

Security Audit

What is a Security Audit?

- ◆ A Security audit is an technical assessment of how a company's security policy is implemented. This is done in a systematic and quantifiable process. The audit is usually conducted with substantial inside information on the network so all aspects of a company's resources are analysed. Security audits are part of an ongoing process in ensuring that a companies security polices are correctly implemented and working.
- ◆ Security audits are less about the use of the latest vulnerability assessment tools or exploits and more about using a consistent and accurate analysis of your systems to produce measurable findings that can be corrected.

Why is it necessary?

- ◆ Over time as organisations evolve, their security structures will change as well. Additionally threats constantly change and new vulnerabilities of software and hardware applications are constantly found.
- ◆ Antivirus, firewalls and software need to be updated constantly. A system that has been configured securely and then left alone becomes more vulnerable over time. Additionally new changes on a system that was setup securely in the first place can open up security holes and make the system more vulnerable to attack.
- ◆ Most organisations believe the biggest risk of attack is from outside the organisation. However the majority of system compromises happen within the company. This can be by either disgruntled employees or employees consciously or unconsciously allowing an unauthorised user onto their computers.
- ◆ With this in mind a security audit is not just a one off review, but a continuous effort to improve the security of an organisation's systems.

Why use Redblade?

- ◆ When conducting a security audit you are entrusting critical issues into the hands of another company. Redblade has the knowledge and experience to provide the skills, expertise, processes, tools and methodologies needed to manage your business environment.
- ◆ With years of experience in a wide range of industries our technical engineers are known for their skills to unearth vulnerabilities and inconsistencies on a network.

How does the Security Audit work?

- ◆ Usually most companies start with an external security audit as this is the part of the organisation that is most at risk, but the scope of the audit is agreed before the audit is undertaken.
- ◆ Typically an internal audit is conducted at the same time. The results of these audits may result in further audits such as application or remote access audits.



Audit Options

The following aspects of your organisation can be audited:

- ◆ External Security Review
- ◆ Internal Security Review
- ◆ Remote Access/Wireless Audit
- ◆ Application Review

External Security Audit

- ◆ The objective of this audit is to analyse external Firewalls, Internet routers and internal systems that are visible from the Internet.
- ◆ Any systems that are open to the internet are audited against a current up to date list of security vulnerabilities.
- ◆ The audit can be carried out with known information about the company such as IP address ranges and server information or it can be completely blind with no information about the company in advance.
- ◆ Additionally the audit can be carried out with detection avoidance. This is usually done with companies that have IDS systems and they want to see if they can pick up the attack.
- ◆ The combination of approaches that are used will determine the length of the audit. A audit with detection avoidance will take a lot longer than an audit with network information available.

Internal Security Audit

- ◆ This audit is conducted on the internal core resources of your network. These include servers, routers, firewalls and any other networked systems visible only on the internal networks.
- ◆ The audit also focuses on security policies and practises that the company has in place. Some examples are what are the password polices, who has access to backup media, do audit logs exist and are they reviewed on a regular basis?

Remote Access/Wireless Audit

- ◆ This audit focuses on external access to your network. This can be through VPN client access, Terminal Services , Remote Desktop access and Wireless access. Also covered are modems, ISDN or DSL lines which are often overlooked in security procedures and policies. Unless each of these areas are controlled and monitored they can be easy points of access for the remote attacker.

Application Audit

- ◆ This audit is a more traditional penetration test of various applications. The audit is usually conducted on internet facing applications though sometimes internal systems can also be audited.
- ◆ These applications commonly have a web-based front end interface with a back-end database server. The application audit is an investigation into all aspects of the application's operation to determine any security risks. The aim is to demonstrate unauthorised access to these applications.



Conclusion

What is provided at the end of the audit?

- ◆ Redblade will provide a report at the end of the security audit.
- ◆ The first part of the report will provide a broad summary of any findings that are more suitable for management perusal.
- ◆ The second part of the report will be a detailed list of any vulnerabilities found including potential risks and any recommendations to fix the vulnerabilities. This will provide information to help the system or network administrator further protect and lock down the environment.

The Advantages of the Security Audit

- ◆ Discovering any security issues that could be exploited by unauthorised users
- ◆ Ensuring your network is conforming to best security business practices
- ◆ Allows IT departments to concentrate on their core responsibilities without worrying about security problems
- ◆ A detailed, easy to read report that details any security problems with recommendations on how to fix the issues

About Redblade Ltd

Redblade is a Managed Services company offering a number of services including:

- ◆ IT Support Solutions
- ◆ Network Services
- ◆ Managed Firewall Solutions
- ◆ Hosted Solutions
- ◆ Online Backup Services
- ◆ IT Technical Services

Redblade has the knowledge and necessary skills to provide a service which is unrivalled, as we aim to exceed your expectations. We aspire to have continued growth in our company with integrity and determination, we look forward to building a mutually beneficial relationship with you as our client.

Our goal is to provide fast, reliable and easily accessible networking solutions to small, medium and large enterprises by supplying Managed Services.



redblade