COMMVAULT®

Defending Against the Siege of Ransomware

6 TIPS TO FEND OFF SECURITY THREATS WITHOUT PAYING A KING'S RANSOM

The threat of ransomware is still – unfortunately – alive and well. According to a 2018 study by SentinelOne, their survey of decision makers working in IT and risk, fraud or compliance functions found that six in ten (56%) reported that their organization suffered a ransomware attack in the last 12 months - compared to under half (48%) who said the same in 2016.[1] While financial and healthcare organizations are often targeted, history has proven that no organization is immune from attack. The monetary costs to these organizations is bad enough, but they also risk suffering even bigger hits to their reputations (wouldn't you think twice before trusting them with your personal data?).

Ransomware is indeed big business. But to win the war against this cyber threat, without paying a king's ransom, you need a strong defense. Rather than arming yourself with catapults and battering rams, consider these six tips to protect against the threat of ransomware and take control of your enterprise's kingdom for good.

1 SentinelOne, "Global Ransomware Study 2018," March 2018

THE GROWING MALWARE THREAT

The truth is, ransomware isn't new. It has been around in one form or another for decades. Traditionally there are two forms of ransomware: "blockers" which simply block the user's ability to access files and "encryptors" that encrypt the users' files, usually irreversibly. Both hold the victim "ransom" forcing them to pay for continued access to data.

Of course ransomware is just one form of malware. The following list is just a sample of what's out there:

- Adware: As the name implies, it's usually a display ad on a web page. With just a click, your exposing your company to risk.
- Spyware: This "spies" on your on-line activity to collect information.
- Virus: This "contagious" code attaches to your software - it replicates and spreads using shared files.
- Worm: Like a virus, is does replicate, but it usually attacks data files and your operating files.
- Trojan: This nasty piece of code looks for financial information. It's known for denial-of-service attacks.
- Rootkit: Think of this as an accomplice, it hides in your system and provides access for other malware.
- Backdoors: Provides another way for malware to enter your system.
- Rogue security software: It looks like it's there to help you, but turns off your real protection

The rapid evolution of new types of malware and ransomware seems to be happening faster than ever. One possible reason for this is that cyber criminals are now sharing techniques and base code (off-the-shelf malware) with other criminals – which accelerates the time to market for new and more robust malware.

"Ensure backups are not connected permanently to the computers and networks they are backing up. Examples are security backups in the cloud or physically storing backups offline... Backups are critical in ransomware recovery and response; if you are infected, a backup may be the best way to recover your critical data."

"HOW TO PROTECT YOUR NETWORKS FROM RANSOMWARE,"
A U.S. Government Interagency Technical Guide

RANSOMWARE: A BIG AND LUCRATIVE BUSINESS

What's driving the business of ransomware? Simply put - it's lucrative and it's easy. However, what's often just as bad as the payment of a ransom is all the other costs associated with downtime, loss of productivity and diminished company reputation. According to Cybersecurity Ventures, cybercrime will cost the world $6 trillion annually by 2021.[2] Yes, that's a staggering amount of money.

Digging a little deeper into this, a recent report from BECKER'S noted that seventy-seven percent of the organizations [they] surveyed suffered a form of cyberattack in 2017.[3] And just over half (55 percent) of respondents fell victim to a ransomware infection in 2017.[4] Of the organizations that suffered a ransomware attack, 38.7 percent of victims

2 Cybersecurity Ventures, "2017 Cybercrime Report," October 2017
3,4 BECKER'S Health IT & CIO Report, "Half of ransomware victims who pay the ransom don't get their data back: 5 things to know," March 2018

decided to pay the ransom demand. However, only 49.4 percent of those organizations actually recovered their data, as opposed to 86.9 percent of organizations that refused to pay the ransom and were able to recover their data.[5]

What's the most common way ransomware enters a system? Email. As much as industry continues to educate and inform about the ramifications of malware - gaining access through emails found on endpoints – including laptops and desktops – remains the number one culprit. More than 90 percent of successful hacks and data breaches stem from phishing, emails crafted to lure their recipients to click a link, open a document or forward information to someone they shouldn't.[6]

But the truth is, no matter how the ransomware breaks in, data is at risk everywhere it's stored. And whether it's on-premises or in the cloud, data must be protected and managed - which means having a rigorous backup and recovery strategy is paramount. This is still your best risk mitigation plan against cyber threats.

6 TIPS TO BUILD YOUR BEST DEFENSE

If you're ready to protect your data from the increasing risk of ransomware, consider these six tips. They just may ensure your organization can achieve business continuity in the face of the unexpected malware attack.

1 **Protect Data, Regardless of Where It's Stored.** It's important to do a complete assessment of your data assets and to know precisely where all of your most valuable data is stored. Map out the data's location (including data centers, remote facilities, cloud, and service provider datasets) and understand the data flow between each. Pay specific attention to those systems that store, process or transmit sensitive data and understand which systems could present the highest risk for your operations. Then select, apply and manage security controls based on risk.

2 **Integrate Your Data Protection Strategy.** Select solutions that give you a complete, integrated view into all of your stored data. This will ready you for rapid response in the event of a breach, while also simplifying day-to-day management and control. The most powerful solutions will protect everything from file servers and storage arrays to third-party file sharing apps in the cloud, all from a single solution. They will also monitor, alert and identify the rate of file change across your enterprise so that suspicious activity can be quickly discovered and investigated before potential malware hops and infects other systems.

Ransomware: 4 Ways to Protect and Recover

Learn best practices from organizations that have effectively managed ransomware attacks.

READ NOW

PDF

http://bit.ly/2rYszBd

5 BECKER'S Health IT & CIO Report, "Half of ransomware victims who pay the ransom don't get their data back: 5 things to know," March 2018
6 Cybersecurity Ventures, "2017 Cybercrime Report," October 2017

3 **Employ a Dual Backup Configuration.** For assured protection, best practices state that it's vital to have a dual backup configuration, where only one system is connected at a time. In fact, this is a core recommendation of the Center for Internet Security (CIS) Critical Security Control (CSC) for ransomware protection. The standard states:

> *"Ensure that key systems have at least one backup destination that is not continuously addressable through operating system calls. This will mitigate the risk of attacks like CryptoLocker which seek to encrypt or damage data on all addressable data shares, including backup destinations."*

This can be a powerful protection against ransomware. If the hackers can't find an access path to online backup sets, they can't break through to delete the attached backup pool. Further, if you use a secure, centralized and searchable virtual repository, you can also protect cold storage by using a protective "gap" that will prevent stored data from being corrupted while still ensuring its active use for business insights.

4 **Keep a "Gold" Image of Systems and Configurations.** Should a ransomware attack penetrate and infect one of your systems, eliminate the need to pay the ransom by having a "gold" image at the ready. This fundamental element of your data management policy could eliminate the risk of ransomware altogether. If a system is infected, you can easily clone the infected system with your master image. However, it's vital to have intense security and protection around your gold images to ensure attacks can never infect them.

5 **Protect Vulnerable Endpoints.** Laptops and desktops are easy targets for ransomware, especially if they are not sufficiently protected. Be sure to deploy web browser URL reputation plug-in solutions that will display the reputation of the websites users access. Restrict software to corporate-approved applications and deploy two-step authentication on any website or application that offers it. Finally, employ comprehensive endpoint backup solutions that will ensure that you can rapidly recover a user's system in the event of an infection – so you can prevent further contamination throughout the enterprise.

6 **Train, and Retrain Your Users.** The best security from ransomware is to prevent it from entering your infrastructure in the first place. Because the majority of attacks enter via email, you need to train, train, and retrain your users. Every user should be educated on the risk of email attachments and know not to open anything that isn't from a known sender or trusted source. They should also be informed not to execute software that has been downloaded from the internet, unless it's first been scanned for malware. They should also be extra cautious

Financial loss from cybercrime in the U.S. exceeded $1.3 billion in 2016.

FEDERAL BUREAU OF INVESTIGATION [7]

7 Federal Bureau of Investigation, "2016 Internet Crime Report," June 2017

when clicking on URLs in emails or social media programs, even when coming from trusted sources and friends. Finally, encourage employees to sound the alarm if they see anything suspicious or fear they've become infected. The more quickly you are altered, the easier infections will be to contain.

Don't let the risk or cost of ransomware storm your organization's castle. It will wreak havoc on your valuable data and impact business continuity. Instead, employ a multi-layer security strategy that not only includes anti-malware, firewall, and hard disk and file encryption, but also data loss prevention technology and standards-based data protection. Being able to rapidly recover data, whenever you need to, and resume business as usual - even in the face of a ransomware threat - should be a top priority. Each are critical to mitigate cybersecurity risks and protect vital information so you can avoid business disruption without ever paying a king's ransom.

"More the 90% of successful hacks and data breaches stem from phishing..."

CYBERSECURITY VENTURES

COMMVAULT

COMMVAULT.COM | 888.746.3849 | GET-INFO@COMMVAULT.COM