BDO KNOWS:

CYBERSECURITY

CYBER VULNERABILITY ASSESSMENTS & PENETRATION TESTING – TOOLS, TECHNIQUES, & BEST PRACTICES

Cyber-attacks and their success rate in network breaches are increasing in frequency and sophistication. At the root of many successful cyber-attacks are the vulnerabilities that exist within network infrastructure, software applications and the very humans that use those networks and applications. The human element of cybersecurity deals with normal human interactions through email and social media (e.g., vulnerabilities such as email phishing, LinkedIn and Facebook hacking, etc.) and general cybersecurity awareness and good cyber hygiene (e.g., proper use of USB memory devices, remote connections and weak passwords). These vulnerabilities are best addressed through email phishing campaigns to identify gaps in organizational policies and lack of associated email-related security infrastructure, and overall security awareness training. This chapter focuses on vulnerabilities associated with network infrastructure and software applications and leaves the topic of human factors to be addressed separately.

CONTACTS:

ANDREW SILBERSTEIN
Director of Cybersecurity Advisory Services
703-770-0537
asilberstein@bdo.com

GREGORY GARETT
Head of U.S. and International Cybersecurity Advisory Services
703-770-1019
ggarett@bdo.com

A well-established technique to minimizing and mitigating vulnerabilities within network infrastructure and software applications is the use of Vulnerability Assessments and Penetration Testing (VAPT). The use of VAPT is a proven and powerful technique to manage the security risk within an organization or family office. Further, performing a VAPT is very effective in determining your cybersecurity risk profile and general security posture. Understanding and establishing a proven VAPT process and methodology together with utilizing the right tools and techniques will ensure the VAPT accomplishes its goal of improving the overall security of the organization.

Before diving into the details of how to best implement a VAPT, it is important to establish some baseline definitions and the reasons how and why adversaries pursue and exploit vulnerabilities.

Let's start with a simple definition of terms; what do we mean when we discuss a "vulnerability".

vul·ner·a·bil·i·ty[1]
(within general dictionary usage)

noun: vulnerability; plural noun: vulnerabilities.

The quality or state of being exposed to the possibility of being attacked or harmed, either physically or emotionally.

Refining this definition towards cybersecurity:

vul·ner·a·bil·i·ty
(within cybersecurity[2])

Vulnerability is a cybersecurity term that refers to a flaw in a system that can leave it open to attack. A vulnerability may also refer to any type of weakness in a computer system itself, in a set of procedures, or in anything that leaves security exposed to a threat.

Cyber adversaries look to exploit vulnerabilities everyday with new and innovative techniques. Adversaries come in many shapes and sizes and are looking to steal your sensitive and proprietary information, cause political or reputational damage, acquire financial gain, and simply steal whatever is available to sell to the highest bidder. Adversaries range from the most sophisticated foreign, state-sponsored adversary to organized crime to the ever increasing number of hackers in the world.

1 Google definition
2 Technopedia definition

Adversaries translate the definition of a vulnerability into two basic approaches; 1) attacking an organization from the outside of a network referred to as an external vulnerability, and 2) attacking an organization from the inside of the network, referred to as an internal vulnerability.

Let's have one more definition to help clarify how adversaries execute an attack:

at·tack vec·tor[3]

An attack vector is a path or means by which a hacker (or cracker) can gain access to a computer or network server in order to deliver a payload or malicious outcome. Attack vectors enable hackers to exploit system vulnerabilities, including the human element.

Once the adversary chooses either an external or internal attack (or both), he then decides on specific attack vectors which typically takes on one of two forms; 1) exploiting vulnerabilities within the network infrastructure and/or 2) exploiting software programs and applications. Software programs and applications can be running as an external facing application such as a web site or a web-based application or mobile application or a software program/application for internal use running on an internal network server or desktop. It should be noted that an adversary may use an external vulnerability to gain access to the internal network and then exploit the network from within the network.

With an understanding of how an adversary can attack a network or organization, and the types of attack vectors employed by these adversaries, we can now address the kind of vulnerabilities typically found during VAPT assessments. Network infrastructure (i.e., desktop computers, laptops, servers, firewalls, routers, and switches) and software application vulnerabilities generally fall into a few common categories; 1) infrastructure configuration issues, 2) software and application version control or patching updates, and 3) vulnerabilities resulting from web application code and its development. It should be noted these categories are not inclusive of all possible vulnerabilities but rather common vulnerabilities most often found during a VAPT assessment. Only by performing your own VAPT, will you gain an understanding of your specific security exposure and a complete list of network vulnerabilities. In summary, performing regular VAPT assessments will help manage the risk associated with vulnerabilities within your network infrastructure and applications and improve your cybersecurity posture against network attacks and their exploits.

3 Internet definition

BACKGROUND

VAPT is essentially two separate testing techniques with their own process, methodology and associated tools. Vulnerability Assessment (VA) is a process that inspects the potential points of exploit on network infrastructure and software applications to identify gaps in security. A typical VA uses vulnerability scanning techniques to detect and classify system weaknesses. Further, it provides actionable recommendations to mitigate those vulnerabilities. The VA process employs automated scanning tools that essentially perform a deep and thorough search of a network's infrastructure and software/web-based applications to find and categorize security vulnerabilities. While VA scanning is typically performed with automated software tools, manual vulnerability scanning is also used in certain tests to provide even deeper testing. Manual testing of vulnerabilities requires subject matter experts that can manually navigate through infrastructure configuration parameters and application code. The VA process will generate a report that identifies all vulnerabilities, categorized based on their severity and provide recommendations to resolve those vulnerabilities. The results of the VA are then used to perform the next step in the overall VAPT process which is penetration testing. Two important aspects of any VA that should always be considered are : 1) that the VA is performed with a non-intrusive process to ensure IT infrastructure and applications are not affected, and 2) that the VA process does impact the network performance.

A penetration test, or PT, involves thorough ethical hacking techniques attempts to exploit the vulnerability through a simulated attack. The PT process verifies, through executing an attack vector, if a vulnerability is present within a network or application and ascertains the level of severity the specific vulnerability. It acts as a proof point for the VA process and the identified vulnerabilities. With the vast number of existing vulnerabilities and the growing number of new vulnerabilities on a daily basis, the PT is also effective in determining if a particular vulnerability is a "false positive" (a result that incorrectly indicates a specific outcome or condition or how it could impact the network or application). While penetration tests leverage automated techniques, most testing is performed through manual techniques since many application vulnerabilities hinge on logical and semantic flaws (i.e., business logic) which, unlike syntactic bugs, are difficult to identify using automated analysis. While PT is by definition an obtrusive test, such testing can and is recommended to be performed with similar guidelines to the VA testing, namely to ensure that the PT is performed with a non-intrusive process to ensure the simulated attack does not actually execute the exploit but rather demonstrates its ability to exploit the IT infrastructure and applications.

Undertaking a VAPT process on a regular basis (at least four times per year) has proven to be an effective testing technique to address the need to secure the evolving and increasingly complex IT environment organizations face every day while delivering their business objectives. Performing the VAPT on the three most common attack vectors; external network, internal network, and software applications will increase the probability of identifying security weaknesses that are accidentally exposed or maliciously exploited. Secondary benefits from the VAPT process, once you have secured your infrastructure and applications include:

- Improvements in the overall technical IT environment
- Establishing greater confidence in the security controls within your IT environment
- Understanding areas within the IT environment that require budget allocation for security

VAPT is an involved, sophisticated process that requires the proper methodology, tools and techniques. To learn more about VAPT, please check out **Cybersecurity in the Digital Age**.