First
Security
Technology

IT Vulnerability Management

Pascal Mittner
CEO & Chairman of the Board

White Paper

IT Vulnerability Management

Foreword by Pascal Lamia

Dear readers,
Do you still trust your IT infrastructure? Are you sure that your infrastructure and network, does not look like a cheese full of holes? Actually, you would think that a functioning Vulnerability Management is a basic element of any IT operation and services provider. Experience shows, however, that in recent years that has not been the case. Infrastructure devices and services that communicate mostly via a network are being installed and then usually no longer maintained. Depending on the size of the company and time, it is difficult to have a current inventory of all components and their current software versions.

There are most likely vulnerabilities in the IT Infrastructure that can be taken advantage of by attacks. Most such attacks are noticed far too late and the damage, whether an information theft or reputation damage, is enormous. Here, usefully employed IT Vulnerability Management is an effective solution. It can identify the vulnerabilities and prioritise troubleshooting and knows your IT infrastructure and its components. In addition, you are always able to carry out a new assessment with regard to the vulnerability of your IT infrastructure.

This alone is surely not enough to deter possible attackers breaking into your systems. However, the entry barrier is raised so high that potential attackers will probably refrain from intruding or tampering with your systems.

You thus perceive your responsibilities are to ensure an optimal protection for your IT infrastructure. Thus, you protect not only it, but also your customers.

Pascal Lamia, Head of the Reporting and Analysis Centre for Information Assurance MELANI

The detection and fixing of vulnerabilities within an IT infrastructure are key elements in protecting the business processes. However, there are very different approaches to achieving this goal.
Hardly anyone will disagree that the detection and fixing of vulnerabilities within an IT infrastructure represent a crucial component in the protection of business processes. However, there are very different approaches to achieving this goal. Some companies opt for a pure “output only” approach, whereby some engineers rely on strong controls and manual reviews of existing systems. Others prefer a more responsive approach by fixing known vulnerabilities using disclosed patches.

Intuitively you will probably want to make both. You could probably be in the right position but you are missing the most critical operational element. You need a way of identifying and fixing the vulnerabilities quickly and globally. The required technology is already available cross-company. This article shows the basic functionality of the technology, how it can be executed and what important operational issues need to be worked on.

Before we start with the details, we should explain some relevant concepts:

- **Scanner** a device for the automatic discovery of IT infrastructure and its vulnerabilities
- **Target** the IT hardware to identify and verify the existence of vulnerabilities
- **Vulnerability** a configuration parameter or a software version that could weaken the security of the company

Model of Vulnerability Management

Actually, one would expect that the issue of Vulnerability Management (IT Vulnerability Management or abbreviated to “Vuln. Mgt.”) in the framework of ITIL (IT infrastructure library) would be dealt with. But that is not the case. The removal of vulnerabilities is rather a function of safety instead of a service management, because they have a big impact on IT services.

Nevertheless, it is rather likely that the area of Vulnerability Management will be included as part of Service-Management: The basic components of Vulnerability Management are:

Testimonials

Andreas Kölliker, IT Security Officer
Axpo Informatik

“As an IT service provider of the Swiss energy economy we carry out Web server platform services for our customers. Hosted pages and Web services have a higher expectation for integrity and availability. VulnWatcher is an intuitive tool, with which we can use to check the security of the platforms, rapidly initiate measures, and control to ensure continuity. Vulnerability Management is an essential activity of every safety officer – VulnWatcher helps Axpo Informatik with the efficient completion of this task.”

1. Inventory: identification of infrastructure equipment and services – mostly over a network
2. Network identification and prioritisation of vulnerabilities and risks of identified bodies
3. Resolving vulnerabilities
4. Reassessment of the security plan of the company and the underlying causes of threat patterns

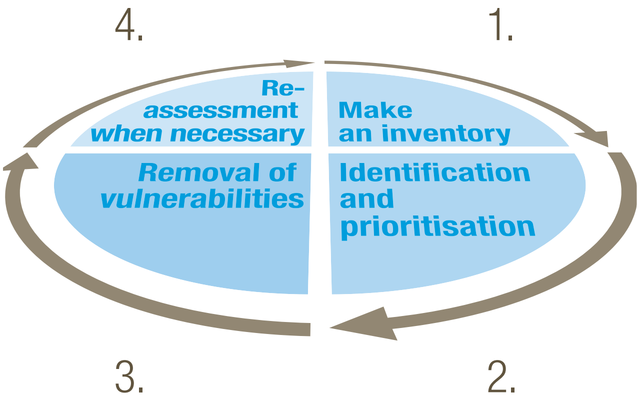

4.
1.
Re-assessment when necessary
Make an inventory
Removal of vulnerabilities
Identification and prioritisation
3.
2.

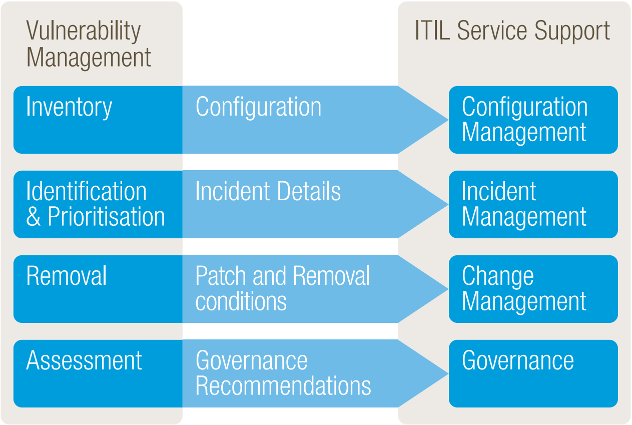
FIG. 1 VULNERABILITY MANAGEMENT PROCESS

This process is a cycle: the progressive activities of each step provide the foundations for the next step. The last step, the new assessment, is a critical foundation for the improvement of the organization and Vulnerability Management processes. For example, it can happen that the removal of a particular vulnerability requires extensive modifications of the organizational process for the processing of incidents.

It is entirely possible that a subsequent assessment of the troubleshooting step reveals that some types of vulnerabilities must be fixed faster on the basis that they are a fundamental attribute of the business-technology architecture. An alteration in this architecture can potentially be impossible as it is part of the underlying business model.

> **Dr. Stephan Amann,** Managing Director
> fence IT AG
> fence IT AG operates sophisticated ICT systems with enhanced security requirements. Located exclusively in Switzerland with extra data centres, Fence IT AG provides a safe environment for the applications and data of its customers. Fence IT AG is ISO 27001 certified. VulnWatcher is one of the tesserae that has helped to get the ISO 27001:2005 certification.

This closed loop process is important for the maintenance of effective Vulnerability Management, as it represents more than just patching.



Vulnerability Management		ITIL Service Support
Inventory	Configuration	Configuration Management
Identification & Prioritisation	Incident Details	Incident Management
Removal	Patch and Removal conditions	Change Management
Assessment	Governance Recommendations	Governance

FIG. 2 VULNERABILITY MANAGEMENT AND ITIL

Process

The four above mentioned stages of the Vulnerability Management process can require the participation of several working groups and extensive coordination depending on the size and complexity of your company. Let us first talk about the interaction with the IT service support functions. Figure 2 shows the integration of the ITIL Service support functions with Vulnerability Management.

Inventory

The first task is to record all the devices of the IT environment which are connected and in operation. Here, we assume that all of these devices are connected to an extensive IP network. Each device is automatically detected and recorded on an inventory. In some cases, you might want to compare this with your infrastructure database or a configuration management database.

The depth of this investigation depends on the capability of the product and the platform type. It may be that you find only one computer type and name, IP address, operating system and main software installed. On the other hand, it could be that you get a complete list of detected applications and operating services.

Identification and prioritisation

Its main task is to scan vulnerabilities. A vulnerability database is used to perform a scan while information about software versions is collected, configurations analysed and services identified. The known vulnerabilities are identified and usually delivered in a structured report.

Several products use one of the following methods to convey the degree of risk of the vulnerability. Often, the products take into account the criticality and importance of the infrastructure as factors in the risk assessment. A few go a step further in trying to look at the vulnerability in the context of your business: i.e. they look at the location of the device in your network and the accessibility by different attack vectors.

All the information should enable you to make a very important decision: which vulnerabilities should be eliminated first.

Fix

The critical stage is when the security organization and Service Support Department strongly interact. Typically, the process is managed via a ticketing system that is accessible to the Service Support Department. As soon as the scanner has detected a vulnerability according to your criteria, a ticket for the responsible person of the target system can be issued automatically. Alternatively, the Security Manager can review the list of vulnerabilities and manually create the ticket. After the administrator has completed the removal, he will usually close the ticket. Then, verification is carried out either manually or automatically. If the troubleshooting was successful, the ticket remains closed, otherwise it is opened again.

Reappraisal

Now, the Security Manager checks all the business reports and its different functional areas. These reports can show the trend, how effectively the vulnerabilities are fixed and what the overall security plan looks like.

This step is a unique opportunity to identify operational problems and system configuration errors. For example, if the same vulnerability in every activated new production system is in place, it could indicate a problem with the installed server base image. Or maybe the patches have not been installed before setup.

Other detectable problems have to do with management changes. The configuration parameters are sometimes adapted after a system alteration so that the alteration can work. This could reveal a fundamental defect in the implementation process of a particular application. The Security Manager should develop, together with the responsible entities, a plan for how to customize the application and which steps needs to be taken in order to improve safety. A final advantage of the reassessment is the application of the security plan of other security systems.

The security event tools and programs of correlation (correlation engines) can use this information to better analyse the actual risk of an attack. If a worm attack is detected that exploits software vulnerabilities, the number and types of affected systems can be defined more clearly since they are without patches. Afterwards, the responsible person can choose the right level of response.

A final minor function of a vulnerability scanner concerns compliance monitoring. As a scanner checks all installed software, unauthorized applications are identified. The person responsible for compliance monitoring may use this information to bring these systems separately to conformity.

Technical issues

Some technical issues must be resolved during the implementation of Vulnerability Management. As the scanner uses a network, most of the host issues that relate to the network still have some problems that must be addressed.

Hosts

A host will be scanned in two ways for vulnerabilities: Network Fingerprinting and authenticated scanning. The first involves the detection of vulnerabilities through identifying vulnerable services that provide specific information about the software version. For example, sometimes several general passwords and strings of the SNMP area must be tried. This is usually a harmless activity, but in rare cases it can lead to host problems:

- If many TCP connections on the host are opened on one side, this can overload the connection table
- Access will be blocked after a critical number of failed password attempts
- An exploit code will be used with «more aggressive» scanning; this can lead to the systems or services crashing

Such problems can easily be resolved by application of best practices. For example, some “service accounts” will not be locked after failed login attempts. Normally only highly stressed web servers have the problem that the connection table is overloaded.

«Aggressive» scanning should generally be avoided in a production environment. However, it is useful to check the reliability of a new server or desktop images.

The host is usually not unduly affected when performing authenticated scanning. The registry database on Windows computers is scanned in read-only mode, whereas the setting of the credentials setup should be restricted appropriately.

Some suppliers offer an agent-based approach as an alternative to existing authentication and remote

Testimonials

Igor Djurdjevic, Security Officer
BHF Bank AG

“As a private bank we make the highest demands on the security and confidentiality of our customers’ data. We opted for VulnWatcher from First Security, as only a permanent safety monitoring of our Internet connection gives us the certainty to be adequately protected against attacks from the Internet.”

access mechanisms on a host. This requires the installation of an agent on the target platforms. A well-known service that could possibly represent an attack vector must not be active on the target platform. On the other hand this introduces an additional software component which may lead to operating and compatibility problems. Another problem with the agent approach is that agents are not available for each platform and unknown hosts according to traditional methods must still be determined through Port Scanning or Ping Sweeping.

Network

As a scan is carried out over a network it can influence every device between the scanner and the target or is itself influenced. The installed location should be considered before using the scanner. Overall, a scanner creates inconsequential network traffic. As long as the network doesn't include thousands of hosts and only 256 Kbps-connection exists, the effect is quite low. Nevertheless, the Network Engineer and Security Manager should work together matching and limiting the bandwidth properties for determining the configuration of the scanner.

In addition, the scanning should not exclude network devices administrative addresses. In these networks, there are also hosts that are vulnerable to attacks like any other device.

Firewall This is the most likely mechanism that can influence scanning. A scanner can be simultaneously included in multiple network segments but this again raises the question whether this is not against segmentation philosophy. Otherwise, a single scanner must be included on each network segment. There are also companies that have a management network segment available which can limitlessly access the other network segments. In such a case, the scanner can reside in the management network segment and have unrestricted access to other network segments. Following are some specific problems with firewalls:

- Blocking port scanning for detection services
- Proxy connections to the target, providing inaccurate scanning results
- QoS properties that cause more than the actually active hosts to be identified; this happens mostly with H. 323-protocols

VPN A VPN (virtual private network) allows the transmission from one network to another by tunnelling. In some cases tunnelling with VPN from one firewall to another is used, i.e. to reduce some of the above mentioned problems. A disadvantage is that a VPN can slow down the scan, depending on the performance and the overhead of the VPN gateway. This should be carefully assessed before the scan.

Router These devices should cope easily with the relatively inconsequential scanner traffic, as long as they are not subject to high volume. Sometimes an ACL (access control list) will interfere with the scanning and thereby distort the results.

IDS/IPS The intrusion detection alarm e.g. attack defence system (IDS = intrusion detection system or IPS = intrusion prevention system) of a network will be raised with security, if it is not set to ignore the scanner traffic. It is advisable to configure the behaviour of the IP address and its targets as normal (whitelisting). A best practice is to configure the alarm so that it is only raised when scanned with the wrong scanner outside the normal IP range. This could imply an unauthorized use of the scanner by the user or by spoofing (concealment) of the scanner during an attack.

Switch A 2- or 3-layer switch is normally not influenced by a scanner, except when the administration address is also scanned. In this case, you should take the same precautions that correspond to the scanning of a host. The access/admission control components of the network such as 802.1 x should be configured so that the switch port to which the scanner is connected, is not included. The NAC software and hardware (Network Access Control) can be integrated with the progressive implementation of vulnerability scanners.

Directory services

Access codes instead of an agent are used to maximize the use of the scanner; this makes it possible for the scanner to identify vulnerabilities that would otherwise be not identifiable at the network interface. Usually, the scanner needs a service account that allows only a limited read-only access to the registry database, files, and directories of the target host. As the passwords of these accounts are rarely changed, they should be very safe (more than 12 characters with a mix of uppercase, lowercase and special characters). Any change should be discussed to prevent the failure of scanner services. If multiple business units have access to their own service accounts, the passwords of service

“

Patrik Thoma, Information Security Officer
National Administration Liechtenstein

The Liechtenstein National Administration is perceived by the public and the economy as a competent, reliable and safety-conscious administrative branch of the government. This means that we will use commercially reasonable means to live up to these expectations.
In this regard, VulnWatcher has become an indispensable tool for our efforts to effectively check attacks from the Internet at any time. ”

accounts should be kept strictly secret and managed carefully so that the Manager of a unit cannot influence the access codes of other units.

Application tips

The mantra for the successful establishment of Vulnerability Management measures is: Plan! Plan! Plan! Please consider the following points before you immerse yourself in this important area of security:

- Consider how the troubleshooting process will interact with other groups. Alternatively, you can work through the approach of limited application discovery steps. This gives you the ability to identify process problems before a large-scale operation completely overwhelms you.
- Ensure that the operating personnel has enough time to provide the requirements prior to product evaluation.
- Inform those who are responsible for problem solving and bring them on board early.
- Make sure that the existing security policies create the conditions for the implementation of the solution. It may be necessary to adapt the policies or create new and eliminate critical vulnerabilities in a timely manner.
- Consider the compatibility with the existing system for processing tickets. Much of the use of a Vulnerability Management solution might be generated by repair work carried out on the existing system. If this system is not available, find out whether you can use the Vulnerability Management products' built-in ticketing system.
- An integration with the Patch Management system is very interesting, but it offers less value than you would perhaps expect. Most of the patch-management tools have limited abilities to maintain thousands of products with patching. Often, these tools have a built-in check of the supported patches.
- To maximize the first use, you should identify the critical infrastructure so that it is scanned from the start: directory server, Internet Site Server, and other critical hosts are excellent Initial objectives.
- Check your policy for the management of the IT infrastructure, which has perhaps been forgotten and make sure that you can assign a value and a criticality to each part of the infrastructure. A great advantage of the Vulnerability Management tools is that these tools have the value in reporting what the level of risks of the vulnerabilities can be.
- Consider whether and how you will integrate a SIEM Tool (Security Information and Event Management). Then before the implementation of the interface, check how it works. The Vulnerability Management process output can significantly influence the effect of SIEM.
- Sit together with all persons and groups of the Vulnerability Management project to define the process. The result should be a cross-functional flowchart, accepted by all. Dependent on the maturity of the IT operation, you can also take into account the creation of SLAs (Service Level Agreements).

Why invest in Vulnerability Management

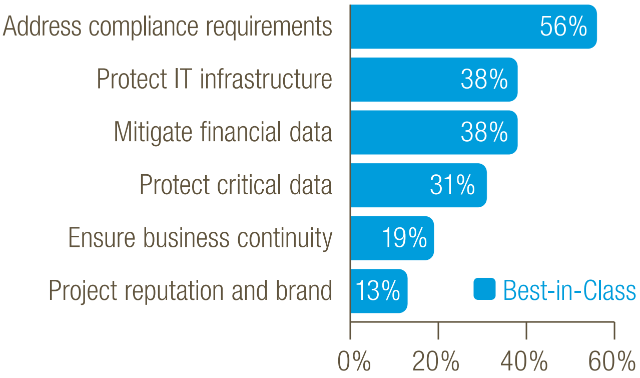


FIG. 3 PRESSURE TO INVEST IN VULNERABILITY MANAGEMENT

Patch Management is not Vulnerability Management

Vulnerability Management and Patch Management lie nearly together, but must not be confused with each other. Vulnerability Management is the process upstream of Patch Management, as it is a proactive system to detect vulnerabilities. A good Vulnerability Management system detects not only weaknesses, for which there is a patch, but the vulnerabilities are included immediately after their emergence in the database. Not only are the vulnerabilities of applications, operating systems and protocols recognized, but also configurations, which can lead to a security problem.

Patch Management checks to what extent there are patches for the operating system and installed applications. From becoming aware of a vulnerability to the availability of a patch can often take months. During this time, the Patch Management shows no need for action although there is a security risk. Patch Management builds on the Vulnerability Management and helps with the distribution of patches within the IT infrastructure. The following table shows a comparison between Vulnerability and Patch Management

⇣	VULNERABILITY MANAGEMENT	PATCH MANAGEMENT
IDENTIFY KNOWN WEAKNESSES	IMMEDIATELY (IN A FEW DAYS)	ONLY AFTER THE ISSUE OF PATCHES USUALLY FROM THE MANUFACTURER (UP TO SEVERAL WEEKS OR MONTHS)
RECOGNIZE WEAKNESSES BY INCORRECT CONFIGURATION	YES	NO
BEST PRACTICE SECURITY SCAN	YES	NO
COMPLIANCE REPORTS	YES	NO
RISK EVALUATION OF IT INFRASTRUCTURE	IMMEDIATELY (IN A FEW DAYS)	ONLY AFTER THE ISSUE OF PATCHES USUALLY FROM THE MANUFACTURER (UP TO SEVERAL WEEKS OR MONTHS)
RECOGNIZE WEAKNESSES BY INCORRECT CONFIGURATION	YES	NO OR ONLY PARTLY
VALIDATED SYSTEMS	ANYTHING REACHABLE OVER AN IP-ADDRESS. PROTOCOLS, OPERATING SYSTEMS, APPLICATIONS, NETWORK COMPONENTS (SWITCH, ROUTER, FIREWALL), MULTIFUNCTIONAL PRINTER, NAS ETC.	CLIENT AND SERVER: USUALLY ONLY OPERATING SYSTEM AND STANDARD APPLICATIONS
SHOWS A SOFTWARE SECURITY PROBLEM	YES	NO

TABLE 1 COMPARING VULNERABILITY MANAGEMENT AND PATCH MANAGEMENT

Vulnerability Management doesn't replace Patch Management and vice versa. They are complementary and greatly improve the productivity and safety together.

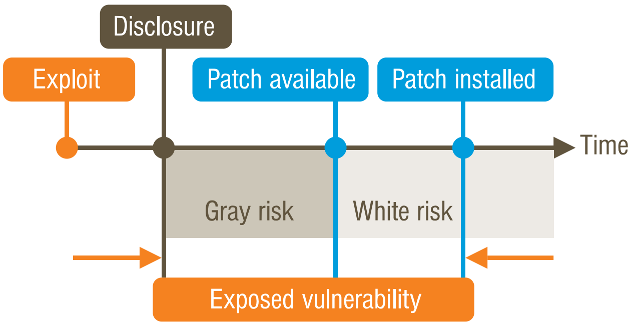


FIG. 4 SIMPLIFIED VULNERABILITIES CYCLE

Life cycle stages of a vulnerability. Different phases of a Vulnerability to show the status and risk.

«Exploit» is the availability of hacking tools, malware, data or commands.

«Disclosure» is the public description through a trusted, independent source including risk assessment.

«Patch available» is the earliest point at which a solution is offered by the manufacturer. Solutions and "Work-arounds" of third-party providers do not count as a patch.

«Patch» is the time at which the vulnerability by means of patch applied on the system and the vulnerability that is fixed.

First Security
Technology AG
Bahnhofstrasse 7
CH-7000 Chur

www.first-security.com

About First Security Technology (FST)
Swiss Made Vulnerability Management!
FST was founded in 2001 with the headquarters in Chur and is the leading manufacturer of vulnerability assessment and management solutions in Switzerland. FST provides security solutions such as Software-as-a-service, Virtual-machine-based or as an appliance and distributes them through a network of established dealers and distributors. FST‘s security solutions include fully automated vulnerability detection, IT Infrastructure assessment, removal of vulnerabilities and – monitoring thus fulfilling IT compliance reporting mechanisms.

For more information http://www.first-security.com