Importance of Vulnerability Scans and Penetration tests in SOC Report

Overview

The evolvement of technology has increased the practice of outsourcing business functions to third parties. While, the third-party service providers help in managing data and business processes, they can also increase the vulnerabilities within the parent organization. The solution lies in having the right controls in place to identify exposed areas, extent of exploitation and the need for security testing.

Even the smallest of vulnerabilities can lead to a cyber-attack and a data breach putting the organization at risk. These can include use of unsecure protocols, delayed patching of identified risks, expired licenses for antivirus software, weak passwords, and absence of QA review processes. A regular vulnerability assessment can help in validating the effectiveness of current security practices and identify any new risks. Following is a brief overview about the VA and PT tests

Vulnerability Assessments

A vulnerability assessment is designed to identify, measure, and classify vulnerabilities in each system and the whole IT environment. This assessment provides a classified list of patches and systems that require attention. An effective vulnerability assessment should include following:

- Identify the security issues and their risk impact to the organization
- Function to identify and measure vulnerabilities within the systems
- Use vulnerabilities to breach systems and circumvent security controls
- Detect, identify, define and prioritize system vulnerabilities or gaps to prioritize any security issues

Penetration Test

Penetration testing aims to identify weaknesses that can be exploited. An effective pen test should include following:

- Prepare a listing of vulnerabilities based on the severity
- Assist in identifying the path of the attack used to take over a system
- Conducted after an assessment, and after the company has appropriate security practices
- Identify potential flaws on a secondary stage
- Achieve specific goals in identifying vulnerabilities.

SOC 2 and VAPT

While the SOC 2 TSCs does not specifically require companies getting a SOC 2 report to have vulnerability scans or a pen test done, companies must consider the unmitigated risks in absence of such reports. This more of an industry-standard for evaluating framework integrity and working with CPA firms that do not ask for vulnerability scans or penetration tests is doubtful. The SOC 2 Trust service criteria do mention VA and PT in the points of focus, which shows they are key components.

This avoids any confusion if the pen test and vulnerability assessments are required to become SOC 2 compliant. It is the discretion of to the management team to completely understand the criticality od a SOC 2 certification for the organization and having the right protocols and testing in place is for establishing benchmarks moving forward.

Addressing the ACIPA points of focuses

Although SOC 2 is less of a rule-based audit than ISO27001, CPA firms have the authority to request vulnerability scans and penetration tests as part of a service provider's design of controls to meet the Trust Services Criteria. Frequent vulnerability scans and penetration tests are required for service providers to fulfil the purpose of CC7.1 and pass a SOC 2 test.

The Approach

Even though penetration testing and vulnerability scanning are not expressly required by the SOC 2 guidelines, they are clearly stated in the Points of Focus, and a CPA firm should avoid issuing a SOC 2 report on an organization's information security stance without appropriately addressing the risk associated with misconfiguration and absence of regular patch management. Control Objective CC7.1 from the SOC 2 Common Criteria (Security) related to vulnerability scanning is as follows:

“To meet its objectives, the entity uses detection and monitoring procedures to identify (1) changes to configurations that result in the introduction of new vulnerabilities, and (2) susceptibilities to newly discovered vulnerabilities.”

Under these criteria, there is a related point of focus that states:

“The entity conducts vulnerability scans designed to identify potential vulnerabilities or misconfigurations on a periodic basis and after any significant change in the environment and takes action to remediate identified deficiencies on a timely basis.”

Given the risks associated with misconfiguration and patch management, our take is that companies should at least practice quarterly vulnerability scanning performed either internally or externally.

Further, in addition to scanning, we advise for vulnerability management to close any high-risk findings from the scans and mitigate the associated risks. This can be achieved by identifying process owners to take care of entire vulnerability management process.

CC4.1 (COSO Principle 16) notes the following about penetration testing:

” The entity selects, develops, and performs ongoing and/or separate evaluations to ascertain whether the components of internal control are present and functioning.”

A similar point of focus for CC4.1, which applies to all engagements involving the TSC, is as follows:

“Management uses a variety of different types of ongoing and separate evaluations, including penetration testing, independent certifications made against established specifications (for example, ISO certifications), and internal audit assessments.”

Since there are so many different forms of security assessments, we believe that a penetration test isn't needed if the entity can show that another security assessment is performed on a regular basis.

Summary

Based on our evaluation of the associated risk, recognition of the purpose of SOC 2 reporting, and consideration of the needs of the general reader of the SOC 2 report, vulnerability scans are required to meet CC7.1, but penetration tests are not required to meet CC4.1 as long as the individual requesting a SOC 2 report is conducting another periodic security assessment.

Following are few examples of security vulnerabilities that, may not be reported in a SOC study but pose significant security risks to all parties involved

- Weak passwords that give an intruder complete access to the system
- Open network services that reveal essential business systems, such as SQL Server
- SQL injection on a Web page that allows for remote database deletions that are undetectable.

You must search deeper before assuming all is well with security based on a vendor's SOC reports. Inquire about the results of their most recent penetration test or vulnerability evaluation. Take a closer look at the technological problems than you can at the higher-level policies and procedures.

We believe this the article would have enhanced your understanding about importance of vulnerability reports and penetration tests in a SOC report. Please feel free to reach out if you have any queries related to SOC reports or need to get a SOC/ISO/GDPR/VA-PT certification done for your organization.

You can also visit our website https://accorppartners.com/soc/index.php to read more articles related to SOC reporting.