IPSYSTEMS.INC.
ALL ABOUT DATA SECURITY

CYBERSECURITY 101:

A STEP-BY-STEP GUIDE ON HOW TO DO A COMPLETE VULNERABILITY ASSESSMENT

We know that hackers live on the internet, and they are always lurking to find vulnerabilities that they can exploit. If you don't want your organization to fall victim, you need to be the first to find these weak spots!

In other words, you need to be proactive in uncovering your network's vulnerabilities. The first step in achieving this is by performing a vulnerability assessment.

Read our expert-approved guide to help you and your security team perform this assessment and stay ahead of cybercriminals.

How do you perform a vulnerability assessment?

Using a vulnerability scanner, a software/application that comes in various types. Some focus on network scanning, others at web application scanning, IoT devices, or container security.

If you have the right tools in hand, you can easily perform a vulnerability assessment through the following steps:

Asset Discovery

Prioritization

Vulnerability Scanning

Result Analysis & Remediation

Continuous Security

LET'S BEGIN!

1. Asset Discovery

You need to decide what you want to scan.

One of the most common cybersecurity challenges that organizations face is the lack of visibility into their digital infrastructure and the devices connected to it. This lack of visibility makes it difficult for your IT and security team to implement a foolproof security - because how can you secure it if you can't see it?

Luckily, the discovery aspect can be automated for modern vulnerability assessment tools have a feature specifically designed for it.

2. Prioritization

Can you afford to run a vulnerability assessment to all of them?

In a perfect world, you would be running a vulnerability assessment on all of your systems daily. However, if you prioritize, not only can you stay organized, you can also better keep track on the health of your systems.

For example, you can put your internet-facing servers, customer-facing applications, employee laptops, and databases containing sensitive information on top of your list for these usually are the most common vectors for mass attacks.

3. Vulnerability Scanning

It's time to start scanning your chosen systems, applications, and networks.

Vulnerability scanners are designed to identify known security weaknesses and provide tips on how to fix them. During scanning, your chosen vulnerability assessment tool initially sends probes to systems to identify open ports & running services, software versions, and configurations.

These types of probes can uncover vulnerabilitie such as "Command Injection", "Cross-site Scripting or XSS", use of default usernames and passwords in your system, and more. Depending on the infrastructure that you're scanning, it may take anywhere from a few minutes to a few hours.

4. Result Analysis & Remediation

Make improvements based on the vulnerability scanning report.

Once your scan is complete, you will now be provided with an assessment report by your solution. While reading the report, you should consider two things: Serverity and Vulnerability Exposure. This means that you should take action on weak spots based on its severity and exposure to malicious actors.

After applying a fixes and improvements, it's a good idea to rescan the system to ensure the fix is applied correctly. If it isn't, it may still be vulnerable to exploitation. Also, if the patch introduces any new security issues, such as security misconfigurations (although rare), this scan may uncover them and allow them to be corrected as well.

5. Continuous Security

Ensure that your organization will never be vulnerable again.

A scan provides a point-in-time snapshot of the vulnerabilities present in your organization's digital infrastructure. However, new deployments, configuration changes, newly discovered vulnerabilities, and other factors can quickly make the organization vulnerable again. For this reason, you must make vulnerability management a continuous process rather than a one-time exercise.

Vulnerability assessment can be done by your in-house IT and security team, but if you are looking a vulnerability scanning tool or experts to guide you and enable you to properly address vulnerabilities, we're here!

IPSYSTEMS is a value-added cybersecurity partner of SMEs here in the Philippines. We have more than 14 years of expertise and have certified experts that handle our extensive line of cybersecurity solutions and services.

INTERESTED TO KNOW MORE ABOUT VULNERABILITY SCANNING?

Get in touch with us and let's talk about it!

+63 (2) 8638 - 3264 inquiry@ipsystems.ph www.ipsystems.ph