Secure Backup

Your Last Line Of Defense Against Ransomware

The Rise Of Ransomware

THE RISE OF RANSOMWARE

64% of IT leaders cite improved data security for their organization as their top objective over the next 12 months.[1]

It should be no surprise that 71% of cybersecurity experts are more worried about ransomware attacks as a result of Covid-19.[2] Cybercrime has risen dramatically due to the expanding threat landscape and the evolution of cyberattacks. The global pandemic caused accelerated digital transformation and rapid migration to the cloud as employees and networks became more distributed. Effectively securing infrastructure and data has become increasingly complex. Threat actors have focused on exploiting vulnerabilities across remote endpoints and cloud workloads. Remote work has left many employees more vulnerable to email phishing. The frequency and severity of ransomware attacks has increased in the past two years and there is little evidence of reprieve.

During the first year of the pandemic, ransomware attacks increased by nearly 500%.[3] Not only must organizations work to understand all potential attack vectors and secure themselves against these pathways and methods, but they must enhance their security strategies with increased cyber resiliency so that they can recover quickly should an attack occur.

Interactive poll not supported

View online version

veeam
Value-Added
Reseller
Platinum

The Evolution Of Ransomware

THE EVOLUTION OF RANSOMWARE

Ransomware is defined as cyber extortion that occurs when malicious software infiltrates computer systems and encrypts data, holding it hostage until the victim pays a ransom.[4]

Cyber extortion, and ransomware in particular, has become increasingly profitable and easier to execute. Cryptocurrencies have enabled cyber criminals to extort payment anonymously. Early in the pandemic, threat actors adopted new ransomware attack methods in which a company's data was stolen and encrypted, and the attacker threatened to publish the stolen data. This method is known as double extortion, as it helps to ensure that a payment is made even when an organization is able to restore their data from backup themselves.

As payouts from ransomware continue to skyrocket, attackers have employed a triple extortion technique, where they also demand payment from those who may be affected by the leaking of data stolen from another company. In addition, ransomware as a service (RaaS) is a subscription-based model that has recently become popular. RaaS enables cybercriminals with little technical knowledge to purchase or rent already existing ransomware tools to deploy against targets, which has increased the frequency of attacks.

Strengthen Your Backup Environment

Ransomware: Not If But When

RANSOMWARE ATTACKS: NOT IF BUT WHEN

The rapid evolution of the cyber threat landscape during the pandemic has shifted the question for most companies from *if* to *when* they will be a victim of cybercrime.

An increasing number of ransomware attacks are neither targeted, nor are they sophisticated. Cyber criminals are often looking for the most vulnerable firms and focus their efforts on where there is the best chance of receiving a payout for the least effort. In a recent year-long study of ransomware attack campaigns, 75% used social engineering (phishing emails) to propagate, while 25% of them involved exploiting a vulnerability in remote access software.[5] Email phishing, remote access, and exploited vulnerabilities constitute the top modes of ransomware entry.

Any host not kept up to date on a network can be an entry point for attack through an exploited vulnerability, in particular zero-day vulnerabilities for which there are no patches or updates. In addition, threat actors compose convincing email phishing campaigns using information publicly available on the internet. Cyber criminals have become increasingly innovative with how they use stolen identities and credentials to bypass legacy defenses. Once a foothold is gained on the machine of an employee though email phishing, the attacker can pivot and gain control of other devices and potentially compromise the entire network.

READ: The Future Of Disaster Recovery: Three Reasons Enterprises Need DRaaS

Ransomware Defense: Prepare For An Attack

RANSOMWARE DEFENSE: PREPARE FOR AN ATTACK

Preventative measures include implementing security-related internet access changes, making it more difficult for attackers to infiltrate a network. Many organizations are investing in detection technologies, which are designed to quickly discover the presence of ransomware.

Multiple layers of resiliency should be in place, because if an attack occurs, there is no guarantee that the stolen data will be recovered if the ransom is paid. IT teams should implement or bolster backup and recovery solutions that leverage ultra-resilient media. These are media types that are offline, air-gapped, or immutable. Having one or more copies of backup data with one (or more) of these characteristics is critical to a successful recovery from ransomware. Further, it is important to have an orchestration and automation solution in place to aid response and recovery.[6]

Interactive poll not supported

View online version

The Best Practices For Ransomware Protection

BEST PRACTICES FOR RANSOMWARE PROTECTION: NIST CYBERSECURITY FRAMEWORK

Drafted by the National Institute of Standards and Technology (NIST), this cybersecurity framework (CSF) provides a uniform set of rules, guidelines, and standards for organizations of all sizes and all industries.[7]

The NIST CSF and its five functions – identify, protect, detect, respond, and recover – is widely considered to be the default standard for building a robust cybersecurity program. The NIST framework can be applied to help businesses identify and prioritize opportunities for improving their security and resilience against ransomware attacks.[8] Let's take a look at how the five NIST functions apply to ransomware risk management and preparedness and examine some best practices.

BEST PRACTICES CONTINUED >

NIST CYBERSECURITY FRAMEWORK

1. Identify

The identify function focuses on developing an understanding of your environment to manage cybersecurity risk to systems, assets, data, and capabilities. Organizations should identify all assets, processes, networks, and environments, the risks associated with each, and which are critical to business function. A strong asset management program is essential, as cybercriminals are looking to exploit overlooked and neglected infrastructure elements.

Technology alone can't strengthen a company's cybersecurity posture. Many breaches are due to human error caused by carelessness, simple mistakes, or lack of knowledge of cyber threats and how cybercriminals operate. Evaluation of your organization's cybersecurity maturity awareness can identify knowledge gaps within your workforce; email phishing simulation testing is particularly relevant and useful. Full visibility over all employees, processes, and technology is critical for organizations to fortify themselves against ransomware.

BEST PRACTICES CONTINUED >

NIST CYBERSECURITY FRAMEWORK

2. Protect

Protecting your organization against ransomware involves employing multiple layers of defense. Understanding current attack vectors makes it easier to take the correct countermeasures. Organizations should focus on hardening security with respect to phishing, remote access (RDP), and software updates, as these are the three main entry mechanisms for cybercriminals. Regular staff training and education around cybersecurity is a highly effective and efficient way to protect against ransomware attacks.

Proper backups ensure that cyberthreats become more of an inconvenience than a disaster. Best practice includes following the 3-2-1 data protection rule: keep three copies of each important piece of data, backup data should be stored on two different media types, and one copy of data should be replicated offsite. Retaining backups from multiple points in time is critical to ensure that a copy free from ransomware is available.

Network segmentation can reduce the attack surface as it divides infrastructure into smaller sub-networks or network segments with limited interconnectivity between them, restricting the lateral movement of ransomware. Subnets or zones containing the most valuable data can be fortified with additional layers of defense, including restricting network traffic and access privileges to only when it is essential. Best security practice includes ensuring that ports and protocols not needed for business purposes are locked down. Limiting traffic though firewalls using whitelisting and default deny rules can also provide protection against ransomware.

Devices connected to the network, as well as access to the network should be kept up to date and secure as cybercriminals often gain entry though finding and exploiting vulnerabilities on software, hardware, and firmware that is not patched or updated.

BEST PRACTICES CONTINUED >

NIST CYBERSECURITY FRAMEWORK

3. Detect

The detect function allows for the timely discovery of cyberthreats. The faster a cyber event is detected, the sooner it can be mitigated. Prompt ransomware discovery centers around deploying antivirus and malware detection software and keeping the signatures up to date, as well as monitoring accounts, infrastructure, and network traffic. Early identification of ransomware attempts is possible through monitoring for cybersecurity events that commonly occur prior to ransomware attacks, such as a flurry of spam emails with links to unknown websites. Timely detection can also occur though monitoring firewalls, endpoints, critical files, device logs, and user accounts for non-authorized changes, signs of compromise, and abnormal behavior.

BEST PRACTICES CONTINUED >

NIST CYBERSECURITY FRAMEWORK

4. Respond

The respond function develops your organization's ability to quickly react to a ransomware attack with the goals of containing and mitigating the impact as well as maintaining business continuity. Creating an incident response plan that outlines priorities, running incident response tabletop exercises, and having the appropriate response tools and protocols in place can help your organization to be prepared and remain calm in the event of a cyberattack. Best practice also includes implementing an automated disaster recovery solution, such as the Veeam® Disaster Recovery Orchestrator.

BEST PRACTICES CONTINUED >

NIST CYBERSECURITY FRAMEWORK

5. Recover

The recover function supports timely recovery to normal operations, which reduces the impact of a ransomware attack. Preparedness involves hardening your organization’s digital resilience through a robust backup system, as well as having a tested recovery strategy in place. Backup systems should be designed with recovery in mind and data should not be accessible by an attacker; offsite (air-gapped) or read-only (immutable) copies are crucial for recovery.

BEST PRACTICES CONTINUED >

Automated Recovery From Ransomware

AUTOMATED RECOVERY FROM RANSOMWARE

Veeam® Disaster Recovery Orchestrator (Orchestrator) takes recovery to the next level by automating your disaster recovery (DR) processes. Orchestrator provides critical capabilities for response functions needed to recover from disasters of many types, including ransomware.

It is a powerful add-on to Veeam Backup & ReplicationTM and the perfect complement to Veeam ONETM. [9, 10, 11]

Orchestrator also extends the functionality of Veeam Availability SuiteTM to orchestrate disaster recovery processes in VMware vSphere environments, NetApp, and HPE storage system, and to support one-click recovery for critical applications. Orchestrator enables you to streamline and automate your DR planning and testing with a simple tool, no matter the workload you are protecting.

Orchestrator leverages the backup, replication, failover, and restore capabilities of Veeam Backup & Recovery to build DR workflows, automate recovery processes, and eliminate error-prone manual steps. Orchestrator also provides reporting capabilities that let enterprises document their DR plans to meet compliance requirements. With Orchestrator, you can do the following:

- **Orchestrate disaster recovery:** Create workflows to orchestrate recovery operations for both Veeam Backup & Replication backups and replicas, and for replicated storage snapshots created on storage systems.
- **Automate DR testing:** Build test schedules to automate the verification of orchestration plans, with isolated and low impact testing of VM backups, replicas, applications, and storage snapshots.
- **Meet DR compliance requirements:** Generate and automatically update documentation for DR procedures, eliminating the problem of outdated DR plans.

AUTOMATED RECOVERY FROM RANSOMWARE

As part of plan creation, a DR plan document is automatically generated along with a full audit log of changes as they occur. This saves time and reduces the risk of human error as well as issues with configuration drift. DR tests in Orchestrator can be scheduled to run daily or on demand. Test reports indicate if the target Recovery Point Objective (RPO) and Recovery Time Objective (RTO) are both met.

Application verification ensures that common enterprise applications are functioning as expected after recovery. The testing environment can be left running after a test to provide access to a copy of production data, which can be leveraged for patch and application testing and security scanning to further enhance security efforts.

Plans in Orchestrator are automatically checked to ensure that the environment is ready for failover at any moment, which allows organizations to confidently recover when needed. As testing DR plans is key to ensuring that they can be used to successfully recover from ransomware, automated verification and reporting can help organizations to meet internal and external compliance initiatives. One-click recovery allows for the recovery of single apps or an entire site from anywhere with a single click from the web interface. Orchestrator enables your organization to be ready to recover your whole environment at a moment’s notice.

Conclusion

CONCLUSION

Cybercrime is a highly successful and profitable industry; the incidence of ransomware attacks is on the rise, and ransom demands are increasing. In fact, 73% of companies have suffered at least one ransomware attack in the past 24 months.[12] Rapid and reliable recovery from ransomware is an integral part of the overall cybersecurity incident response process.

Verified, tested, and secure backups are your last line of defense against ransomware. When considering automation and orchestration recovery solutions, WEI can help you take your disaster recovery preparedness to the next level with Veeam DR Orchestrator.[13]

Talk to WEI today
Contact the Veeam and cybersecurity experts at WEI to find out how you can win the war against ransomware hackers. Remember, it's not if but when ransomware will strike.

ABOUT WEI
At WEI, we're passionate about solving your technology problems and helping you drive your desired business outcomes. We believe in challenging the status quo and thinking differently. There are a lot of companies that can take today's technology and create a great IT solution for you. But we do more. We go further.

And we have the customer, vendor and industry awards to prove it. WEI is a premier technology partner, who always puts our customers first while providing the most innovative solutions for over 30 years.

Sources:

1. Foundry Research commissioned by WEI, December 2021.
2. CrowdStrike, 2022 Global Threat Report: https://www.crowdstrike.com/global-threat-report/
3. Bitdefender, 2020 Consumer Threat Landscape report: https://www.bitdefender.com/files/News/CaseStudies/study/395/Bitdefender-2020-Consumer-Threat-Landscape-Report.pdf
4. Gartner, 6 Ways to Defend Against a Ransomware Attack: https://www.gartner.com/smarterwithgartner/6-ways-to-defend-against-a-ransomware-attack
5. Allianz – Cyber Insights, Ransomware Trends – Risks and Resilience: https://www.agcs.allianz.com/news-and-insights/news/cyber-risk-trends-2021-press.html
6. 6,7. Veeam, 5 Ransomware Protection Best Practices: https://www.veeam.com/wp-protection-yourself-from-ransomware.html
7. NIST, Ransomware Risk Management – A Cybersecurity Framework Profile: https://www.nist.gov/publications/ransomware-risk-management-cybersecurity-framework-profile
8. Veeam, 5 Ransomware Protection Best Practices: https://www.veeam.com/wp-protection-yourself-from-ransomware.html
9. Veeam, Product Overview – Veeam Disaster Recovery Orchestrator: https://www.veeam.com/disaster-recovery-orchestrator.html
10. Veeam Disaster Recovery Orchestrator 5.0:
11. https://helpcenter.veeam.com/docs/vdro/userguide/welcome.html?ver=50
12. Cybereason, 2022 Ransomware – The True Cost to Business: https://www.cybereason.com/ransomware-the-true-cost-to-business-2022
13. Veeam, Ransomware – Secure Backup is Your Last Line of Defense: https://www.veeam.com/blog/secure-backup-ransomware-defense.html

Thank you for reading

Secure Backup: Your Last Line of Defense Against Ransomware