CSTL's informative guide to Network Best Practice

Securing a network can be difficult and costly, so below are some suggestions to make the maximum impact with the minimal resources. CSTL have formulated a series of Strategy Steps, which are based on the initial building blocks of essential security controls that any and every organisation should consider as a minimum. Where the risk is elevated a formal proactive stance of security management should be adopted above these minimum controls.

Have you ever heard the term "S*ecurity best practise"* and wondered just what this meant to you?

At some point in a given period a network will be insecure, and it seems few companies have the time or resources proactively to prevent exploitable conditions. Companies tend to react after the event, subsequently pumping time and resources into the problem that could have been avoided. The analogy of 'closing the stable door after the horse has bolted' is a sobering comparison.

A review of the last eight months of security issues shows that managing vulnerability would have prevented the threat, or at the very least reduced its impact to a minimum.

Below are some reasons why:

• Patching

Microsoft, Cisco, IBM and even Check Point (to name a few vendors), release software that becomes commercially widespread, only then to identify a security hole that requires a new version, update and patch to close the security hole again. The problem is that not every user of the original software is aware of the security hole, let alone the remedy, or if they do, they do not have the resources to upgrade. Ask yourself if you can list every desktop and server operating system, along with its version and patch status and then contrast them with all the associated vulnerabilities and finally identify what inline updates or patches are required to close the exploit?

• Internal attack

The precedent has long been to ensure the perimeter is resistant to attack, with little else. Unfortunately computing needs have meant that:

1. It is not just trusted staff, that have internal access; temps, contractors, suppliers, customers and alliances with other organisations potentially access your systems, all facilitated with the ever popular VPN, remote access and web services applications.
2. Staff and the business alliances now have more reason and opportunity, as the skills to probe & compromise a system are at anyone's fingertips. The web provides a library of easily available and easy to use hacking, cracking and discovery utilities.

When the above two factors are combined with user curiosity, disgruntlement and ignorance, and the more nefarious of motives of fraud, espionage, R&D interception and defacement, the perimeter-only stance loses its sense of proportion. It is also why a firewall will not defend against such threats as it is a perimeter ONLY protection as opposed to complete network defence.

• Virus (or more specifically blended threats)

Just about every organisation we assist has anti virus software to detect viruses. But just about every organisation leaves their virus defence to just anti virus software. The strange anomaly is that instead of virus threats petering to nothing as vendors get better, it is actually the reverse. Viruses are now the most commonly reported security issue, making market and press headlines every month and resulting in more lost resources than any other single threat. Why is this? The virus threat has evolved from mere executable code that infects other executable codes, to a threat that actively seeks exploitable conditions in network hosts. Hence, it will only take one laptop/client/PC/server that has its AV disabled or is slightly out of date to be the weak link in the defence. All of the major virus outbreaks of late have used widely publicised operating system exploits, so closing the exploits deprives the virus of its method to propagate and is a method of prevention rather than the standard detection. For example the Klez, Slammer and Blaster viruses all exploited vulnerabilities announced by

various vendors 9 months, 5 months and 2 months prior to the detection of the virus. Interestingly the time between announcement and the exploit being used within a virus has shortened, thus providing even less notice to act.

- Network administration -

The security of a server is based on a principle that only authorised users have access. This is compromised if the account parameters are weak or the workstations & servers are insecurely configured. Below are some parameters that are widely recognized, but are easily overlooked:

1. Password length
2. Password age
3. Usage of Administrator privileges
4. File/folder/directory access rights

Below are some parameters that not so widely considered and are normally overlooked:

1. Allowing only relevant services and applications to run rather than the default installation.
2. Renaming the admin account and creating decoy privilege accounts.
3. Restricting executable installation.
4. Using stronger rather than default hashing algorithms
5. Removing remote registry access permissions
6. Safeguarding internal LAN access points

We do not deny that network best practice cannot be treated as single entity with reference to staff training, remote access, mobile devices, back up, disaster recovery, information retention or physical security, but we do believe that by focussing on the suggestions below you can prevent threats and mitigate damage.

CSTL Suggestions

Other than the points made previously consider the following:

- Anti virus detection on every host, configured for on access scanning with daily updates and the use of an additional scanner (if possible different to the host version) at the gateway for traffic that could support an infected file.
- A robust patching policy that applies critical security patches within two weeks of their availability
- A user access control policy encompassing password control, user rights, credential allocation and a formal starter's and leaver's policy for all domain objects.
- Restricting executable installation, device usage and shared admin accounts
- Quarterly exploit condition scan with an annual penetration test.

Our approach is one of consultative and education and welcome the opportunity to have informative and informal discussion with you, being independent from any single vendor allows us contrast the many options and provide real world insight. You can request a meeting at our city demo suite or at your offices now on: security-info@cstl.com

Alternatively for further information on Network Best Practice please contact CST on: 020 7621 7832.