The Driz Group

How Companies Can Improve Website & Web Application Security

Even with a Tight IT Budget

Website and web application security is no longer a luxury – it's a necessity. We live in the age of cyber warfare where no web application is safe, unless security is taken seriously. If you are not protecting your digital assets today, being hacked is not a matter of "if", it's a matter of "when".

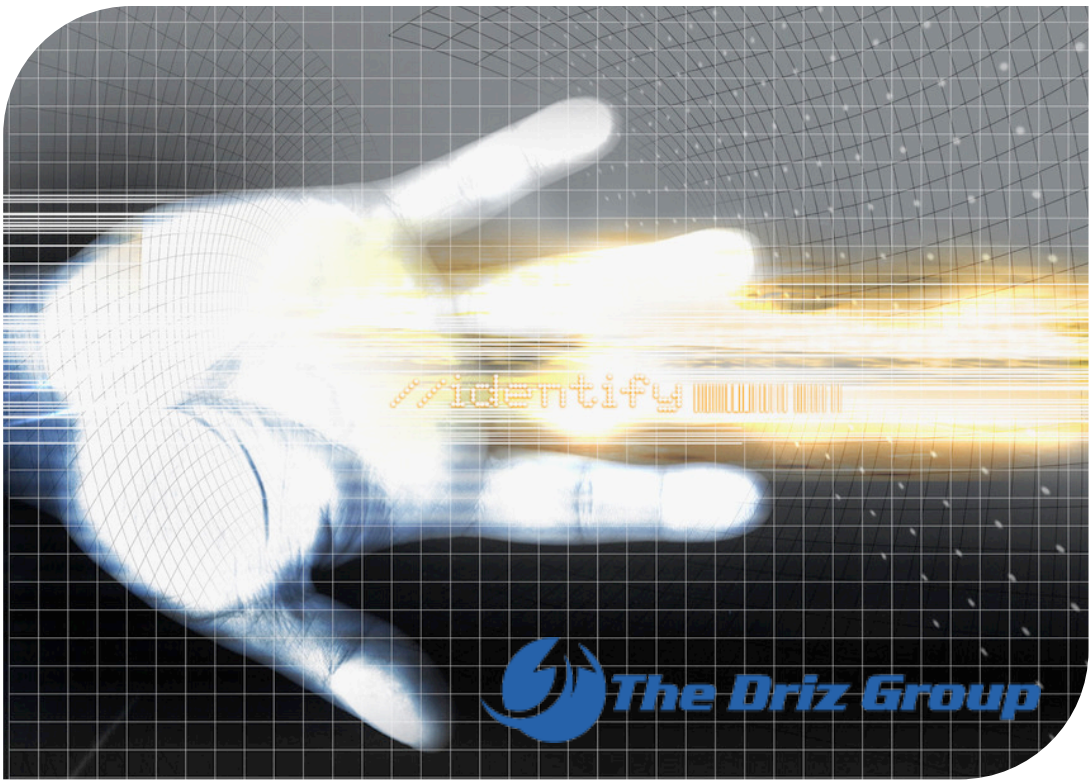
Website & Web Application Security
Website and web application security is no longer a luxury. The days when the costs of a website and web application protection were not affordable for many organizations are long gone. A new generation of security technology companies has emerged. They deliver cutting-edge and affordable security solutions to companies of all sizes, from SMEs to large enterprises.

Website & Web Application Security Landscape
The landscape is complex and difficult to navigate without appropriate guidance from security experts. CIOs are often busy supporting organizational strategy while at same time addressing day-to-day technology-related issues. Websites and web application development is seen as convoluted and somewhat decoupled from the overall IT governance process. Senior executives may not have the necessary knowledge to ask the right questions concerning web security or implement relevant security controls. At the end of the day, as we acquire additional digital assets to deliver more services online, understanding and choosing the right technology becomes particularly important.

Understanding the Process
While developing websites and web applications, two critical security components require constant attention: code security and web application protection.

While everyone understands that code security is important, many organizations either lack the necessary controls or rely on highly manual code reviews performed within development teams. If the code security process is not fully automated, like any other manual process, it is prone to human errors. This could potentially result in running "bad" code, which can open the company's digital assets to vulnerabilities often detected after the damage is already done.

Website and web application protection, on the other hand, is something that has been misconstrued by many, including senior level executives and security professionals. The biggest misperception is generally the difference between traditional perimeters vs. web application firewalls. Web application firewalls were specifically developed to address security issues concerning websites and web application protection. Moreover, they provide web application acceleration using smart content caching and distribution.



We must protect our organizations against cyber criminals that often unleash sophisticated attacks such as SQL injection, cross-site scripting (XSS), and denial of service (DoS).

Website and web application protection approaches and technologies have matured over the last 10 years and now deliver sophisticated protection to fight cyber criminals. A handful of technology vendors concentrate on protecting digital assets while ensuring that your websites and web applications deliver quality customer experience, which include web application speed, reliability, privacy, and security. Some vendors also provide facilities that support compliance requirements, including but not limited to PCI DSS 6.6 compliance, without having to invest in hardware or software.

Both individuals and organizations may fall prey to cyber criminals. When your web application is “hacked”, the consequences might range from significant reputation damage to customer data loss, including disclosure of personal information. Organizations that rely on third-party hosting service providers for web application security often forget that, in most cases, the hosting provider does not assume any responsibility for company-owned website or application security. Even when hosted in-house by the organization, without stringent controls and automation, web applications often remain vulnerable to an attack.

A false sense of security can be costly. Industry leaders estimate that an ecommerce website's downtime may cost as much as $40,000 per minute. In addition, reputational issues resulting in mistrust could jeopardize an entire brand due to a single incident.

To prevent that, companies must establish the standards and programs delivering state of the art protection for all digital assets.

Fixing What's Broken

To succeed, companies must implement solid security programs and develop broader overall strategies to address online threats proactively. In most cases, a simple user error may put an entire organization in jeopardy. Hence, having a development team and educating end users are key to successful implementation of the organizational security program.

Additionally, understanding risks and implementing code security and web application firewall technologies will supplement and support such programs. These will allow for proactive monitoring and timely response to threats with minimal reliance on third party hosting or software providers. After all, it's your company that will be in the news following an incident, not your vendor's. Taking control is the first step to success.

Not knowing that you are vulnerable does not mean that cyber criminals aren't trying to penetrate your website or web application right now. They employ sophisticated bots that scan web applications to discover vulnerabilities automatically, without user intervention.

The number of attempts to harm digital assets amazed most customers who have configured web application firewalls. Instantly, those companies obtain invaluable analytics and insights into online threats related to their digital assets without any investment in hardware or software. Since many IT departments often don't have sufficient resources, fully-managed web application security services may be of great benefit to organizations of all sizes. Keep in mind that most automated solutions can be deployed within hours without any resource requirements from corporate IT.

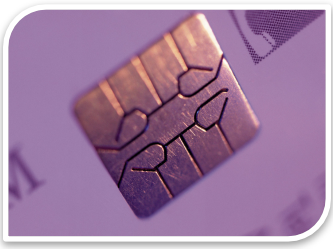
"The Driz Group staff were able to isolate the website security issue following content injection attack, addressing security concerns, while protecting web properties in less than 24 hours."

- VP of Marketing, mid-size recruiting firm

The following checklist includes the steps that you need to follow to safeguard your website and/or web applications.

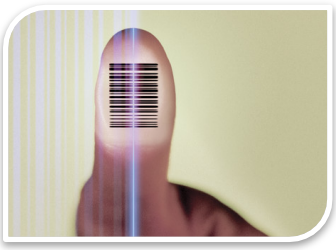
Security Program

Develop and implement the company's security program, which includes security training for software developers, IT staff, and end users. Deliver training at least annually. Don't shy away from sharing important security bulletins and tips with all staff, and do it often. Ensure your security policies and procedures are up to date, and communicate it to all staff.



Vulnerability Assessment

Test, test, test. Perform web application vulnerability assessments quarterly using either a third-party vendor or in-house resources using best in-breed vulnerability assessment tools and methodologies. Document results and actions taken to address vulnerabilities discovered by the internal/external audit, and build internal knowledge base.



Secure Web Applications

Set up free automated monitoring to understand threats and configure your Web Application Firewall (WAF) accordingly. Engage your online security vendor to monitor and fine-tune the WAF to free up valuable IT resources. Select and implement a code security scanning framework to mitigate risks.

Response Readiness

Make sure you have a security services partner you trust to help you with the response readiness assessment based on your current security incident processes. Identify strategic initiatives to help your organization prepare responses to cyber-attacks.

Proactive Monitoring

Implement a fully managed online security monitoring service with your trusted online security services partner. Concentrate on growing your business while your partner proactively monitors critical online security components.

Questions?

We'd love to hear from you.

Please contact us at security@stevedriz.com with any questions, call 1.888.900.DRIZ (3749)

The Driz Group
www.DrizGroup.com