GFI White Paper

Vulnerability management: Key questions you should be asking

Is vulnerability management critical for a business? Aren't traditional security tools sufficient to protect and secure the network? Yes, to the first question and a resounding no, to the second! Every system can be made more secure and vulnerability management solutions will not only show where to secure, but how to do it and deliver the patches and updates to achieve it. This whitepaper explains why.

GFI®

Contents

Introduction

Vulnerabilities in IT systems present a continuing challenge for any IT department or IT manager, with an ongoing need to address vulnerabilities as they are discovered in applications, operating systems and firmware, as well as in the configurations of key hardware such as printers, switches and routers.

While it can be argued that some of the common known vulnerabilities that are discovered in software and systems are a result of errors introduced at the application programming stage, many more come about more innocently, as a result of poor or inadvertent configuration of systems, legitimate changes made to enable functionality or to address an issue elsewhere in the IT ecosystem. Or vulnerabilities can even manifest when a unique set of circumstances or software combinations come together in one environment, creating incompatibilities and clashes that create an exploitable vulnerability.

Often, vulnerabilities are caught early on in their lifecycle and addressed through the established process of applying patches and service packs from the software vendor. Others are not addressed straight away, or affect such a small number of users that it is neither practical nor financially viable to make changes to the affected application. In this instance, the issue needs to be identified and managed locally, using security and network management tools to ensure that perimeter defenses are robust enough to protect systems and users within.

With the variety of vulnerabilities that exist, or that can manifest themselves within an IT environment, vulnerability management has become a critical part of the IT department toolset to aid in identifying, classifying, remediating and mitigating vulnerabilities, both known and unknown.

Vulnerability management is one of the fastest growing segments within the IT security sector, with analysts predicting 11.3 percent compound annual investment growth in the technology annually through to 2015, with market revenues of $5.7 billion , driven by growing concern over compliance and a legal and regulatory need to address security breaches and data loss incidents in the workplace.

Using vulnerability management tools, IT professionals can build a clear map of the vulnerability state of the organization's IT estate, using this not only as a guide to target and address areas of risk, but also to develop IT policy to mitigate the fallout of the threats and to prevent accidental creation of vulnerabilities in the future.

In order to achieve this, IT professionals need to know what questions to ask not only about the IT environment they are managing, but also about the applications and solutions being used or considered for vulnerability management scrutiny, resolution and mitigation.

What is vulnerability management?

Vulnerability management is a component of network and security management solutions that can provide organizations with the ability to assess and secure multi-platform and multi-device environments. Vulnerability management tools allow you to examine the network and the devices attached to it, query configurations of key devices such as network switches and routers, and collect data on the current level of patching applied to endpoints such as desktops, laptops and servers that connect to the network and interact with network resources. Dedicated vulnerability management solutions check against regularly updated databases of upwards of 50,000 known vulnerabilities in the course of a scan, minimizing the amount of manual identification from report data required.

Vulnerability management is key to attaining risk management goals as it provides policy and compliance context, and mines the network for vulnerability information, remediation opportunities, and ultimately, a comprehensive view of enterprise risk .

The identification process can be divided into two groups, internal and external vulnerabilities.

Identification of and protection from internal vulnerabilities:

- Machines that do not have the latest application and operating system patches and service packs installed
- Users that have been assigned inappropriate permissions and access rights
- Users who have no passwords or easily guessed passwords
- "Ghost Accounts" – User accounts that have not been disabled once an employee has left the organization
- Employees who are contravening corporate policies on data handling and data retention

Identification and protection from external vulnerabilities:

- Unknown/unsecured IP devices connected to the network that are either outside of a permitted IT device policy, or that form part of a "bring your own device" (BYOD) approach to consumer devices in the workplace
- Open ports on routers and in firewall configurations that do not have a specific and necessary purpose
- Easily guessed passwords from outside the organization

Understanding the core group of vulnerabilities and how they can manifest within an SMB computing environment will enable an IT professional to examine and understand vulnerability reports and make decisions on how to address discovered vulnerabilities and other areas for concern.

Key questions to ask

When approaching vulnerability management, IT professionals should put together a checklist of key questions in order to understand their IT estate and tackle subsequent security issues and failings as they are identified, as well as put pre-emptive procedures in place to head off future challenges brought about by the introduction of new technology and inadvertent misconfiguration of key network security resources.

What is the organization's legal responsibility for its data, systems and users?

- Understanding liability from the outset is important, so that any subsequent vulnerability management investment can be made ensuring that it satisfies legal and regulatory requirements. In the US, Section three of the Gramm-Leach Bliley Act, also known as the Financial Services Modernization Act of 1999, contains some useful and clear guidance as to the legal obligations that US financial organizations have with regard to information security. The guidance is also a clear framework for most organizations in the US and overseas, regardless of market segment. The Act states that organizations have a legal responsibility to:
  - Develop and implement an information security program
  - Identify reasonably foreseeable internal and external threats that could result in unauthorized disclosure, misuse, alteration or destruction of customer information or customer information systems
  - Assess the likelihood and potential damage to these threats, taking into consideration the sensitivity of customer information systems
  - Assess the sufficiency of policies, procedures, customer information systems, and other arrangements in place to control risks

What degree of known attacks is the organization currently vulnerable to?

- Using a network monitoring and management tool designed for vulnerability management, you can quickly build up a picture of how exposed the IT estate is to known internal and external threats. Before commencing rectification or taking steps to mediate the threat, it is important to know the extent of the problem. Not only will this help you in apportioning appropriate time and manpower resources to the task, but also in building a policy to limit recurrences and an action plan for dealing with future security challenges.

What percentage of applications, users and devices has been reviewed for security issues?

» With the growing popularity of BYOD strategies within the workplace – whereby consumers bring their own devices such as laptops, smartphones, tablets and storage devices into the workplace with the expectation of connectivity and shared usage – knowing what has been checked and when is essential. Regular scans, and documented "State of the Union" snapshot reports provide important intelligence into exposure and the changing shape of the IT estate, showing how BYOD is expanding the device range and increasing the risk of or indeed introducing new threats into the IT estate, as well as identifying high-risk users, unchecked users and groups, and workgroups where risk is most prevalent.

What percentage of downtime is the result of security problems?

» When the organization has fallen foul of an exploited vulnerability, it has an added effect on the rest of the business in terms of lost productivity and cost of IT time. In order to quantify the impact of vulnerabilities, particularly for the purposes of mitigation and justification of investment in countermeasures, it is important to document and understand in cash terms the entire effect of an unchecked vulnerability if it is exploited.

What percentage of network devices is managed by IT?

» In light of the growing consumerization of IT hardware, software and services in the workplace, IT departments need to be mindful and aware of exactly which devices are under its direct control and maintenance obligation, and which devices form part of a BYOD approach within an organization. Devices bought and introduced into the working environment by end users need to be managed and, if necessary, isolated from the core network, but do not necessarily fall under the legal control of the IT department when it comes to enforcing policy and pushing software to said devices.

With answers to these key questions in place, organizations can then evaluate and deploy solutions effectively in order to maximize visibility of vulnerabilities, address them as soon as possible and put measures in place to mitigate the impact of an exploited vulnerability if steps can't be taken to eliminate it.

Summary

It is important to remember that security is not just a nice-to-have option, and not even a necessary evil in today's economic, competitive and Internet-centric society. For organizations of any size, security is an essential component of an overall approach to IT that not only protects the organization as a whole, but also users within it and the customers and suppliers that interact with it. Added to that is the legal and regulatory requirement to demonstrate all reasonable care with regard to data protection. Although data theft and loss can never be 100 percent avoided, when it does happen organizations need to show that they have taken all reasonable steps to minimize the chances. Vulnerability management is a substantial part of that process.

Many organizations understand that their systems, storage, network connectivity and endpoints need to be inherently secure, mandating the need for regular monitoring and maintenance. IT managers and front-line staff need to ask important questions of their equipment, software and users to ensure that these tasks are being performed effectively and efficiently.

Challenging how security, patch management and configuration is managed and performed is critical to building a longer term policy-based approach to vulnerability management. Keeping applications patched and getting those patches in place quickly is paramount, but also important is taking a holistic view of how the IT environment works, to ensure that changes made at one stage in the environment don't create a vulnerability elsewhere, or as a by-product (for example, opening up a port to support one application, could expose another to critical vulnerability).

Perhaps the most important question that can be asked by any IT manager or support operative is – can this system, service or application be any more secure than it already is? Invariably, the answer is yes, and vulnerability management solutions will not only show where to secure, but how to do it and deliver the patches and updates to achieve it.

About GFI LanGuard®

GFI LanGuard acts as a virtual security consultant offering: Patch management, vulnerability assessment and network auditing. GFI LanGuard is unique in providing all three, reducing total cost of ownership of these essential security tools. It also assists in asset inventory, change management, risk analysis and proving compliance. Easy to set up and use, GFI LanGuard gives a complete picture of the network setup and helps to maintain a secure and compliant network state. It does this faster and more effectively through its automated patch management features and with minimal administrative effort.

About GFI®

GFI Software provides web and mail security, archiving and fax, networking and security software and hosted IT solutions for small to medium-sized businesses (SMB) 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, UK, 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 ISV Partner.

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

1. *Critical Capabilities for Security Information and Event Management, Gartner, 21 May 2012*
2. *Worldwide Security and Vulnerability Management Forecast 2011-2015, IDC, November 2011*
3. *Key Elements of a Threat and vulnerability management Program, ISACA*

GFI 3748 aug12

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