MARCH 2014

Cyber security incidents: are you ready?

Introduction

1. The effective management of a cyber security incident can greatly decrease the severity and cost of the incident. Providing all relevant information to ASD upon request will enable ASD – when required – to act faster in response to a cyber security incident.

2. This Protect is not a substitute for – but rather draws upon – existing policies on record retention as outlined in the *Australian Government Information Security Manual* (ISM) and required under the *Archives Act 1983*. The following advice aims to enable a quicker and more effective response to cyber security incidents. For an explanation of acronyms and terms used in this Protect, please consult the *Supporting Information* section of the ISM.

Can your agency answer these questions?

Event logging

3. *Have we configured workstations to log events to a central server? Could we provide, at a minimum, the last three months' worth of these logs to ASD upon request and in a timely manner?*

Why is this important? Providing logging data will assist ASD to establish the cause, extent and duration of the compromise.

Workstation logs	Network logs	Server logs
Application whitelisting logs	Proxy logs	Mail server logs
Event logs	DHCP logs	Authentication server
Anti-virus logs	DNS logs	Web server access
Firewall logs	VPN logs	Remote access servers
Authentication logs	Firewall logs	
	Network device logs	

Roles and responsibilities

4. *Have we documented policies and procedures for cyber security incident response?*

Why is this important? Defining your agency's policies and procedures – and making staff aware of them – will give your agency the best chance of a rapid and coordinated response.

5. *Do our staff understand their incident response roles and responsibilities? Does our service provider understand its roles and responsibilities in the event of an incident? Do we have detail of our outsourced ICT infrastructure and gateway provider readily available (including the public-facing IP address range)?*

Why is this important? Clearly defining roles and responsibilities will mean agency staff and providers understand their specific tasks in the event of an incident.

Contact details for your agency

6. *Does our agency have a current OnSecure account with correct contact details for our Information Technology Security Advisor?*

Why is this important? Providing up-to-date details will allow ASD to quickly contact the right person in your organisation. Furthermore, OnSecure is where ASD posts and publishes Alerts on significant threats as well as Protect publications and advice that your agency will need to keep up to date with in order to respond to some cyber security incidents.

Initial incident treatment

7. *How quickly can we identify, physically locate and isolate an infected machine on our network? Do we know what our baseline network traffic looks like? Do we have the ability to recognise and assess anomalies in network traffic? Would we pull all plugs on the identified machine, or ensure capture of volatile information for investigation?*

Why is this important? A good understanding and sound documentation of your network and all workstations will assist when particular workstations need to be identified quickly. Understanding your network traffic, along with any anomalies when asked, will assist ASD to tailor incident response to your needs. Your agency may choose to contain the identified machine. In this case, it is important to configure the machine for hibernation and then hibernate rather than fully shutting down the machine. This will preserve valuable volatile artefacts that will be used in investigation of the incident.

Assisting with investigations

8. *Once identified, can our agency effectively and safely isolate malware and provide it to the Cyber Security Operations Centre (CSOC)?*

Why is this important? Malware provided to CSOC is used to prevent the reoccurrence of similar cyber security incidents across government.

Further Information

9. The *Cyber Security Incidents* and the *Information Security Documentation* chapters of the ISM contain information on planning for, detecting, reporting and managing cyber security incidents. The *Access Control* chapter of the ISM outlines the requirements for event logging and auditing.

10. ASD's Protect publication *Preparing for and Responding to Cyber Security Incidents* provides guidance for senior managers on cyber security incident response.

11. To apply for an OnSecure account go to www.onsecure.gov.au.

Contact Details

Australian government customers with questions regarding this advice should contact the ASD Advice and Assistance Line on 1300 CYBER1 (1300 292 371) or asd.assist@defence.gov.au.

Australian businesses or other private sector organisations seeking further information should contact CERT Australia at info@cert.gov.au or by calling 1300 172 499.