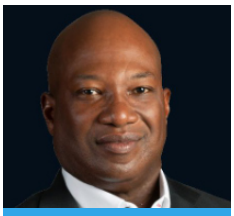
precision CYBERTECHNOLOGIES & DIGITAL SOLUTIONS

CYBER DIGITAL WORLD

NEWSLETTER

Volume 5: Issue No.2 January 2022

Common Vulnerabilities in Cybersecurity



Dr. Ronald Walcott
Managing Director

In our last issue, we discussed what happens after a penetration (pen) test is completed. Pen tests reveal vulnerabilities and security gaps in your business, along with recommendations to fix them.

In this issue we will look at some common vulnerabilities in cybersecurity, which if left unattended can place your company at risk.!

WHAT IS VULNERABILITY IN CYBER SECURITY?

A vulnerability in cyber security refers to any weakness in an information system, system processes, or internal controls of an organization. These vulnerabilities are targets for cyber criminals and open to exploitation through the points of vulnerability. Hackers use these weak points to gain illegal access to the systems and data and cause severe damage.

Therefore, cybersecurity vulnerabilities are extremely important to monitor as gaps in a network can result in a full-scale breach of systems in an organization.

To manage these risks, we must know what they are, so let's explore some of the most common vulnerabilities in cybersecurity.

1. **Unsecured Networks**
   An unsecured network most often refers to a free Wi-Fi (wireless) network, like at a coffeehouse or retail store. It means there's no special login or screening process to get on the network, which means you and anyone else can use it. What that means to you is that there's no guarantee of security while you use that network (unsecure = not secured). So, if a hacker were nearby and felt like doing dirty deeds online on that unsecured network, there's very little that can stop him.

   Once they infiltrate the system, they have access to all devices and systems connected to the network.

   For safety, make sure all of your devices are protected by a rigorous anti-malware and security solution — and ensure that it's updated as regularly as possible.

2. **Unsecured Communication Channels**
   Communication channels are the means of transmission of information between devices and users on a network. Businesses exchange sensitive information regularly, so it's important to secure all communication chan-

In this Issue:

nels. Investing in an encrypted e-mail platform is an excellent way of ensuring secure communication with clients.

3. **Outdated Systems**
   Technology is fast-paced, ever-evolving and fuelled by innovation. As a result, software and systems are sustained by ongoing updates and upgrades. When software no longer has updates to sustain it, it becomes outdated and exposes your company IT infrastructure.

   Software developers and hardware engineers are constantly coming out with new patches to fix bugs and errors to reduce vulnerabilities.. Once they find an issue, they patch it to eliminate the threat. However, outdated software doesn't have patches if vulnerabilities are found, and can fall prey to advanced cyber-attacks.

   To safeguard your business, set devices and software to auto-update so they fetch any incoming patches designed to fix known security gaps.

4. **Unknown Bugs**
   Bugs in an application give cybercriminals easy access to user accounts. This could be from a flaw in the application programming interface that integrates two different apps, or a fault in the software being used through a third party.

   While detecting and preventing every bug is impossible, you can enhance security by proactively scanning your applications and carefully scrutinise your vendors.

5. **Lack of Cybersecurity Strategy**
   Very often businesses neglect developing a robust cybersecurity strategy. However, as more firms move to a virtual work environment, protecting data is more important than ever. Without an effective cyber protection strategy against hackers and other cybercriminals, a firm could lose everything: profits, customers, employees, reputation and ability to recover. The financial blow can be staggering.

   Having a strategic approach to cyber security lays the foundation for placing security top of mind in the organisation and serves as a guide for anticipating and responding to attacks.

6. **Lack of Monitoring**
   Monitoring traffic and proactively scanning for distributed denial of service (DoS) attacks and ransomware are all actions that your company should take. A DoS attack occurs when legitimate users are unable to access information systems, devices, or other network resources due to the actions of a malicious cyber threat actor. Services affected may include email, websites, online accounts (e.g., banking), or other services that rely on the affected computer or network.)

   Proper monitoring is essential to safeguard against these types of invasions. The latest monitoring techniques incorporate artificial intelligence for even greater vigilance.

7. **Lack of Employee Training**
   90% of data breaches are the result of human error.

   This happens when an employee involuntarily hands a password over to someone. In turn, they gain access to the company's data, opening the way for attacks to surface.

   Training employees on best practices in cybersecurity teaches them to use strong passwords, identify various attacks in advance, and how and when to use company networks.

   It is prudent for companies to provide consistent training for employees, to ensure that they retain the information associated with best practices and to create a culture of security.

8. **Internet of Things and Multiple Connection Points**
   The IoT (Internet of Things) is one of the technologies' companies use to leverage business. This can involve several connection points on a single network. While IoT provides businesses with higher productivity and efficiency, it presents more points of vulnerability.

   Creating awareness of IoT dangers and being prepared for possible remote access threats can help to mitigate the IoT risks.

Upcoming Events

VIRTUAL ANZ SUMMIT
February 16, 2022

VIRTUAL ZERO TRUST SUMMIT
February 22, 2022

HYBRID CANADA SUMMIT
March 08, 2022

HEADLINE NEWS:

UK Issues Fresh Proposals to Tackle Cyberthreats

The U.K. government is considering new measures to boost security standards in the country. The proposed laws recommend levying large fines on essential digital service providers for noncompliance with strict cybersecurity rules, and improving incident reporting.

The Network and Information Systems, or NIS, regulations, which came into force in 2018, must be updated to improve the cybersecurity of companies offering essential services such as transport, healthcare, water, energy and digital infrastructure, the government's statement says.

The NIS regulations currently require essential service providers to undertake risk assessments and provide adequate security measures to protect their network, as well as report significant incidents and have plans for quick recovery.

Organizations that fail to put in place effective cybersecurity measures can be fined as much as 17 million pounds, according to the statement.

This move follows a 2021 research report conducted by the Department for Digital, Culture, Media and Sport, that shows that only 12% of companies review cybersecurity risks from their immediate suppliers and only 5% address vulnerabilities in their wider supply chain.

The announcements come on the back of "notable global increase in ransomware attacks, causing severe disruption to critical national infrastructure and government agencies," according to a policy paper from the department.

High-profile cyberattacks in the recent past include Colonial Pipeline, SolarWinds and an attack on Microsoft Exchange Servers.

The government had also recently introduced a 2.6-billion pound National Cyber Strategy to ensure that at-risk businesses improve their cyber resilience (see: New UK Cyber Strategy Adopts Whole-of-Society Approach).

SOURCE : DATABREACHTODAY.COM

Frequently Asked Questions:

1. WHAT IS A CYBER RISK?

cyber risk: A risk assessment that has been assigned to a cyber threat, such as DDoS attack or a data breach. A cyber risk assessment may be either qualitative or quantitative, where the latter should estimate risk (R) as a function of the magnitude of the potential loss (L) and the probability that L will occur (i.e., R = p * L).

2. WHAT IS CYBER THREAT MITIGATION?

In the context of cyber threats mitigation refers to reducing the severity or damage caused by cyber-attacks. Compare with cyber threat remediation, which refers to a more effective counter measure.

3. WHY IS CYBER THREAT REMEDIATION?

In the context of cyber threats remediation refers to reversing or stopping the damage caused by cyber-attacks. Compare with cyber threat mitigation, which refers to a less effective counter measure.

868-610-7237

salesinfo@precision-cyber.com

www.precision-cyber.com

1st Floor, Brair Place, 10-12 Sweet Road
St. Clair, Port of Spain, Trinidad