The 7th International Scientific Conference
“DEFENSE RESOURCES MANAGEMENT
IN THE 21st CENTURY”
Braşov, November 15th 2012

CURRENT ISSUES
IN INFORMATION SYSTEM SECURITY MANAGEMENT

Săpunaru Doru

Romanian Air Force Headquarters

Abstract:

Determining the exact requirements for security for a given organization is essential for implementing the proper security measures. Such measures are designed to protect information systems from security breaches. The Internet and computer networking requires a new security measures and policies to reduce the threats and challenges inherent from these new technologies and software applications and network devices. The information security attacks of an organization’s assets have high dollar impact, loss of customer confidence, and negative business reputation. An organization must analyze its assets and the threats these assets face from either inside attacks or outside attacks.

Key words: security measures, countermeasures, malicious attacks.

1.Overview

Security Management involves protecting a network from all kinds of unauthorized access. This includes many sub functions like collecting and reporting security related information, proactively detecting and preventing intrusions, etc.

The Internet and computer networking means that there is a need for new security measures and policies to reduce the threats and challenges inherent from these new technologies and software applications and network devices. Information, network equipments, transmission media, computer systems, and servers are subject to threats. “Yet the use of information and communication technologies has increased the incidents of computer abuse.”

Security measures and countermeasures are implanted to protect organizations from different security attacks. To guarantee the security requirements of a given organization, it is essential to be able to evaluate the current security demands of an organization as well as the measures taken to achieve such requirements. Security weaknesses cause a negative impact on organizations such as financial loss, reputations, and loss of customer confidence.

The intention of implementing security measures, controls, and policies is to guard information security objectives and information assets. Information security objectives, which are confidentiality, integrity, and availability, are the main concern in categorizing information security level.

2. Information Systems Security Assessment

Today, the evaluation of Information Systems (IS) security in accordance with business requirements is a vital component of any organizations business strategy. While there are a few information security assessment standards, methodologies and frameworks that talk about what areas of security must be considered, they do not contain specifics on HOW and WHY existing security measures should be assessed, nor do they recommend controls to safeguard them.

The reason for which you have to run a vulnerability assessment is to check that all systems have been patched for vulnerability, or obtain a list of systems that require a patch. This is a great way to verify that your patch management software actually did its job and rolled out the patches.

Vulnerability assessments (VA) can be broken down into three steps: information gathering/discovery, enumeration, and detection.

2.1. Information Gathering/Discovery

Information gathering is used to determine the breath of the assessment by gathering IP addresses, available port information, and possible contact information of the target.

Information gathering and discovery is the process an individual or group performs to ascertain the breath/scope of an assessment. The purpose of this step is to identify and determine the total number of systems and applications that will be assessed. Output of this step typically consists of host names, Internet Protocol (IP) addresses, available port information, and possibly target contact information.

2.2. Enumeration

Enumeration validates the underlying operating system and running applications of the target.

Enumeration is the process used to determine the target operating system—a process called OS fingerprinting—and the applications that reside on it. Upon determining the operating system, the next step is to substantiate the applications that reside on the host.

2.3. Detection

Detection determines what vulnerabilities exist.

Detection is the method used to determine whether a system or application is susceptible to attack (i.e., vulnerable).This step doesn’t confirm that vulnerabilities exist; penetration tests do that. The detection process only reports the likelihood that vulnerabilities are present.

To detect vulnerabilities we’ll need to utilize a vulnerability assessment tool such as Tenable Network Security’s Nessus or eEye Digital Security’s Retina. Neither tool is free, so we’ll need to evaluate the cost or pursue open source alternatives prior to conducting this step.

Once we have procured a VA tool, we can continue the assessment, targeting the systems we’ve evaluated in steps 1 and 2 to determine whether they have any vulnerabilities.VA tools detect vulnerabilities by probing remote systems and comparing the systems’ response to a set of good (expected) and bad (vulnerable) responses. If the VA tool receives what it considers a bad response it assumes the host is vulnerable.

2.4. Detecting Vulnerabilities via Security Technologies

Traditionally when we want to ascertain system- or application-level vulnerabilities, we need to install vulnerability assessment scanners throughout our enterprise.

These scanners are responsible for detecting network hosts (information gathering), discovering available applications (enumeration), and ascertaining vulnerabilities (detection). Vulnerability assessments scanners are typically network appliances running VA software. Figures 1 represent a typical organization's VA infrastructure.

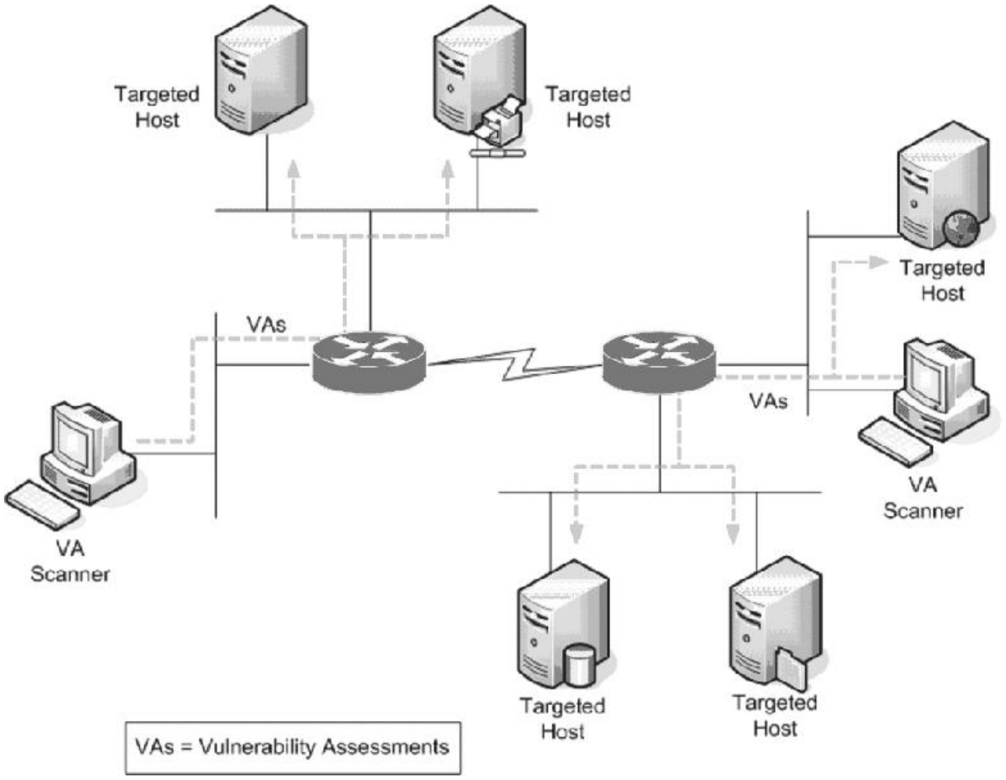

Fig.1 An enterprise VA deployment

3. Information Security Threat and Vulnerability

Vulnerability is the weakness of information and information systems which can lead to attacks, harm, modification, destruction, disclosure, interruption, and interception.

The relationship between information assets, threats, vulnerabilities and existing defenses is illustrated in Figure 2, which depicts an information asset that is only partially protected by the defenses of the media and systems handling it. Some threats will be defeated by these defenses, but other threats can take advantage of unprotected vulnerabilities and, in the worst case, compromise the information asset.

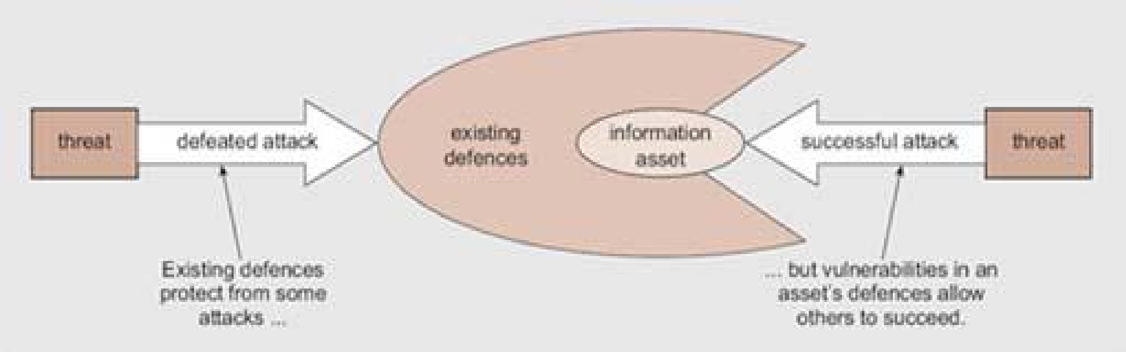
threat
defeated attack
existing defences
information asset
successful attack
threat
Existing defences protect from some attacks ...
... but vulnerabilities in an asset's defences allow others to succeed.

Fig.2 The relationship between information assets, threats, vulnerabilities and existing defenses

An effective vulnerability management framework will enable the organization to:

- establish an appropriate frequency for detecting vulnerabilities
- detect such vulnerabilities across the enterprise's public services and internal resources
- attribute an appropriate severity rating to the vulnerability
- link the detection capability to the enterprise change, configuration and release management processes
- appropriately address the issues according to their vulnerability
- confirm that remediation activities have lowered the exposure to, or removed in total, the initial vulnerability
- perform ongoing vulnerability management through a continuous improvement lifecycle

An effective threat management framework will enable the organization to:

- identify threats that may lead to a degradation in performance, or an attack, of an enterprise resource
- evaluate the risk that a threat presents and take appropriate action
- direct the appropriate information about threats to the affected parties so an informed decision can be made to the response
- ultimately have the capability to focus and utilize the security resources where most needed

With threat and vulnerability management systems running in harmony, the exposure of the network is greatly reduced thereby bringing security, reliability and availability to the enterprise network.

4. Current Information Security and Compliance Issues

4.1. Voice over IP (VoIP) / Voice over Broadband (VOB)

VoIP and VOB applications are becoming increasingly interesting to businesses everywhere, because of their combination of flexibility and cost-effectiveness. They also bring information security challenges.

A VoIP network is subject to all the same threats as wired network: " …viruses, spam, phishing, hacking attempts, intrusions, mismanaged identities, Denial of Service (DoS) attacks, lost and stolen data, voice injections, data sniffing, hijacked calls, toll fraud, eavesdropping, and on and on and on." (VOIP Security Alliance, 1 December 2006). While there is little formal guidance on effective VoIP security, it is clear that risks to these networks need to be analyzed and assessed, and appropriate (largely technology-based) controls implemented.

4.2. Phishing

Phishing attacks use ’spoofed’ e-mails and fraudulent websites that are designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, and so on. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers are able to convince up to 5% of recipients to respond to them. Phishers then use this data to commit fraud.

Clearly, phishing poses dangers for both consumers and for the organizations whose identities are hijacked; IT governance and risk management frameworks should all be addressing this issue as a matter of urgency.

The Anti-Phishing Working Group has a website that provides information that is relevant and helpful to those who recognize the need to take appropriate action now.

4.3. Wireless Networks

Some estimate that deploying wireless networks can reduce MIS costs by at least 30%. That type of saving, combined with all the user benefits of easy access to network resources, has driven the number of UK organizations deploying wireless networks up to 34% of the total, from just 2% in 2002. 53% of those organizations, however, admit that they have no security controls in place over their wireless networks. This is a failure of IT governance; it needs to be addressed as a matter of urgency by all organizations that have deployed wireless.

The emerging standard for Wireless Fidelity interoperability and security is 802.11i; the website of the Wi-Fi alliance is a useful resource for those who recognize the need to consider the risks of deploying this technology.

4.4. Blue Exploits

Bluetooth devices, particularly mobile phones, are at risk from two types of attack from nearby or passing devices, blue jacking and bluesnarfing. A blue jacking attack involves sending text messages to the mobile phones of any users who are within range, and it could be used both maliciously and for ‘blue spam’. A bluesnarfing attack is potentially more serious, and involves the theft of all contact information stored in the phones. Not all phones are vulnerable to these sorts of attacks and as manufacturers respond to the discovery of these vulnerabilities, so there will be changes.

5. Conclusion

Information system security is essential to organizations that depend on information systems. This fact becomes more obvious when an organization’s information is exposed to the risk of cyber attacks and the resulting damages. Managers need to know the extent of the damage that a cyber attack can cause and the possibility of occurrence, so they can determine what they need to do to prevent the attack by selecting appropriate safeguards or repairing damage.

CURRENT ISSUES
IN INFORMATION SYSTEM SECURITY MANAGEMENT

References:

[1] Manzuik S., Pfeil K. Network security *assessment, Andre Gold, 2007.*

[2] Farahmand F., Navathe S. B., Shar G. P. *Managing Vulnerabilities of Information Systems to Security Incidents, , 2003.*

[3] Deepak R., Gonsalves T. A., Murthy H. A., Usha Rani N., *Network Security Management for a National ISP, , 2004.*

[4] *Information Systems Security Assessment Framework, Balwant Rathore, 2005.*