1 Introduction

Our group was founded over 25 years ago when a university student hacked NASA in his spare time.

This breach triggered a chain reaction for improving information security.

In the early 1990's three Australian Universities came together and formed AusCERT - the central source for information security and protection.

On 8 March 1993, the Security Emergency Response Team (SERT) commenced Incident Response operations in Australia which then became known as AusCERT.

Today, The University of Queensland (UQ) has embraced AusCERT as part of their organisation.

A fuller depiction of AusCERT history of this group can be found on our website publication "Forming an Incident Response Team"[1].

The following profile of AusCERT has been established in adherence to RFC2350.[2]

1.1 Date of Last Update

Version Number: 1.0
Published Date: 10th February 2020
Authorised By: AusCERT Director
Authorised Date: 4th February 2020

1.2 Distribution List for Notifications

Changes to this document are not distributed by a mailing list.

Any specific questions or remarks please address it to the AusCERT email address: auscert@auscert.org.au

1.3 Location where this document may be found

The current version of this profile is always available on: https://www.auscert.org.au/publications/auscert-rfc2350

2 Contact information

2.1 Name of the Team

Australian Cyber Emergency Response Team
Short Name: AusCERT

2.2 Address

AusCERT
The University of Queensland (UQ), Brisbane QLD 4072
Level 4, C Block, Building 1019 "Foxtail"
UQ Long Pocket Site (Long Pocket)

2.3 Timezone

AEST Australian Eastern Standard Time (UTC+10:00)

2.4 Telephone Number

+61 (7) 3365 4417

2.5 Facsimile

+ 61 (7) 3365 7031

2.6 Other Telecommunication

-None-

2.7 Electronic Mail Address

auscert@auscert.org.au

2.8 Public Keys and Encryption Information

AusCERT uses PGP for digital signatures and to receive encrypted information. Every two (2) years a new team key will be generated.

The key is available on public PGP/GPG keyservers and at:

https://www.auscert.org.au/1967/

2.9 Team Members

A full list of AusCERT team members is not publicly available.

Team members will identify themselves to the reporting party with their full name in an official communication regarding an incident.

3 Charter

3.1 Mission Statement

Vision

AusCERT to be the trusted Australian cyber emergency response team for the information economy, providing valued incident prevention and detection to members and incident reporters.

Mission

To be a Center of excellence in handling incidents and improving member's cyber security posture by providing:

- Timely and impartial incident response, security advice, threat intel and analysis;
- Information Sharing and Analysis Centre (ISAC) and Security Operations Centre (SOC) functions;
- Value added benefits and services such as the Certificate Service and the world class information security conference;
- To employ and develop talented and passionate professionals and be the place they want to work.
- To engage with the global CERT community for the benefit of AusCERT and its members.

3.2 Constituency

AusCERT, due to its origins, continues to assist Australian private and public organisations and companies.

This is made possible by providing priority incident handling and additional services to our membership base of which covers all industry definitions under the ANZ Standard Industry Classification. [3]

3.3 Sponsoring Organisation / Affiliation

AusCERT is a centre of expertise on cyber security and incident handling based in the University of Queensland.

It is aimed at preventing ICT and internet related incidents and coordinates response to these incidents.

3.4 Authority

In the early 1990's three Australian Universities came together and formed AusCERT - the central source for information security and protection.

Today, The University of Queensland (UQ) has embraced AusCERT as part of their organisation.

The structure can be found as:

UQ https://www.uq.edu.au/departments/unit.html?unit=1

=>UQ COO https://www.uq.edu.au/departments/unit.html?unit=1027

==>UQ ITS https://www.uq.edu.au/departments/unit.html?unit=22

===> AusCERT https://www.uq.edu.au/departments/unit.html?unit=260

====> AusCERT Services https://www.uq.edu.au/departments/unit.html?unit=851

====> AusCERT Operations https://www.uq.edu.au/departments/unit.html?unit=849

4 Policies

4.1 Types of incidents and Level of Support

All cyber security incidents are considered normal priority unless otherwise explicitly labelled EMERGENCY or URGENT.

The level of support is best effort and depends on the type of incident and severity as determined by AusCERT.

Processing of incidents is given priority to members over any other types of reporting sources.

The incidents will be received 24/7 by email. Should a member require immediate 24/7 assistance then member is required to accompany the email report with a phone call on the member hotline.

Otherwise all incidents will be triage and processed during normal office hours.

4.2 Co-Operation, Interaction and Disclosure of Information

AusCERT highly regards the importance of operational cooperation and information sharing between CERTs, NCSCs, CSIRTs and organisations which may contribute towards or make use of their services.

All incoming information is handled confidentially by AusCERT, regardless of its incident's priority.

AusCERT will use the information provided to help solve security incidents only distributing anonymised information adhering to the Traffic Light Protocol [4].

Information that is evidently very sensitive in nature is only communicated and stored in a secure environment, encrypted as necessary.

4.3 Communication and Authentication

The preferred method of communication is via email. AusCERT protects sensitive information in accordance with relevant regulations and policies in Australia.

Communication security (Encryption and Authentication) is achieved by agreed means.

The default is that AusCERT will sign all emails that it is issuing out with the PGP key.   All sensitive communication to AusCERT should be encrypted with AusCERT's PGP Key [5].

5 Services

5.1 Incident Response

This is provided by our service named "Incident Handling" [6]

5.1.1 Incident Triage

- Investigate whether indeed and incident occurred.
- Determine the extent of the incident.

5.1.2 Incident Co-ordination

- Determine the initial cause of the incident
- Facilitating contact with other sites which may be involved.
- Communicate with stakeholders.

5.1.3 Incident Resolution

- Providing advice to the reporting party that will
- help remove vulnerabilities that cause the incident.
- secure the systems from the effects of the incident.
- Evaluate which actions are most suitable to provide desired results regarding the incident resolution
- Provide assistance in evidence collection and data interpretation when needed.

5.2 Proactive Activities

Prevention and preparation consists of all activities aimed at reducing the probability or impact of an incident for the constituent.

AusCERT provide constituents with current information and advise on new threats, and attacks which may have an impact on their operation, building awareness and skills of the constituents through the following services.[7][8]

- Security Bulletins
- Member Security Incident Notifications
- Sensitive Information Alert
- Early Warning SMS
- Malicious URL Feed
- Certification Services
- AusCERT Education
- Information Sharing & Analysis Centres (ISAC)
- AusCERT Conference

6 Incident Reporting Forms

Although there is no set form for the reporting of incident the following information will be elicited from the reporter to be able to action on an incident.

It should be noted that some of the information listed could be automatically added depending on the mode of reporting.

Contact details and organisational information

- Name of the person
- Organisation Name
- Email Address
- Phone Number
- other items of the likes...

Observation

- IP Address
- Malicious code
- Malicious URL
- other items of the likes...

Actions Sought

- Website take down
- Notification of possible compromised host
- Analysis of Malicious Code
- IoC extraction
- other items of the likes...

7 Disclaimers

Announcements, alerts and warnings, and services are performed in best-effort manner, and to contact information currently known to us.

While every precaution will be taken in the preparation of information, notifications and alerts, AusCERT assumes no responsibility for errors or omissions, or for damages resulting from the use of the information contained within.

Note 1: https://www.auscert.org.au/publications/forming-incident-response-team
Note 2: https://tools.ietf.org/html/rfc2350
Note 3: https://www.fwc.gov.au/awards-and-agreements/minimum-wages-conditions/annual-wage-reviews/previous-wage-reviews/annual-wa-0
Note 4: https://www.first.org/tlp/
Note 5: https://www.auscert.org.au/1967/
Note 6: https://www.auscert.org.au/services/incident-management/
Note 7: https://www.auscert.org.au/services/
Note 8: https://conference.auscert.org.au