Recent Hacker Attacks Underscore Need for Multi-faceted Cyber Security

The cyber security landscape continually evolves. Hackers, increasingly operating as well-run businesses, adapt quickly to changes in business practices and tools. Consequently, smart organizations stay up to date on recent hacker attacks and adjust their own cyber security strategies accordingly.

For example, security reports suggest that, while ransomware attacks continue to pose a major threat, robust cyber security strategies help. Additionally, tried and true attack methods like phishing, living off the land (LotL) hacks and supply chain attacks continue to deliver dividends for bad actors.

Timely Patching Critical

Security experts have long advised companies to strengthen their patching strategies and apply security patches to software and firmware quickly. Recent reports underscore the importance of that advice.

For instance, experts warn that hackers continually scan vulnerability announcements. Meant to alert customers to possible security issues, these announcements unfortunately also provide detailed roadmaps for bad actors. And hackers can act within minutes.

As a result, system administrators need to stay on top of vulnerability reports and apply security patches as soon as they come available. Patch management can prove complicated, but patch management software can help by automating the process.

Guard Against Living Off the Land (LotL) Attacks

In its recent report on cyber security trends, Trellix warned that Living off the Land (LotL) attacks continue to grow. While not new, LotL attacks have proved highly successful over the years and thus present an ongoing threat.

People live off the land by eating only the food harvested from the surrounding area. Similarly, LotL attacks use existing legitimate processes and programs to hack systems. For example, the Windows operating system includes over 100 system tools that cyber attackers can use. And because the hacks use whitelisted programs, they often fly under the radar.

LotL attacks can prove extremely difficult to spot. Therefore, effective security strategies begin by preventing unauthorized access to the network in the first place. Thus, implement multi-factor authentication and strong credential management. Additionally, invest in endpoint detection and response solutions, as well as behavioral analysis tools that highlight anomalous activity.

Ransomware: Good News and Bad News

Recent cyber security reports suggest a decline in attempted ransomware attacks, a welcome spot of good news. Experts credit a number of factors, including improved defenses, the war in the Ukraine and companies refusing to pay ransoms.

However, ransomware continues to pose a significant threat, particularly in areas like healthcare that tend to underfund security efforts. At the same time, businesses find that insurance providers require more robust security before they will extend cyber insurance. Required security measures often include tools such as endpoint protection and segmented backups.

Cyber Criminals Still Love Phishing Attacks

The continued success of social engineering attacks underlines the importance of ongoing security awareness education. When end users know how to recognize phishing attacks, they provide a critical defense against hackers. In addition to regular security training, conduct periodic phishing simulations.

Supply Chain Security Critical

An attack this year on Blue Cross Blue Shield (BCBS) of Massachusetts highlights the ongoing importance of supply chain security. In May, an employee of a vendor servicing BCBS improperly emailed sensitive data to their own personal email and the personal email of another employee.

Insider data breaches, both accidental and intentional, continue to pose a threat to security. Organizations can counter those threats by carefully approaching access management and adding automated behind-the-scenes protection. For instance, companies should continually monitor access points and limit vendor access to only strictly necessary systems and services.

Applying Lessons Learned from Recent Hacker Attacks

As cyber-attacks evolve, businesses need to continually assess and adjust security measures accordingly. The cyber security experts at eMazzanti can help. Beginning with a cyber security risk assessment to determine priorities, we will help you design and implement a cyber security strategy tailored to your needs and budget.