GFI White Paper

Monitoring the Web is all about security and nothing but security

Contents

Introduction

The Web is a mainstay of daily working process – we use it for everything from communication, research and commerce to entertainment, news and advertising. Yet, the freedom of information access afforded by a broad and open Web has brought with it numerous management and monitoring challenges for the IT department.

Monitoring Web activity can be a contentious issue, but it is a function that is critical to the productive and safe continuance of open Internet access in the workplace. The process of monitoring, whether it is monitoring the uptime of a Web server or monitoring the Web traffic going in and out of an organization, is fundamentally a security activity, rather than one of content control or oversight of personnel online activity. The Web traffic generated by end users brings with it heightened risk of exposure to an array of security challenges, from malware and online scams to a heightened risk of confidential data being shared or exposed to outside entities via Web sites such as social networking services, forums, and Web-based email platforms.

Web monitoring is therefore crucial to the organization's security, and while it can be viewed negatively by some end users, combined with education and clearly explained IT policy, it can deliver substantial benefits and reduce instances of compromised data and user security through careless or unintended Web access activities[1].

Furthermore, moving Web monitoring into an auto updatable hybrid model of on-premise and in the cloud can deliver previously unobtainable levels of accuracy, reliability and scope of cover, ensuring that all users, regardless of whether they are inside or outside the corporate network, can benefit from the most-up-to-date Web site filtering information, aligned with IT policy and local overrides for acceptable and unacceptable Web sites[2].

The good and bad parts of the Web

At the core of any Web monitoring strategy is filtering – using pre-determined lists of bad and prohibited websites to block or allow access at the point of initial request. While so-called whitelists and blacklists can be used to block and prevent Web site access for a number of non-security reasons, it is as part of an overall security strategy and security technology suite that Web filtering is most effective – eliminating the security threat posed by compromised or known malware sites at the point of request, rather than relying solely on a client-side antivirus solution to combat malcode after the site loads and the code executes.

Predominantly a security-driven concept, Web filtering is a robust and flexible technology that enables IT administrators to respond to trends in Web traffic use and augment the lists provided by the Web monitoring software or service vendor with entries of their own, broadening the list of prohibited sites in order to fit prevailing IT policy within the organization, or simply to curtail casual surfing practices that pose a potential security risk, such as data leakage or exposure to malcode.

Web monitoring and filtering provides multiple lines of security defense for an organization, centered on the following areas:

- **Preventing data leakage:** By blocking access to websites and services that are known to be hosting socially engineered phishing scams or other illegitimate attempts to harvest information, unintentional data leakage can be drastically reduced from the offset. Furthermore, organizations can decide to manually block access to Web-based services that can be used to transport company data outside of the protection of the network boundary, such as free webmail services, forums and social networking sites[3]. This extra level of security-driven site blocking can be applied globally or on a per-user basis, with Web access restrictions and permissions applied based on role, workgroup or location.
- **Avoiding lost productivity:** Not always seen as a security consideration, yet malware-driven disruption can substantially affect operational productivity, if clients and server-side systems are infected with malware or suffer software or operating system damage as a result of malicious code deployed from a compromised or otherwise infected website.

- **Reducing instances of compromised client and server systems:** Systems that become infected with viruses, botnets, Trojans and other forms of malware launched from infected websites not only become useless in the short-term, they create substantial additional work for the IT department which will be charged with wiping, reinstalling and redeploying the affected system. The organization also incurs the cost associated with losing one or more machines while they are disinfected and made safe, along with the cost associated with the initial helpdesk call and subsequent remediation work.
- **Corrupted data silos and OS installations:** Given the substantial time needed to recover clean versions of data from backups, minimizing the risk that key documents such as Microsoft Office files, email PST files and other key data silos are not compromised as a result of unchecked web surfing is essential.
- **Monitoring use of secure and insecure connections:** Using Web monitoring to see where users are using secure connections, and where sites are failing to use HTTPS secure pages for the transfer for sensitive data such as passwords can provide valuable insight for the IT department when looking to augment the vendor-supplied lists of prohibited sites with additional lists of untrusted and insecure websites that should be blocked to protect data integrity.

The cost of resolving malware and other infections caused by users visiting compromised websites can be substantial to an organization. According to analyst firm Gartner, end-user contact with the IT service desk costs the organization, on average, $20 per call. But contacts handled by experienced staff, for example for business application installs and hardware upgrades, can cost as much as much as $50 just for the initial call[4].

Protecting against legal challenges

While the potential benefit of protecting users from malware and other malicious code embedded in and deployed from websites is clear, there is a wider consideration for the organization – protection from illegally shared content that may be accessed, intentionally or otherwise, by end users via company-owned hardware or company Internet connections that can be traced by the authorities or copyright holders:

- **File sharing:** Restricting access to sites known to be sharing commercial content without the permission of the copyright or intellectual rights holder, such as movies, TV shows, music and other entertainment products, not only protects the end user from potential litigation by the copyright holder, but also protects the organization from being hit by any such legal action due to complicity by providing the Internet connection, computer and other enabling resources
- **Illicit content:** Blocking access to pornography not only ensures that illegal material is not accessed by users, protecting both the user and the organization from litigation, but also prevents follow-on litigation being brought by employees against the organization if they are exposed to other users accessing illicit and offensive material in the workplace
- **Regulatory compliance:** Ensuring that unmonitored Internet use does not compromise regulatory compliance considerations including data protection, communications tracking and adhering to the correct timetables for making public announcements such as financial results or any company announcement that could affect an organization's share price is essential. Web filtering can be used to prevent access to websites where users might inadvertently put compliance at risk, protecting the organization from fines, sanctions and reputational damage.

Summary

Monitoring Web traffic within an organization is not only a major component of the security software and service architecture, but is also an important part of security policy.

Monitoring and limiting access to websites can be seen by some as an attempt to limit Internet freedoms for reasons other than security – to limit freedom of information or to limit distractions that could otherwise hamper business productivity. While it is true that Web filtering can be used with these notions in mind, the savvy IT department will realize that a happy workforce is one that is trusted to use the Internet responsibly. That said, even responsible users require help and support in the form of security safeguards to prevent malicious, fraudulent and otherwise troublesome Web content from imposing risk on the organization and from affecting the end user Web experience.

Organizations not only need to implement clear IT policy to support Web monitoring, they also need to reinforce this with clear training and communication to ensure that users understand both the reasons why Web monitoring is in place, and the wider implications of not monitoring and filtering Web traffic in the workplace.

GFI WebMonitor®

GFI WebMonitor has been designed to cover as many facets of web security as possible without adding to an IT administrator's workload or impacting negatively on budgets. The Unified Protection Edition provides protection against all the above mentioned security risks. The primary goal is always to provide comprehensive protection at a low cost.

Security related features:

- Two antivirus engines, with a 3rd optional engine for scanning all downloads including downloads coming over HTTPS channels
- Download prevention policies using real file types
- WebGrade database covering 280 million websites (and growing) in 77 categories including a number of security categories which can be implicitly blocked
- Automatic blocking of known bad websites – hundreds of thousands of sites known to be distributing malicious content are blocked
- Support for blocking popular IM clients
- WebGrade Web Reputation Index to allow blocking policies based on the reputation of a website

The best way to assess the web risk to your own organization is to try GFI WebMonitor. Visit http://www.gfi.com/internet-monitoring-software to download and begin a 30-day free trial.

1. IT Security: A Step-by-Step Guide For Growing Businesses: Dr John Leach
2. http://www.pcworld.com/businesscenter/article/253609/what_should_cloud_providers_know_about_their_customers.html
3. http://www.windowsecurity.com/articles/data-leakage-prevention.html
4. Putting Your Users In Charge Could Save You Millions: Richard Cudd & Martin Anderson, August 2010

USA, CANADA AND CENTRAL AND SOUTH AMERICA

15300 Weston Parkway, Suite 104, Cary, NC 27513, USA
Telephone: +1 (888) 243-4329
Fax: +1 (919) 379-3402
ussales@gfi.com

33 North Garden Ave, Suite 1200, Clearwater, FL 33755, USA
Telephone: +1 (888) 243-4329
Fax: +1 (919) 379-3402
ussales@gfi.com

UK AND REPUBLIC OF IRELAND

Magna House, 18-32 London Road, Staines-upon-Thames, Middlesex, TW18 4BP, UK
Telephone: +44 (0) 870 770 5370
Fax: +44 (0) 870 770 5377
sales@gfi.co.uk

EUROPE, MIDDLE EAST AND AFRICA

GFI House, San Andrea Street, San Gwann, SGN 1612, Malta
Telephone: +356 2205 2000
Fax: +356 2138 2419
sales@gfi.com

AUSTRALIA AND NEW ZEALAND

83 King William Road, Unley 5061, South Australia
Telephone: +61 8 8273 3000
Fax: +61 8 8273 3099
sales@gfiap.com

For a full list of GFI offices/contact details worldwide, please visit http://www.gfi.com/contactus

Disclaimer

The information and content in this document is provided for informational purposes only and is provided "as is" with no warranty of any kind, either express or implied, including but not limited to the implied warranties of merchantability, fitness for a particular purpose, and non-infringement. GFI Software is not liable for any damages, including any consequential damages, of any kind that may result from the use of this document. The information is obtained from publicly available sources. Though reasonable effort has been made to ensure the accuracy of the data provided, GFI makes no claim, promise or guarantee about the completeness, accuracy, recency or adequacy of information and is not responsible for misprints, out-of-date information, or errors. GFI makes no warranty, express or implied, and assumes no legal liability or responsibility for the accuracy or completeness of any information contained in this document.

If you believe there are any factual errors in this document, please contact us and we will review your concerns as soon as practical.