SOPHOS

Closing the Back Door on Network Application Vulnerabilities

Web Server Protection and Your Security Strategy

By **Angelo Comazzetto**, Senior Product Manager, Network Security

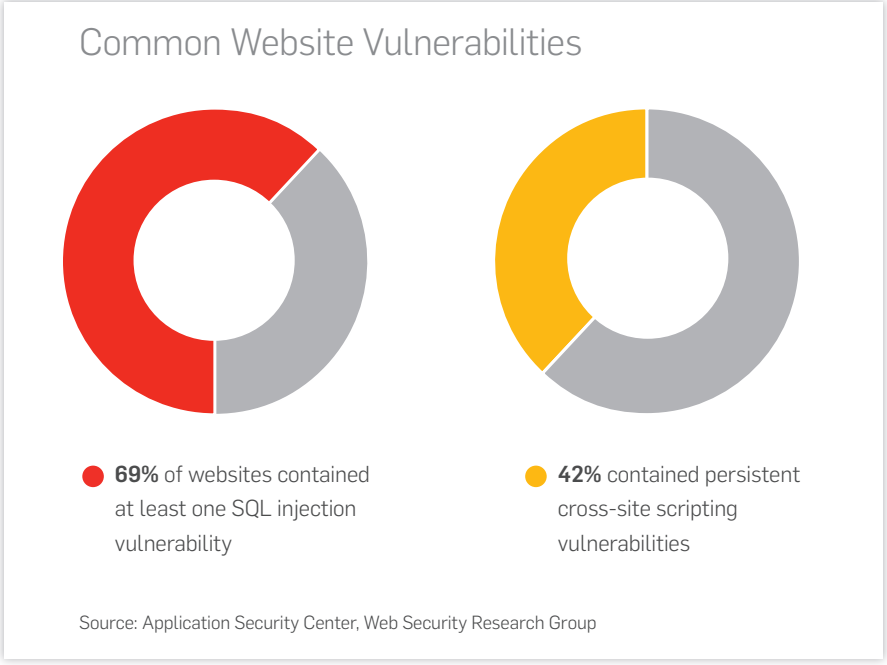
With new attack techniques and new vulnerabilities affecting web servers, traditional firewalls are no longer enough to protect modern networks. Including web server protection as part of a complete IT security infrastructure creates a more secure environment. However, web application firewalls tend to be expensive and difficult to manage, making it unrealistic for SMBs to deploy these solutions. This whitepaper explains how and why cybercriminals target web servers, and how SMBs can use unified threat management (UTM) to simplify management and deployment of web application firewalls to protect web servers.

Web server vulnerabilities

Just about every organization, whether a worldwide conglomerate or a locally owned business, has a website. The website is the public-facing part of the organization, where prospective and current customers go to interact with a company. Customers can use websites to manage their accounts, find new information and order products. Unfortunately, some SMBs neglect to protect this public, vulnerable part of their network.

At this point, most companies have a firewall and URL filter in place as well as antivirus and anti-spam programs. The challenge, however, is that threats are increasingly sophisticated and web-based. In fact, a recent report stated 80% of network attacks targeted web-based systems.[1] While first- and second-generation firewalls can prevent some infections from getting onto your network, they aren't enough to block all malware from getting in, such as ransom and fake antivirus malware.

A firewall-only strategy is like locking the front door to your house and hoping no one notices you left the back door unlocked, with only a screen to stop intruders. Cybercriminals will have no problem pushing the screen in and getting into your network. With new attack techniques and new vulnerabilities in web servers, traditional firewalls are no longer enough to protect modern networks. Integrating web server protection as part of a complete IT security infrastructure creates a more secure environment.



1. Top Cyber Security Risks Report, HP TippingPoint DVLabs, SANS Institute and Qualys Research Labs, September 2010

Evolution of the firewall

Firewalls emerged in the late 1980s, when the Internet was a new technology with limited global use and connectivity. So called first-generation firewalls leveraged packet filters that inspected the packets transferred between computers on the Internet. If a packet matched the packet filter's set of rules, the packet filter dropped (silently discarded) the packet, or rejected it outright (discarded it, and returned "error responses" to the source).

Second-generation firewalls performed the work of their first-generation predecessors, but operated up to layer 4 (transport layer) of the OSI model. They examined each data packet as well as its position within the data stream, a technique known as stateful packet inspection. A second-generation firewall recorded all connections passing through it to see if a packet was the start of a new connection, part of an existing connection, or not part of any connection.

Today the firewall has evolved with the addition of application layer filtering. It can "understand" certain applications and protocols such as File Transfer Protocol, DNS, or web browsing. And it detects if an unwanted protocol is sneaking through on a non-standard port, or if a protocol is being abused in a harmful way.[2]

See the evolution of network security over time.

Download our infographic

The OWASP Top 10 Web Application Security Risks

1. Injection
2. Cross-site scripting (XSS)
3. Broken authentication and session management
4. Insecure direct object references
5. Cross-site request forgery (CSRF)
6. Security misconfiguratation
7. Insecure cryptographic storage
8. Failure to restrict URL access
9. Insufficient transport layer protection
10. Unvalidated redirects and forwards

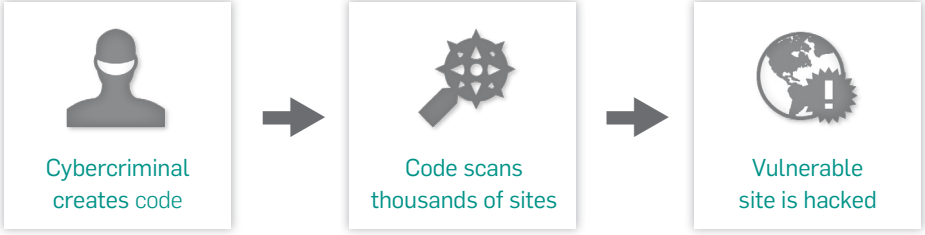
2. Wikipedia, Firewall (computing): http://en.wikipedia.org/wiki/Firewall_%28computing%29

3. The Open Web Application Security Project (OWASP) is an organization that specializes in bringing visibility and awareness to web application security. See The OWASP Top Ten for 2010, https://www.owasp.org/index.php/OWASP_Top_10

Cybercrime and small organizations

SMBs may feel their size makes them less of a target. To many cybercriminals, however, size doesn't matter. Cybercriminals don't often target specific companies or sites. Their goal is making as much money as possible with the least amount of effort. Cybercriminals create code to take advantage of a specific type or class of web server vulnerability. This code will then scan hundreds to thousands of websites looking for a vulnerability. When one is found the code is deployed and the website hacked.

How Cybercrime Works



It doesn't matter how large or small an organization is and how much information a cybercriminal can steal from a single server. For a single piece of malware the results are cumulative, so the cybercriminal gets rich regardless of an organization's size. Because SMBs are less likely to have strong web server protection in place they are actually more likely to suffer a breach than a larger, more well-known company. The reason one might think otherwise is that smaller organizations rarely make the news when they have a breach.

SMBs often forgo implementing a web application firewall because it can be expensive to manage and complicated to deploy. SMBs instead choose to rely on their traditional firewall or other network security device to protect web servers. This wouldn't be an issue if companies didn't need to allow outsiders to submit information to the web server to submit orders, access accounts or edit personal information. But they do.

As a result, when a company creates a forum, for example, they need to protect or delete the administration tools used to initially set up the forum, for instance www.mydomain.com/admin.php, so no one outside the company can access it or see it. If an SMB omits this step, cybercriminals may take advantage and gain a back door into the network. Once there, they can find any data stored on the server such as credit card information and email addresses.

In many countries, organizations that process credit card data are required to meet minimum security requirements. The Web Application Security Consortium notes that 99% of web applications are not compliant with the PCI Data Security Standard.[4] Using a web application firewall or a code review can help ecommerce companies prevent common exploits and stay compliant with industry and government regulations.

Similar to SMBs, local governments are offering services online. In these self-service portals, residents can update driver's licenses, register their pets, pay taxes or utility bills, fill out census forms or register to vote. While this type of portal makes life more convenient, some local governments do not employ a security expert. Without an easy-to-manage web server protection solution, governments striving to make life easier for their residents make it easier for cybercriminals to steal their personal data.

Closing the back door to your network

If every organization with a website is vulnerable to web server attacks, how can SMBs close and lock the back door to their network?

Below are seven tips for securing web servers.

1. Know your network and how it appears to others

SMBs should review what information is readily available to would-be attackers. The less unintended information available, the better. Start by examining public DNS records to make sure only valid corporate information is available and no personal employee information is listed. Attackers may use publicly available information about an organization and its employees to launch an attack against it.

Next, check web server responses to make sure information about operating systems and applications used is not available. Finally, review error pages and make sure they don't give out information such as local machine name or directory structure.

2. Limit responses to probes and errors

Rather than providing responses to "malformed" requests (e.g., those your web server was unable to understand or process), SMBs should eliminate them altogether. This cuts down on the amount of information provided, and helps to avoid filling up logs, which could result in a resource issue or downed server.

4. Web Application Security Statistics 2008, Web Application Security Consortium, http://projects.webappsec.org/w/page/13246989/Web%20Application%20Security%20Statistics

3. Remain vigilant

IT administrators should monitor logs and reports for signs of anomalies, attackers and vulnerabilities. Knowing what others are doing is important so that organizations can maintain sufficient defenses. It may also help administrators spot holes you missed in your network review.

4. Perform active review

User NMAP (Network Mapper) and other tools ensure only allowed ports are available to the public. Know what ports are open on web servers and what IPs are visible on the Internet. Ideally, an organization will deny all traffic and only allow specific ports and applications to and from their servers.

5. Deploy a decoy or proxy name

Using decoy names and information in public records and for error messages may help organizations find attack attempts. If you notice someone trying to contact the decoy name or launch attacks based on that misleading information, it can confirm when someone is probing your defenses.

6. Don't depend on a single layer of defense

Firewalls and IPS (intrusion prevention systems) can help guard against simple exploits and denial of service (DoS) attacks, but these solutions can't protect against web server attacks such as cross-site scripting and SQL injections. To properly protect valuable web servers, you need a web application firewall.

Most web application firewalls also function as a reverse proxy. Instead of passing traffic from the Internet through to the server, the web application firewall makes a new connection on its behalf. A web application firewall offers advanced features such as malware scanning and SSL offloading.

7. Separate resources to minimize the results of a breach

Install a web application firewall in a protected zone without access to the local LAN or internal users. This means you won't open up the entire organization to threats should a successful exploit occur.

Limits of firewall-only network security

As we have seen, traditional network security depends on standalone devices to secure the network environment. These standalone products are generally deployed as software, running either on a PC or an appliance, and provide product-specific network security functions, like a firewall. Firewalls generally protect the internal network from outside attack and prohibit access from the internal network to outside sources. But firewalls on their own fail to provide SMBs with the security, deployment flexibility and performance they need to defend against today's growing and sophisticated cyber threats.

Standalone network security products, such as firewalls, introduce significant challenges:

1. Today's rapidly evolving cyber threats are more sophisticated and evade one or more standalone technologies. It's easier to target a standalone device that gives an attacker a clear passage to the network.

2. Managing and maintaining an increasingly distributed network with no clear perimeter is costly and complicated. This not only creates a security gap but also adds burden to already-taxed resources.

3. The performance and processing power required to provide complete content-level protection is difficult to achieve without purpose-built hardware.[5]

Advantages of UTM based network security

The best way to counter the diverse threats associated with web access is to consolidate security in a gateway-based, all-in-one solution that works with the existing firewall. The IT administrator gains oversight and control of inbound and outbound web traffic, and can selectively install filters, monitors, and throttling controls to regulate traffic in a safe, orderly, system-wide manner.

Unified threat management (UTM) is an otherwise traditional firewall appliance that also performs duties traditionally handled by multiple systems, including content filtering, spam filtering, intrusion detection and antivirus. UTMs are designed to combat all levels of malicious activity on the computer network.

An effective UTM solution delivers robust and fully integrated security and networking functions such as network firewalling, intrusion detection and prevention systems (IDS/IPS) and gateway antivirus. Other features include security management and policy management by group or user. A UTM protects against application layer threats and offers centralized management through a single console, all without impairing the performance of the network.

5. Network security: Using unified threat management, SearchNetworking, TechTarget, http://searchnetworking.techtarget.com/tip/Network-security-Using-unified-threat-management-UTM

Organizations that implement an all-in-one web security solution gain distinct advantages over more costly and complex single-function web filtering solutions. A single point of control over web access and usage has a number of benefits:

- **Malware protection:** Threats from malware, spyware, viruses, worms and other attacks can be mitigated by a robust first line of defense.
- **Reduced costs:** A centrally managed appliance for web security reduces IT management tasks and simplifies routine maintenance and upgrades.
- **Legal compliance:** Companies can block access to inappropriate or illegal web content to comply with internal policies and legal mandates.
- **Increased productivity:** Employees won't be surfing non-business sites during business hours, lowering the risk of infection from malware on questionable sites. And network-taxing activities such as bit streaming can be eliminated.

Conclusion

For SMBs in particular, an appliance-based web security gateway provides cost-effective, easy-to-deploy protections and network-use controls in a centrally managed solution. This approach enhances traditional security measures while protecting against emerging threats such as web-based attacks that exploit vulnerabilities at both the user and the server level.

An all-in-one approach to web security offers simplified management, more consistent security across the network, better control of web application usage within a company, and reduced exposure to emerging web-based security threats.

Following the tips in this whitepaper and deploying the Webserver Protection subscription within Sophos UTM can help you close the back door to your network.

Sophos Webserver Protection—part of Sophos UTM

Configuring a web application firewall can be difficult and expensive. UTM devices are designed with the SMB in mind, offering management of multiple security functions from a single console. Because a UTM device is deployed on the network gateway, it is in the ideal position to protect the web server.

Sophos Webserver Protection is available as a subscription in the Sophos UTM console. Because it is managed through the Sophos UTM WebAdmin interface, it provides SMBs with a simple way to manage web application security along with the organization's other security functions.

Sophos Webserver Protection offers the following functions so SMBs can secure applications like Outlook Web Access (OWA) while protecting against attacks like SQL injection and cross-site scripting:

Web application firewall: Cybercriminals silently test your sites and applications for security holes until they find a weakness. The web application firewall within the Sophos Webserver Protection subscription keeps hackers from using SQL injection or XSS by scanning activity and using patterns to identify probes and attacks.

Form hardening: Sophos' unique form hardening technology inspects and validates the information submitted by visitors via forms on the website. This stops malicious users from using forms to pass invalid data that can damage or exploit servers.

Reverse proxy: Sophos UTM protects web servers and Outlook Web Access. Admins scan all incoming and outgoing transactions in real time, using various security features to control how visitors interact with the servers over normal HTTP and encrypted HTTPS.

Antivirus: The Sophos Webserver Protection subscription provides two separate scanning engines that operate in parallel to prevent infection and keep your users and servers safe. Content is scanned and blocked at a central point before it is allowed to enter or leave the network.

URL hardening: Sophos' URL hardening feature allows website visitors to access only the content they should be allowed to see. By forcing visitors to interact with servers in the correct way, this feature keeps creative hackers from performing unexpected operations to cause harm.

Cookie protection: Cookie protection keeps cookies—commonly-used "information packages" given to visitors by web servers—safe from tampering. By digitally signing each cookie, this feature verifies the integrity of this information when it returns from the user.

United Kingdom Sales:
Tel: +44 (0)8447 671131
Email: sales@sophos.com

North American Sales:
Toll Free: 1-866-866-2802
Email: nasales@sophos.com

Australia & New Zealand Sales:
Tel: +61 2 9409 9100
Email: sales@sophos.com.au

Boston, USA | Oxford, UK

A Sophos Whitepaper 4.12v1.dNA

SOPHOS