CSO
SECURITY AND RISK

Print Close Window

From: www.csoonline.com

10 ways to secure browsing in the enterprise

Make users' browsing safe (or safer) by thinking holistically about Web security, from browser settings to policies and education

Joseph Guarino, CSO

November 01, 2011

It goes without saying that the Internet isn't a safe place—it's a veritable jungle. In the world of browsers, we, the users, are seen as a delicious and commonly exploited target by many adversaries. Much like in the real jungle, we most often fall prey to lurking predators that bring us down using spear phishing, drive-by downloads and all manner of malware.

The browser itself, Java, Javascript, HTML5 and plug-ins such as Adobe Flash allow us great opportunities to use rich applications, but they also open the door wide to cybercriminals.

[Also read Guarino's 7 Firefox plug-ins that improve online privacy]

Every technology has a downside that will be exploited. As a result, the browser, often called the universal client, is an ever-growing conduit of malware into the modern enterprise. Truth is, malware and its risks are ever evolving with the demands of cybercriminals and black hats, and browsers just happen to be a particularly soft and tantalizing target. Unfortunately, history has shown us that the trend is only accelerating. Despite the more recent evolution of additional security features, the browser remains a good soft target when care isn't taken to lock it down in your enterprise.

It's possible to improve your browser security stance by making some changes to people, procedures and technology. We don't have to be lunch for the piranhas or a quick snack for the tiger; we can defend ourselves in the Internet jungle. Here are my top 10 recommendations for improving the security of your browsing environment.

1. Holistic Patch Management

Patch management is nothing new, but it's rarely done in a holistic, all-encompassing way. Most organizations do a great job of patching core operating systems but sometimes neglect associated core Web technologies such as Adobe Flash and Reader, Apple Quicktime, and Java. Holistic patch management addresses the entire desktop of native and third-party applications, including the browser and all its associated plug-ins, in a comprehensive way.

As if the complexity of the desktop isn't enough, consumerization (the effort of many users to bring their own device into the enterprise) introduces new perils in both patch management and security. Whether it's the executive who wants to use a shiny new tablet with known unpatched vulnerabilities or the user who wants to use a smartphone running an ancient and exploitable browser, patches must be kept up to date. A coherent, holistic effort to patch is helpful in defending against a multitude of known vulnerabilities. Obviously it isn't a panacea—nothing is—and you can't fix zero-day vulnerabilities, but by addressing what you can, you'll reduce your risks and costs.

2. Browser Lockdown

Although I'm a user of open-source software such as Mozilla Firefox and Google Chrome, I'm going to address browser security with a focus on the browser with the most market share in the enterprise: Microsoft Internet

Explorer. All current browser usage statistics put Explorer at the top of the heap, and because Microsoft dominates the corporate desktop space, its penetration there is even greater.

Microsoft has made many strides in beefing up Internet Explorer's security, and many of those are available in the Active Directory through Group Policy. The Active Directory is not only a centralized directory service offering authentication and authorization for your Windows domain, but it also can control security policies throughout your Windows environment. Group Policy allows administrators to centrally control the configuration of Internet Explorer and thus efficiently lock down an entire enterprise's browsers.

Internet Explorer versions 8 and 9 offer nearly 1,500 configurable settings, so you would be hard-pressed to say it's not flexible enough to meet your security requirements. Of particular use to the enterprise is the ability to control the user interface by disabling certain menus or configuration options—

- tweaking security zones (which allow you to set the level of trust that the client or browser should have)
- setting up smart screen filters (which help protect from malicious phishing or malware sites)
- using Active X control and filtering (which provide the ability to control add-ons)
- managing and blocking downloads, and more.

Books have been written on this subject, but suffice it to say you might want to explore these features to further lock down your enterprise browsers.

3. Filtering Proxy with Malware Scanning

As an additional layer of security and as part of an effort to add depth to your defenses, a filtering proxy with malware scanning can prove invaluable. Vendors offer products such as unified threat management devices and dedicated filtering proxies with advanced Layer 7 filtering and anti-malware scanning.

These devices allow you to have additional deep application-layer insight into the traffic coming into your enterprise; coupling them with URL blocking, malware scanning and enhanced logging should provide overall cost reduction and performance improvement.

4. Evolved Anti-Malware Defense

Anti-malware has evolved from simple signature and engine models and can now include heuristics or behavior-based functions. This is a welcome evolution in light of today's many Web threats.

Features such as malicious URL detection, advanced client-side firewalls, light host intrusion detection, sandboxing and white- or blacklisting applications are all now available. These anti-malware defenses add an additional layer of proactive defense to your enterprise at one of its key weak points. Your anti-malware suite should have many of these core features and great management tools to maintain it in your enterprise; if it doesn't, it's time to start shopping around.

5. Minding Your Mobile Devices

Smartphones and tablets have a growing presence in the enterprise, and malware comes with them. Leading mobile computing players such as Google Android and Apple iOS have had their share of security issues, and we can only expect this to continue. System and network administrators have nowhere near the management capacities or security features on these mobile devices as they do on traditional desktop operating systems. Users can fall prey to downloading malicious code, phishing or social engineering much more easily on these mobile devices that lack the protections provided by a real desktop operating system's security protocols and hardened browser.

[Also read Social engineering: 3 mobile malware techniques]

Apple could do much more than assert that its software is secure and claim that it doesn't need anti-malware. Google, too, could offer more insight into what it allows in its much-less-walled marketplace. Truth be told, both companies need to strive for improvements in security terms. For now, third-party vendor-management suites for Android and iOS are providing greater manageability and increased security.

6. Good Password Policies or Two-Factor Authentication

Cracking passwords isn't rocket science; the tools and knowledge exist and are freely available. As a result, your passwords and policies should be strong enough to stymie hackers. Whenever possible, your password policies should enforce password age, complexity and length requirements. This is as true for your corporate Web presence as it is for your network or VPN.

Two-factor authentication is often a good choice, but it can be prohibitively complex and costly. For those using traditional passwords, augmenting the browser with a password manager can help stop users from plastering their cubicles with sticky notes displaying sensitive passwords. Sad to say, I still see this happen all the time. For those managing these password nightmares, there are many password managers available, some native to the browsers themselves and others made by third parties. These include

- RoboForm
- LastPass
- and the open-source KeePass.

No matter where you use passwords, strong policies are always a smart idea.

7. Frequent, Required User Security Training

While many organizations have embraced end user security training, it is far from universal. But users play a strong role in information security—safer and more secure environments are created by well-trained users. End user security training should happen with some frequency, as the threats never stop evolving. At the very least, yearly training should revisit issues and update end users' skills in responding to current threats. A security-aware workforce can be a huge asset in the fight against today's multifarious threats.

8. Proper Policy and Procedures

Proper computer security policy will help users understand how they should and shouldn't use information resources.

Users should have to read, agree to and sign security policies. Procedures should be in place so users acknowledge their role in ensuring enterprise security. Policies and procedures should be reviewed during user training so users are aware of and properly engage them.

Wrapping these policies and procedures around regular end user training can create a user base that understands these security risks and how to properly respond to them.

9. Minimal Privileges

It's hard to imagine, due to the risks, but some organizations still run desktops with administrative privileges. To avoid constant requests to install or configure software, IT operations sometimes allow users to install whatever they like.

End users generally lack the expertise needed to identify malware, so they often fall prey to it. Additionally, insider threats are very real, and by running your desktop machines in this manner you are simply asking for security nightmares.

To reduce the potential damage that Web-based malware can wreak, users should only be given the minimum amount of privileges they need to do their jobs.

Thankfully, I'm seeing less and less of this problem in my consulting engagements, but I do still run into it, and I laugh (and sometimes cry a bit) when I do. Reducing privileges simply makes security sense.

10. Thinking Defense in Depth

Don't be lulled into a false sense of security that many security products seek to give you. No single effort, action, product or service is a security cure-all.

What is required is a comprehensive, consistent effort to reduce your risk by using the aforementioned methods, which are just a few of the many good security practices you should adopt. Security isn't a simple point-and-click solution, but rather a concerted, ongoing, multifaceted, iterative process.

[Learn infosecurity defense-in-depth lessons from a bronze-age fort]

While these top 10 techniques don't make up the entire exhaustive list I could provide on this topic, they are a step in the right direction. Technology alone doesn't make your organization more secure, but having a holistic view of security can lessen your Web-borne risks. With the rise and continuing evolution of Web-based malware, cloud computing and mobile devices, there's no reason to think these risks are going away anytime soon.

Your organization doesn't have to be a haven for cross-site scripting, malicious Javascript, plug-in flaws or browser-based exploits. You can tame the browser beast, or at least temper it.

So, take a holistic defense posture, investigate your Web-based threats in-depth, and reap the reward of fewer risks.□

Joseph Guarino is CEO of consulting company Evolutionary IT.