Swizznet Shows How to Prevent Ransomware Attacks

September 11, 2022

It started out as a quiet Tuesday. Then, halfway into his second cup of coffee, Swizznet's Security Engineer was alerted to suspicious activity occurring inside a client's private server. Not only had an employee of the state-based construction company logged on from an unusual IP address, but their behavior was outside of their normal usage patterns. Within 60 seconds, AI-enabled technology powered by CrowdStrike flagged the atypical actions, signaling our team to take a closer look.

Minutes later, Swizznet staff contacted the employee directly. The employee confirmed that they were not personally logged into the network. This was a clear signal to our team that the employee's credentials had been stolen and were being used by an unauthorized person.

Ransomware Attacks on the Rise

Recent business news only scratches the surface. A 2021 survey by Sophos revealed 37% of respondents' organizations were hit by ransomware in the last year. Ransomware attacks are proliferating, and small to medium businesses are increasingly in the crosshairs. Smaller firms are less equipped to fend off cyber-attacks, and thus are perfect targets for bad actors.

Swizznet Springs Into Action

Luckily for this construction company, their Sage accounting software was hosted on a Swizznet server. Our experts recognized the intruder's behavior and understood the client was being set up for a ransomware attack. The intruder was in the process of setting up to gain full access to the client's server and potentially other machines. If they had not been stopped, they could have collected information and exfiltrated data about the client, its server, and other machines on the network, ultimately holding them hostage in a ransomware attack.

Within 15 minutes from the time that the suspicious activity was discovered and confirmed, our team contained the attack by isolating our client's server and taking it offline. For the next 60 minutes, the multi-step process of containment, removal, and recovery kicked into overdrive. Our team took an extra precautionary step of keeping things shut down for a complete check of the client's systems because the client did not have end device protection and did not use MFA.

Once fully satisfied that the systems were 'clean,' our team re-enabled access to the server so that the client could continue business as usual. Additionally, all users at this client were urged to immediately change all their passwords to all their accounts.

Protect Your Organization from Cyber-threats

As we continue further along the path of remote work and online collaboration, firms of all sizes must realize that using a secure and dedicated hosted environment with proper monitoring and protocols will be the non-negotiable key to cybersecurity success.

In addition to a secure hosted environment, individuals and organizations should take these key steps for staying secure:

- Implement MFA and end-device management – used in combination, these tools can prevent most cybersecurity attacks.
- Don't click on any links or attachments inside phishing emails. Doing so instantly compromises the email account and puts the firm's IT network into the hands of a criminal or criminal network.
- Never upload or offer your credentials unless you are expecting to access a known system. When in doubt, don't enter anything in and call your IT support team.
- Pay attention to the senders of inbound emails. "Spoofed" email addresses look similar enough to a legitimate address and can trick the unsuspecting receiver into giving away access or information to a cyber thief.
- Have your IT support team implement a cybersecurity training and testing program for your entire organization on data protection and cybersecurity protocols.

When it comes to cybersecurity and data protection, businesses can’t be too careful. Cybersecurity is an ongoing 24/7 process, and it only takes a few short minutes for a hacker to infiltrate a system and cause irreparable damage. A massive business failure for our client was avoided because Swizznet hosted environments employ CrowdStrike technology that understands and flags the sophisticated behavior of bad actors, and we acted quickly to thwart their intentions. Just another Tuesday at Swizznet!

Want to learn more about MFA and our other managed IT services? Email Swizznet Insides Sales or call us at 855-959-0065 X1.