Ransomware Attacks Are On the Rise

We Asked a Certified Information Security Manager for Tips

HAI Group®

Cyber attacks are on the rise, particularly at housing organizations. That's because the data you collect and store is extremely attractive to criminals. Richard Moore, HAI Group's virtual information security officer and a Certified Information Systems Security Professional (CISSP) and Certified Information Security Manager (CISM), tells us how to protect our organizations.

HAI GROUP: Let's dive right in, Rich. Ransomware attacks are on the rise. Why is this happening?

RICHARD MOORE: In 2020, there was a whirlwind of ransomware and phishing attacks across multiple industries. According to the Ponemon Institute, attacks were up by 600 percent! The pandemic played a large part. Since many organizations are still in work-from-home mode, 2021 will have an even larger impact on organizations as their typical defensive activities and procedures are diminished. For example, in the previous work environment, you could simply walk over to a co-worker's desk and ask them if they actually sent an email you suspect of being a phishing attack. Working remotely doesn't provide that same defense. Phishing or fraudulent emails are how ransomware is commonly introduced into the environment.

HAI GROUP: Can we do anything about it?

RM: There are definitely steps you can take to mitigate cyber risk. Best practices include enabling multi-factor authentication, backing up your data, training your employees to spot—and avoid—social engineering attempts, and securing open remote desktop protocol (RDP) ports. People should also pay attention to the simpler things they can do—like practicing good cyber hygiene. This includes creating strong passwords, using different passwords for different sites, and making sure to update your applications and operating systems when new versions become available.

HAI GROUP: We touched on social engineering and multi-factor authentication in earlier interviews. Let's talk about employee training.

RM: Sure. Cybersecurity training is not just about watching videos or taking tests; it's also about having personal interactions with subject matter experts. Those personal interactions enable you to ask questions so the trainer can understand your specific worries. When people can see real-world examples of malicious emails and activities and learn how to spot them, it helps organizations protect their data. When looking for a training organization, look at their accreditation and whether they provide both computer-based training and instructor-led training (since people learn differently). The organization should be listed in industry journals and should be able to provide multiple references.

HAI GROUP: Good to know. Can you tell us more about RDP ports and why they're a particular concern?

RM: Of course. RDP ports, which enable remote computer access, are dangerous in their standard configurations since they provide direct access to a given system. There are also vulnerabilities in the way the standard RDP is configured, which allows for malicious

users to overwhelm the system's ability to differentiate authorized from unauthorized access. Luckily, RDP can be configured to be much more secure. First, you should require multi-factor authentication—that is, more than just a username and password. Next, the protocol should be tunneled through secure protocols to prevent a "man-in-the-middle attack," which essentially allows the malicious actor to read your communications and allows your credentials, such as username and passwords, certificate information, etc., to be forged. Ultimately, securing RDP ports is done through tunneling protocols, restricting direct access from the public internet, ensuring the operating systems that are running RDP are up-to-date and vulnerabilities are patched, monitoring for internal lateral movement—that is, if I get on to one system via RDP, I cannot log in to another system—deploying multi-factor authentication, configuring session security so that it doesn't stay open for long periods by using just-in-time (JIT) access, and finally, if it's necessary to continue to access a system via RDP, to switch to Windows Virtual Desktop for better performance, more secure access, and the ability to scale and monitor it for unauthorized use.

HAI GROUP: Should we be keeping copies of our data offline?

RM: Offline backups have been performed since the dawn of computing. Today, though, the best practices are usually implemented in the programs used to run the backup. Because malware can remain dormant for years, keeping copies of your data offline doesn't provide additional protections. Offline backups also won't be able to keep up with the online-transaction-type processing that performs thousands, if not millions, of transactions per minute. The best way to back up your data today is to have active backup and active recovery setups. With virtual data centers, and the way backup-as- a-service runs today, it is cost effective to create backups more frequently and to stand up East and West Coast redundant systems that can communicate and restore each other, should one side of the country experience an outage. External offline backups require more physical security controls, more testing, and resources dedicated to monitoring and moving backups, as well as more frequent testing to ensure the media you use can actually restore your information. Too often organizations do not test their offline backups, or do not monitor them for failures. Of course, it's usually the backup that failed that contains the most valuable information.

HAI GROUP: Any other tips for our members?

RM: The best thing an organization can do to protect their environments and data is to reduce the amount of legacy systems they use, and to constantly keep up with patching to remove vulnerabilities.

HAI GROUP: Thanks, Rich!

RM: My pleasure.

HAI Group®