TOP **10**
SYSTEMS TO SAFEGUARD TO HELP THRWART RANSOMWARE ATTACKS

SwitchThink solutions®

In 2023, there were 2,365 cyberattacks that affected more than 300 million people. That year also saw a 72% increase in data breaches from 2021, which previously held the record. Ransomware attacks, specifically, rose by 128% year-over-year in 2023.

The United States' Cybersecurity & Infrastructure Security Agency ("CISA") provides organizations with numerous guides to help us understand the methods used by attackers and how to better defend against their attempts. If best practice guides are readily available, then why do attacks continue to rise? The answer is attackers will target specific systems to maximize damage, prevent recoverability, and bypass many of the most basic controls.

Here are the top 10 areas to harden to heighten your protection against ransomware attacks while you continue to follow CISA's recommended guidance.

1. **VPN Gateways.** The quickest and fastest way into a trusted network is through an exploitable VPN gateway. When VPN providers publish a patch to a critical vulnerability, attackers can create a fully functioning exploit within a few hours. Your IT teams must be acutely aware of your VPN product and version to maintain maximum protection.

2. **Active Directory and Certificate Services.** Ransomware operators are on a quest to achieve Domain Administrator credentials. There are numerous ways to elevate to a Domain Admin through legacy authentication protocols, insecure certificate server templates, and cached credentials on PCs and Servers. Understanding and blocking these threats is critical to thwarting attackers.

3. **VMWare.** Internal cloud environments are highly sought after. Attackers know that patching ESX servers is time consuming, and balancing uptime can be challenging. By targeting unpatched and default VCenter and ESX servers, attackers can quickly encrypt your entire virtual server infrastructure.

4. **Patch Management Platforms.** Patch management platforms, like Microsoft's Configuration Manager (SCCM), typically have admin rights on every PC and server within your company. To encrypt an entire workforce, attackers don't need domain admin rights to every machine if they can simply compromise your patch management solution.

5. **Evilginx Phishing.** Evilginx is a nasty form of phishing where a simple phishing email will grant attackers access to your systems, bypassing your MFA. These emails are typically delivered as a request to share files with DocuSign, Adobe, or OneDrive. Quarantining these messages will ensure your IT teams have a chance to review the message before users fall into the trap.

6. **Endpoint Protection.** Your endpoint protection suite likely includes numerous application-level defenses. Blocking common exfiltration and lateral movement tools is a great step to prevent an attacker from compromising an adjacent system. It's best practice to enable application allow-listing on all endpoints and block known attacker tools.

7. **Logging and Event Management.** Enable advanced logging on your endpoints and keep your log management tools away from your internal virtual environments. You do not want your key investigation and detection methods encrypted in an attack. A cloud solution may be better for your organization – even if you have a robust private cloud infrastructure.

SwitchThink solutions

8. **Browsers and Saved Credentials.** Browser providers aim to provide a seamless experience across all devices through synchronized profiles. Logging into the browser will synchronize your history and passwords to your websites. Attackers will target administrators on their home computers to gather saved passwords to attack their work devices. You can use Group Policies to tightly manage Edge, Chrome and Firefox.

9. **Monitor Privileged Groups.** Most likely you know already when your Domain Administrator membership changes. What about VMWare Admins or SQL Admins? Windows Event Forwarding uses built-in tools to allow your IT teams to track these privileged group changes centrally.

10. **Backups.** Last but not least, hardening your backup infrastructure can be as simple as two key steps. 1) Do not use Single Sign-On (SSO) or connect your backup system to your Active Directory. The goal is to create standalone access credentials. 2) Implement strict network segmentation rules and isolate your backup management platform on a separate network that is inaccessible, except from a secure jump host.

It's clear that as technology continues to advance and evolve, hackers and malware are also keeping pace. Hyper diligence, ensuring continued best practices, and staying one step ahead on the most advanced security solutions are all required. By having a formal cybersecurity strategy and putting these extra measures in place to enhance security, you are taking an important step to minimize cyberattacks against your business.

SwitchThink solutions

About Us

SwitchThink Solutions is an IT Services CUSO formed in partnership with Corelation. As credit union professionals dedicated to optimizing & expanding KeyStone's capabilities for our clients, we've developed deep domain expertise in the areas of conversion, development, hosting, & operational best practices. Leverage our knowledge to unlock new strategic possibilities through performance improvement & rapid innovation.

Services include managed & infrastructure cloud solutions; disaster recovery as a service; development & consulting services; & conversion support services specifically designed for credit unions. Whether you're an existing user or preparing for implementation, let our experts help you rapidly apply the transformational powers of KeyStone & Cloud Computing.

Contact SwitchThink Today

Phone: 602.335.3500
Email: sales@switchthink.com

www.switchthink.com

SwitchThink solutions®