

**Every
organisation
has a
weakness
in their IT
system.
Our one-day
security audit
is there to
help you find
them!**



**Where is the Achilles
heel in the security of
your network?**

Computer
Security
Technology

*No single security vendor or solution
can protect your business
One independent security specialist can*

Implementing an IT security policy is one thing... Maintaining a strong security posture is another.

Computer Security Technology Limited (CSTL) along with IT research companies like Gartner and IDC, have witnessed that companies are experiencing issues with the increase in malicious threats from inside and outside their businesses. These threats affect data protection, system productivity and the security of proprietary data & business practices.

Seven out of ten networks are probably insecure, and it seems few companies have the time or resources to proactively prevent exploitable conditions. Companies tend to react after the event, subsequently pumping time & resources into the problem that could have been avoided. The analogy of 'closing the stable door after the horse has bolted' is a real sobering comparison.

A review of the last 8 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 exploit, 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 to identify what inline updates or patches that 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.

The above two factors combined with user curiosity, disgruntlement and ignorance, let alone the more nefarious of motives: 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's a perimeter ONLY protection as opposed to complete network defence.

- **Virus (or more specifically blended threats)**
Just about every organisation we assist have an 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. Virus's are now the most commonly reported security issue, making market & press headlines every month and result in more lost resources than any other single threat. Why is this? The virus threat has evolved from mere executable code that infect other executable code, 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 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; hence closing the exploits deprives the virus of its method to propagate and is a method of prevention rather than the standard detection. eg: The 'Klez' virus exploited a condition announced by Microsoft some 9 months beforehand. The 'Slammer' virus was some 5 months and the 'Blaster' virus some 2 months prior to it being announced. Interestingly enough 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 rightsBelow are some parameters that not so widely considered and are normally overlooked:
 1. Allowing only relevant services & 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

Introducing the Security Audit and Report.

To help you solve this growing issue we would like to offer you a single days worth of consultancy by one of CSTL's Qualified Engineers, resulting in a security report. In a single day, our consultant will be able to advise how you can tighten up the vulnerable areas within your IT infrastructure, protecting it against unwanted intrusions, viruses and other potential threats.

Why use the Achilles heel?

The Achilles heel audit is meant to be the first step to identify weaknesses, rather than an all encompassing vulnerability assessment. Typically employed to either justify a more in-depth review, provide a rationale for where to secure your network or indeed act as a cost effective tool to ensure your security posture is where you believe it to be. The service comprises one element of our vulnerability assessment services, these include:

- **External penetration scan:** useful for probing your gateway security and is the traditional method for gauging the strength of your firewall and/or any other public facing servers.
- **Full internal penetration scan:** In-depth & intensive host vulnerability scan that provides a strength report of critical network elements like web servers, domain controller etc.
- **Remote/Mobile strength testing:** A review of a typical laptop's security settings to ascertain the ability if lost or compromised to connect to the network by an un-authorised party.
- **Security policy and management review:** Report on the adherence of the organisations stance to security; encompassing high level policy review through to operational procedures, staff awareness and EN ISO BS 7799 standards.

What you will achieve in one day

On a day of your choice, our consultant will work with you to establish:

- What your security policy is trying to achieve.
- What you need to protect.
- What you have in place.

With the use of vulnerability assessment software tools to:

- Test designated network infrastructure for security vulnerabilities and provide recommendations on how to fix them.
- Reveal the root cause of vulnerabilities.

The objective of the day is essentially to provide your organisation with a snapshot of the state of the security on your network.

**Computer
Security
Technology**

Computer Security Technology Limited
31-33 Lime Street
London EC3M 7HT
Tel: 020 7621 9740 • Fax: 020 7621 9730
Email: info@cstl.com • www.cstl.com