

# Vulnerability Management with the GSM

## Content

- [Vulnerability Assessment](#)
- [Vulnerability Management](#)
- [Where to start and how big is the risk?](#)
- [Control of the Scan Engine](#)

## Introduction

Vulnerability management provides a substantial benefit in the organisation of IT security in general and in particular the hardening of IT systems to prevent internal and external attacks from succeeding.

Realisation of these benefits is dependent upon incorporation of vulnerability management into a security process. Detection of vulnerability must be followed either by the appropriate remedy (update, patch or reconfiguration) or by a reaction through other security mechanisms (IDS, firewall rules). Vulnerability management allows system administration to detect and remedy vulnerabilities. It also provides IT management with a useful tool to manage risk and compliance, as well as monitor the quality of IT security.

## Vulnerability Assessment

Vulnerability assessment refers to the detection of vulnerabilities in IT systems. The causes of vulnerabilities are misconfiguration and programming mistakes ("software bugs"). Vulnerability assessment detects and documents such cases. The vulnerability can then be remedied by a patch or reconfiguration of the software. If reconfiguration is not possible, other measures can be taken to reduce the risk, such as creation of a firewall rule or a so-called "intrusion prevention" rule.

## Vulnerability Management

The information generated by the detection of vulnerabilities needs to be embedded into a management process. This process is referred to as "vulnerability management".

This process enables documenting the state of IT security and respective changes to the security status, as well as benchmarking security. Transferral vulnerability assessment results into this management process allows to use simple rating numbers or traffic lights to visualise known vulnerabilities, whether they have been addressed by IT administration, or whether new vulnerabilities have been discovered as part of the consecutive vulnerability assessment.

### Patching is not a substitute for Vulnerability Management

Regular application of security patches is not a substitute for vulnerability management.

This is due to a variety of factors, such as dependencies of the system that do not allow applying the current patch-level because a certain database or other business-critical application which might become unusable or lose its certification.

There are also issues caused by lack of available patches for some vulnerabilities, or vulnerabilities that have been created by misconfiguration despite software that has been kept up to date.

A classic example is an administrator password "12345678" or shared disks that are accidentally exposed to the internet.

### **Scanning for vulnerability is insufficient without follow-up action**

The security of an IT infrastructure is not increased by registering and documenting all vulnerabilities by means of vulnerability assessment. It is essential that vulnerabilities are handled by a designated person as part of an organisational process.

This needs to be accompanied by a management process that ensures adequate follow-up to the vulnerabilities, including technological or managerial consequences, if necessary. These countermeasures must be documented as part of the process to assess their technical effectiveness. This can be addressed by a repeated vulnerability assessment scan or a detailed test with another software tool.

A vulnerable service that is not necessary for core business processes can be disabled temporarily or permanently, or be hardened by means of a firewall or IPS rule set. In case other alternatives are unavailable, a vulnerable service can also be secured by documentation with control and monitoring. An example would be a logging rule in the firewall providing documented evidence of authorized and unauthorized access to a potentially vulnerable system, allowing to disprove allegations of attempted attacks.

### **The misunderstanding of vulnerability management as a purely technical issue**

Successful vulnerability management is always based upon organisational processes which translate the technical findings by vulnerability assessment into a working process to remedy the vulnerability. In order to achieve this, system administration must be supplied with the appropriate tools to map this security process according to the respective risk.

It is likewise necessary to provide the technical IT department with the means to close or at least defuse the vulnerabilities. Security guidelines that help prevent misconfiguration likewise need to be mapped through an organisational process.

### **Organisational framework of Vulnerability Management and Security Guidelines**

As part of the organisational process it is possible to implement testing for compliance with the various guidelines in Greenbone test scripts. The resulting automation of compliance testing substantially improves ease of work.

## **Where to start and how big is the risk?**

Practical experience suggests starting where the operational risk is the greatest.

This risk can be determined by an in-house risk management system. Less complex situations can be assessed by the following rule of thumb:

$$\text{Risk} = \text{Threat Probability} * \text{Possible Damage}$$

It is also possible to adapt this calculation to a known vulnerability "V":

$$\text{Risk(V)} = \text{Threat Probability(V)} * \text{Possible Damage(V)}$$

In this case the threat probability is a function of the threat scenario and severity of the vulnerability, resulting in

$$\text{Risk(V)} = \text{Threat Scenario(V)} * \text{Severity of Vulnerability(V)} * \text{Damage(V)}$$

The threat scenario for a web server in a DMZ which is therefore connected to the internet is certainly higher than that of a web server which is only reachable via telephone dial-in. Damage to a production machine will be much more costly than damage to an in-house server for image movies.

Even with substantially simplified categories for threat scenarios, severity of vulnerability and damage it is possible to obtain a reference number that will allow setting priority of which vulnerability to address first. Since the severity of vulnerability is automatically supplied for each vulnerability, management only needs to categorise threat scenario and damage according to a set of predefined categories.

### **New Tool, new risk**

Every new IT security tool also carries an inherent risk.

Because they are being used in sensitive and security relevant places, such software tools can negatively impact daily business operations. Vulnerabilities in security software can additionally turn it into a security risk.

Some vulnerability scanners require the administrator password for the domain, the digital equivalent of an all-access pass. How and for what operations this pass is used is typically unknown, including whether a back door in the software allows unauthorized third parties to access the software for maintenance or other, potentially malign purposes.

Centralist solutions are inefficient and bring additional risk

The so-called "Scan-Engine" is the core of a vulnerability scanners. Some providers are running this engine centrally in their own data processing centre. The scan appliance places at the customers location opens a so-called "Layer-2 Tunnel" between the customer's IT network, the target of the scanner, and the data processing centre of the scan provider.

All information about known vulnerabilities is then being made available over the internet by means of a web portal.

On the contractual level it is often difficult to impossible to obtain information about storage of your company's vulnerability information. In many cases it is stored on servers in central locations in the USA or India. Such a concentration of known vulnerabilities provides an extremely attractive target and a sought-after source of data for insider attacks.

From a risk-management perspective it is hardly acceptable to introduce tunnels into sensitive infrastructures and then store all known vulnerabilities outside a companies' guidelines and control. Such a solution does not allow a customer to directly influence archival and deletion of their data. At a time when company guidelines

to control the IT department have become topical, e.g. due to cases of used hard disks being offered on Ebay, either from insolvencies or simply as part of the usual hardware replacement cycle. Typically the data on those disks can be restored, if the deletion of data has been attempted, at all.

If, on the other hand, the scan engine is operated in its entirety from an appliance in the data centre of the company it requires additional effort for the maintenance of the scan engine. On the upside this solution provides higher security by reduction of incalculable risk factors and consequently reducing operative and business risk.

### **Proprietary solutions are black boxes**

A unique selling proposition of the Greenbone Security Manager is its proven and independently verifiable security. Because the entire scan engine and all test routines are available in source code as Open Source Software it can be audited by customers and third parties in their entirety.

Where proprietary solutions offer marketing promises and assurances, Greenbone Networks provides facts that can be assured by any third party that enjoys the confidence of the customer.

By opening the entire process, any customer is in the position to better assess the risk associated to deployment of the Greenbone Security Manager. The transparent scan engine provides proven security and the subscription to the daily update of test routines ensures discovery of most relevant vulnerabilities and insight into the technology used for testing.

## **Control of the Scan Engine**

The Greenbone Security Manager (GSM) core is provided by the scan engine and its control module. The scan engine control module administrates the database and allows usage of the GSM appliance through the various user interfaces.

The control and administration is flexible and can be adapted to the needs of the customer.

### **Remote control via Command Line Interface (CLI)**

The CLI client allows controlling specific scanning tasks through scripts or periodically (e.g. through a CRON daemon), providing the necessary flexibility for seamless remote-controlled integration into the company specific system. The security state and its change over time as well as the individual scan results can be retrieved via XML and translated into clear and attractive reports.

### **Expert-Client**

Greenbone Networks provides a Expert-Client addressing security experts. This graphical user interface allows very complex and fine-grained scan configurations.

This very extensive expert tool is primarily used by auditors and security specialists.

### **Web-interface Greenbone Security Assistant (GSA)**

In order to allow installation-free deployment over existing web browsers, a common requirement for many SMEs, the GSM can also be used via the Greenbone Security Assistant, which Greenbone Networks developed and made a regular component of the GSM.

The intuitive web interface allows the administration of users, scans and resulting reports, scan-configurations, target-configurations and access data.

Scan profiles can also be imported from the Expert-Client to the GSA, making special tests available also to less technically trained personnel or management directly.

The GSA provides a simplified overview of the security state and its trend on the web. Reports in PDF, HTML and XML of the reports can be automatically generated with just a few clicks.

*Status: 20091125*