GamaSec

Explore your
Web Vulnerabilities

White paper
Web Application Security: GamaSec Solution

1. Web Applications: An attractive target

How do you cost effectively defend web applications from attack? Your organization relies on mission critical business applications that contain sensitive information about customers, business processes and corporate data. Moving away from proprietary client/server applications to web applications gives you a simpler, cost-effective, highly extensible delivery platform. These applications are more than a valuable tool to power your business operations; they are also a valuable and vulnerable target for attackers.

Web applications are increasingly the preferred targets of cyber-criminals looking to profit from identity theft, fraud, corporate espionage, and other illegal activities. The impact of an attack can be significant, and include costly and embarrassing service disruptions, down-time, lost productivity, stolen data, regulatory fines, angry users and irate customers. Beyond preserving the corporate brand, federal and state legislation and industry regulations are now requiring web applications to be better protected.

As you take action to protect web applications in a timely and effective manner, you must balance the need for security with availability, performance and cost-effectiveness. Protecting web applications requires both zero-day protection and rapid response with minimal impact to operations without impacting performance or changing system architectures.

2. Web applications are increasingly vulnerable

Rapid growth leads to emerging problems

The number of corporate web applications has grown exponentially and most organizations are continuing to add new applications to their operations. With this rapid growth come common security challenges driven by complexity and inconsistency. New awareness into web application vulnerabilities, thanks to organizations such as the Open Web Application Security Project (OWASP), has helped organizations identify application security as a priority. But according to a June, 2006 survey1, while 70 percent of software developers indicated that their employers emphasize the importance of application security, only 29 percent stated that security was always part of the development process.

1 Symantec, http://www.symantec.com/about/news/release/article.jsp?prid=20060919_01

The overlooked vulnerabilities

Unfortunately, it is not just application flaws that are leaving systems vulnerable. In addition to application issues, every web application relies on a large stack of commercial and custom software components. The operating system, web server, database and all the other critical components of this application stack, have vulnerabilities that are regularly being discovered and communicated to friend and foe alike. It is these vulnerabilities that most organizations overlook when they're considering web application security.

As new vulnerabilities are found, patches become a critical part of managing application security.
The process of patch management is complex and difficult to do successfully. Even the most proactive IT team must often reassign critical resources to deploy urgent patches, disrupting normal operations. The time required to patch responsibly lengthens the window of time an attacker has to exploit a specific vulnerability. With thousands of vulnerabilities and patches being announced each year the problem continues to grow. Even organizations with the most efficient patching processes in place can't rely on this alone to protect them from attacks targeting web application vulnerabilities.

Attackers look for the path of least resistance

Today's sophisticated attackers target corporate data for financial and political gain. They know they can more easily exploit vulnerabilities in web application stacks versus trying to defeat well built network and perimeter security. With myriad numbers of vulnerabilities and many different techniques - including SQL Injection, Cross Site Scripting, Buffer Overflow, Denial of Service there is no shortage of options for savvy attackers. In fact there have been over 4,000 vulnerabilities identified in the first 9 months of 2006 and Web flaws made up the three most common 2.

According to zone-h.org, 45% of attacks make use of vulnerabilities rather than configuration issues or brute force. Attackers are working hard to find and exploit new vulnerabilities in web applications faster then they can be patched. The window of time, from when an attacker identifies a vulnerability to when it is communicated and eventually patched, makes a defense-indepth strategy critical to prevent a potentially damaging intrusion.

3. The GamaSec remote online web vulnerability-assessment service

Web applications are increasingly vulnerable and protecting them requires a system that can both ensure compliance today and meet the evolving needs of an organization for tomorrow.
To meet this challenge, by sitting at a remote, online location, Gamasec's solution locates these vulnerabilities as they are seen from the Internet, thus accurately mimicking the attacker's view. Thus, the Company's service will address all the areas covered by the typical software tools pertaining to web traffic.

GamaSec's Web application scanner is an automated security service that searches for software vulnerabilities within Web applications. A Web application scanner first crawls the entire website, analyzing in-depth each file it finds, and displaying the entire website structure. After this discovery stage, it performs an automatic audit for common security vulnerabilities by launching a series of Web attacks.

GamaSec provides a powerful, full-featured,security-scanning service, by providing a constantly updates VA assessment as an online service. Gamasec introduces the following advantages and value proposition which enable it to finally provide a web vulnerability solution for majority of businesses with a web presence.

The GamaSec service identifies security vulnerabilities together with recommended solutions in order to recommend, fix, or provide a viable workaround to the identified vulnerabilities

4. GamaScan, the next advanced generation of online web application security.

GamaSec service is provided remotely. It requires no installation, no set-up, no hardware purchases, no software development, and no IT security expertise. Customers do not even need special training to use it. Complete online and on demand management consul, phone and email support provided by certified security professionals is included for every customer by the GamaSec R&D department.

GamaSec is the next advanced generation of web application security. GamaScan the most complex web application security services executes continuous dynamic tests combined with simulation web-application attacks during the scanning process.

Web Application Attacks Engine – GamaSec is the only company today that covers more than 20 web vulnerability application families with the capacity to create a tailor made attack. We can adapt to any web site configuration and produce dynamic tests, which will create relevant reports of online scan findings.

Automatic False Positive Prevention Engine GamaSec effectively addresses this issue by creating dynamic false-positive filter rules automatically without any manual interference. The sophisticated GamaSec proprietary hashing system manages and inspects seven dynamically generated pages & includes them internally for automatic rules generation.

Enhanced Report Generation for Scanning Comparison - GamaSec includes an internal report creation engine. With enhanced features it provides the ability to create comparison and

trend analysis of your web applications vulnerabilities based on scan results generated over selected time periods. Customers can view their report through the secure GamaSec control panel

Once a scan is complete,GamaSec report provide the ability to validate security breaches & risks against a continually updated service database provides real-time vital business solutions. GamaScan identifies the security vulnerabilities and recommends the optimally matched solution. The fix or workaround solution is identified & implemented when you need it not after it's too late.

GamaSec is unique as an Israeli technology company that has over 10 years of IT security experience and an active in-house R&D Department that published hundred of security advisories worldwide .

GamaSec provides a robust set of reports and charts designed to provide a clear and concise view of security vulnerabilities, as well as recommended solutions.

The Vulnerability Report identifies all services and open ports, with known vulnerabilities listed, as well as descriptions and patches provided. The Security Notification Report provides vulnerability details and subsequent issues, as well as recommended fixes.