ltd today.