RANSOMWARE RESILIENCE SUMMIT USA

Benchmarking ransomware resilience and business continuity planning

RANSOMWARE RESISTANCE AND VENDOR MANAGEMENT

By The Cybersecurity Association of Maryland

Kisaco Research

RANSOMWARE RESILIENCE SUMMIT USA

CYBERSECURITY ASSOCIATION OF MARYLAND, INC.

Ransomware attacks have increased by 570% from 2015, with as many as 3 in 5 businesses suffering a ransomware attack according to statistics from Nasdaq and Mimecast. There have been almost 500 million attempted ransomware attacks in 2021 and SonicWall has speculated that the figure will rise to 714 million by the end of 2021. With ransomware being such a monumentally lucrative form of cyberattack, 2022 is likely to be marked by an even larger wave of ransomware attacks. Maintaining secure systems to safeguard against ransomware is more important now than ever.

How do supply chain vulnerabilities lead to ransomware attacks?

While ransomware is not a new threat, there has been an uptick in ransomware attacks on supply chains. Ransomware, which operates by encrypting the files on a device and demanding payment to the attacker before the files are released, is generally proliferated manually by attackers. However, when ransomware is deployed in a supply chain attack, its spread effectively becomes automatic. This type of attack occurs when the ransomware is placed into a software or other mode that is passed through a supply chain. Attackers use vendor supply chains as a vehicle to carry ransomware, targeting unsecure network protocols, unsafe coding practices, and unprotected server infrastructures. The targeted files are infected at the source and then sent out, unknowingly, by the vendor to their customers. Ransomware is elusive because it's able to go undetected and is alarmingly destructive because of its nearly irreversible nature.

The increasing prevalence of ransomware supply chain attacks necessitates the implementation of strengthened security protocols aimed at ensuring the protection of an enterprise on every level of the supply chain.

How can enterprises mitigate supply chain vulnerabilities?

There are several layers of protection against ransomware that organizations should incorporate into their strategy to mitigate supply chain vulnerabilities. This is top of mind for CAMI Advisory Council Member, Phil Mellinger, who serves as Vice President of Information Security & Information Security Officer for Tower Federal Credit Union. He shared six required controls against ransomware:

There are several layers of protection against ransomware that organizations should incorporate into their strategy to mitigate supply chain vulnerabilities. This is top of mind for CAMI Advisory Council Member, Phil Mellinger, who serves as Vice President of Information Security & Information Security Officer for Tower Federal Credit Union. He shared six required controls against ransomware:

The first layer is Border-Level Controls. Organizations should inspect received traffic to prevent ransomware from penetrating its security perimeter. This can be done via hardening and patching systems, encrypting storage, using up-to-date antivirus detection and removal, maintaining firewalls, runtime inspection, and relying on intrusion prevention to detect and prevent attacks within network traffic.

The second layer is Device-Level Controls. Organizations should ransomware functioning on internal devices. The steps for this are essentially the same as border-level controls.

The third layer is Network-Level Controls. Organizations should segment or partition their networks to prevent potential lateral movement of ransomware across networks. Internal network routers and switches should be protected by hardening and patching systems, using firewalls, and deploying other segmentation tools.

The fourth layer is Storage-Level Controls. Organizations

should maintain backups to enable recovery from ransomware attacks that prove successful. Backups are crucial for organizations to maintain because data stolen in a ransomware attack cannot always be recovered. It is best practice to store backups off-network.

The fifth layer is Employee-Level Controls. Organizations should maintain security awareness programs for training their employees about ransomware attacks. Regular security assessments should be conducted, such as phishing-by-email tests, to ensure that employee security training against ransomware is effective.

The sixth and final layer is Incident Response Controls. Organizations should maintain an incident response plan that is responsive to ransomware attacks. Testing and exercises should regularly be used to validate the effectiveness of incident response plans against ransomware.

Redundancy is key when protecting against ransomware--if one layer of security is compromised, each of the others will act as a failsafe.

How can enterprises help their supply chain improve their security?

The first step for enterprises to improve supply chain security is to properly assess security risks.

One Fortune 100 company in a highly-regulated industry shared a series of questions they ask their vendors who have exposure to any restricted or confidential information. These questions include:

1. Does the vendor have an industry-recognized Information Security Policy published and available to all employees and contractors?
2. Is there an obligation for employees of the vendor to follow the Information Security Policy as a condition of their employment?
3. Are there written policies and guidelines for monitoring and maintaining the security of customer data?
4. Does the vendor use antivirus software on all devices that are either corporate devices or used by employees to access company information?
5. Does the vendor regularly update and define its anti-virus signature?
6. Does the vendor contract with subcontractors or fourth-party vendors for the development or delivery of services?
7. Are background checks conducted by the vendor for every employee?

In developing these questions, the company conducted focus groups with their vendors. They quickly learned that outside support was often needed for their vendors to complete the assessment and subsequently perform remediation.

We have partnered with this company to curate a list of coaches who can help their vendors understand their vulnerabilities and improve their security posture, ultimately protecting our critical infrastructure.

Ransomware in the Future

While there is no surefire way to eliminate the possibility of being targeted by ransomware, maintaining a fortified and overlapping security system and keeping each individual in a company and its partners educated on how to protect themselves from ransomware attacks can lead to exponentially higher chances of avoiding the theft and encryption of its files. Following guidelines such as those provided above can significantly reduce the risk of an enterprise losing its data.