July 14, 2021

Mitigations and Hardening Guidance for MSPs and Small- and Mid-sized Businesses

The Threat and How to Think About It

Cyber threat actors, including state-sponsored advanced persistent threat (APT) actors, increasingly target managed service providers (MSPs). MSPs provide remote management of customer IT and end-user systems. A large number of small- and mid-sized businesses use MSPs to manage IT systems, store data, or support sensitive processes. MSPs typically enable customers to scale and support network environments at a lower cost than if the customer were to manage these resources themselves.

MSPs generally have direct access to their customers' networks and data, which makes them a valuable target for cyber actors. These actors can exploit trust relationships in MSP networks and gain access to a large number of the victim MSP's customers. Compromises of MSPs can have globally cascading effects and introduce significant risk—such as ransomware and cyber espionage—to their customers.

Mitigations and Hardening Guidance for MSPs

The Cybersecurity and Infrastructure Security Agency (CISA) recommends the following mitigations and hardening guidance:

- Apply the principle of least privilege to customer environments.
- Ensure that log information is preserved, aggregated, and correlated to maximize detection capabilities.
- Implement robust network- and host-based monitoring solutions.
- Work with customers to ensure hosted infrastructure is monitored and maintained.
- Manage customer data backups.
    - Prioritize backups based on business value and operational needs, while adhering to any customer regulatory and legal data retention requirements.
    - Develop and test recovery plans, and use tabletop exercises and other evaluation tools and methods to identify opportunities for improvement. See CISA's Cyber Resilience Review resources for guidance on conducting a non-technical evaluation of your organization's operational resilience and cybersecurity practices.
    - Review data backup logs to check for failures and inconsistencies.

Mitigations and Hardening Guidance for Small- and Mid-Sized Businesses

CISA recommends the following mitigations and hardening guidance:

- Manage supply chain risks.
    - Understand the supply chain risks associated with your MSP, such as network security expectations.
    - Manage risk across your security, legal, and procurement groups.
    - Use risk assessments to identify and prioritize allocation of resources and cyber investment.
- Implement strong operational controls.
    - Create a baseline for system and network behavior to detect future anomalies; continuously monitor network devices' security information and event management appliance alerts.
    - Regularly update software and operating systems.
    - Integrate system log files—and network monitoring data from MSP infrastructure and systems—into customer intrusion detection and security monitoring systems for independent correlation, aggregation, and detection.

  - Employ a backup solution that automatically and continuously backs up critical data and system configurations. Store backups in an easily retrievable location that is air-gapped from the organizational network.
  - Require multi-factor authentication (MFA) for accessing your systems whenever possible.
- Manage architecture risks.
  - Review and verify all connections between customer systems, service provider systems, and other client enclaves.
  - Use a dedicated virtual private network (VPN), to connect to MSP infrastructure; all network traffic from the MSP should only traverse this dedicated secure connection.
- Manage authentication, authorization, and accounting procedure risks.
  - Adhere to best practices for password and permission management.
  - Ensure MSP accounts are not assigned to administrator groups and restrict those accounts to only systems they manage. Grant access and admin permissions based on need-to-know and least privilege.
  - Verify service provider accounts are being used for appropriate purposes and are disabled when not actively being used.
- Review contractual relationships with all service providers. Ensure contracts include:
  - Security controls the customer deems appropriate;
  - Appropriate monitoring and logging of provider-managed customer systems;
  - Appropriate monitoring of the service provider's presence, activities, and connections to the customer network; and
  - Notification of confirmed or suspected security events and incidents occurring on the provider's infrastructure and administrative networks.
- Implement CISA's Cyber Essentials to reduce your organization's cyber risks.

Resources

- For technical resources with more detailed information on hardening MSP and customer infrastructure in response to general and specific cyber threats, refer to:
  - CISA webpage: Kaseya Ransomware Attack: Guidance for Affected MSPs and their Customers
  - CISA webpage: APTs Targeting IT Service Provider Customers
  - CISA Technical Alert: TA17-117A: Intrusions Affecting Multiple Victims Across Multiple Sectors
  - CISA Technical Alert: TA18-276A: Using Rigorous Credential Control to Mitigate Trusted Network Exploitation
  - CISA Technical Alert: TA18-276B: Advanced Persistent Threat Activity Exploiting Managed Service Providers
  - National Cybersecurity Center of Excellence (NCCoE): Improving Cybersecurity of Managed Service Providers
  - Australian Cyber Security Centre: Managed Service Providers: How to manage risk to customer networks
  - Canadian Centre for Cyber Security Alert: Malicious Cyber Activity Targeting Managed Service Providers
- CISA's Cyber Essentials is a guide for leaders of small businesses as well as leaders of small and local government agencies to develop an actionable understanding of where to start implementing organizational cybersecurity practices.
- For general incident response guidance, see Joint Cybersecurity Advisory AA20-245A: Technical Approaches to Uncovering and Remediating Malicious Activity.
- CISA offers a range of no-cost cyber hygiene services to help organizations assess, identify, and reduce their exposure to threats. By requesting these services, organizations of any size could find ways to reduce their risk and mitigate attack vectors.

CISA's Role as the Nation's Risk Advisor

CISA collaborates with industry and government partners to help organizations understand and counter critical infrastructure and cybersecurity risks associated with the malicious activities of nation-state and non-state actors. CISA provides recommendations to help partners stay vigilant and protected against potential foreign influence operations.