Prevent Cyber Attacks in 2022 Using Lessons from the Major 2021 Attacks

Cyber-criminals attacked a variety of industries last year, from insurance companies to schools, computer manufacturers, and the NBA. By looking back at the major 2021 cyber-attacks, we see a few patterns emerge. Business leaders who take to heart the lessons learned from 2021 attacks are better positioned to prevent cyber attacks in 2022.

Lesson 1: Everyone is a Target

A profile of the usual data breach victim in 2021 is hard to pin down. Large corporations like Experian and Volkswagen were victims. On the other hand, many small, low-profile businesses suffered in the Microsoft Exchange and Kaseya attacks. Ransomware crippled manufacturers, municipalities, hospitals, retail, and more.

Regardless of size, any organization with an internet connection is a target of attack. Hackers continually hone their skills and add to their toolsets. Consequently, businesses cannot afford to be casual about cybersecurity. Start 2022 out right by committing to invest in protective measures.

Lesson 2: Train and Filter to Fight Phishing

It shouldn't come as a surprise that in 2021, phishing remained the most common type of cyber attack. In a phishing attack on Nebraska Medicine, hackers gained access to the system and planted malware, eventually exposing over 200,000 patient records.

The most important anti-phishing safety measure remains regular, targeted security awareness training. In addition to addressing the human factor, organizations should implement email filtering and continuous network monitoring. A multi-pronged approach protects best against phishing and other social engineering attacks.

Lesson 3: Remote Work Requires Stronger Endpoint Security

The pandemic-pushed switch to remote work completely changed the security perimeter for many organizations. And observant hackers took full advantage. For example, when insurance giant CNA suffered a ransomware attack, 15,000 devices, including those used by remote employees, were encrypted.

With remote work continuing in 2022, organizations need to strengthen endpoint security. Begin by creating and updating an inventory of all devices connecting to the system. Then monitor the endpoints for unusual activity when connected to the network. Additionally, enforce strong authentication policies and keep endpoints encrypted.

Lesson 4: Monitor Your Supply Chain

In April, the REvil gang attacked Quanta, an Apple vendor. REvil used the attack to pressure Apple, claiming to have obtained secret blueprints for upcoming Apple products. Likewise, parking app Park Mobile suffered a breach because of a vulnerability in a third-party software app.

While strengthening internal security, organizations must not forget about their business partners. Make sure to vet third parties and build security policies into vendor contracts. Then perform regular audits while continuing to monitor those relationships.

Lesson 5: Apply Security Patches Quickly and Automate

The recent Log4j vulnerability serves as a pointed reminder of the need to stay up to date on patches. Take the time to apply software and firmware updates quickly. Take it a step further and turn on automatic updates where possible. This applies not just to servers but to all devices with access to the system.

When hackers exploited vulnerabilities in the Microsoft Exchange server, they disrupted 60,000 companies and government agencies in the United States. Microsoft released security patches quickly. However, many organizations delayed applying the patches. The attack group Hafnium then ran internet scans to find and exploit unpatched servers.

Lesson 6: Reliable Backups Enable Quick Recovery

Fortunately, the 2021 cyber attacks plague includes some redemption. Hackers struck Polish video game development firm CD Projekt, encrypting devices and accessing source code. Nevertheless, since

the company was prepared with quality backups, they quickly restored the lost data without paying the ransom.

For decades, security experts have emphasized the importance of performing regular, verifiable backups. Automating the process takes the burden off IT and delivers peace of mind like having money in the bank.

Lesson 7: Implement Multi-factor Authentication

In April last year, attackers used a compromised password to access the networks of Colonial Pipeline, disrupting gas supplies and causing panic. As government officials investigated, they concluded that stronger protections, such as multi-factor authentication, could have prevented the attack.

Identity and access management form a critical component of securing valuable digital assets. Companies should assess and strengthen authentication methods and tighten access controls.

Help to Prevent Cyber Attacks in 2022

The cyber attacks of 2021 serve as valuable data points to apply in protecting our organizations. Examining the high-profile attacks of the past year provides both the reason and the plan to prevent cyber attacks in 2022. Let the cybersecurity experts at eMazzanti Technologies bring the expertise and tools needed to optimize these solutions so you get the most from them in the coming year.