5 ESSENTIAL STEPS FOR A

RANSOMWARE PROTECTION PLAN

Infrascale™

Infrascale™ © | +1.877.896.3611 | www.infrascale.com

Infrascale™

EBOOK

The Expanding Threat of Ransomware to MSPs

Ransomware attacks continue to evolve, and managed service providers (MSPs) are increasingly becoming prime targets. According to the Verizon 2024 Data Breach Investigations Report (DBIR), ransomware and extortion techniques accounted for nearly one-third (32%) of all breaches. The report also highlights a 180% increase in attacks exploiting vulnerabilities, with ransomware actors leveraging these methods. The human element remains a significant factor, contributing to 68% of breaches, emphasizing the need for comprehensive security measures across all organizational levels (Verizon 2024 DBIR).

Targeting MSPs and Their Clients

MSPs are attractive targets for ransomware actors due to their ability to infiltrate multiple client networks through a single point of entry. Many small and medium-sized businesses (SMBs), which make up a significant portion of MSPs' client base, mistakenly believe they are less likely to be targeted due to their size. However, the reality is starkly different. According to the 2024 DBIR, 47% of cyberattacks are aimed at small businesses. SMBs often lack the extensive cybersecurity infrastructure of larger enterprises, making them attractive targets. Moreover, ransomware attacks on SMBs are less publicized due to differing reporting regulations.

Example MSP Ransomware Attacks

REvil: The FBI and cybersecurity firm Huntress have reported that Kaseya fell victim to a supply chain ransomware attack affecting multiple MSPs and their customers. Huntress attributes the attack to an authentication bypass vulnerability in Kaseya's VSA software, which allowed the attackers to upload and execute malicious code.

BlackCat: a new ransomware variant, targeted several MSPs, including MSP360 and N-able. The attack affected over 100 MSPs and their clients, resulting in significant data loss and downtime. The attackers demanded ransoms ranging from $500,000 to $7 million to decrypt the affected systems.

AvosLocker: Targeted a California-based MSP was targeted by a ransomware attack that affected several of its clients, including a local government agency. The attack encrypted data and demanded a ransom of $1.5 million.

Targeting Data of All Types

While payment data remains a valuable target, attackers have broadened their scope. The DBIR notes, "Attackers are increasingly targeting any data that will impact the victim organization's operations." This shift aims to increase the likelihood of ransom payments by exploiting the critical nature of various data types.

The Rise of Ransomware-as-a-Service (RaaS)

The ransomware threat is further compounded by the rise of ransomware-as-a-Service (RaaS). This model lowers the barrier to entry for cybercriminals, allowing them to purchase ready-made ransomware tools and infrastructure. As a result, even those with minimal technical expertise can launch sophisticated attacks.

The Need for Comprehensive Protection

Given ransomware threats' diverse and pervasive nature, MSPs must adopt a holistic protection strategy. This includes not only preventing attacks but also ensuring robust recovery capabilities. The following sections outline a comprehensive ransomware protection plan, starting with identifying critical assets and risks.

5 ESSENTIAL COMPONENTS OF A RANSOMWARE PROTECTION PLAN

The NIST Cybersecurity Framework (CSF) provides a structured and flexible approach to managing and reducing cybersecurity risks. It is organized into five core functions: Identify, Protect, Detect, Respond, and Recover. Here's how MSPs can apply these steps to safeguard their clients:

01 IDENTIFY

Understanding Your Assets and Risks

Conduct a thorough inventory of you, and your clients' assets, including hardware, software, data, and critical systems. Assess the potential impacts of different cyber incidents on operations and compliance requirements. Identify threats and vulnerabilities specific to you and your clients' environments. The updated NIST CSF emphasizes the importance of a thorough risk assessment:

> “
>
> Understanding the business context, the resources that support critical functions, and the related cybersecurity risks enables an organization to focus and prioritize its efforts, consistent with its risk management strategy and business needs.

Conducting a Comprehensive Risk Assessment

A comprehensive risk assessment involves several steps:

Inventory Assets:
Catalog all hardware, software, data, and other critical assets. This includes understanding where data is stored, processed, and transmitted.

Identify Threats and Vulnerabilities:
Assess potential threats to your assets and the vulnerabilities that could be exploited. This involves reviewing historical data and industry reports and conducting vulnerability scans.

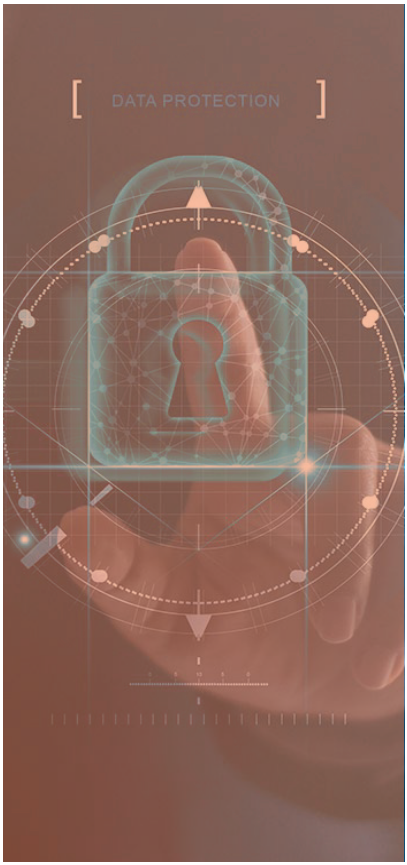
Evaluate Potential Impacts:
Determine the potential impacts of different cyber incidents. This includes direct and indirect impacts (e.g., data loss and system downtime) (e.g., reputational damage and regulatory fines).

By thoroughly understanding and evaluating your assets, threats, and risk tolerance, you can make informed decisions to effectively protect your organization and ensure business continuity.

02 PROTECT

Creating and Maintaining Safeguards

Implement technical and administrative safeguards to prevent cybersecurity incidents. Key practices include:



Least Privilege:
Ensure that users and systems have only the permissions necessary to perform their tasks. This reduces the potential for attackers to spread laterally across the network.

Multi-Factor Authentication (MFA):
The FBI recommends MFA as a crucial step to minimize ransomware risks.

Up-to-Date Security Solutions:
Regularly update antivirus software and other security tools to protect against the latest threats.

Zero Trust Architecture
Adopt a Zero Trust approach, which focuses on securing applications and data rather than just the network. According to Gartner,

> “Zero trust architecture (ZTA) represents a shift in network security, emphasizing the need for granular access controls and continuous verification of trust.

Endpoint Protection
Endpoints are common targets for ransomware attacks. Ensure comprehensive endpoint protection, including updating and patching operating systems and applications. Utilize IT policy management tools to enforce software versioning and patch management.

Backup and Disaster Recovery
A comprehensive backup and disaster recovery solution is essential because no system is entirely un-hackable. Disaster Recovery as a Service (DRaaS) can provide backup and recovery capabilities using third-party cloud environments. Regularly test backups and conduct drills to ensure preparedness.

03 DETECT

Detect and Continually improve

Monitoring and Anomaly Detection
Implement continuous monitoring to detect abnormal or malicious activity. Early detection allows for prompt action to isolate and mitigate threats. Endpoint Detection and Response (EDR) tools can detect and alert on suspicious behavior, providing a critical layer of protection.

Continuous Improvement

The NIST CSF emphasizes the need for ongoing improvement. Regularly evaluate and update your security measures to address new threats and vulnerabilities. Use feedback from incidents to enhance your detection and response capabilities.

Enhancing Backup and Disaster Recovery

Backup and Disaster Recovery (BDR) is an essential component of a robust cybersecurity strategy, providing the means to recover from ransomware attacks and other catastrophic events.your detection and response capabilities.

Automated Backups

- Implement a backup solution that supports automated, regular backups of all critical data and systems. This ensures data is always up-to-date and can be quickly restored.

- Utilize incremental backups to reduce storage requirements and speed up the backup process.

Offsite and Cloud-Based Backups

- Store backups in multiple locations, including offsite and cloud-based environments, to protect against physical disasters and localized ransomware attacks.

Backup and Disaster Recovery

- Implement tools that regularly verify the integrity of backups to ensure they are complete and uncorrupted.
- Use anomaly detection to identify unusual patterns in backup data that might indicate a ransomware infection or other malicious activity. This can trigger alerts and preemptive actions.

Regular Testing and Drills

- Conduct regular tests and drills of your backup and disaster recovery plans to ensure that all processes work as intended and that staff are familiar with their roles during an incident.
- Use these exercises to identify any gaps or weaknesses in the plan and make necessary improvements.

Comprehensive Recovery Planning

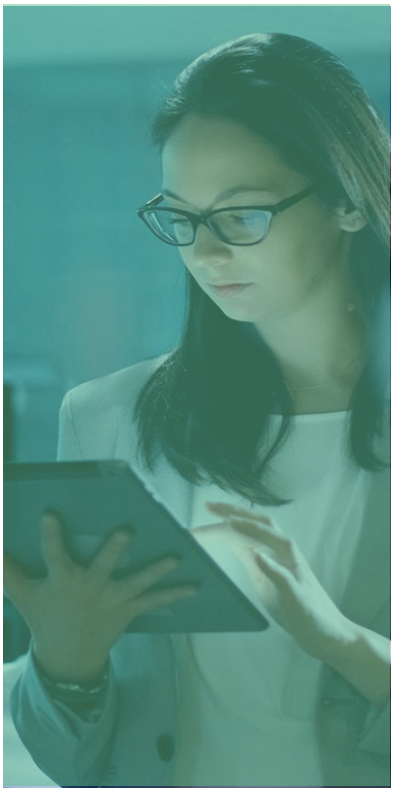
- Develop detailed recovery plans that include step-by-step procedures for restoring data and systems from backups. Ensure these plans are well-documented and accessible to all relevant personnel.

- To ensure comprehensive coverage, include provisions for restoring data in SaaS applications, endpoints, and mobile devices.

04 RESPOND

Incident Response Planning

Develop and practice an incident response plan to contain and mitigate the impact of security events.



Key steps include:

Identify the Infection Timeline

- Forensic Analysis: Perform a detailed forensic analysis to determine when the infection occurred by examining system logs and security alerts.
- Establish a Timeline.
- Document events leading up to the detection of the ransomware to understand the scope and spread.

Minimize Damage

- Endpoint Detection and Response (EDR): Utilize EDR tools to generate real-time alerts and identify, isolate, and remove infected systems.
- Network Segmentation: Implement network segmentation to limit the spread of ransomware by separating critical systems from less critical ones.
- Quarantine Infected Systems: Disconnect infected systems from the network to prevent further spread, ensuring backups are also isolated.

Employee Communication

- Immediate Notification: Inform employees about the ransomware attack and provide clear instructions on securing their data.
- Training and Awareness: Conduct regular training sessions to educate employees on identifying phishing attempts and suspicious links.
- Incident Updates: Regularly update employees throughout the incident response process.

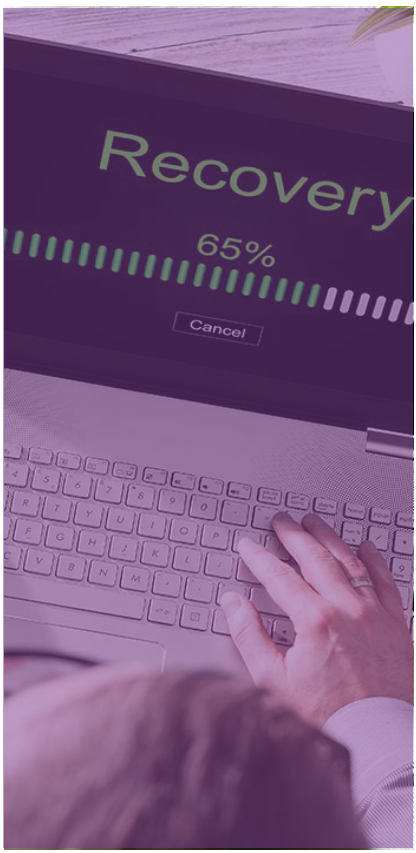
Coordination and Communication with External Entities

- Compliance Reporting: Report the incident to relevant regulatory bodies if required.
- Public Relations: Prepare a communication strategy for informing stakeholders and the public.
- Cybersecurity Experts: Engage cybersecurity experts to assist in the response and recovery process.

05 RECOVER

Restoration and Prevention of Reinfection

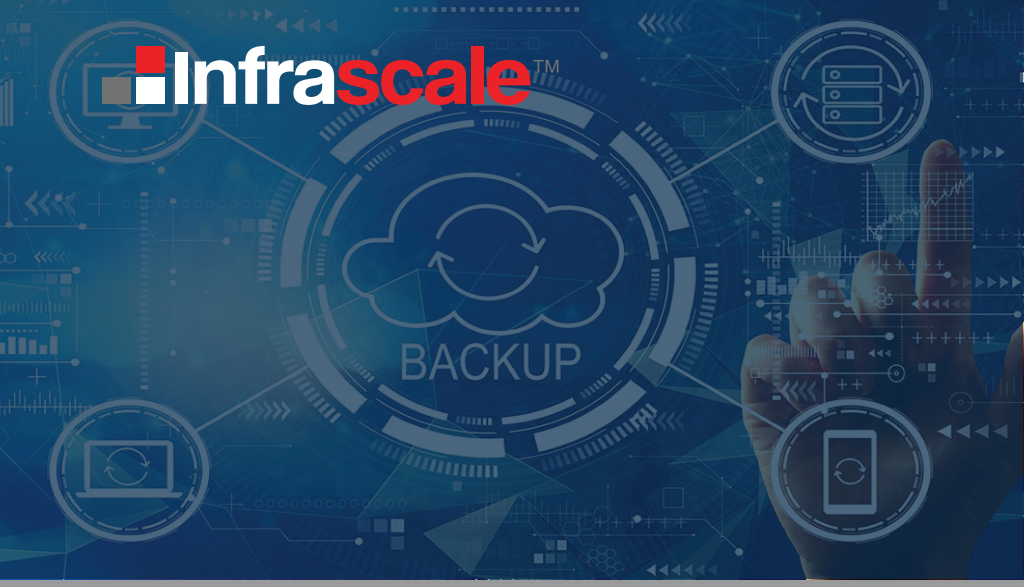
Implement a robust cyber resilience program, including backup and restoration strategies for onpremises, cloud, and SaaS data.



- **Documentation and Reporting:** Maintain detailed records of the incident, including response actions taken and communications. Report the incident to relevant regulatory bodies if required.
- **Comprehensive Recovery Planning:** Develop detailed recovery plans that include stepby-step procedures for restoring data and systems from backups.
- **Preventing Reinfection:** Ensure complete removal of ransomware to avoid recurring infections.
- **Regular Testing and Drills:** Conduct regular tests and drills of your backup and disaster recovery plans.
- **Post-Incident Review:** Discuss the incident, lessons learned, and improvements to prevent future attacks.
- **Continuous Improvement:** DUse incident feedback to update your protection plan and enhance your security measures.

Protect Your Business and Clients from Ransomware

By focusing on these strategies, MSPs can enhance their ability to recover from ransomware attacks and prevent future incidents, ensuring business continuity and data integrity for themselves and their clients.



About Infrascale

Infrascale provides comprehensive, cloud-based data protection of SaaS applications, endpoint devices, and servers by removing the barriers and complexity of secure, offsite data storage, and standby infrastructure for real-time disaster recovery.

Partners and customers choose Infrascale because we empower them to manage multiple products from a single dashboard. Our tools are easy to use and backed by award-winning technical support.

Infrascale offers multiple ways to protect your business:

Backup SaaS Applications Protect Microsoft 365, Google Workspace, Box, Dropbox, and Salesforce data from accidental deletion, malicious attacks and limited retention policies.

Protect Endpoints and Devices Direct-to-cloud backup and recovery solution for mobile devices, laptops, or remote offices.

Prepare for Anything with Disaster Recovery Ensure your entire environment is boot-ready in minutes to recover from outages, failures, or ransomware attacks. Learn more at infrascale.com

Infrascale™

Infrascale HQ
12110 Sunset Hills Road, Suite 600
Reston, VA 20190
United States

Contact us:

877-896-3611
www.infrascale.com
team@infrascale.com