Six Steps To Stopping Ransomware Damage

Table of Contents

Executive Summary

While ransomware has been on the radar of cybersecurity teams for quite some time, activity increased seven-fold just in the second half of 2020.[1] One reason for this jump is the rapid growth of the Ransomware-as-a-Service (RaaS) industry. RaaS continues to make it easier for pretty much any bad actor to mount targeted ransomware attacks, even if they do not have the skills to develop and launch them on their own. The combination of low risk, low barrier to entry, and high profits means ransomware will continue to be a favorite attack of hackers. More cyber criminals will launch more attacks, more often.

But even with ransomware's increasing sophistication and volume, it is possible to avoid being a victim. When an organization is in the midst of a ransomware attack, it's too late to put the processes and technology in place to stop the damage. Planning and preparation before it occurs is critical. This eBook will explain the key steps to take to mitigate the impacts of ransomware.

“The persistent spread and evolution of ransomware is culminating in the 2021 iteration of advanced Ransomware-as-a-Service, a highly organized, business-like, and particularly impactful ransomware attack ecosystem.”[2]

How To Keep Ransomware From Succeeding

Back up data

In the event of a disaster, whether man-made, like ransomware, or a natural disaster such as earthquake or flood, it's essential for organizations to be able to recover data and systems right away.

The primary steps are backup of data, testing/optimization of recovery, and security of the data and process.

Backups: Backing up typically involves storing data either off-site or in a removable drive. Backing up, on its own, is typically insufficient without a process for recovery because the network infrastructure is still left inoperable.

The first step is to figure out what must be backed up in case a disaster hits. The organization also has to make sure the backup methods are established and maintained. In addition, the responsible party and process for creating the backups as well as performing any restorations or migrations must be determined. The plan should involve a recovery point objective (RPO), which dictates how frequently backups are made, and a recovery time objective (RTO), which outlines the maximum acceptable amount of downtime the organization is willing to tolerate after a disaster. It is also important to decide whether you are restoring data and applications to the original systems (if you are confident in your remediation) or to fresh ones to reduce the risk of reinfection.

"Backup recovery is also known as disaster recovery or DR. This solution helps businesses quickly and efficiently recover software, settings, and data to an as-before state in the event of computer, server, or other infrastructure failure."[3]

Testing and optimization: The recovery team is responsible for making sure the backup system remains current and available for an event by continually testing it and updating its various elements.

Security: As with the rest of the network, backups require effective security. For an organization to get back up and running, it will need uncontaminated systems and data. The team must make sure the security measures in place are up to date and protected against the most recent cyber threats.

Train users

The majority of successful cyberattacks start with a user not recognizing a threat, and taking action that puts the organization, and possibly themselves, at risk. This holds true for ransomware attacks. Cyber criminals are fully aware of the user vulnerabilities exacerbated by remote workers and are successfully launching convincing, timely attacks to take advantage of them. Although most organizations now deliver phishing training, an alarming number of users still cannot spot malicious emails. Bad actors are experts at the art of masquerading, manipulating, influencing, and devising lures to trick targets into divulging sensitive data, and/or giving them access to networks and/or facilities.[4]

Cybersecurity awareness training teaches employees how to act safely, both online and in an office—wherever that may be. And an effective, continuous training program is essential for turning an unpredictable workforce into savvy defenders. But that is not enough. Remember, all it takes is one click by one user.

Employees must also feel invested in security and understand the consequences of their actions. Once everyone is engaged, there should be direct improvements on how they behave when exposed to suspicious behavior or questionable emails.

When evaluating security awareness training options, it is important to include all the types of threats, such as phishing, social engineering, and ransomware. But it's equally important to provide context and demonstrate how users can protect themselves and the information they access. Make sure current, real-world examples are included along with types of bad actors and their motivations and methods.

“Using trademark logos of major pharmaceutical companies producing approved COVID-19 vaccines, fake websites are suspected of being used to conduct phishing attacks and/or dupe victims into giving charitable donations.”[5] – *INTERPOL public warning*

Reduce the attack surface

That said, not all ransomware relies on user action. In the case of DearCry ransomware, for example, cyber criminals utilized a recent vulnerability in the Microsoft Exchange software as an initial insertion point. Out-of-band, emergency patches will be required from time to time. Organizations need to have a plan in place through change control processes to ensure they can respond to emergency patches. Attackers are no longer taking days to weaponize vulnerabilities. They are taking hours. In addition to patching, it's important to disable unnecessary services, take a least-privilege approach to system configuration, and to the extent possible, limit user control to the applications allowed to run devices.

Shore up security along the Cyber Kill Chain

Given human fallibility, organizations can reduce their risk through implementation of strong security technology. The Cyber Kill Chain model was created by Lockheed Martin and identifies what cyber criminals must do to complete their objectives. There are a number of phases, and they must go through all of them to succeed, meaning organizations have the opportunity to block them at any stage to thwart the attack.

"Cyber criminals have combined social engineering tactics … with older exploits targeting unpatched vulnerabilities found in devices deployed in many home networks. Once the corporate network has been breached, cyber criminals are delivering new, more malicious strains of ransomware and other malware."[6]

To reduce the risk of a ransomware incident, organizations need to deploy the right mix of security controls to thwart delivery, shield vulnerabilities from exploits, prevent installation, block execution, cut off external communication, and contain lateral movement. A broad set of security technologies deployed at multiple stages of that Cyber Kill Chain are a great way to stop a ransomware attack from achieving its ultimate goal of interrupting business operations.

Security controls should include, at a minimum:

- **Next-generation firewall (NGFW)** for inspection of encrypted traffic, web filtering, and intrusion prevention (IPS)
- **Secure email gateway (SEG)** to stop email-based threats and loss of sensitive data
- **Sandbox technology** to detect and analyze previously unknown malware and other threats
- **Web application firewall (WAF)** to prevent web-based attacks
- **Multi-factor authentication** to prevent "authorized" configuration changes or code installation using stolen credentials
- **Endpoint security with detection and response capabilities** to combat ransomware on the targeted devices
- **Deception technology** to engage attacks in progress and slow their spread
- **Analytics and security information and event management (SIEM)** for collecting data and monitoring activity throughout the organization

The seven steps of the Lockheed Martin Cyber Kill Chain present multiple opportunities to thwart ransomware:

1. Reconnaissance: Identify the Targets
2. Weaponization: Prepare the Operation
3. Delivery: Launch the Operation
4. Exploitation: Gain Access to the Victim
5. Installation: Establish a Beachhead at the Victim
6. Command & Control (C2): Remotely Control the Implants
7. Actions and Objectives: Achieve the Mission's Goal[7]

Segment the network

If a threat gets into the network, it's critical not to let it move around unchecked, collecting information and causing damage. Network segmentation divides a network into smaller sections to stop threats from moving laterally. Each segment has its own access and security controls, letting organizations control the flow of traffic between sections. This also means that traffic in one segment can be stopped from entering another. Sensitive data can essentially be "walled off" from the rest of the network, protecting it from unauthorized access.

Speaking of access, network segmentation also enables control of who can access certain parts of the network, so even if a user's credentials are compromised, an intruder won't be able to reach critical data.

There are additional benefits of network segmentation such as improved performance and faster detection of suspicious activity. In the case of performance, segmentation reduces congestion and improves user experience. Simplifying traffic monitoring makes it easier to see suspicious activity, log events, and record connections. The chances of a missed threat are thus reduced.

Traditional technologies like virtual local-area networks (VLANs), which improve traffic management and access control lists, add a layer of security by acting as a firewall across subnets. These can help segment network traffic. However, they can be cumbersome to design, implement, and maintain for today's agile organizations. Dedicated network access control (NAC) solutions, paired with an NGFW, enables easier-to-use, granular control to reduce the risk of a widespread ransomware incident.

"Segmentation also plays a critical security role in securing dynamic multi-cloud environments, IoT, and BYOD strategies in today's highly distributed environments."[8]

“In 2021 and beyond, reactive security measures—typically cumbersome and costly—are no longer sufficient. Instead, proactive strategies that anticipate potential risks or vulnerabilities and prevent them before they even happen are required. One such strategy, network segmentation, is critical for any organization.”[9]

Put an incident response plan in place

Without a plan for what to do during a security event, response will be slow, causing far more damage and longer recovery time. A clearly defined and practiced incident response plan will go a long way to ensuring a better outcome in the event of a breach.

The SANS Institute has recommended a six-step plan, summarized below:

Step 1: Prepare

The most critical and most involved step is preparation. The main elements range from writing down the organization's policy, to the response plan, to the tools that will be used, to training.

Key steps include:

- Thinking through the potential impact the security incident may cause
- Informing internal executive, engineering, PR, and legal teams
- Communicating externally to incident response, law enforcement, and others
- Establishing a communications protocol

Step 2: Identify

This phase involves detecting and determining whether an incident has occurred. Error files and log messages must be gathered and the incident response plan process must be started.

In addition, an organization should work on:

- Identifying which ransomware variant has attacked
- Pinning down the initial entry, device, and time
- Assessing scope of the incident
- Determining if decryption tools exist

Step 3: Contain

At this point, a threat has been identified and the organization now must prevent any further damage. The incident response team will take action to enable short- and long-term containment, as well as system backup.

More specifically, it's critical to isolate the threat to stop it from spreading. If the ransomware is already widespread, it may be necessary to isolate traffic at the switch or the firewall edge, or even take down the internet connection temporarily. If the incident has only affected a few systems, isolating them at the device level by pulling the Ethernet or disconnecting the Wi-Fi are options.

Step 4: Eradicate

In step 4, the response team makes sure malicious content has been removed from affected systems and restores systems affected by the incident.

If all of the active malware and incidents of persistence have been identified, it may not be necessary to rebuild. However, it may just be easier and safer to create new, clean systems. Some organizations choose to build a totally separate, clean environment to migrate to.

Step 5: Recover

This is the stage when affected systems are brought back into the production environment. The systems must be tested, monitored, and validated to make sure they are not reinfected.

A ransomware attack will attempt to wipe online backups and volume shadow copies to decrease the chances of victims recovering their data and ultimately not paying the ransom. Organizations must ensure their backup technology was not affected by the incident and is still operational.

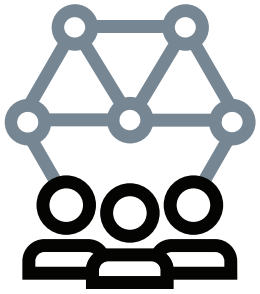
It's also possible that attackers planted malicious payloads in backups that will reinfect a clean system if used to restore. Organizations should try to restore systems from backups dated the day before the attack. And of course, backups must be scanned to determine their integrity.

Step 6: Learn

It's important to review and document the incident so improvements can be made to the organization's incident response plan. The report can also be used to train new employees and guide drills.

To help ensure continuous improvement of response and recovery capabilities, organizations should record both what went right and what went wrong during the attack. This is the best way to identify and understand opportunities for improvement.

For more details, visit the incident response page.



“Despite pace of the threat landscape, over a third of organizations leave a year or more between cyber crisis simulations and 42% don’t have regular cross-team incident planning.”[10]

Only a Proactive Approach Will Thwart Ransomware

It's difficult to imagine a day when ransomware will not be a major cybersecurity challenge. Security leaders need to be diligent and take many steps to reduce the risk of ransomware incidents, but with the right preparation, it is possible to stop ransomware—even after it's gotten into the network.

1 "Global Threat Landscape Report: A Semiannual Report by FortiGuard Labs," Fortinet, February 2021.

2 "Evolution of Ransomware-as-a-Service and Malware Delivery Mechanisms," Infosecurity, March 4, 2021.

3 Alexa Drake, "Your Data Is at Risk: Why Backup Is So Important," G2, January 24, 2020.

4 Aamir Lakhani, "Social Engineering in a Pandemic: How to Prevent Attacks," Fortinet, August 13, 2020.

5 "Online vaccine scams: INTERPOL and Homeland Security Investigations issue public warning," INTERPOL, March 24, 2021.

6 Derek Manky, "The Importance of Good Cyber Hygiene—Now More than Ever," Fortinet, October 26, 2020.

7 "Gaining the Advantage: Applying Cyber Kill Chain Methodology to Network Defense," Lockheed Martin, 2015.

8 Nirav Shah, "Why Network Segmentation Matters," Network World, February 24, 2020.

9 Mark Stone, "What is network segmentation? NS best practices, requirements explained," AT&T, March 15, 2021.

10 "Osterman Research Finds Cyber Crisis Preparation Failing to Adapt to Modern Threats, Leaving Nearly 40% of Security Leaders Without Confidence in Responders," Osterman Research, August 12, 2020.

FORTINET

www.fortinet.com

June 28, 2021 6:01 PM

1003516-0-0-EN