THREAT BULLETINS

Joint Cybersecurity Advisory – Protecting Against Cyber Threats to Managed Service Providers and their Customers

TLP:WHITE

May 11, 2022

On May 11, 2022, the cybersecurity authorities of the United Kingdom, Australia, Canada, New Zealand, and the United States released a joint Cybersecurity Advisory (CSA) (AA22-131A) to provide guidance on how to protect against malicious cyber activity targeted managed service providers (MSPs) and their customers. The report was created in response to an observance of increased activity against MSPs and their customers in which malicious operations are expected to continue.

The advisory provides actions MSPs and their customers can take to reduce their risk of falling victim to a cyber attack including. Additionally, the advisory shares cybersecurity best practices for information and communications technology (ICT) services and functions, to include guidance that allows transparency between MSPs and their customers to secure sensitive data.

All members are encouraged to review AA22-131A: Protecting Against Cyber Threats to Managed Service Providers and their Customers.

The joint Cybersecurity Advisory (CSA) identifies MSPs as entities that deliver, operate, or manage ICT services and functions for their customers via a contractual arrangement, such as a service level agreement (SLA). In addition to offering their own services, an MSP may offer services in conjunction with those of other providers. Offerings may include platform, software, and IT infrastructure services; business process and support functions; and cybersecurity services. MSPs typically manage these services and functions in their customer's network environment either on the customer's premises or hosted in the MSP's data center.

MSPs provide services that usually require both trusted network connectivity and privileged access to and from customer systems. Many organizations, ranging from large critical infrastructure organizations to small- and mid-sized businesses, use MSPs to manage ICT systems, store data, or support sensitive processes. Many organizations make use of MSPs to scale and support network environments and processes without expanding their internal staff or having to develop the capabilities internally.

Threat Actors Targeting MSP Access to Customer Networks:

Whether the customer's network environment is on premises or externally hosted, threat actors can use a vulnerable MSP as an initial access vector to multiple victim networks, with globally cascading effects. The UK, Australian, Canadian, New Zealand, and U.S. cybersecurity authorities expect malicious cyber actors, including state-sponsored advanced persistent threat (APT) groups, to increase activities targeting MSPs in their efforts to exploit provider-customer network trust relationships. For example, threat actors successfully compromising an MSP could enable follow-on activity, such as ransomware and cyber espionage against the MSP as well as across the MSP's customer base.

The UK, Australian, Canadian, New Zealand, and U.S. cybersecurity authorities have previously issued general guidance for MSPs and their customers. This advisory provides specific guidance to enable transparent, well-informed discussions between MSPs and their customers that center on securing sensitive information and data. These discussions should result in a re-evaluation of security

processes and contractual commitments to accommodate customer risk tolerance. A shared commitment to security will reduce risk for both MSPs and their customers, as well as the global ICT community.

Reference(s)	CISA
Report Source(s)	CISA

Recommendations

The UK, Australian, Canadian, New Zealand, and U.S. cybersecurity authorities recommend

Prevent initial compromise

In their efforts to compromise MSPs, malicious cyber actors exploit vulnerable devices and internet-facing services, conduct brute force attacks, and use phishing techniques. MSPs and their customers should ensure they are mitigating these attack methods. Useful mitigation resources on initial compromise attack methods are listed below:

- Improve security of vulnerable devices.

- Selecting and Hardening Remote Access VPN Solutions (CISA, NSA)
- Vulnerability Scanning Tools and Services (NCSC-UK)

- Protect internet-facing services.

- Protecting internet-facing services on public service Critical National Infrastructure (CNI) (NCSC-UK)
- Strategies for protecting web application systems against credential stuffing attacks (CCCS)

- Defend against brute force and password spraying.

- Microsoft update on brute force and password spraying activity (NCSC-UK)
- Russian GRU Conducting Global Brute Force Campaign to Compromise Enterprise and Cloud Environments (NSA, CISA, FBI, NCSC-UK)

- Defend against phishing.

- Phishing attacks: defending your organisation (NCSC-UK)
- Spotting malicious email messages (CCCS)

Enable/improve monitoring and logging processes

It can be months before incidents are detected, so UK, Australian, Canadian, New Zealand, and U.S. cybersecurity authorities recommend all organizations store their most important logs for at least six months. Whether through a comprehensive security information and event management (SIEM) solution or discrete logging tools, implement and maintain a segregated logging regime to detect threats to networks. Organizations can refer to the following NCSC-UK guidance on the appropriate data to collect for security purposes and when to use it: What exactly should we be logging? Additionally, all organizations—whether through contractual arrangements with an MSP or on their own—should implement endpoint detection and network defense monitoring capabilities in addition to using application allowlisting/denylisting.

- MSPs should log the delivery infrastructure activities used to provide services to the customer. MSPs should also log both internal and customer network activity, as appropriate and contractually agreed upon.
- Customers should enable effective monitoring and logging of their systems. If customers choose to engage an MSP to perform monitoring and logging, they should ensure that their contractual arrangements require their MSP to:

- Implement comprehensive security event management that enables appropriate monitoring and logging of provider-managed customer systems.

- Provide visibility—as specified in the contractual arrangement—to customers of logging activities, including provider's presence, activities, and connections to the customer networks (Note: customers should ensure that MSP accounts are properly monitored and audited.); and
- Notify customers of confirmed or suspected security events and incidents occurring on the provider's infrastructure and administrative networks and send these to a security operations center (SOC) for analysis and triage.

Enforce multifactor authentication (MFA)

Organizations should secure remote access applications and enforce MFA where possible to harden the infrastructure that enables access to networks and systems. Note: Russian state-sponsored APT actors have recently demonstrated the ability to exploit default MFA protocols; organizations should review configuration policies to protect against "fail open" and re-enrollment scenarios.

- MSPs should recommend the adoption of MFA across all customer services and products. Note: MSPs should also implement MFA on all accounts that have access to customer environments and should treat those accounts as privileged.
- Customers should ensure that their contractual arrangements mandate the use of MFA on the services and products they receive. Contracts should also require MFA to be enforced on all MSP accounts used to access customer environments.

Manage internal architecture risks and segregate internal networks

Organizations should understand their environment and segregate their networks. Identify, group, and isolate critical business systems and apply appropriate network security controls to them to reduce the impact of a compromise across the organization.

- MSPs should review and verify all connections between internal systems, customer systems, and other networks. Segregate customer

data sets (and services, where applicable) from each other—as well as from internal company networks—to limit the impact of a single vector of attack. Do not reuse admin credentials across multiple customers.

- Customers should review and verify all connections between internal systems, MSP systems, and other networks. Ensure management of identity providers and trusts between the different environments. Use a dedicated virtual private network (VPN) or alternative secure access method, to connect to MSP infrastructure and limit all network traffic to and from the MSP to that dedicated secure connection. Verify that the networks used for trust relationships with MSPs are suitably segregated from the rest of their networks. Ensure contractual agreements specify that MSPs will not reuse admin credentials across multiple customers.

Apply the principle of least privilege

Organizations should apply the principle of least privilege throughout their network environment and immediately update privileges upon changes in administrative roles. Use a tiering model for administrative accounts so that these accounts do not have any unnecessary access or privileges. Only use accounts with full privileges across an enterprise when strictly necessary and consider the use of time-based privileges to further restrict their use. Identify high-risk devices, services and users to minimize their accesses.

- MSPs should apply this principle to both internal and customer environments, avoiding default administrative privileges.
- Customers should ensure that their MSP applies this principle to both provider and customer network environments. Note: customers with contractual arrangements that provide them with administration of MSP accounts within their environment should ensure that the MSP accounts only have access to the services/resources being managed by the MSP.

Deprecate obsolete accounts and infrastructure

Both MSPs and customers should periodically review their internet attack surface and take steps to limit it, such as disabling user accounts when personnel transition. (Note: although sharing accounts is not recommended, should an organization require this, passwords to shared account should be reset when personnel transition.) Organizations should also audit their network infrastructure—paying particular attention to those on the MSP-customer boundary—to identify and disable unused systems and services. Port scanning tools and automated system inventories can assist organizations in confirming the roles and responsibilities of systems.

- Customers should be sure to disable MSP accounts that are no longer managing infrastructure. Note: disabling MSP accounts can be overlooked when a contract terminates.

Apply updates

Organizations should update software, including operating systems, applications, and firmware. Prioritize applying security updates to software containing known exploited vulnerabilities. Note: organizations should prioritize patching vulnerabilities included in CISA's catalogue of known exploited vulnerabilities (KEV) as opposed to only those with high Common Vulnerability Scoring System (CVSS) scores that have not been exploited and may never be exploited.

- MSPs should implement updates on internal networks as quickly as possible.
- Customers should ensure that they understand their MSP's policy on software updates and request that comprehensive and timely updates are delivered as an ongoing service.

Backup systems and data

Organizations should regularly update and test backups—including "gold images" of critical systems in the event these need to be rebuilt (Note: organizations should base the frequency of backups on their recovery point objective. Store backups separately and isolate them from network connections that could enable the spread of ransomware; many ransomware

variants attempt to find and encrypt/delete accessible backups. Isolating backups enables restoration of systems/data to their previous state should they be encrypted with ransomware. Note: best practices include storing backups separately, such as on external media.

- MSPs should regularly backup internal data as well as customer data (where contractually appropriate) and maintain offline backups encrypted with separate, offline encryption keys. Providers should encourage customers to create secure, offsite backups and exercise recovery capabilities.
- Customers should ensure that their contractual arrangements include backup services that meet their resilience and disaster recovery requirements. Specifically, customers should require their MSP to implement a backup solution that automatically and continuously backs up critical data and system configurations and store backups in an easily retrievable location, e.g., a cloud-based solution or a location that is air-gapped from the organizational network.

Develop and exercise incident response and recovery plans

Incident response and recovery plans should include roles and responsibilities for all organizational stakeholders, including executives, technical leads, and procurement officers. Organizations should maintain up-to-date hard copies of plans to ensure responders can access them should the network be inaccessible (e.g., due to a ransomware attack).

- MSPs should develop and regularly exercise internal incident response and recovery plans and encourage customers to do the same.
- Customers should ensure that their contractual arrangements include incident response and recovery plans that meet their resilience and disaster recovery requirements. Customers should ensure these plans are tested at regular intervals.

Understand and proactively manage supply chain risk

All organizations should proactively manage ICT supply chain risk across security, legal, and procurement groups, using risk assessments to identify and prioritize the allocation of resources.

- MSPs should understand their own supply chain risk and manage the cascading risks it poses to customers.
- Customers should understand the supply chain risk associated with their MSP, including risk associated with third-party vendors or subcontractors. Customers should also set clear network security expectations with their MSPs and understand the access their MSP has to their network and the data it houses. Each customer should ensure their contractual arrangements meet their specific security requirements and that their contract specifies whether the MSP or the customer owns specific responsibilities, such as hardening, detection, and incident response.

Promote transparency

Both MSPs and their customers will benefit from contractual arrangements that clearly define responsibilities.

- MSPs, when negotiating the terms of a contract with their customer, should provide clear explanations of the services the customer is purchasing, services the customer is not purchasing, and all contingencies for incident response and recovery.
- Customers should ensure that they have a thorough understanding of the security services their MSP is providing via the contractual arrangement and address any security requirements that fall outside the scope of the contract. Note: contracts should detail how and when MSPs notify the customer of an incident affecting the customer's environment.

Manage account authentication and authorization

All organizations should adhere to best practices for password and permission management. Organizations should review logs for unexplained failed authentication attempts—failed authentication attempts directly following an account password change could indicate that the account had been compromised. Note: network defenders can proactively search for such "intrusion canaries" by reviewing logs after performing password changes—using off-network communications to inform users of the changes—across all sensitive accounts. (See the ACSC publication, Windows Event Logging and Forwarding as well as Microsoft's documentation, 4625(F): An account failed to log on, for additional guidance.)

- MSPs should verify that the customer restricts MSP account access to systems managed by the MSP.
- Customers should ensure MSP accounts are not assigned to internal administrator groups; instead, restrict MSP accounts to systems managed by the MSP. Grant access and administrative permissions on a need-to-know basis, using the principle of least privilege. Verify, via audits, that MSP accounts are being used for appropriate purposes and activities, and that these accounts are disabled when not actively being used.

Alert ID 7c9e1919

This Alert has 1 attachment(s). To view or download the attachment(s), click "View Alert" to login to the web portal.

View Alert

Tags Joint Cybersecurity Advisory, managed service providers (MSPs)

CISA CISA is the Nation's risk advisor, working with partners to defend against today's threats and collaborating to build more secure and resilient infrastructure for the future.

For Questions or Comments Please email us at toc@h-isac.org

Download Health-ISAC's Information Sharing App. 

For more update and alerts, visit: **https://health-isac.cyware.com**