OVERVIEW

As IT has become more and more important to the modern business, so security has become a business issue.

Security challenges

IT SECURITY IS BECOMING MORE AND MORE complex. Viruses, worms, firewall management, patch management, intrusion detection, intrusion prevention: the list of security technologies that IT staff need to manage is long and growing longer every day. What should IT managers do to address these growing challenges?

There are three points to consider: management, technology implementation and policy design. In many cases, a network (and any existing IT security approaches) will have evolved over time, with users, applications, data, wireless links, and so on being added or removed on an ad hoc basis, often with little thought for security. Initially, organisations should begin by identifying and dealing with such points of weakness and implementing a structured management process.

Risk assessment

Conducting a risk assessment — a crucial first step — begins by understanding the configuration of IT and data, and grading the level of protection given to resources. Once common vulnerabilities have been identified, organisations can make simple corrections, such as amending access rights and privileges and installing security-related software patches — and putting in place the business processes to ensure that these are implemented on a regular basis in future.

Then, the organisation can set a baseline for testing and alert purposes, using reporting tools to audit against that level, looking at how people and process changes can bring systems into line with the security policy.

Decisions also need to be made about what else to protect. Security involves compromises and organisations need to identify what parts of their networks are most at risk and patch and protect these accordingly.

Devices operating in isolation are no longer sufficient. An integrated approach is necessary, with two or three different solutions required to make sure malicious code does not compromise the whole network.

Vulnerability assessment

Analysis must also be ongoing. Risks continuously evolve and security should be checked regularly by locating where information is stored, understanding the security measures that are currently in place to guard that information and identifying areas of weakness and suspect configurations that place information at risk.

Some organisations, such as online gambling company Blue Square, take no risks at all. Blue Square conducts vulnerability assessment tests every week and it does not rely solely on automated tools, but employs outside security specialists.

IT managers also need to ensure that the technology used is intuitive. Platforms that can simplify the deployment, configuration, management and updating of security tools are vital, since an administrator has to be able to install and configure multiple security tools without having to learn multiple interfaces.

In particular, the enforcement and implementation of security policies must be straightforward, as should the task of making modifications to the security that reflect changes in the business environment. Equally, the ongoing task of updating both security software and 'attack signatures' associated with intrusion detection systems must be manageable for administrators.

Blurred boundaries

Indeed, keeping up with the thousands of IT security threat alerts, most of which are probably irrelevant, is one of the biggest sources of information overload, and often, relevant alerts get lost among the 'noise' of benign alerts. Services such as Computer Associates' eTrust Threat Information Center monitor vul-

ISO 17799 VIEW OF THE SECURITY DOMAIN

KEEP BAD GUYS OUT
- Intrusion Prevention
- Vulnerability Mgt
- Accept Use Enforce
- Encryption

KEEP GOOD GUYS IN
- Identify Management
- User Admin
- Access Control
- Authentication
- Communications:
  Remote Access
  Site to Site
  Application to Application
  User to User

KEEP THE WHEELS ON
- Policy
- Organisation
- Personnel
- Education
- Incident Response
- Physical Security
- Business Continuity
- Development Security
- Compliance
- Legal/Regulatory
- Security Mgt
- Audit
- Outsourcing

Source: Gartner

nerabilities in technologies, operating systems and applications and can automatically deliver security notifications to organisations.

The service can be set up so that only those threats that are important to the organisation are delivered, enabling appropriate action to be taken in a timely manner.

One of the reasons for the increasing number of security risks is that network boundaries have become so blurred. Technologies that on the one hand promise to increase corporate productivity and flexibility can, on the other, introduce new vulnerabilities.

For example, secure connection protocols, such as SSL and IPSec, enable organisations to use the Internet to exchange information with employees in remote locations, branch offices, customers, suppliers and partners.

But such applications reduce the effectiveness of firewalls. For example, attackers can enter the corporate network undetected over a trusted, secure virtual private network (VPN) connection from an employee's compromised home PC.

That is how software giant Microsoft was broken into in 2000: the machine of a developer working from home was infected with the QAZ Trojan horse and outsiders used that to surreptitiously access Microsoft's systems.

Strategic decisions

As a result, a simple perimeter strategy has long been redundant. Organisations need defence throughout their network, with security services layered throughout a compartmentalised network if they are to prevent an attack being propagated across the enterprise.

For these organisations, security must be deep and pervasive, reinforcing the perimeter with layers of firewalls internally and intrusion detection and prevention systems (IDPSs) to plug back-door security holes and detect and eliminate attacks. Security should also be compartmentalised in order to isolate important assets and contain attacks to limit damage.

In a layered security strategy, firewalls and IDPSs are placed throughout the network – around the perimeter, in front of application servers, in front of network segments, and between application tiers – with security policies become increasingly stringent towards the centre of the network.

In a compartmentalised strategy, network segments and assets are sectioned off into individually secured compartments.

But is it easier to deploy this kind of layered approach or to decide on a management approach that makes it unnecessary? It is far easier to identify what is good and stop everything else, than to try to identify what is bad. So the 'white list' approach can be a much simpler and more effective solution for many organisations. It focuses on what executable software is required to run the business efficiently, authorises what to run and denies everything else.

Some users will almost certainly complain, but the key benefits of the white list approach are that it helps IT keep track of what is running in the organisation and to therefore patch accordingly, and it is cheaper than the reactive approach of intrusion detection. It also does not need regular updates. Significantly, there are security products available that can help organisations to administer a blanket 'default deny' policy.

A final, but important consideration is security policy: organisations need to spend sufficient time designing their policies — not forgetting to implement and manage them correctly, making changes and rewriting the policy as necessary.

Having a policy in place often proves cheaper and more effective than buying products without understanding where the risks to the business actually are. It should also help to ensure that companies are maximising the return on investment from products they have already bought. ■