Protecting Your Business from Ransomware

303-449-6400 • 800-833-1132 • 6285 Lookout Road • Boulder, CO 80301 USA

SPECTRALOGIC.COM

Contents

Introduction

Hackers attack every 39 seconds, or an average of 2,244 times a day[1]; 51% of businesses have been impacted by ransomware in the last year[2]; and 50% of IT professionals don't believe that their organization is ready to defend against a ransomware attack[3]. What are we doing wrong? Or more to the point, what could we do better?

What is Ransomware?

Ransomware is a type of malware that prevents users from accessing their systems or personal files and demands ransom payment in order to regain access. There are many things to help avoid a ransomware attack from getting through – educating users, strong malware protection software and a VPN for remote workers should all be givens in today's data center environment. Along with these precautions, there's still not a lock that can't be picked if the threat actors are smart enough and persistent enough. They are both.

First-Hand Experience

Spectra falls into the second statistic above as the company experienced a ransomware attack in May 2020. We fared exceptionally well, but realized there were a few basics concepts that are often overlooked. We created this checklist based on that experience - five things to do *before* a ransomware attack occurs and four things to do *if* an attack gets through. If you can check off each of these items, any attack you experience can be mitigated and your organization can have a strong path to recovery.

Before a Ransomware Attack

So what should you do *before* a ransomware attack occurs? These 5 steps will get you started:

1. Mitigate your blast radius

Limit what the attack can compromise within your infrastructure. Have multiple copies of your data on multiple storage platforms. Disk and tape are the obvious candidates. The only guarantee of recovering your data (paying the ransom is no guarantee) is to have a copy that hasn't been compromised. The attackers are good, some argue the best in the world, and they come from all over the world. There's not a system they can't enter if they can get one employee to click on one bad attachment. If your users have access to email, it's difficult to create an environment that's 100% secure, but you can put up road blocks – that's mitigating the blast radius.

2. Create an air-gap

Multiple copies of data don't assure multiple copies are not attacked. This requires an air-gap. Literally "air" that an electronic virus cannot travel across. Historically, an air-gap was created by establishing an offsite copy of data.

Ransomware Preparedness Checklist

5 Steps To Take Before An Attack:

- ☐ Have multiple copies of your data on multiple storage platforms
- ☐ Have an air-gap copy of your data
- ☐ Limit your mission-critical data recovery time by migrating inactive data that can be recovered over time
- ☐ Build a "First Hours" communication plan
- ☐ Get cyberattack insurance

4 Steps To Take After An Attack:

- ☐ Shut down all systems
- ☐ Report the incident to the FBI and insurance or security group
- ☐ Implement your "First Hours" communication plan
- ☐ Ensure your golden copy is safe to avoid paying the ransom

That was tape in an offsite vault. Today, many organizations use the cloud for offsite storage. While that can be effective for several purposes, it's typically disk storage accessible by WAN which can also carry an attack. Ransomware focuses on destroying data backups. The threat actors know that's your silver bullet. Assure that you have a truly air-gapped copy of your data at all times. Tape is the most cost-effective low-cost option. Some disk can also be air-gapped.

3. Reduce the surface area of an attack

If you've checked off the first two boxes, you've got a clean copy from which to restore. But how much data is that, and how long will this take? By archiving inactive data off of tier-1 storage, the recovery process can be cut by days, weeks or even months, depending on your situation. Archived data can be relinked as time allows. It isn't mission critical for running your business or reopening your doors. Studies show that as much as 80% of an organization's data is "cold" or inactive. If it's all sitting on tier-1 storage, and tier-1 storage needs to be rebuilt, there's no way to identify which files are critical and which are not. Make that decision ahead of time by implementing a storage lifecycle management solution which moves inactive data and finished projects off of tier-1 storage to a secondary tier.

4. Create a game plan for the first few hours after an attack has been identified

Time is of the essence. Decide ahead of time how you will communicate to the company if the mail servers are encrypted. Decide how you will communicate with remote employees. Know how you will communicate with customers and users of your services. Make a plan as to whom you will call first, second and third. For instance, the FBI should be a "first to contact" on your list. Do you have their number? Most organizations have some feel for how they'd recover from a disaster in the long-run, but few are thinking in terms of what happens in the first hours after all systems have been encrypted and the entire organization comes to a halt. Make that detailed plan.

5. Consider cyberattack insurance

Yes, this exists. It's most often referred to as "cyber-extortion coverage." Not only can your organization be reimbursed for losses, these insurance groups can provide security specialists who are capable of assessing damage, determining if data was stolen or accessed and, most importantly, help you "stop the bleeding" of the current attack. While policies and offerings vary, this insurance can become your complete security follow-up team. Few organizations have ransomware experts on staff just waiting for an event to happen. Specialized insurance gives you access to trained experts.

By putting the above actions into play, your response to a successful ransomware attack will be more straightforward.

After a Ransomware Attack

And, what should you do after a Ransomware attack? These 4 steps should help you prevail against an attack.

1. Shut down all systems immediately

Once ransomware is in place, it continues to "burrow" into every path it can find. While it's virtually impossible to stop an active attack before it does damage, fast action in bringing down servers can substantially lessen the damage done. Keep in mind many ransomware attacks also open back doors into your systems which are then sold to other threat actors to steal data. You have to protect against further data egress or hacking. Put a process in place for what this would look like, and ensure that responsible IT personnel are familiar with the drill.

2. Report the incident

This is essentially the act of implementing the "immediate game plan" you created in step 4 above. Have the names/numbers/emails for outside sources that need to be contacted (FBI, Insurance Group or Security Group). Have cell phones for key personnel throughout the organization so texting is an option if the mail server is infected. Have it all on paper or in your own cell phone in the event all computer access is stopped.

3. Assess the damage

Many ransomware variants are well known by the FBI and security experts. Knowing the "strain" of ransomware can be as important as assessing how much damage has been done. This will help in the level of harm effected. Often a server directory will show a single, compressed and encrypted file rather than the hundreds/thousands you would typically see. Along with that is often the ransomware note. If you have the resources to do so, split teams between assessing actual damage done and finding the last secure (hopefully air-gapped) backup that you have. Depending on the time you've been allotted by the ransomware, you may have to make a decision as to whether or not to cooperate with the threat actor before you know the full extent of the damage. That's why a golden backup copy can alleviate some of the pressure. Figure out if you have a fall-back as soon as possible.

4. Evaluate your options

While this may sound obvious, the process by which you make your final decision may not be obvious. Know ahead of time who will have input or make final decisions for your organization. If you do opt to pay the ransom, it's also possible to negotiate with the threat actor. Having the support of the FBI is critical in understanding your options. If you have access to security experts as well, all the better. Recovering 100% of your organization's data without paying the ransom is possible, and even probable, if you prepare before an incident occurs. Contact Spectra Logic if you would like to learn more.

Footnotes:

1: https://eng.umd.edu/news/story/study-hackers-attack-every-39-seconds
2: https://enterprise.comodo.com/blog/recent-ransomware-attacks/
3: https://www.comparitech.com/antivirus/ransomware-statistics/

About Spectra Logic Corporation

Spectra Logic develops data storage and data management solutions that solve the problem of long-term digital preservation for organizations dealing with exponential data growth. Dedicated solely to storage innovation for more than 40 years, Spectra Logic's uncompromising product and customer focus is proven by the adoption of its solutions by leaders in multiple industries globally. Spectra enables affordable, multi-decade data storage and access by creating new methods of managing information in all forms of storage—including archive, backup, cold storage, private cloud and public cloud.

To learn more, visit www.SpectraLogic.com.