FrankelZacharia LLC

Certified Public Accountants

Are Hackers Living in Your Network? (Why Monitoring Security Inside Your Network Matters)

Hackers could be "living" inside of your network right now. This sounds paranoid and delusional, but it is absolutely true of every network on the planet.

How did they get in?

- Phishing emails: Someone clicked a link or opened an attachment.
- Drive-by malware: Someone looked at a Web page.
- Zero Day attacks against the outside: There have been multiple high-profile examples of these like the Hafnium back door into Microsoft Exchange in the past couple of months alone, and those are just the ones we know about.

So, unless your staff never reads email or surfs the web and you employ a really good psychic to predict Zero Day flaws in your equipment, this is reality.

For much of the history of computing technology, the threats were against the outward facing defenses of a network. If you had a good firewall, decent anti-virus software, and kept things reasonably patched, you really could sleep pretty well at night. This was especially true for small to medium sized businesses, against whom the thought of a targeted or advanced attack was practically laughable. Yes, it **was** true, and not that long ago.

Security today is certainly no laughing matter for anyone, and small businesses are the victims of the vast majority of attacks. The time for attackers to "stalk and wait" once they are inside also becoming increasingly longer, allowing criminals to devise a solid plan for maximum damage before revealing themselves in a final attack, typically attempting a fatal blow of ransomware.

Since you can no longer be assured that hackers can be kept at bay outside the walls, you must increase your defenses to detect them after they are inside. Larger organizations already do this with systems that are out of the budget of a small business but thankfully there are tools on the market which can help.

As your Technology Success Partner, we are constantly on the lookout and implementing more tools to detect attacks inside of the network. These include tools like CyberHawk which runs frequent security scans on your domain looking for the behavior patterns of a lurking presence such as multiple failed logins, activity outside of normal parameters, and scans all of the devices on the domain looking for security patches or other weaknesses which can be missed through normal maintenance.

We also offer next level End-Point Protection through Sentinel One which incorporates behavior-based alerts, artificial intelligence, and other elements to detect threats traditional Anti-Virus may miss.

For even higher levels of security, our newest partner is RocketCyber. Interesting name for a serious security tool which pulls logs from every endpoint on the network as well as your firewall and cloud-based systems to watch for the behavior leading up to attacks before they are launched. This is augmented by 24/7 monitoring by live security professionals, a service that previously would only be available to organizations who could afford the enormous price tag such tools have typically carried.

Yes, internal security is no laughing matter which is why these types of controls and many others should be part of your cyber-defense. Even if you have internal IT resources or a third-party technology partner, we can still work with you to implement ongoing controls to lower your risk of a successful cyber-attack.

Call me at 402.963.4375, email tweidman@fzacpa.com, or click to schedule an appointment, and I would love to chat further.

https://resultdriventech.com/schedule