
Security risk assessment and management in Web applications

WHITE PAPER

1. Introduction

Security risk assessment and security risk management have become vital tasks for security officers and IT managers. Corporations face increased levels of risk almost daily, from software vulnerabilities hidden in their technology systems to hackers and cyber crooks trying to steal proprietary corporate intellectual property, including sensitive customer information.

An ever-growing list of government regulations aimed to secure the confidentiality, integrity and availability of many types of financial and health-related information also is increasing IT risks and making a comprehensive security risk assessment a modern-day corporate necessity.

But how do organizations perform an accurate security risk assessment of their IT systems and the critical information they store? Risk surrounds us everyday in the physical world, and we take precautions to mitigate those risks, from wearing seat belts to purchasing life insurance.

But it's not so easy to comprehend Web security risk management. How much does it actually cost a company when a Web server is breached, or if an attack disrupts the availability of critical Web systems? What are the costs associated with a hacker or competitor snatching proprietary information or customer lists from an unsecure Web server? How Web security risk management is performed depends entirely on knowing the answers to these questions.

2. The Security Risk Assessment Equation

Such risks can be seen more clearly through the following simple equation that quantifies a security risk assessment:

$$\text{Risk} = \text{Value of the Asset} \times \text{Severity of the Vulnerability} \times \text{Likelihood of an Attack.}$$

In this equation, you can provide a weighting of 1-10 (10 being the most severe or highest) for each risk factor. By multiplying the factors, it's easy to arrive at an aggregate security risk assessment for any asset.

Let's take an everyday example. We have an e-commerce server that performs 40 percent of all customer transactions for the organization. It has a very severe and easy-to-exploit vulnerability:

$$\text{E-commerce server risk} = 10 \text{ (value of the asset)} \times 10 \text{ (severity of the vulnerability)} \times 10 \text{ (likelihood of an attack).}$$

In this example, the e-commerce server risk equals 1,000, the highest security risk assessment possible. The company would then structure its security risk management policies accordingly, allotting more resources to mitigating this risk.

Now, let's compare the results of a security risk assessment in two other instances: a moderate vulnerability with an e-commerce server and a severe vulnerability with an Intranet server used to publish internal announcements.

* E-commerce server risk = 10 (value of the asset) x 4 (severity of the vulnerability) x 4 (likelihood of an attack). The e-commerce server risk = 160, a moderate risk ranking.

* Intranet server risk = 2 (value of the asset) x 8 (severity of the vulnerability) x 6 (likelihood of an attack). The Intranet server risk = 96, a lower security risk assessment ranking.

Even though the Intranet server has greater vulnerability, the value of the asset creates a lower relative risk value than the e-commerce server.

Performing an overall security risk assessment allows organizations to make wise decisions when it comes time to deploy scarce resources to optimize the protection of their assets. Security risk management is a process of managing an organization's exposure to the threats to its assets and operating capabilities. The goals of the security risk management process are to provide the optimal level of protection to the organization within the constraints of budget, law, ethics and safety.

3. How Web Applications and Web Servers Create Risk

One of the most critical sources of risk to organizations today resides within their Web servers. This is because Web servers and applications open systems and information to be accessed by suppliers, partners, and customers.

Performing a security risk assessment and implementing adequate security risk management policies in this area can be critical. Compromised Web servers can damage organizations in many ways, from surrendering customer privacy data and accepting fraudulent transactions to indirectly damaging corporate prestige as the result of a defaced homepage. While it may seem that myriad bad things can happen as the result of a million different vulnerabilities, we can succinctly categorize the core pain points to be addressed in Web security risk management plan in a few primary areas:

Default configuration. Web servers often are installed with default configurations that may not be secure. These insecurities include unnecessary samples and templates, administrative tools, and predictable locations of utilities used to manage servers. Without appropriate security risk management, this can lead to several types of attacks that allow hackers to gain complete control over the Web server.

User input validation. Web sites and applications need to be interactive in order to be useful. However, Web applications that do not perform sufficient validation of user input screens allow hackers to directly attack the Web server and its sensitive databases. Invalid input leads to many of the most popular attacks. A thorough security risk assessment on your organization's internal and external Web applications can reveal what, if any, actions need to be taken.

Encryption. It is a sad fact that although modern encryption algorithms are virtually unbreakable, they are underutilized. In years past, performance considerations were cited as a factor in limited usage of encryption. However, today's high-performing CPUs and specialized cryptographic accelerators have broken down the price/performance barriers related to encryption. The issue with limited encryption has more to do with poor application design and a lack of awareness among developers. Nearly all Web traffic passes in the clear and can be snooped by an alert hacker.

Secure data storage. While it is critical to secure data in transit, it is just as important to implement security risk management policies that keep data stored securely. This includes encrypting data at rest, but it does not stop there. Many Web applications store sensitive files on publicly accessible servers, rather than on protected servers. Other applications do a poor job of cleaning up temporary files, leaving valuable data accessible to the hacker who knows how to find it.

Session management. Another factor one should consider when developing a security risk management plan is that many Web applications do a poor job of managing unique user sessions. This can include using weak authentication methods, poor cookie management, failure to create session timeouts and other session weaknesses. This often leads to session hijacking and other compromises of legitimate user identities. A security risk assessment can determine whether this is a potential problem for your organization.

Maintenance. Failure to implement security risk management policies that keep Web servers updated with the latest vendor patches, as well as neglecting to perform continued testing of proprietary Web applications, creates additional risk.

All of these major problems usually are the result of a lack of due care within the Web application development and maintenance processes. In organizations where security is not “baked in” to both the business planning and application development processes, there can be an appalling lack of awareness of the need to incorporate security best practices from day one. This is a dangerous situation, and the results of the general lack of awareness about the risks associated with Web servers and applications are evident from the weekly headlines reporting stolen consumer and corporate information.

4. Conclusion

The best way to avoid such disasters is to establish an ongoing security risk management process that begins with quantifying the value of Web applications, as well as the data they manage, through a complete security risk assessment. Organizations then must continuously identify and mitigate the vulnerabilities and risks associated with those systems from the beginning and throughout their lifecycle, from development through production.

This approach to security risk management—consistently performing a security risk assessment, then identifying and remedying vulnerabilities by correcting application development errors, applying security patches and fixing system misconfigurations—will lead organizations to continuous improvement of their technology infrastructure and a thorough reduction of risk.