

The secure sysadmin

When paranoia is not enough

Devdas Bhagat

The meaning of Security

- Security is the **process** of increasing the difficulty of unauthorized access to data, while still keeping authorized data access easy.
- Security is not having a firewall, or an IDS or a fancy GUI.
- Security is about knowing your business better than anyone else.

Sysadmin virtues

- People skills
- Understanding of business requirements
- Understanding of technology used
- Laziness
- Paranoia: Only the paranoid survive

The security paradigms

- You can never be totally secure.
- The security of a system depends on the administrator.
- Just because you aren't paranoid doesn't mean they aren't out to get you.
- Bad system administrators are worse than having none.

Designing secure systems

- Security is not a patch
- Security is designed into the system from day 0
- Merely good design is not enough
- Be ready to throw the first one away
- Have management support

Implementation

- Have the beancounters do a risk analysis
- Decide what you minimally need for the system to work
- Get management to write a security policy that is actually implementable
- The rest is then a piece of cake

Technology

- Specific implementations are not really relevant during design
- Choose the best implementation that matches your security policy
- Always do a cost benefit analysis
- Harden everything
- Airgaps are cheap

Firewalls

- Design firewalls to limit traffic
- Default deny
- Draw your traffic matrix
- Put the matrix in your ruleset

The matrix

Service	Source	Dest	Input i/f	Output i/f
---------	--------	------	-----------	------------

Defense in depth

- Physically secure your systems
- Implement 802.1q on any network
- Implement DHCP on any non trivial network
- Lock down switch ports
- Don't use vulnerable applications

Patch management

- Test patches first
- Patch fast.
- The window before patch and released exploit is decreasing.
- Ensure all machines are patched.
- Automate this for desktops!

More defense in depth

- Lock down from the edge. Your edge router is your first firewall
- Lock down at the core. Edge security is not enough.
- Walnut like networks are bad
- Strong passwords!
- TLS-ize as much as possible

Wireless

- Avoid wireless if possible
- Wireless networks must be separate from your regular LAN
- Laptops that go out of the office must stay on separate networks
- Get laptops to VPN in over wireless.
- Limit access to resources for wireless networks.

Logging

- Remember to log.
- Analyse your logs.
- Do this regularly. Automation is better.
- Dedicate a server to this if need be.
- Regular audits are required

Intrusion detection

- Any system can be broken, given enough time
- The attacker always has more time
- IDSs are supposed to automate the job of watching the network for break-ins.
- Use HIDS and NIDS in combination.
- System log analysis, data correlation, network traffic log analysis are crucial.

Backups

- Security is about keeping the business running
- Backups are important. Remember Sep 11
- Regularly backup and verify the backups
- Secure the backups as well as you secure active data