



Assess the readiness of Pacific Island nations to establish a regional CERT capability

Graham Ingram
General Manager AusCERT



- What is a CERT?
- Goal of Study
- Approach taken
- Key findings
- Plan of action
- Threat environment

What does a CERT mainly do?



AusCERT
Australian Computer Emergency Response Team

- Monitors and provides advice about cyber threats and vulnerabilities and security management
- Helps coordinate a response to computer attacks to stop or mitigate an attack and help recovery between affected parties around the world
- Builds and maintains links with national and international stakeholders vital for effective incident response.





- Assess the capability and readiness of Pacific Island (PI) nations to build a sustainable regional CERT capability.
- Consult with stakeholders to identify and analyse cyber security requirements of the region
- Sponsored by ITU and the Australian Department of Broadband, Communications and the Digital Economy
- Study and report prepared by AusCERT



- Analyse
 - Nature and use of, and dependence on, ICT infrastructure within PI nations
 - cyber threat affecting PI nations
 - stakeholder capabilities, attributes and current activities relating to CERT activities
 - ability and willingness to support a regional PI CERT capability
- Based on stakeholder feedback, assess the ‘readiness’ to support a sustainable regional PI CERT capability
 - Including suggested plan of action
- Draft Report prepared for ITU



- A regional CERT functionality was identified as only one aspect of cyber security readiness which needs to be developed for PI nations
- Consensus among stakeholders that the following was more critical
 - ICT reliability, robustness and availability
 - Improved access to ICT and ICT security training for government, telecommunication providers and business sector; and anyone managing a network in PI region
 - Awareness raising for decision makers, ICT practitioners/professionals and public



- Still a definite need for a regional PI CERT capability
- PI nations are “ready” to develop a regional CERT capability
- AusCERT has recommended a plan which considers all cyber security priorities in parallel with PI regional CERT capability



- Why should PI nations develop a regional CERT capability?
 - High level of use of, and reliance upon, ICT infrastructure to support ordinary communications but also for essential services (where it is available)
 - High level of reliance on Internet technologies, including Skype to provide voice communications for ordinary use and essential services.



- Why should PI nations develop a regional CERT capability?
 - Noticeable level of cyber attack already affecting users and operators of ICT, including Internet and PSTN
 - Lack of cybercrime legislation, low ICT/security skills base and lack of dedicated CERT services mean threat is likely to worsen
 - In response to perceived need, some stakeholders already providing CERT-like services internally and externally
 - Albeit limited scope, ad hoc



- Plan provides options for
 - Addresses stakeholder's key priorities to improve general cyber security readiness by:
 - Improving access to ICT and ICT security training for the region
 - Ongoing cyber security awareness raising program
 - Provides access to essential CERT services on a temporary basis (eg, for 1-2 years) now
 - Develop a sustainable, ongoing CERT capability as part of a wider program of activities to improve cyber security readiness within the region more generally in 12-18 months



- Now
 - Provide access to essential CERT services on a temporary basis (eg, 1-2 years)
 - Outsource essential services
 - Threat and vulnerability bulletins
 - Incident coordination and response and incident handling
 - Commence planning for a new ICT training centre utilising resources (human, ICT and accommodation) within USP's new ICT Centre currently being built
 - Includes training for formal tertiary IT qualifications and
 - Professional development courses and certifications
 - Partner with experienced ICT training groups such as SANS, ICS2, Cisco, Microsoft, CompTIA, ISACA etc.
 - security awareness raising program



- In 12 – 18 months
 - Commence delivering a broad-based approach to ICT and ICT security training and education
 - Commence delivering awareness raising program for :
 - Public
 - ICT professionals and practitioners
 - Senior government policy makers
- In 20 – 24 months
 - Commence operations for an ongoing sustainable CERT capability that is based within USP, Suva



- Pacific Island regional CERT
- Region includes 22 SPC member countries (minus Australia, NZ, France, USA)
- Dedicated staff and resources in ICT Centre, part of Information Technology Services, USP, Suva
- Smaller regional office in another country (optional)
- Service the needs of constituents in 22 PI nations (including government, telecommunications, business users and operators and public)



- Outsourcing CERT functions is not sustainable and carries some disadvantages
- Sustainable PI regional CERT capability addresses
 - Governance
 - Structure
 - Funding
 - Independence of operations
 - Access to reliable ICT infrastructure



Threat Environment and What is at risk



- Access to your country's online systems and services
- Example - Estonia is a small country but highly dependent on its online systems
 - 100% use e-government
 - 99% use online banking
 - 86% online taxes
- Estonian DDOS attacks lasted for 3 weeks (May 2007)
 - targeted government and commercial systems
 - Attacks politically motivated but with financial and social impacts
- **CERT-Estonia played a significant role coordinating response to defend and mitigate these attacks**
 - Sought assistance from experts around the world (including ISPs, CERT communities, network and infosec communities)
 - Developing lessons-learned reports



- Security of e-government transactions depends on the security of the entire channel
 - Channel includes the remote client PCs that connect to those systems
 - For all personal information accessed or submitted online
- In event of remote system compromise, technology exists to protect integrity of financial transactions (eg, online banking)
 - Eg transaction signing off untrusted device
- For compromised remote client systems there is no way to protect the confidentiality of those transactions.
 - For e-government services confidentiality is paramount security goal
- Assume remote client PC is compromised when developing your risk management strategy

The threat and motivation



AusCERT
Australian Computer Emergency Response Team

- Since 2003 – cybercrime economy started with phishing
- Criminals are actively targeting e-commerce and e-government services
 - Motivation is money – illicit financial gain
 - Many types of cybercrime
 - identity theft features prominently
- Returns are high – risk is low
- Common attacks directed at:
 - Client PCs (home and work)
 - Web applications/servers



- Ability to defeat various forms of two factor authentication
 - Ability to initiate transactions in the background after legitimate user has authenticated during the authenticated session.
- Ability to defeat SSL digital certificates by using HTML injection and retaining connection to legitimate site with legitimate digital certificate
- Ability to modify browser stored root certificates
- Ability to access all information on the computer including protected store data (passwords), including soft certificates and protected store
- Ability to hide itself (rootkits) and disable or by pass security counter-measures
- Ability of attacker to control hundreds of thousands of computers simultaneously, via the malware



- Cybercrime and malware
 - OECD, Malicious software (malware) – a security threat to the internet economy, Ministerial Background Report, June 2008, available online
 - House of Lords, Personal Internet Security, Science and Technology Committee Report, Volume 1, 2007, available online
- E-government risks
 - Managing risk associated with online ID theft for government and providers of e-government services, 2005, www.auscert.org.au



Thank you.

Questions?

graham@auscert.org.au

www.auscert.org.au