Cybersecurity Awareness Month

the NetWork

LeadingIT

Chicagoland CybersecurITy Support

October 2022

Cybersecurity Is More Than Technology, It's People Too

Testing Security With Vulnerability Scans And Penetration Tests

CISA and Cyber.org K-12 Cybersecurity Program

Password Best Practices

GoLeadingIT.com ☎ 815-893-2525 in @goleadingit

Cybersecurity Is More Than Technology, **It's People Too**

We hear about cyberattacks and data breaches constantly. If you have a pulse, you're probably aware of the heavy emphasis on cybersecurity's technical side. However, it is not enough to place sole emphasis on technical solutions to these problems. According to IBM, human error is the root cause of 95% of data breaches. Cybersecurity also requires people to think critically and make good decisions based on various scenarios with different implications. A team-wide understanding of cybersecurity best practices is essential for effectively managing cyber risks.

Collin

Cybersecurity Awareness Is Becoming A Culture Shift

By now, most of us are well aware that cybersecurity is no longer merely a topic that demands our attention – it's an essential part of modern life. In fact, it's increasingly becoming a culture shift within companies.

Social engineering is involved in 98% of cyber attacks. Social engineering focuses primarily on human interaction and manipulation to obtain unauthorized access to systems, networks, or physical locations. For example, a simple phishing email is the starting point for 91% of all cyber attacks.

The mission to protect against cyber attacks is a team effort, and companies must start from the top down and ensure everyone is on board with the mission. Company leaders must define employee goals and expectations by clearly outlining their cyber security policies. This way, everyone understands that there's a common goal and knows what steps they need to take to succeed.

Having written policies in place is critical to developing a culture that takes cybersecurity seriously. By taking these steps and establishing this culture now, companies can avoid falling behind in this new cybersecurity arms race.

Continue reading on page 4

Pictured on the cover: Salvador, Peter, Eric, Jeremiah, Stephen

CISA and Cyber.org expanding access to K-12 cybersecurity access across the country.

Implementing this curriculum will help create a workforce that is equipped to protect organizations and consumers from cyber threats with a holistic approach to cybersecurity.

Testing Security With Vulnerability Scans And Penetration Tests

Did you know that 76% of all software has at least one vulnerability? Over the last decade, we've seen an increased need for security due to the mass transition to a digital world. With everything kept online, it has become vital to ensure your data is safe and protected.

One of the best ways to test your company's security is through penetration testing and vulnerability scans. But, while vulnerability scans and penetration tests are similar, they're not exactly the same.

What is Penetration Testing?

Penetration testing, also known as pen testing, is a simulated cyberattack where professional, ethical hackers try to gain access to systems and data using the same techniques as real, malicious hackers.

What are Vulnerability Scans?

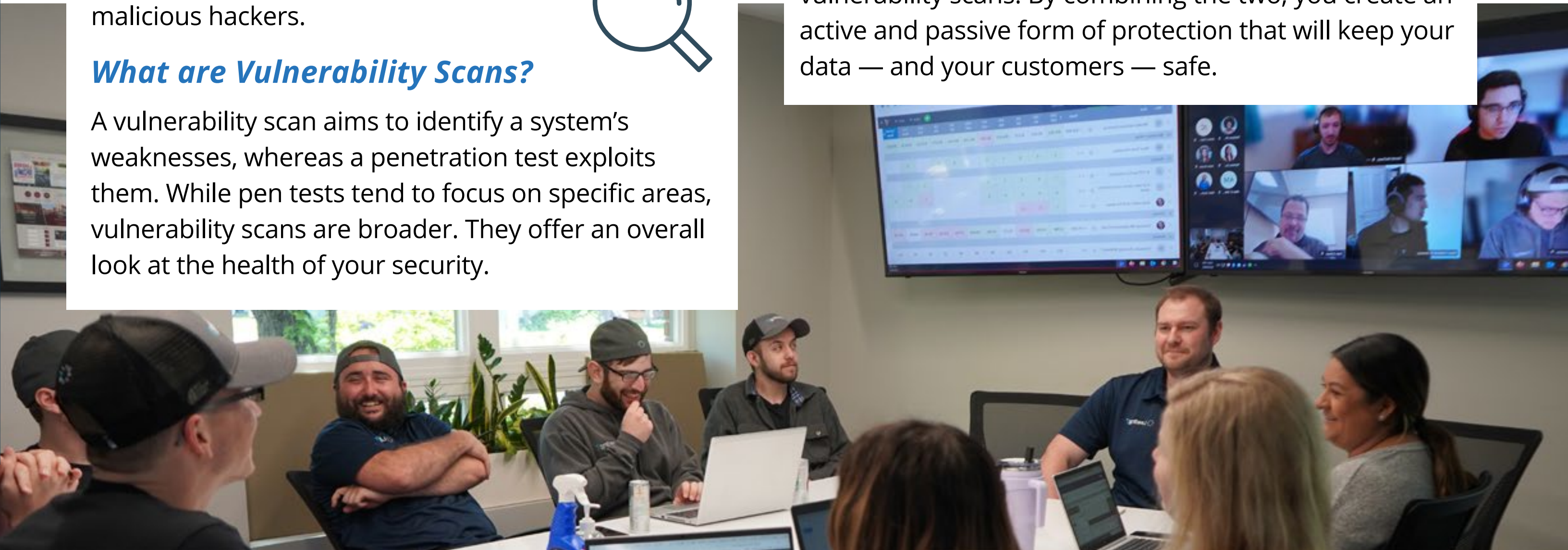
A vulnerability scan aims to identify a system's weaknesses, whereas a penetration test exploits them. While pen tests tend to focus on specific areas, vulnerability scans are broader. They offer an overall look at the health of your security.

How Crucial are Pen Testing and Vulnerability Scanning?

A significant advantage of combining pen tests and vulnerability scans is that they offer active and passive protection. Vulnerability scanning is passive, meaning it identifies potential threats. Pen testing is dynamic because it takes measures to exploit vulnerabilities. So, if you want to be sure your systems are secure, you need both.

Be Proactive

Investing in cybersecurity is no longer an option; it's a necessity. The best way to ensure your systems are secure is by conducting regular penetration tests and vulnerability scans. By combining the two, you create an active and passive form of protection that will keep your data — and your customers — safe.



Password *Best Practices*

Use a password manager

Create strong passwords and manage them all in one place.

Set Up Multi-Factor Authentication (MFA)

An additional layer of protection, MFA requires your identity to be verified a second time.

Do Not Recycle Passwords

59% of people continue to use the same password everywhere.

Cybersecurity Is More Than Technology continued...

Companies Should Implement A Holistic Approach To Cybersecurity

Employees can help in implementing a holistic approach to cybersecurity based on a full understanding of the risks and vulnerabilities. This includes knowing the company's policies, participating in user education programs, and following and keeping up-to-date with cybersecurity best practices.

There are many different types of threats and vulnerabilities at work. These include both operational and technical threats, as well as human errors like clicking on malicious links or mishandling protected credentials. Employees should be trained to identify risks and vulnerabilities quickly to take action before any issues escalate.

Most companies educate employees on how to do this with cybersecurity training programs. When businesses invest in cybersecurity training and awareness, security risks are decreased by 70%.

It's A Team Effort

Cybersecurity is no longer just a technical issue; it's a people issue, and it's the responsibility of everyone within an organization. Everyone on the team, from leadership to non-managerial employees, must be on board and be willing to take the initiative. Not everyone needs to know how to configure a firewall, but everyone can take responsibility for keeping the organization safe.

By working together as a team, businesses can detect and respond to threats before an incident occurs. This way, companies can prevent hackers from obtaining sensitive information that could lead to financial losses, reputational damage, or even potential harm to employees, customers, or other stakeholders.

Continue reading on our blog at goleadingit.com/blog

LeadingIT

Serving the Chicagoland area with offices in Woodstock, Downtown Chicago, and now in Manteno, IL.

WE ARE CELEBRATING

Birthdays

Garrett McCleary - October 5th
Katelynn Ware - October 17th

Anniversaries

Devin Lindelof - 10/5/2020