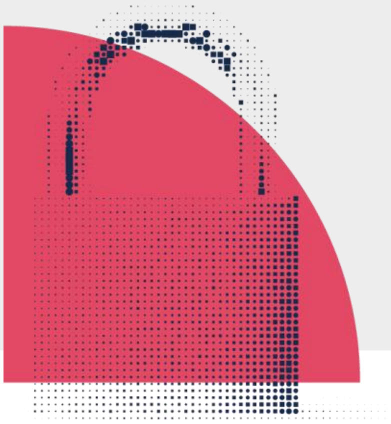
Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

ACSC PROTECT:

How to manage your network security when engaging a Managed Service Provider



December 2018

Introduction

- The compromise of several global MSPs was reported in 2017. In response, the ACSC provided stakeholders with the information they needed to protect themselves and others from this threat. Impacted MSPs were informed.
- In 2018, sophisticated cyber adversaries continue to target and compromise MSPs and, through them, their customers. The ACSC reiterates the need for organisations to scrutinise the cyber security measures implemented in contracted ICT solutions to combat the threat.

Managed Service Providers and the ACSC

To provide a level of confidence and improve the standard of cyber security of MSPs, the ACSC has developed an MSP Partnership Program. MSPs are encouraged to participate in the program and provide feedback. Likewise, prospective MSP customers are encouraged to consider their potential providers' participation in this program as a factor in their procurement process. Please see https://cyber.gov.au for more details[1].

Mitigation strategies

This document shows organisations the actions they can take to manage the security risks posed by engaging and authorising network access to MSPs. Many of the following recommendations apply to any outsourced Information Computer Technology (ICT) service provider, not just MSPs.

The number and type of controls used with an MSP will vary depending on the sensitivity of your systems. The ACSC recommends the following strategies to reduce the risk of compromise via MSPs:

1. Get security in the contract

(a) Security may not be a primary consideration when outsourcing the management of a system; however, the cost of remediation after a compromise far exceeds the cost of upfront implementation.

[1] https://cyber.gov.au/government/publications/msp-better-practice-principles/

(b) Clearly state **cyber security expectations** upfront. Ask candidate MSPs to provide evidence of their ability to meet your security requirements while administering your network. During negotiations you may ask a candidate MSP to walk through how they administer a customer's network.

(c) During negotiations, ask the MSP for contact information for other clients. You should be able to have an open conversation about another customer's experience of the MSP's ability to protect customer systems.

(d) Ensure your contract requires your **MSP to maintain a good internal security culture**, and to implement contemporary security standards such as the ACSC Essential Eight to make it a measurable deliverable.

(e) Include **breach notification clauses** in your contract with your MSP. The MSP must be obligated to notify the customer in the event of any breach that may endanger the customer network. This may include cases in which MSP systems related to the administration, management, or storage of information on the customer network have been compromised or accessed by an unauthorised and/or unknown party.

(f) Define the **clearance level expected of MSP staff working on your systems** and ensure that this is provided to you for validation. There is additional risk from insider threat if the MSP engages staff outside your normal clearance and background check procedures.

2. Control MSP access to your network

(a) To perform their contracted duties, a MSP must administer either a system on your network, or your entire network. Without proper controls, this high level privileged access, combined with the unknown security posture of a network that you do not control, can leave your network vulnerable to intrusion.

(b) **Know where the boundaries are between you and your MSP.** Ensure that your organisation clearly identifies which systems each MSP can access and how, and keep the record up to date. These accesses should be treated as untrusted for anything outside the scope of the MSP's responsibility. For example, a connection from an MSP into a specific customer system should be treated as an untrusted access with regards to other systems on your network.

(c) **Segment your network from the MSP's.** This will limit an adversary's ability to move laterally from a compromised MSP network into the customer network. The ACSC has observed cyber adversaries using compromised MSP workstations to move laterally to customer domain controllers located in foreign countries, increasing access to the victim's network. Examples of segmentation include:

(i) Where an MSP administers an entire network, the customer may stipulate that the MSP network not be used to administer a customer's systems. Instead, MSP staff administer the customer's network from a system within the customer's network.

(ii) Consider segmenting your network into trust zones. [2]

(d) **Utilise a secure jump host** for MSPs to perform administrative tasks. If a MSP must access your network from theirs, or remotely, specify a dedicated workstation on which MSP administrative staff should perform sensitive administration duties, with restricted access to critical servers. Combine this with multi-factor authentication to limit an adversary's ability to compromise critical assets. [3]

3. Mitigate the impact of stolen or abused credentials

(a) **Credential management** is part of controlling and restricting MSP access to your network. As a key exploitation vector, credentials require special protection. Typically, when an intruder has full access to your MSP they will have access to all the credentials on their network. This not only includes corporate credentials of the MSP, but

[2] https://acsc.gov.au/publications/protect/network_segmentation_segregation.htm

[3] https://www.acsc.gov.au/publications/protect/Secure_Administration.pdf

also credentials for their client's devices and systems managed by the MSP, if they are stored on the MSP system.

(b) **Implement least-privilege administration** to decrease the impact of cyber adversaries gaining MSP-level access to customer networks. Provide the MSP with the least privileged account(s) required to do their job.[4]

(c) **Strongly control enterprise and domain administrator accounts**. Enterprise and domain administrator accounts should have no members by default. Utilise just-in-time principles for broad privilege accounts like the domain administrator. Use a manual process or privileged access management software to add named accounts to the domain administration role, for a limited duration.

(d) **Provide attributable accounts.** Accounts should be attributable to the MSP to enable easy identification of MSP activity in privilege allocation and logs. The ACSC has observed cyber adversaries using legitimate support accounts provisioned by MSPs to deploy malware to customer networks; rapid attribution of such activity would assist the customer to work with their MSP to remediate their network.

(e) Enable **multi-factor authentication** (MFA) on remotely accessible services used by your MSP to access your network and systems. This will ensure that, even if a malicious actor has compromised credentials of MSP accounts, they remain incapable of logging on without a second factor such as a token. Cyber adversaries have used Remote Desktop Protocol directly from the MSP network to deploy malware to servers anywhere in the administered network; MFA can prevent an adversary from obtaining unauthorised access. Also consider blocking MSP access by default and allowing remote access at an agreed time. Correlate this access with a specific job ticket. [5]

4. Ensure visibility of MSP actions on your network

(a) **Capture relevant logging** to improve visibility of potentially malicious activity. Logs should be stored in a centralised location. A Security Administrator or independent party without access rights/accounts should regularly review logs for suspicious activity in the reviewed systems. Also consider including a contract requirement for your MSP to perform logging of hosts and networks used to remotely connect to the customer environment. Relevant logging includes:

(i) **Host-based event logs** to provide visibility of malicious activity on workstations and servers. [6]

(ii) **Firewall and proxy logs** to provide visibility of network connections associated with malicious actors.

(iii) **Remote access logs** to help identify unusual network access from accounts used by MSPs.

(b) MSPs should be responsible for **reviewing their logs** to ensure their access to the customer network aligns with an actual business requirement and/or job ticket. Further, the MSP should be obligated to provide detailed logs if the customer has security concerns they wish to investigate further.

(c) The recommended **event log retention time** is at least 18 months; however, some organisations may have a regulatory requirement to retain event logs for a longer period.

(d) Maintaining default sizes of event logs may cause older logs that contained key information to be overwritten prior to commencing an investigation; it is therefore advised that organisations increase the default sizes or **forward logs to a central location for storage**.

[4] https://docs.microsoft.com/en-us/windows-server/identity/ad-ds/plan/security-best-practices/implementing-least-privilege-administrative-models.

[5] https://acsc.gov.au/publications/protect/multi_factor_authentication.htm

[6] https://acsc.gov.au/publications/protect/windows-event-logging-technical-guidance.htm

5. Make sure your own network is secure

(e) **Implement a cyber security standard,** such as the **ACSC Essential Eight** developed by the Australian Signals Directorate; a prioritised list of strategies to mitigate Cyber Security incidents. [7] These strategies are effective in defending against malicious activity such as preventing the execution of malware and reducing the vulnerability surface of an organisation.

[7] https://acsc.gov.au/publications/protect/essential-eight-explained.htm

6. What if my MSP compromises me?

(a) If you detect a cyber security breach, or have been notified by your MSP of a possible breach, ensure you **get as much detail as possible**. Look for indications of what level of access enabled the incident to occur. A web facing scan of services is very different to an external system logon, or internal lateral movement. Information to request includes:

(i) What sort of incident is it?

(ii) What specific data and systems are known to be affected?

(iii) What was the indication that there was an incident?

(iv) Date and time of the incident?

(v) Is the incident ongoing?

(vi) What actions is the MSP taking to investigate and remediate?

(vii) Has this incident been reported anywhere?

(b) **Communicate securely.** If the compromise involved your corporate network, you may no longer be able to trust corporate communications. Ensure you have alternate, secure communication channels internally and with your MSP. Keep records of any engagement with the MSP for future reference.

(c) **Report to the relevant authorities.** Firstly, ensure that the appropriate person(s) within your organisation have been notified. If personal information has been lost or compromised, you may be legally required to report the breach to the Office of the Information Commissioner. You should also report the incident to the ACSC for advice and assistance on how to remediate your network.

Further Information

- The ACSC has developed a set of questions that customers can ask MSPs prior to engaging their services. The full document can be found at: https://cyber.gov.au/government/publications/msp-questions-for-msps/
- For services outsourced to a cloud service provider, see ACSC cloud computing advice at: https://acsc.gov.au/infosec/cloudsecurity.htm
- The United States Computer Emergency Response Team (U.S CERT) have also produced guidance on mitigating the risks of engaging with MSPs. The full document can be found at: https://www.us-cert.gov/ncas/alerts/TA18-276B.

Contact details

If you have questions about this advice, contact the ACSC by emailing asd.assist@defence.gov.au or calling
1300 CYBER1 (1300 292 371).