Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Cyber Security for Contractors

JUNE 2020

Introduction

Adversaries regularly target Australian Government information held by contractors, both classified and unclassified, in an attempt to gain an economic or strategic advantage.

This document has been developed to assist contractors with appropriately securing Australian Government information on their systems.

Contractors hold valuable information

Foreign intelligence services are the foremost cyber threat to Australia. Such adversaries seek both national security and commercial information to identify vulnerabilities in Australian capabilities or to further their own economic or strategic advantage.

Contractors, both in Australia and overseas, have reported significant increases in malicious cyber activity against their systems and are priority targets for adversaries[1]. Often the value to an adversary of the information contained on a contractor's systems is not immediately evident. Unclassified information can still be sensitive; in particular, wholesale aggregation of unclassified information can present a threat to Australia's interests.

Examples of adversaries compromising contractors include the compromises of:

- US aerospace company Boeing, which resulted in gigabytes of information relating to 32 US projects, including information on the Lockheed Martin F-35 and F-22, as well as the Boeing C-17 aircraft, being sent to China[2].
- US security vendor RSA, which led to subsequent targeting of US defence contractors Lockheed Martin, L-3 Communications and Northrop Grumman. This cyber security incident is reported to have cost RSA 90 million[3].

Cyber intrusion techniques are many and varied. A common cyber intrusion technique used by adversaries is socially engineered emails targeting high-ranking members of contractors and their support staff. These emails often aim to exploit common security vulnerabilities such as unpatched applications or operations systems, the use of similar passwords across systems, or the use of personal devices for work purposes. These emails may be sent directly from an adversary or from a supplier or subcontractor that an adversary has already compromised in order to leverage a trusted relationship with their intended target.

[1] https://www.washingtonpost.com/world/national-security/confidential-report-lists-us-weapons-system-designs-compromised-by-chinese-cyberspies/2013/05/27/a42c3e1c-c2dd-11e2-8c3b-0b5e9247e8ca_story.html
[2] https://www.theregister.co.uk/2016/07/15/hacker_gets_46_months_cooler_time_for_shipping_f35_f22_secrets_to_pla/
[3] https://arstechnica.com/information-technology/2011/06/rsa-finally-comes-clean-securid-is-compromised/

Essential mitigation strategies

To protect information provided by or developed for the Australian Government, contractors should implement the Essential Eight from the ***Strategies to Mitigate Cyber Security Incidents***:

- **Application control** to prevent execution of unapproved/malicious programs including .exe, DLL, scripts (e.g. Windows Script Host, PowerShell and HTA) and installers.
- **Patch applications** e.g. Flash, web browsers, Microsoft Office, Java and PDF viewers. Patch/mitigate computers with 'extreme risk' vulnerabilities within 48 hours. Use the latest version of applications.
- **Configure Microsoft Office macro settings** to block macros from the internet, and only allow vetted macros either in 'trusted locations' with limited write access or digitally signed with a trusted certificate.
- **User application hardening.** Configure web browsers to block Flash (ideally uninstall it), ads and Java on the internet. Disable unneeded features in Microsoft Office (e.g. OLE), web browsers and PDF viewers.
- **Restrict administrative privileges** to operating systems and applications based on user duties. Regularly revalidate the need for privileges. Don't use privileged accounts for reading email and web browsing.
- **Patching operating systems.** Patch/mitigate computers (including network devices) with 'extreme risk' vulnerabilities within 48 hours. Use the latest operating system version. Don't use unsupported versions.
- **Multi-factor authentication** including for VPNs, RDP, SSH and other remote access, and for all users when they perform a privileged action or access an important (sensitive/high-availability) data repository.
- **Daily backups** of important new/changed data, software and configuration settings, stored disconnected, retained for at least three months. Test restoration initially, annually and when IT infrastructure changes.

Additional mitigation strategies

Perform regular vulnerability assessments

It addition to implementing the Essential Eight, systems should be regularly reviewed for security vulnerabilities, particularly after significant changes. Vulnerability assessments can be done in-house or by an independent provider using both automated and manual methods.

Implement an education program for employees and subcontractors

An education program will provide employees and subcontractors with a better understanding of common cyber threats such as socially engineered emails, malicious websites and the danger of poor password policies.

Beware of malicious insiders

Adversaries will often attempt to influence contractors' employees in an attempt to gain access to Australian Government information or to have them perform actions on a system to benefit their strategic goals. By conducting ongoing vetting of employees, especially for those with privileged access, controlling the ability to remove Australian Government information from systems, and implementing a comprehensive audit program, this risk can be lowered.

Report cyber security incidents early and often

This includes informing the Australian Cyber Security Centre (ACSC) of any cyber security incidents that could potentially threaten Australian Government information. Seeking assistance early can mitigate or reduce a potentially

dangerous and embarrassing compromise. By immediately informing the ACSC[4], assistance can be provided without delay and will contribute to safeguarding Australian Government information.

Use available cyber security resources

Initiatives such as the Defence Industry Security Program (DISP)[5] helps to ensure that contractors are provided with appropriate security guidance. For example, contractors with membership to the DISP have access to the ***Defence Security Principles Framework*** (DSPF)[6] which details the standards, processes and procedures that direct the application of protective security measures by Defence personnel and external service providers.

Further information

The ***Australian Government Information Security Manual*** (ISM) assists in the protection of information that is processed, stored or communicated by organisations' systems. It can be found at https://www.cyber.gov.au/acsc/view-all-content/ism.

The ***Strategies to Mitigate Cyber Security Incidents*** complements the advice in the ISM. The complete list of strategies can be found at https://www.cyber.gov.au/acsc/view-all-content/publications/strategies-mitigate-cyber-security-incidents.

Contact details

If you have any questions regarding this guidance you can contact us via 1300 CYBER1 (1300 292 371) or https://www.cyber.gov.au/acsc/contact.

[4] https://www.cyber.gov.au/acsc/report
[5] http://www.defence.gov.au/dsvs/Industry/
[6] http://www.defence.gov.au/DSVS/dspf.asp