GFI White Paper

Vulnerability scanning – Your company's personal virtual security consultant

Contents

Introduction

Managing a large and growing PC estate is no simple matter, particularly if you are doing it manually. Keeping a close watch on a couple of PCs can be straightforward, and a diligent IT manager will manage to keep such machines fully patched and free of troublesome software. But what happens when your estate grows beyond one or two machines?

Proactively identifying and tackling security threats and system weaknesses before they become bigger problems presents a particularly big challenge for IT managers in organizations of all sizes, but particularly for smaller organizations where IT resources and manpower to check servers and PCs are limited.

This is why vulnerability scanning is a critical component in your security and PC reliability toolkit, helping to automate the process of monitoring and checking PCs around the organization for issues and weaknesses, allowing IT staff to concentrate on implementing fixes for both security issues and potential reliability flaws before they become a problem, rather than spending significant amounts of time hunting for hitherto unseen issues in areas such as the Windows Registry, IP stack and in key everyday software such as Web browsers and mail clients.

However, vulnerability scanning offers much more than simply identifying known issues; it can provide much deeper vulnerability analysis and risk assessment for an organization, forming the basis of a virtual security consultant that can keep you on top of what is going on with your servers and PCs across the estate, as well as helping you make the right choices with regards to data and user security, efficiency, disaster recovery and productivity.

Automating the vulnerability discovery process

Vulnerability scanning solutions deliver multiple functions, starting with automating the most labor-intensive parts of the risk discovery process, allowing IT managers to scan a multitude of devices from afar and cross-reference them against a regularly updated database of known security flaws, existing patches and other software problems that may inhibit the safe and secure use of a given PC.

Not only will automating this process cut the time taken to discover vulnerabilities, it will massively reduce the manpower needed to achieve this initial goal. Rather than needing desk-side visits to run diagnostics or check patching levels, the process can be triggered and overseen from a single console and a single window view, with the status of an entire desktop estate distilled into a single report, detailing exactly where to send expensive manpower in order to rectify any threats or issues. IT analyst firm Gartner[1] estimates the average asset cost of a desk-side IT support visit to be between $35 and $250 per visit, with a phone call to a helpdesk representative costing between $10 and $37 per call. Therefore, it is essential from both budget-control and workload perspectives to minimize the number of IT interactions of both types, particularly in business environments where there is little on-site IT technical support expertise, such as branch offices, retail stores and smaller businesses that don't have a dedicated IT resource.

An automated process, working in conjunction with a regularly updated and accurate database of known issues and fixes will provide the IT department with a clear and concise report of where the problems are, what they are and details of known fixes, thus allowing the IT department to address those vulnerabilities as necessary. Automated scanning performs an assessment of the target PC or multiple PCs, checking tens of thousands of elements of the operating system, applications and even virtual environments in search of known unpatched vulnerabilities and other exploitable weaknesses. Such solutions use a variety of in-house and external vulnerability databases such as vulnerability check databases including OVAL[2] and the SANS Top 20[3], which collect data from test appliances and live software running within thousands of targeted organizations in order to build a clear picture of the type of threats being discovered and exploited so that others can take action before they fall foul of the same threat.

The cost of an exploited vulnerability

An important consideration when evaluating the cost of purchasing and deploying a security solution is the potential cost to the business of suffering the security or operational failure you are trying to prevent. Exploited security vulnerabilities can manifest themselves in many ways, from creating instability in an operating system install to allowing an off-site user access to data stored on the target PC, or indeed the wider network that PC is connected to.

An exploited vulnerability can result in substantial lost productivity as a result of PCs and back-end systems being down while damage is repaired and problems are patched, in turn costing organizations money in lost business and delays. However, a bigger concern is when PC and server vulnerabilities are exploited in order to allow external parties to copy, steal or otherwise corrupt sensitive business data, such as customer contact details and credit card numbers.

Recent data from the Ponemon Institute[4] reveal that the financial cost to organizations of data thefts and losses, caused by both internal and external unauthorized access to data, has reached $214 per compromised record, while the overall cost of a public data breach event has hit an average of $7.2 million, taking into account the value of the data compromised, the loss of reputation and the costs associated with settling claims from affected users.

There is little doubt that the general public are concerned about how organizations, be they public or private sector, look after the information they hold about them. Companies that are seen to be failing in this area soon lose public trust, and with it lose revenue from lost ongoing trade.

Policy and culture

Vulnerability scanning can play an important role in helping to define and implement IT policy with regard to security, patching and installation of unapproved applications, particularly in environments where it is not appropriate or practical to lock down client PCs.

Regular scanning will help you identify trends and patterns with regard to the types of vulnerabilities that most affect the software solutions in use within the organization, allowing you to customize user IT policy to compensate for the most prevalent risks and further minimize the risk they pose prior to being identified and patched. This can include prohibiting the use of problematic Web browsers, insecure network connections, and shared login credentials, as well as the installation of software that is not part of the approved IT build and more.

With regard to policy, it is also wise to implement a schedule for regular vulnerability scans to make sure nothing has been missed. This should be paired with regular patching updates, either pushed from a central location, or by encouraging end users to periodically run Windows Update to ensure that all important and critical Microsoft security patches and stable drivers are installed on their client machines.

Quarterly or semi-annual vulnerability scanning can go a long way to helping you make sure you catch any weaknesses in your network before they are exploited by internal or external threat sources such as malware, hacking and denial of service attacks.

Solutions for vulnerability management

Automation of the most time-consuming tasks is without doubt key to an effective vulnerability scanning solution, but this must be paired with a range of equally important features in order to provide effective vulnerability management in the workplace.

An area for consideration with a vulnerability scanner, as with many external applications that probe and gather information about remote devices, is how it goes about gathering that information and what impact it will have on performance and operation of the device being scanned. Some products in the market undertake deep, invasive scans that, while functional, will hamper the end user in their day-to-day activities while a scan is being run, as both performance and stability will be compromised. Some solutions offer background scanning that does not compromise the use of the machine during the scan. However, in many cases, such scans are unable to access files and services that are in use, providing an incomplete risk analysis of the device.

Therefore, it is essential to balance the need for an unobtrusive background scan with the ability to gain an accurate view of the unaddressed risks affecting the machines being scanned.

As with other security solutions such as antivirus software, regular scanning and regular updates of vulnerability databases are essential. Look for solutions that make use of multiple databases, and which regularly seek out updates to those repositories. Also look for solutions that allow you to schedule regular scans and build an ongoing asset inventory, ensuring that nothing gets missed and allowing the IT department to see what devices – permitted or otherwise – are connected to the network at the time of a scan.

Finally, reporting tools are paramount in helping the IT department gain a clear picture of which devices are at risk and what those risks are. Security issues should be rated based on the severity of risk, allowing you to prioritize the most prevalent vulnerabilities for action. Reports should also illustrate when the devices on the network are free of unpatched vulnerabilities, helping the organization to demonstrate that all reasonable steps have been taken to ensure that data and devices are safe and secure.

Summary

Vulnerability scanning, and with it the broader process of vulnerability management, is one important piece of a wider IT security solution. Solutions that provide effective vulnerability scanning and identify areas for action will not protect systems from adverse threats, be they from external sources such as hackers and malware, or even internal threats such as malicious or haphazard employees. But, deployed in conjunction with a fully featured suite of client and server resources including patch management, network monitoring, antivirus, anti-spam, anti-spyware and firewall technologies, vulnerability scanning and management will provide IT departments and personnel with much-needed insight into the weaknesses within the corporate network, as well as an invaluable 'early warning' system for many threats, helping organizations to combat threats before they become a costly or disruptive problem.

About GFI LanGuard®

GFI LanGuard is an award-winning network security and vulnerability scanner used by tens of thousands of customers. GFI LanGuard provides a complete network security overview with minimal administrative effort, while also providing remedial action through its patch management features. Easy to set up and use, GFI LanGuard acts as a virtual security consultant to give you a complete picture of your network set-up, provide risk analysis and help you to maintain a secure and compliant network state faster and more effectively. GFI LanGuard assists you in patch management, vulnerability assessment, network and software auditing, asset inventory, change management, risk analysis and compliance.

About GFI®

GFI Software provides web and mail security, archiving, backup and fax, networking and security software and hosted IT solutions for small to medium-sized businesses (SMBs) via an extensive global partner community. GFI products are available either as on-premise solutions, in the cloud or as a hybrid of both delivery models. With award-winning technology, a competitive pricing strategy, and a strong focus on the unique requirements of SMBs, GFI satisfies the IT needs of organizations on a global scale. The company has offices in the United States (North Carolina, California and Florida), UK (London and Dundee), Austria, Australia, Malta, Hong Kong, Philippines and Romania, which together support hundreds of thousands of installations worldwide. GFI is a channel-focused company with thousands of partners throughout the world and is also a Microsoft Gold Certified Partner.

More information about GFI can be found at http://www.gfi.com.

1. http://www.lhric.org/files/414/Dependence%20on%20Desk-Side%20Support1.pdf
2. http://www.security-database.com/oval.php
3. http://www.sans.org/top-cyber-security-risks/
4. http://www.ponemon.org/blog/post/cost-of-a-data-breach-climbs-higher

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, 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.