From: IN%"D.Smith@sert.edu.au" "Danny Smith, Security Emergency Response Team, Australia" 7-MAY-1993 15:30:29.81
To: IN%"sert-mgt@sert.edu.au"
CC: IN%"sert@sert.edu.au"
Subj: SERT Status Report - 23-Apr-1993 to 7-May-1993

Status Report for 23-Apr-1993 to 07-May-1993
Security Emergency Response Team

Executive Summary

This reporting period saw an extremely low level of activity in security incidents. Not only did this free SERT staff from commencing new incidents, but the resolution of outstanding incidents means that the administrative overhead of incident handling has dropped away.

This allowed us to concentrate more on some of the issues relating to education and advice on security matters. CERT has put together a one day security course and we are negotiating to use those notes for our own purposes.

Work is well under way to establishing a 24 hour, 7 day operation for SERT. Initially, this will involve the two full time SERT staff, until some other resolution can be reached concerning part time staff.

Despite the second round of requests for registration information, a number of major sites STILL have not sent us any contact information. Whilst we cannot make them use SERT, we still feel that it is in their best interests to register with us. An audit of the returned forms will be performed to ensure that we processed all received forms.

We still do not have any Unix boxes for our own use. This makes tool development and the Megapatch development more difficult. We have currently "borrowed" a SUN box, but it is sadly lacking in disk space. This will need to be returned to its rightful owners towards July.

We have been contacted by the organiser of the CAUSE (Association for the Management of Information Technology in Higher Education) to present a paper at their inaugural conference in Hobart. This paper is to be aimed at more senior management in the education industry.

It is also recommended we start attending conferences like DECUS to gain exposure to areas outside of the AARNet realm. This will provide a number of benefits:
1. It will establish us as the innovators and leaders in incident handling for Australia (!)
2. It will provoke other organisations to consider establishing similar groups;
3. It will provide exposure and publicity for our group to external sites that may wish to contribute to the cause.

We had a very successful meeting with the AFP to resolve some operational issues. Basically, if we can get SERT formally recognised as the security team for AARNet, this will open up a number of different options for us in relation to funding and cooperation.

Outlook

More work is required by the Federal Police to analyse information as they do not have the technical expertise to do this. This analysis takes a significant amount of time. The AFP have indicated that some reimbursement for our time is possible, and we should continue discussions with them in this area. It is expected that the analysis work will recommence within the next few weeks.

Last time I wrote:

"The aftermath of the major incident over the Easter weekend will result in a better understanding of how CERT and SERT should interact, and this will have a direct benefit when we are required to interact with other FIRST member groups. As well, it has revealed a number of deficiencies in our operation. We are taking steps to identify and rectify these problems."

Unfortunately, the aftermath of the major incident for CERT meant that they "shut up shop", and became incredibly busy. To this end, we have had very little interaction with them. I personally am starting to feel that although we still have a good working relationship with CERT, we are now on our own to sink or swim.

The exposure we gain by presenting papers at the various local workshops and conferences will be excellent in raising peoples' awareness of what SERT is about and how it can help them.

Detailed Analysis of Incidents

Since our inception on the 8-Mar-1993, we have recorded 27 incidents. These can be categorised as:

	Open Incident	Closed Incident
Probe (no access gained)	0 (1)	12 (10)
Attempt (serious attempt at access)	1 (1)	5 (4)
Access (non-privileged access gained)	1 (3)	6 (4)
Serious (privileged access gained or demonstrated loss)	0 (0)	2 (2)

(Previous report's figures are in parentheses).

Many of the open incidents are pending input from an external source. It is expected that this input will not be forthcoming in the immediate future, so these incidents will remain on the books for some time yet.

Individual Reports

Current Staff:

DFS	Danny Smith (UQ)
RDM	Rob McMillan (UQ)
GW	Greg Watson (GU) - parttime
PN	Peter Nikitser (QUT) - parttime

DFS:
Incident Handling.
Examining equipment requirements.
Work on password security mechanisms.
Work on login banner Advisory - seek opinions from many sources

RDM:
Incident Handling.
Setting up contact Registry and independently verifying each contact.
Setting up SERT computer systems and security.
Work on Password Security Advisory.

GRW:
Setup our SUN box that we "borrowed" from QTAC.
Establish monitoring tools for the SunOS box.
Incident Handling.
Work on the Megapatch for SunOS V4.1.2

PAN:
Catching up after a prolonged abscence.

(Once again, we lost staff time due to public holidays and illness. Despite this, we are still moving ahead due to the low level of incident activity.)

Proposals

The SERT team needs to become familiar with all the currently known vulnerabilities. We need to formulate a checklist (in conjunction with CERT and other Incident Response Teams) to deal with these vulnerabilities. It is possible to go one further and develop some "expert" systems that examine a system for vulnerabilities, or evidence of intrusion. The hackers are currently doing this themselves. Some work has commenced in this area already.

A Memorandum of Understanding needs to be developed between SERT and the AFP. Currently, they have the ability to call heavily on SERT resources, due to their lack of technical expertise. We need to help them, but we should not be in the role of doing investigations with the aim of prosecution. We should analyse the information with the view of understanding the vulnerability and combatting it.

We need to establish a public FTP site for information dissemination.

Establish procedures for sites to report incidents.

Develop a wide range of security packages and documentation for our constituents to make use of (e.g., checklists, site security policies, tools, and so on).

We need to get the AFP to clarify a number of issues relating to security, privacy, and traffic monitoring. We need to clarify our requirements under privacy legislation, and the Freedom of Information Act. This process has been commenced.

We will develop and release a SERT Advisory of good password policies. Bad password policies are the single highest problem which allows computer intrusions. This has been commenced.

We will develop some tutorials and talks to present to this years QUESTnet Networkshop and SAGE-AU conference. A number of other trips are required to extend our coverage.

Conclusions

We are still forming our relationships with other organisations, but this is progressing well. So far, we have done little to help our constituents in a proactive way, but we are slowly moving towards a position of strength in this area. It takes time to establish the credentials and materials to do this work.

We need to become more publicly visible. I expect this to start occurring as a result of the Megapatch release, the ConSEPT product from SUN, and having a publicly available ftp site for information. Much of the initial information in this site will be a copy of what is currently held by CERT. A SERT advisory with a good password policy will help us to gain more exposure as will presentation of papers at conferences. I'm afraid that travel may be unavoidable!

Annex 1

Summary of incidents by category:

9303051921 -	Serious -	Closed
9303051503 -	Attempt -	Closed
9303101425 -	Attempt -	Closed
9303121138 -	Probe -	Closed
9303181609 -	Probe -	Closed
9303231108 -	Probe -	Closed

9303231447	Serious	Closed
9303101321	Access	Open
9303091118	Probe	Closed
9212211648	Access	Closed
9303011259	Access	Closed
9303081410	Probe	Closed
9303170927	Access	Closed
9303250911	Probe	Closed
9303261055	Attempt	Closed
9303301100	Probe	Closed
9304021327	Access	Closed
9304021349	Probe	Closed
9304131553	Attempt	Closed
9304161104	Access	Closed
9304191550	Probe	Closed
9304211030	Attempt	Closed
9304221010	Probe	Closed
9304221252	Probe	Closed
9304221336	Access	Closed

(New incidents since the last report)

9305041325	Probe	Closed
9305051342	Attempt	Open

Danny Smith.

```
==========================================================================
 Danny Smith                              |  Phone:   +61 7 365 4105
 Security Emergency Response Team |  Fax:     +61 7 365 4477
 The Prentice Centre                      |
 The University of Queensland             |
 Qld.  4072.  Australia                   |  Internet:  d.smith@sert.edu.au
```