Preventing Ransomware Attacks

One major misfortune brought on by the pandemic has been the dramatic increase in cybersecurity breaches and online fraud incidents. At Horizon, the safety of your data is always our top priority. A key component in combatting these attacks is educating all users on ways to prepare and prevent themselves from falling victim to scammers. We urge you to check out these extremely helpful tips in the following blog entry from partner NordicBackup.*

6 Tips to Ensure Your Company Doesn't Fall Victim to Ransomware

Ransomware costs companies an average of $133,000 per attack (sophos.com/en-us/press-office/press-releases/2018/01/businesses-impacted-by-repeated-ransomware-attacks-according-to-sophos-global-survey.aspx), so it's no surprise that this type of attack should be taken seriously with efficient anti-malware systems in place to avoid critical incidents. Knowing that corporations fight against ransomware, malware creators continue to adapt attacks and their code to evade basic cybersecurity defenses. The biggest security risk to organizations is human error, so education and anti-malware systems should work together to reduce risk and protect your company from falling victim to ransomware.

1. Use Email Filters with Artificial Intelligence (AI) Capabilities AI has transformed many applications including email filters that catch malicious messages and quarantine them before they are sent to a user's inbox. Good email filters use AI to detect malicious content and send it to a network location where an administrator can review the message and identify any malicious content. Should the corporation get several phishing messages or emails with malicious attachments, the corporation could be the target of a spear-phishing attack.

If email filters detect an ongoing spear-phishing attack, employees and administrators should stay alert for social engineering. Social engineering plays a part in some ransomware attacks. Attackers will contact employees and convince them to open messages with malicious attachments. These attachments usually contain macros that will download malware including ransomware. Some attacks use additional malware that give an attacker remote control of an employee machine.

2. Install DNS-Based Web Content Filters When employees browse the web, they first need to perform a DNS query to link the friendly domain name with the site's IP address. Companies can intercept these requests and use DNS-based web content filters to identify if the site being accessed is malicious. These web content filters use a database of malicious sites that perform a lookup based on DNS entries and block content if it's on the list. DNS-based content filtering also provides a way for administrators to block websites based on content category.

While ransomware attacks can stem from successful phishing, some attacks trick users into accessing an attacker-controlled website and enter their network credentials. After users end network credentials, an attacker can access the remote network or device without tripping intruder detection

notifications. Web content filters prevent these attacks by blocking users from accessing sites on the watch list.

3. Use Cloud-Based Backups When ransomware installs on a user's computer, it scans the network and the local drive for any potentially important files and encrypts it. The encryption used is asymmetric and requires the private key to decrypt it. Most ransomware uses either AES or RSA 256-bit encryption, which are the current cryptographically secure encryption algorithms. Because these algorithms are still secure, a victim of ransomware will not be able to decrypt data and recover files.

With cloud-based backups, ransomware is unable to scan the remote service and encrypt files. Ransomware searches for backup files, so if you keep backups on a network drive that doesn't block ransomware scans, these files will also be held hostage until you pay the fee. Even worse, there is no guarantee that you will receive the key once you pay the ransom.

Cloud-based backups should be a part of a company's disaster recovery plan. They should be accessible only to administrators, and they should be performed at least once a day. Full and incremental backups can be used to save money when backups grow too large to efficiently transfer files to a remote host.

4. Regularly Patch Outdated Systems After a manufacturer finds bugs and security issues, a patch is released to the public to fix the issue. Several large critical data breaches through the years have been from outdated firmware and software. If an attacker is able to bypass current defenses and install software, it's possible that ransomware can be injected onto the network. The cybersecurity industry curates and lists the latest vulnerabilities at cve.mitre.org, but administrators should also check hardware and software developer sites for any issues that could affect the local network.

It's not uncommon for administrators to hold off on deploying the latest updates for fear that they will cause incompatibility issues or unknown bugs. The longer a network resource goes unpatched, the bigger the risk of a cybersecurity event to the organization. Testing should always be done before deploying an update, but any outdated software with publicly known cybersecurity issues should be given priority.

5. Disable Windows Server Message Block (SMB) In a Windows environment, SMB is usually enabled to make printer and file sharing more convenient. Some ransomware applications scan the network for open SMB shares. Once found, the ransomware application uploads malicious content to the drive and encrypts files stored in the directory.

Any Windows operating system prior to the Windows 10 release is vulnerable to this issue. Administrators should patch systems, but disabling SMB is also suggested if it does not interfere with daily productivity. Since exploits for SMB were released, administrators have reported an uptick in the number of SMB port scans detected on public-facing servers. Any servers that serve public applications should be a priority, but any Windows system on the corporate network should have the latest patches installed.

6. Provide Regular User Training The best defense against any malware is user training. Users should be trained to see the red flags when receiving phishing emails and becoming a target for social engineering attacks. Most ransomware attacks start with a phishing email tricking a user into opening malicious attachments or opening an attacker-controlled web page. Even if the organization

incorporates AI email filters, there is a chance some phishing messages will slip through.

Since the cybersecurity landscape changes every year, user training should be at least once a year. Training can be in the form of classes, documentation, or corporate memos that provide information on the latest attacks. Training is a collaborative effort and most effective when managers help new employees and guide them.

Ransomware attacks can be the most damaging and cost hundreds of thousands in mitigation techniques, recovery and patches. Most companies suffer some data loss, so it becomes a nightmare for IT and employees to recover information and get the organization back to its original state. Cloud backups are best for disaster recovery and restoring data, but corporations should strive to stop an attack before it happens.

User training, email filters using AI enhancements and DNS-based web content filters will help stop attacks entirely. No cybersecurity defense will protect 100%, but implementing these systems into network productivity will stop attacks when users are not able to detect phishing and fraud.

**The full blog post can be accessed at https://partnerblog.nordic-backup.com/5b77nvgngf.*