Security in the .au ccTLD

Presenter: Simon Delzoppo, CEO AusRegistry

The registry operator for .au

- Introduction
- General Security
- DNS Specific Security
- Whols Specific Security (data security)
- Registry Specific Security

Security in the .au ccTLD

- Brief Presentation
- 4 main sections
- High level overview
- Questions

General Security

People Security

- Ensure staff understand security procedures
- Ensure appropriate handling of staff leaving
- Volunteers require special attention
- Keep people up to date and informed

Physical Security

- Virtual Security is useless if physical is not considered
- Strict rules are placed on the location of equipment, location of volunteer equipment
- No unnecessary access to systems –
- Recommend use of commercial data centre facilities

Normal IT Security

- Standard IT security practices
- Implement Fire walling
- Apply Latest patches and updates
- Only allow what is required nothing more
- Separate admin functions from service functions

Registry Data Centre

- 24 hour manned security
- 24 hour video monitoring
- Biometric authentication required
- Redundant fire, power and cooling systems

DNS Specific Security

DNS Software Security

- Keep machines patched with latest security updates
- Different versions of name server software
- Different operating systems
- Recursion is disabled – prohibits cache poisonings

DNS Setup Security

- Servers only used for DNS, don't serve other services eg. HTTP
- Only DNS traffic allowed through firewall, eg no external SSH access
- Use sensible TTL (etc) values
- Use only trusted IP providers for secondary volunteers

Zonefile Security

- Implement TSIG signed zone transfers
- Only accept transfers requests from known hosts
- Access to zone files by other means not allowed
- Updates are made dynamically to “stealth” primary using different TSIG key to the transfer key
- Update forwarding is disabled on all servers

WhoIs Specific Security

(data security)

Whols Access

- .au restricted 20 queries/hour then blocked
- 100 query a day maximum
- 24 hour bans
- Repeat offenders blocked completely at firewall

Whols Access

- Limited information (helps fight spam and unsolicited renewal notices)
- Unlimited Whols check facilities
- Ability to have limits lifted for certain IPs (eg for Registrars)
- Full logging capabilities

Registry Specific Security

Registry Access

- Only Registrar IPs can connect
- Only Registry services on the machines
- Utilizes SSL encryption
- Registrars connect to application servers not data store

Registrar Authentication

- Registrars issue with Username, Password and certificate signed by Registry CA
- Username logged in must match common name in certificate being used
- Source IP address must match those listed with username being used
- Username/Password combination must be correct
- Certificate must be signed by Registry CA

Data Security

- Database not directly connected to internet
- Application servers act as gateways to data store
- No direct SQL executed on database, all interactions done through stored procedures
- Application connects with database user with no privileges
- Backups also secured

Questions?

Thank you