

One of the most publicised risks to information systems is that of unauthorised access, often referred to as hacking. Find out how to protect your business against it with this factsheet.

For some, hacking is seen as something that happens to other people typically large or high profile organisations. But this is not the case. As use of the Internet grows, so too does the number of external attacks. The number of internal attacks is also increasing.

The DTI's Information Security Breaches Survey 2004** shows that two thirds of UK businesses suffered a malicious security incident in the last year which is an increase from just under half two years ago. Another striking result of the survey is the increase in attempts by outsiders to probe Internet gateways. Two years ago only one in twelve UK firms reported probing attempts. Now this figure has risen to one in eight, and to one in three in large companies.

This should prove ample warning that the risks of unauthorised access to information within any company are real. If you haven't done so already, think about prevention and what steps you might take for recovery, if required. This factsheet is for any business wanting to know how to protect itself against hackers. It covers risk, recovery and prevention; the history of hacking and two case studies.

RISK

If you allow access or connectivity of any type to your system, you are at risk from unauthorised access. There will always be cases of internal users trying to gain unauthorised access to applications and information, just as there will always be people outside who are keen to see what your systems are like, or what they contain.

Risks are increased if you have something of interest or value. For example:

- Payment systems
- Research information (especially if you are trying to develop things that will require patents or copyright to protect them after they become public)
- Desirable software that can be downloaded
- Politically and commercially sensitive information, such as salary levels, marketing plans and sales prospects

WHY DO PEOPLE DO IT?

There are many reasons why people attempt to gain unauthorised access to information and systems. For example:

- Stealing company information
- Breaking in for fun
- Disruption of corporate service by competitor
- Social hacking another version of 'fun'

THE ENEMY WITHIN

There is significant evidence that many of the most damaging intrusions come from inside. There is nothing as dangerous as a knowledgeable insider using permissions, skills and knowledge to damage your systems and processes.

UNAUTHORISED ACCESS RECOVERY

There are many variables to be considered when dealing with incidents of unauthorised access. These include:

- The nature of the incident (prank, vandalism, fraud, etc.)

- How long the incident(s) has been going on
- Who's noticed

These factors (amongst others) should help determine the nature of your response. Much of the impact will probably be to the organisation's reputation. Your response is therefore vital in recovering a damaged reputation, or stopping it from degrading further. The following high-level principles should be considered before setting up a formal response:

- The best aid to recovery is preparation consider steps that can be taken for Business Continuity Management.
- Just as reaction to a threat should be proportionate to the risk, response should be proportionate to the impact of the event consider your approach to Risk Management.
- Make sure those involved understand their roles and responsibilities in the incident management process. Ensure that people know who's in charge and that they have the authority to speak for the company.
- Clarify channels of communication to all who need to know, including external parties such as the media and the police.
- Make sure those interested know what you have done to prepare. This should include published policy and education initiatives, warnings and other pre-incident activities.
- The media can be your friend as well as your enemy, make them your friend
- Remember that failing to disclose information to the media can rebound on you if they find it out through other channels; make use of any PR people you employ.
- Remember that the aim is to manage the effects of the incident. Don't be tempted to use 'spin' as an alternative; it will rebound on you.
- Assess (qualify) the intrusion. Ask yourself:
 - What is the nature of the intrusion?
 - Is it ongoing?

- How long has this been going on?
- Who knows about it?
- Is there evidence that needs to be preserved?

Other actions depend on the scale and potential impact of the intrusion. If necessary, you may have to consider escalating the incident to your crisis management team. If there are legal concerns, or there is insider involvement, you should involve Human Resources, and be aware of the implications.

Various Computer Emergency Response Team (CERT) bodies have compiled a more technical recovery checklist for Windows NT or Unix incidents. See: http://www.cert.org/tech_tips/win-UNIX-system_compromise.html

UNAUTHORISED ACCESS PREVENTION

The risks of unauthorised access are best managed with a combination of:

- A defence strategy
- Technology tools
- User vigilance

Defence strategy

A company may have purchased all recommended tools for minimising the risk of unauthorised access, but without a defined strategy for managing them, they can be ineffective. For example, who is responsible for checking log files from these tools? How often are the tools updated? How often are they reviewed to ensure that they are meeting all of your needs?

A defence strategy should clearly define all available resources, including personnel, software, technology, etc. Like any other strategy, people need to have access to it and roles need to be clearly defined.

The best way to establish a strategy is through risk analysis. A sound understanding of

risk will give guidance on the wide range of solutions available to deal with unauthorised access.

Technology tools

Security technologies are used to manage access, and prevent unauthorised access. They include:

- Firewalls
- Intrusion Detection Systems (IDS)
- Virus and content scanners
- Vulnerability assessment
- Patches and hotfixes
- Hardening operating systems and applications

Firewalls

A firewall is a device or system that provides a secure gateway between two networks for example, your company network and the Internet. They are designed to keep unauthorised users out, and private information in. Firewalls can be in the form of:

- A software package that is installed on a server/host system
- An appliance or a network device
- A feature of some other network device (such as a router)

There are also personal firewalls that do the same job but only protect one system, such as a laptop or PC. Firewalls ensure that network traffic of certain types (or from certain applications) is allowed to pass from one network to another according to a set security policy. They can prevent network-based attacks that are often targeted against systems. Amongst other tasks, firewalls can:

- Log connection attempts and traffic
- Authenticate users trying to make network connections
- Inspect network packets and track the state of connections to ensure they are behaving as expected

- Inspect application traffic, for example, e-mail viruses or web pages
- Protect internal networks by performing Network Address Translation (NAT)
By preventing unwanted access to your network, the risk of an information security breach is greatly reduced. A firewall cannot:
- Prevent attacks from the Internet on defined protocols.
- Block dial-up attacks to remote access servers and modems within your network

INTRUSION DETECTION SYSTEMS (IDS)

Intrusion Detection Systems (IDS) act as 'burglar alarms' for a network or system. They can identify someone 'casing' the environment, detect the 'rattling of doorknobs' to see if the house is unlocked, hear the 'shattering of glass' as entry is gained, 'sound the alarm' and 'call the police'. They can also monitor and log forensic evidence to support any legal case. There are two types of IDS system:

- Host based
The IDS is installed on servers to identify activity and anomalies and report on server specific problems or activity. This is akin to virus defence software, except the IDS is looking for behaviour rather than patterns in files
- Network based
The Intrusion Detection System (IDS) 'sniffs' the network to watch traffic, stops or 'snipes' intruders, and reports on suspicious and unusual activity. IDS can be deployed in a number of ways depending on the aim or purpose of the system. It can protect key internal servers, identify Internet-based attacks and monitor network access points. You should consider installing an IDS if you:
 - Have suffered a security breach within the last twelve months
 - Run a website for transacting business

- Want internal partitioning of your network
- Have a high-profile organisation liable to attract malicious attacks
- Have an unattended remote site with ISP links
- Already outsource part/all IT operations
- Connect to clients/business partners
- Have no permanent, full-time security staffing capability
- Nessus
- NetRecon
- Sara
- CyberCop

VIRUS AND CONTENT SCANNERS

Scanners remain the most popular type of virus defence software used today. They contain detection and disinfection information for most known viruses. Scanners tend to be easy to use and are capable of identifying a virus. Their main disadvantage is that they need to be kept constantly updated with the latest virus information in order to remain effective.

VULNERABILITY ASSESSMENT

Vulnerability assessment uses scanning software that checks for known security flaws. These are stored in a database, and your system is scanned to check if any exist. This means that the vulnerability scanner can only find the problems it already knows about. It can't find new ones. You need to ensure that such scanners are kept up to date with the latest problems by downloading regular updates (much like virus scanners). Shareware scanners are freely available on the Internet. Some specialists use these scanners as the sole basis for their vulnerability/penetration tests, with no supporting analysis. As scanner reports may generate false positives and negatives, this is not an effective use of time and effort. They are most effective when used as the basis of a vulnerability assessment, not the totality of it. A number of vulnerability scanners exist, including:

- ISS (Internet Security Scanner)

PATCHES AND HOTFIXES

Most software vendors have websites that provide patches and hotfixes and all systems should be patched to the level recommended by the vendor. Unpatched systems are like an open window into your business. Many commercial operations and hacker sites provide online databases of known vulnerabilities and exploits.

The Common Vulnerabilities and Exploits project (CVE) assigns a unique code number to each known vulnerability. Hardening operating systems and applications hackers are always looking for weak spots. You can reduce these by building your systems using recognised configurations. Operating systems contain a vast number of settings, features and options. If these are set incorrectly they can lead to easy attack and compromise. Many default settings are open, insecure or switched off. Security standards must be defined and implemented for all hosts. These will vary for different operating systems.

Systems should be regularly audited against the intended/documented configuration. You may wish to consider automating the implementation /auditing process. This can be done by:

- Using a 'golden CD'
- Using a script
- Group policies under Win 2K
- Using a third party security audit tool

USER VIGILANCE

There is no more effective security control than an informed, vigilant workforce. Computer systems are best at running repetitive tasks but people are much better at detecting the unusual. Training

and educating staff is perhaps the most cost-effective way of managing your information risks.

HISTORY OF HACKERS

The term ‘hacker’ was originally used to describe a person who had advanced skills in computing. Bill Gates and Steve Jobs (founders of Microsoft and Apple) could be, and probably were, described as hackers during their membership of the pioneering ‘Homebrew Club’. This was an informal society for people interested in early microcomputers. At about the same time, a number of people who called themselves ‘phreakers’ were using various tones (normally used by engineers to test lines and exchanges) to obtain free telephone calls.

Because the tones were transmitted along with the call, it was possible to whistle down the telephone line and control the exchanges. Calls were routed to wherever they wanted, for free. Phreakers became interested in breaking in to many of the computer systems they could contact using their tones. Somewhere along the line, the terms got confused, and the current usage of ‘hacker’ became common.

WHY PEOPLE DO IT

- To learn about the systems they are attacking
- To embarrass the target organisation
- To make a point
- To use someone else's computer power
- Because they see it as fun
- Because they can

Who the media thinks does it

- All hackers are ‘teenage computer whizz kids’
- All hackers are geniuses
- Hacking is glamorous
- Hacking requires an in depth knowledge of computers

Who really does it

- Teenage computer ‘nerds’
- ‘Script Kiddies’
- Evil geniuses
- Naive or disgruntled employees
- Hacking groups
- Bored systems administrators
- Unscrupulous competitors
- Foreign Intelligence services

DIFFERENT TYPES OF HACKER

Generally you can break the hackers down into three tiers:

- First tier Very knowledgeable, find and code new exploits
- Second tier Savvy, able to investigate vulnerable systems
- Third tier ‘Script Kiddies’ often poses the greatest threat

First tier hackers

A first tier hacker is a programmer with extensive, specific experience of systems, protocols and processes. They are often professional programmers who enjoy coding as a hobby on the side. First tier hackers discover vulnerabilities and code programmes to exploit them. They are not common, and carry out a lot of research to stay current.

Second tier hackers

Second tier hackers have experience of networking, different operating systems, and understand how to exploit vulnerabilities. System administrators make good, second tier hackers. They will have a large collection of tools and understand hacking methods, but rely on others to find and code most exploits.

Third tier hackers

Third tier hackers are also known as ‘Script

Kiddies'. These people earn no respect amongst the hacker community because they have no real idea what they are doing. Generally, they are not IT professionals, but will download code from the Internet and run it on the office network or across the Internet. They know just enough to be dangerous.

OTHER SOURCES OF THREAT

- A disgruntled employee will not necessarily know much about IT systems, but their knowledge of your system enables them to attack when it is most vulnerable
- A naive employee can damage IT systems through an inability to operate even the simplest applications

WHAT CAN HAPPEN IF YOU HAVE A SECURITY INCIDENT

- Loss of customer confidence.
 - Brand damage
 - Server or network downtime
 - Loss of business critical information
- All of the above equates to a monetary loss, either directly or indirectly.

CASE STUDIES HACKING

The Organisation

A seller of quality model cars based in the UK. The company involved was small, employing fewer than six people. It originated as a mail order company, and saw upgrading to include Internet-based sales as a natural step. They went into this field early, and used their normal Internet Service Provider to develop their online payment system.

What Happened

The company was infiltrated online by hackers, who altered prices on the site's catalogue. They were able to set any price they wanted for any

product and they did, reducing prices to one tenth of the original. Impact the company suffered substantial losses as a direct result of the attack. Fortunately, they recovered from the event quickly and prevented a recurrence by employing a specialist e-commerce oriented consultancy. This involved additional expense, but less than the amount they lost in the hacking attack.

Such infiltration can go beyond embarrassment and financial loss. A website can be taken over and used to host illegal sites (including pornographic and warez sites). A warez site is one that provides illegal stolen software. It also provides the means to use copy protected and similar programmes illegally.

Lessons

- If you use the Internet for trading, ensure your website is secure
- If you do not have IT staff 'in house', seek information security advice from a specialist company

ETHICAL HACKING

The Organisation

A public organisation in the UK that holds and processes extremely sensitive (in some cases political) information. The organisation was subjected to a deliberate penetration test (known to some as 'ethical hacking') by a specialist company.

What happened

The network was scanned to determine what services were available on application and data servers. Conversations with the client revealed that a data server was used to store highly sensitive information. Testers obtained information from the data server using a tool designed to retrieve information from Windows

machines. Windows will reveal a lot of information without requiring any user identification. The output revealed:

- The system password policy (that password lockout was not set, allowing unlimited attempts to guess passwords)
- Login times
- Usernames and groups
- Shared drives

Impact

This information was sufficient to mount a password guessing attack. Testers found that there were two accounts within the administrator group and that password lockout was not enabled. This allowed the testers an unlimited number of login attempts. It took 11 guesses to reveal the administrator password, the most powerful ID on any Windows system. Knowing this allows the user to do anything, change anything and then cover their tracks.

All machines on the site were connected to an open network. This meant that any user (authorised or otherwise) within the building who could access a workstation on the network could easily gain access to data stored on the data server. At this point testers reported the finding to their client as they had gained access to extremely sensitive information.

Lessons

- If your computer systems are used for handling sensitive information, ensure that adequate security measures are in place
- Ensure that password controls are stringent. In the above example, locking a user out of the system after two or three failed attempts to enter a password would have prevented unauthorised access to systems
- Do not use passwords that might be guessed by other users. For example, never use

personal or company names

- Use network access and permissions to restrict internal access as appropriate

CHECKLIST UNAUTHORISED ACCESS

General

- Is there a firewall for your Internet connection?
- Do you have an Intrusion Detection System?
- Are there established policies for checking that your protection systems are working properly, and that their logs are being examined appropriately?
- Are your systems (especially firewalls) updated with patches and hotfixes to ensure the latest known intrusion techniques are countered?
- Have your systems been hardened for maximum security?
- Do you employ basic housekeeping measures like regular backups, and disabling logon accounts of people as they leave your company?
- Would your staff be aware if somebody was accessing your systems illicitly?
- When did you last review physical security? Do you know who is actually on your premises at any given time? Can you find out easily?

If you have answered NO to any of the above, you should consider taking some steps towards prevention as soon as possible.

E-mail

- If you connect directly to the Internet (using a dial-in modem, ISDN or broadband) from your desktop or laptop machine, it is sensible to install 'personal firewall' software. You should ensure that any network connection (such as an e-mail server) has an appropriate firewall installed.

Unauthorised access information security:

- Ensure all e-mail servers have appropriate

virus-defence software and make sure it is set to check e-mail messages (both incoming and outgoing). It is sensible to use an external virus-scanning service or perhaps a separate mail gateway.

- Consider utilising junk mail filters in your client software (e.g. Microsoft Outlook) or buying a gateway spam (junk mail) filter product. Your Internet Service Provider (ISP) may provide spam filtering services.
- Check with your system software vendors (such as Microsoft) if you need to update security software. This is normally done online. Regularly apply appropriate security patches to mail servers.
- Similarly, regularly update gateway/server virus checkers.
- Perform periodic checks on any event logs stored on your systems for anything unusual or suspicious.
- Produce, publish and circulate an e-mail policy. Ensure it covers what sort of personal use is acceptable (if any) and what content is prohibited (e.g. chain letters, jokes, pornography etc.). Other potential content may relate to the size of file attachments, management of numbers of stored emails, unchecked mailing lists, and the policy on replying to e-mails from unknown or suspect sources etc.
- Archive to CDs all older e-mail from local stores and servers. If there is any sensitive information, make sure it is appropriately protected.
- Set up e-mail signatures that include correct contact information.
- Include a disclaimer containing appropriate legal text. The following sample text may be used: 'This e-mail is sent in confidence for the attention of the addressee only. The contents are not to be disclosed to anyone other than

the addressee. If you receive this message in error please preserve this confidentiality and immediately inform the sender of this error.

- Periodically check for and delete unused e-mail addresses.
- Tidy up servers, deleting temporary files and ensuring servers have enough disc space for your future requirements.
- Periodically check the validity of your contact and address lists and update them appropriately.

GENERAL BUSINESS ADVICE

For more information on achieving best practice in your business contact your local Business Link advisor by visiting the website at <http://www.businesslink.gov.uk> or calling 0845 600 9 006.

Published by the Department of Trade and Industry. <http://www.dti.gov.uk> © Crown Copyright