2021 Cyber Attacks – 7 Lessons to Apply for a More Secure 2022

Hackers have hit a wide variety of industries this year, from computer manufacturers to insurance companies, schools to the NBA. A review of prominent 2021 cyber attacks reveals a few common themes. And organizations that apply the lessons learned from these attacks can look forward to a more secure 2022.

Lesson 1: No One Gets a Free Pass

It would be difficult to describe the profile of a typical data breach victim in 2021. Large corporations like Volkswagen and Experian got hit. At the same time, even small, low-profile businesses suffered in the Microsoft Exchange and Kaseya attacks. Ransomware crippled hospitals, manufacturers, municipalities, retail and more.

No matter how big or how small, any organization with internet connections can become a target of attack. Hackers continually hone their skills and add to their toolsets. Consequently, businesses cannot afford to relax their security stance. Get started early on your New Year's resolutions by committing to invest in cybersecurity.

Lesson 2: Close Vulnerabilities by Applying Security Patches Quickly

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.

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.

Lesson 3: Step Up Endpoint Security

The rapid switch to remote work completely changed the security perimeter for many organizations, and hackers took advantage. For instance, when insurance giant CNA sustained a ransomware attack, 15,000 devices were encrypted, including those used by remote employees.

When remote work takes center stage, organizations need to strengthen endpoint security. Begin by creating and updating an inventory of all devices connecting to the system. Enforce strong authentication policies and keep endpoints encrypted. Additionally, monitor the endpoints for unusual activity when connected to the network.

Lesson 4: Monitor Those Business Partners

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

While strengthening inhouse security, organizations cannot forget about their business partners. Be sure to vet third parties, building security policies into vendor contracts. Then continue to monitor those relationships, including performing regular audits.

Lesson 5: Automate the Backup Process

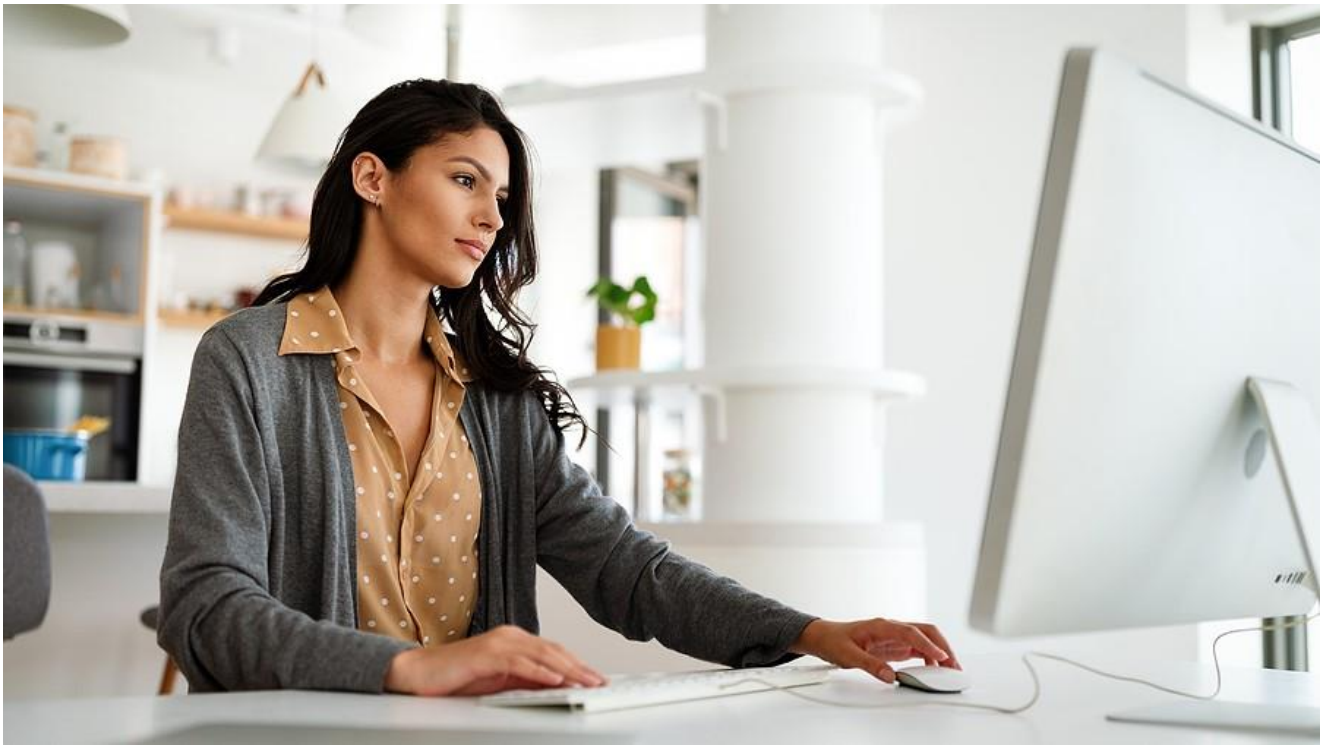
Fortunately, the list of 2021 cyber attacks includes some positive notes. Attackers hit Polish video game development firm CD Projekt, encrypting devices and accessing source code. However, because the company had quality backups in place, they were able to restore the lost data without paying the ransom.

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

Lesson 6: Strengthen Authentication and Identity Management

In April, 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.



Lesson 7: Take Protective Steps Against Phishing

According to a recent report on cybersecurity breaches, phishing remains the most common type of cyber attack. For instance, in an attack on Nebraska Medicine, hackers gained entrance to the system and planted malware, eventually exposing over 200,000 patient records.

To protect against phishing and other social engineering attacks, organizations should implement email filtering and continuous network monitoring. But the most important safety measure remains addressing the human factor with regular, targeted security awareness training.

Treat 2021 Cyber Attacks as a Wakeup Call

Reflecting on the high-profile cyber attacks of the past year can provide both the motivation and a blueprint for addressing cybersecurity. And the cybersecurity experts at eMazzanti Technologies bring the expertise and tools you need to keep your data and networks safe.