the NetWork

LeadingIT

Chicagoland CybersecurITy Support

September 2023

6 Reasons Why You Should Consult With Cybersecurity Experts Before Choosing Your Hardware

5 Benefits of Simulated Cybersecurity Attacks: Preparing Employees for Real-Life Scenarios

A Future Without Password Authentication: New Technologies and Possibilities

What Will You Do With $1000?

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

6 Reasons Why You Should Consult With Cybersecurity Experts Before Choosing Your Hardware

Secure technology infrastructure is essential for businesses and selecting the right hardware can be a make-or-break decision. As tempting as it may be to purchase off-the-shelf products for their convenience and cost savings, this could leave your company vulnerable from a cybersecurity standpoint. That's why consulting with experts in the field is essential before selecting any hardware.

Let's discuss 6 reasons why you should consult with cybersecurity experts before selecting hardware for your business.

1. Understand the Cybersecurity Landscape

Cybercriminals are constantly looking for new ways to exploit weaknesses in hardware. Buying faulty or less-than-ideal hardware can lead to an inability to patch security vulnerabilities, allowing for easy access to sensitive data.

2. Identify Business-Specific Security Needs

No business is the same. From industry to size and operations, each has unique security needs that off-the-shelf hardware can't always meet. That's why calling in the experts makes sense – cybersecurity professionals can assess your company's individual requirements and recommend appropriate solutions tailored to your specific industry and security objectives, ensuring the confidentiality, integrity, and availability of your data.

3. Evaluate Hardware Security Features

Off-the-shelf products often don't have the same level of security as those that are custom-tailored, lacking essential features like strong encryption, advanced authentication measures, secure firmware updates, and integrated intrusion detection systems.

4. Assess Vulnerability to Attacks

Certain hardware manufacturers may have a history of security vulnerabilities or compromised products. Cybersecurity experts are knowledgeable about these hardware trends and can provide invaluable insight into which products are safe for businesses to use – steering you away from any risky options that might lead to data breaches or other malicious online activity.

5. Mitigate Supply Chain Risks

The hardware supply chain can be a tangled web, with multiple vendors and distributors involved. Shopping at big box stores usually means limited insight into the overall flow of goods, leaving your tech open to tampering or worse: counterfeit products and malicious firmware. To keep yourself safe from potential cyber threats, it's important to know who you're buying from.

6. Future-Proof Your Infrastructure

Investing in hardware without taking into account future security needs can be a costly mistake. Consulting with professionals will reduce expenses associated with replacements or retrofitting, but it also guarantees that your hardware remains secure against ever-evolving cyber attacks.

Continue reading on page 4

Pictured on the cover: Matt, Salvador, Scott, Devin, Daniel and Jeremiah

5 Benefits of Simulated Cybersecurity Attacks: Preparing Employees for Real-Life Scenarios

Security measures, such as firewalls and anti-virus software, are the first thing people think of when discussing cybersecurity. But what about simulated cybersecurity attacks?

It's exactly what it sounds like: a way to prepare a company in the event a cyber attack occurs. When thinking of ways to protect your company from a cybersecurity attack, you're probably not considering a simulated attack as your first option. But, as many businesses know all too well, cyber incidents happen every day. One of the most effective ways to safeguard your business is with simulated cybersecurity training.

What is a Simulated Cybersecurity Attack?

Simulated cybersecurity attacks, often referred to as 'red teaming' or 'penetration testing,' involve mimicking the techniques of real attackers to test a company's cybersecurity defenses. This process is more than just assessing their hardware and software security – it also helps staff prepare for real-world scenarios. By simulating attacks, businesses can identify weak spots before bad actors exploit them, giving peace of mind that their systems are secure and employees are ready for whatever comes their way.

Benefits of Simulated Cybersecurity Attacks

1. Proactive Defense

Rather than waiting for an actual attack to uncover their weaknesses (and do a lot of reputational and financial damage in the process), businesses can take a proactive stance against cyber threats by running simulated attacks.

2. Training and Awareness

Human error accounts for over 88% of all data breaches. Businesses have the power to strengthen their defenses and protect themselves by showing employees first-hand what to look for, how to prevent cyber attacks, and what to do if the situation arises.

3. Testing Incident Response Plans

Any business needs an incident response plan outlining the necessary steps for responding to cyber-attacks. Though developing a response strategy is important, it's only effective when tested under real circumstances.

Continue reading on page 4

A Future Without Password Authentication: New Technologies and Possibilities

In a world where cyber threats are on the rise, securing digital assets has never been more critical. With artificial intelligence (AI) becoming more advanced by the minute, the total damage of cybercrime is expected to rise from $11.5 trillion in 2023 to $23.8 trillion in 2027.

If your company still relies on traditional password authentication systems, it might be time for a change. What cybersecurity solutions are out there for you?

Here are a few up-and-coming technologies that will enhance security, and minimize vulnerabilities:

Biometrics

By leveraging unique physical traits like fingerprints, facial features, and voice patterns, biometric authentication provides a higher level of security compared to traditional methods. Plus, users no longer have to remember complex passwords — meaning biometrics also simplifies the password authentication process.

Blockchain Technology

This technology uses something called "private keys," which are just like keys in real-life. They're a 100% unique digital signature only the owner can access. Using a private key is like using a code in a personal digital vault.

Artificial Intelligence

AI is like the emergence of the internet. You should aim to be a part of it. Those who ignore it will fall behind, and the businesses that use it will stay ahead. And in password authentication, AI will help keep your data safe.

Simulated Cybersecurity Attacks continued...

4. Building Confidence and Trust

Regularly conducting simulated cyberattacks can boost confidence and trust among stakeholders, showing them that the business is dedicated to cybersecurity.

5. Compliance and Auditing

For businesses to comply with regulations, they must have robust cybersecurity measures in place. Simulated attacks can provide evidence of these measures and make the auditing process a lot simpler.

Ultimately, these simulations can save you from costly damages caused by real cyber-attacks that are sure to come down the line due to our ever-changing digital landscape. Remember, in the realm of cybersecurity solutions, it's always better to be proactive than reactive.

DURA-TECH IS NOW
LeadingIT
TOGETHER WE ARE PROTECTING CHICAGOLAND ORGANIZATIONS FROM CYBERCRIME AND RANSOMWARE BY IMPROVING THEIR CYBER RESILIENCE.
WHY PARTNER WITH LeadingIT?
Concierge Support
Unsolvable, Solved
Values Driven

Michelle and Jaclyn, Manteno Chamber Golf Outing

Choosing Hardware continued...

Make Informed Choices With Insider Knowledge

You need an expert opinion on what kind of tech is best for your company - someone who understands both the needs of your business and cybersecurity fundamentals. Investing in this expertise beforehand can ensure that all your decisions about hardware are based on sound reasoning, helping build a robust digital defense system for your organization.

Remember, investing in cybersecurity expertise before choosing your hardware is an essential step toward building a cyber-resilient and secure technology infrastructure for your business.

What Will You Do With $1000?

LeadingIT's We Love Referrals Program would love to reward you for referring a new client to us!

1. Share referral information with us at www.goleadingit.com/refer/
2. Once they become a client, we'll show our appreciation by sending you a $1000 AMEX gift card!

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

Geovel Operana - Sept 9th
Amie Koster - Sept 22nd
Matthew McMullan - Sept 24th

Anniversaries

Geovel Operana - 9/1/2022