**Importance of Penetration Testing of Internal Networks and Internal Applications in Cloud Environment**

When we talk about implementing information security within an organization, it does not only mean the physical or external IT environment security, but also includes internal networks and applications that need to be secured against breaches and attack vectors. Although external penetration testing is common practice today, compliance with PCI DSS requires internal penetration testing of network and application layers as well. This needs to be done at least annually, following any significant modification or upgrade to applications or infrastructure.

**Internal Pen Testing: Why Should It Be Part of Practice?**

Unlike external penetration testing, which exploits externally exposed web applications and other vulnerable resources for getting inside a network from the "outside", an internal pen-test mimics an insider attack and what it can accomplish. An attack conjured up by a malicious individual, who has access to a company's Ethernet network, internal server or even a workstation, can potentially be more devastating as the attacker may already know about the location of sensitive information of an organization.

Deployment of an application and its interaction with the operating system and other processes can also introduce security holes. Such an application can be evaluated with the help of internal penetration testing for potential vulnerabilities resulting from improper software and hardware configuration, or application perimeter defense susceptibility. As installation of new software and amendments in system configuration alter the whole system environment, it is beneficial to carry out scheduled internal penetration tests to ensure the sustainability of IT security.

Many companies have developed security gaps that use shared business-critical applications of SAP, for example, Enterprise Resources Planning (ERP), Human Capital Management (HCM) and Supply Chain Management (SCM). Enterprises usually have lack of visibility in SAP infrastructure, uncoordinated internal security procedures, and yet believe that they are protected against all kinds of risks and do not need further security strategies. An internal pen test may identify security flaws for SAP users as well.

**Cyber Security Issues of Enterprises Using Cloud Computing**

Business virtualization and the need of agility, accessibility, disaster recovery and scalability has increased the popularity of cloud computing. Moreover, management of data center resources by a third party is an attractive offer by Cloud Service Providers (CSPs), hence, making Cloud a preferred solution for data storage, service on-demand and infrastructure. Recent analysis of various organizations shows that only 10 percent of IT operational models consist of in-house servers, whereas 90 percent are based on cloud services. Enterprises have shifted their data and some internal applications to cloud services which provide a shared, multi-tenant environment. This is where the issue of cyber security arises and organizations face various challenges to secure their cyber assets within the cloud.

**Who to Blame for Information Security Issues in Cloud?**

In the past, there have been several incidents of breached cloud environments by cyber attackers. For example, the iCloud, Target, Home Depot, Sony Pictures, the United States Internal Revenue Service hacks and many more. All these hacks took place because of various loop holes in public, private and hybrid clouds through different attack vectors. But are these Cloud Service Providers to be held responsible for such security breaches? No, cloud technology cannot be exclusively blamed as it is not more insecure than internal networks and applications.

Most enterprises think that cyber security for all the information on the cloud is the sole responsibility of the CSP. In reality, some responsibility also falls under the enterprises themselves. It is their obligation to ensure the security of what they upload to the cloud. The Cloud providers only have to take care of the basic infrastructure that supports the Cloud. Security of customer information, platform and internal application, internal network, access management and data encryption is the duty of enterprises. Therefore, organizations have to consider additional cyber security routines like internal penetration testing in cloud environments as well.

**Penetration Testing on Internal Networks and Applications**

An internal penetration test is required to overcome internal threats faced by an organization, such as from those arising out of misuse of internal user privilege or disgruntled insiders.

The first step involves collecting as much information as possible about the network and applications used using white box techniques. It is done by identification of possible security vulnerabilities related to applications and systems, through DNS queries and traffic analysis by tapping the internal network.

An attack is then executed by the exploitation of those security holes to gain unauthorized access to active directories, databases, web applications and network services as usual targets. The critical assets of the organization are then located by mimicking a real breach scenario and demonstrating how devastating an actual insider attack can be, as the targets are social security numbers, electronic payment card numbers, employees personal information and an organization's proprietary information. In the end, a detailed test report is generated regarding the success of the breach.

**Internal Penetration Testing in Cloud Environment**

Now that ease of service has caused many organizations to move their critical assets to Cloud, it is mandatory for them to conduct internal penetration tests. Internal penetration testing for on-campus infrastructure can either be deployed with the help of company's own highly skilled IT team or trusted third party service. Penetration testing in a cloud environment is however, somewhat different. Most CSPs may not allow pen testing as per their policies, because they are multi-tenant platforms and security of other user organizations may be compromised during the test.

An organization may first have to negotiate and require permission from the Cloud Provider for a penetration test, which may limit the areas of the test only to the internal applications and data. Cloud pen testing is usually carried out by cloud providers for their own compliance with security standards. The customer that plans to have a pen test can request its CSP for the results of their pen tests and any other related technology audit report, and consolidate their own results with the one they obtain from the Cloud Provider. Another way for the penetration tester is to exploit a system or application and use that as a pivot point for further test attacks on other applications and systems. This allows the ethical hackers to attack the target from the insider’s point-of-view. Such testing is usually allowed by the CSPs that are based on models like Platform-as-a-Service (PaaS) and Infrastructure-as-a-Service (IaaS). Software-as-a-Service (SaaS) based models, however, can have their configuration affected with penetration tests. In other words, testers need to be careful about exploiting their own IPs, ports, instances and applications, to avoid violation of the Terms and Conditions of the CSP.

To sum it up, internal penetration testing of networks is equally important as external penetration testing, because it can help an organization identify its exposure to cyber risks and weaknesses that can be used by malicious insiders to gain access to critical organizational information. It is also important to apply penetration testing on applications that are internal (i.e. on-premises) or in a cloud environment. But working in cloud it is necessary to understand the limitations and types of pen tests Cloud Service Providers allow, and seek authorization before performing them. Security of applications and data in the cloud is still a process that needs meticulous planning and constant vigilance.