Small Registries and Security

Andrej Bagon
Registry .si

Arnes, Tehnološki park 18, SI - 1000 Ljubljana

andrej.bagon@register.si

CENTR Jamboree 2016
Introducing myself

- A technician at Registry .si since January 2014 (host master for .si, maintaining DRS (features, bugs, testing, release software,…), technical documentation for registrars, vmware management (VMs, upgrades, SRM,…), configuration management of servers, server upgrades, service monitoring, web page maintenance,…

- 3rd time on CENTR Security meeting

- First time presenter at a CENTR meeting
Agenda

- Introduction
- Incidents (tasks, projects, wishes, ...)
  - Solved
  - In progress
  - For the future
Registry .si

- Part of Slovenian NREN (Arnes)
- 7 employees
- Head, 2 administrative and 4 technical workers
- About to hit 120,000 domains
- Last 2 years net domain count grows by approximately 3% per year
- A registrar can be any legal person
- Anyone can register a .si domain
Registry .si continued

- Our own domain registration system software (registrars)
- EPP server, registrar portal (registrar settings, otherwise read-only), epp client (cmd and web), whois
- DNS: uni cast and any cast servers
- December 2015 started with security work overview of Registry .si work
Disk failure

- Incident RAID5 – 1\textsuperscript{st} disk fails $\rightarrow$ rebuild $\rightarrow$ 2\textsuperscript{nd} disk fails $\rightarrow$ disaster

- It is even harder to discover if the network team is at the same time maintaining their hardware

- Synchronized mirror of arrays and RAID6

- We migrated to synchronized mirror
Employee leaving

- Main developer leaving Registry .si
- Search for all permissions s/he had
- Revoke all permissions (database, svn, binary repository,...) and server access
- Review and update the list of tasks to do when employee leaves
Unauthorized directory move

- Unauthorized move of /etc directory on SVN server – shared across all NREN
- A couple of technicians working on the server and network access to find what actually happened – thought we had unauthorized access – hacked!
- Make a daily sha256sum on all files in the SVN on a separate server
Authentic software

- DRS release software bundles
- How to guarantee that the software is authentic
- On separate server create a sha256sum on release software bundle files
No password on database

- Database without administrator passwords
- We set up administrator passwords for all our database servers

use mysql;

update user set password=PASSWORD("NEWPASSWORD") where User='root';
Raw database dumps

- Doing database dump every hour and storing on file system
- Unencrypted dumps
- Generated pgp keys
- Encrypted all the backup dumps on disk with the pgp key
- Encrypt the current backup dump with the pgp key
“Open VPN”

- Network access from outside – VPN
- Principle everybody can connect in any network
- Need to reorganize VPN into who needs what (proper routes, firewall,...)
Console access control

- Limit console server access only to who needs access (firewall, acl on router)
- 2 factor authentication (usb/card certificate, google authenticator,…) - pam module
- Applicable only when connecting from VPN
Encrypt log files

- Critical data in log files (username, password, access list)
- Need to encrypt at least the password
Encrypt file system backup

- Unencrypted file system backups
- Need to encrypt data on LTO drives
- Additional license required to encrypt the staging data (the backup to disk)
- New software with encryption integrated (bareos in testing)
Registrar abuse

- One of the registrars had a security issue on its domain registration web page.
- A bulk of domain registration/renew can happen, data corruption (updates), stealing data,...
- Have a DRS role to be read-only or less restrictive for such cases – not just block...
Database anonymization

- Internal testing servers with dump of production data
- Not live data but a point in time dataset
- Anonymize domain, contact, host data
- Quite a lot of work, if you want to preserve all the relations (and history)
- We could share the database for statistical purposes
Asset manager

- For options asked on SecurityWG mailing list
  - ITDB, GLPI, ManageEngine's ServiceDesk
- GLPI
- Thank you for options
Thank you

Questions?

register@register.si
andrej.bagon@register.si