RISK AREA OF NETWORKING

Password Security

Many people think of passwords as just another hoop to jump through - something you have to remember to do but has no real intrinsic value. Yet in many cases, passwords may be the ONLY defence against the hacker and deserve to be taken seriously no matter how low the risk is. If you operate a peer-to-peer network, a single password to gain access to a PC may unlock all of the shared documents on your network as well as your personal files. Make sure it is not widely known and certainly not displayed anywhere near the computer. In a server environment, network administrators centrally control passwords including enforcing minimum length, complexity and frequency of changing passwords. For more information see the Knowledgebase article on Choosing and using secure passwords

Exploited Users

One of the best ways to bypass security is to trick the user into providing information direct to the hacker. In order to mitigate this type of risk, network administrators need to be certain that all of their users are aware of phenomena such as phishing and do not give information out by responding to hoax emails or telephone calls. Similarly, incorporating confidentiality into company handbooks and Human Resources/Employment Policies is a must.

The inexperienced user can also create havoc on a network by visiting high risk websites such as those concerned with shopping, MP3's, smileys, gambling, dating, chat rooms, pornography, free *software*, peer-to-peer file sharing etc. At first this may seem trivial but can expose the network to far more serious risks. The 'cure' for these risks, is to have regularly updated anti-virus software installed and scanning on all machines as well as specialist anti-spyware / pop-up blocking tools where needed. On the preventative side, you will need to ensure that all updates for the operating systems and *web browser* software are downloaded and installed.

If you operate public access PCs, you should consider options for governing the websites that users can access. Web content can be controlled on a network either through an advanced *firewall* or through a proxy server. Both systems regulate all requests for web pages and allow administrators to decide whether access to a particular website or type of website is permissible or not. This will usually involve some form of subscription-based service that actively monitors and categorises web pages.

Viruses

Unlike spyware, popups and trojans, viruses target users indiscriminately. Low risk environments are particularly prone to viruses as those using computer systems often don’t need to think about security with the same levity users in as higher risk environments. Nevertheless, regularly updated and valid virus protection should be considered essential for every PC (especially Windows PCs). Installation is however different from installing on a single PC and you should seek professional help where needed. More information on this in the Knowledgebase article *Dealing with viruses*.

If you are looking after a network, look for specialised virus protection than can be centrally managed and monitored. In this way, you can ensure that updates and scans are not being cancelled and can keep track of threats – and even remove them - without disrupting users. ‘Network’ versions of Anti-Virus software such as AVG Network Edition or Symantec Corporate Edition cost around £8-£15 per PC.

Internet Based Hacking

Automated – and therefore random - ‘probing’ of computers connected to the internet is a fact of modern life. Even those running a low risk environment will need a basic router with some firewall capabilities to ensure that these probes do not yield results. Such routers cost from £40 to £150 and may even come as part of your *broadband* package.

Clearly, the higher the risk, the more sophisticated the firewall needs to be. Whilst a £150 *router* will usually suffice for a medium risk environment, if you run a high risk environment you may need to consider one with more advanced features that can fend off sustained and deliberate attacks. Before you buy, be sure you understand what these firewalls do – they are unlikely to prevent viruses or spyware for example! Oh, and don't forget to change the default password on the router too – the manual will tell you how.

For more on internet security risks see the knowledgebase article How secure is the internet.

Hacking from Within

It is much easier to hack into a network when you are physically joined to it. *Wireless* networks then are perhaps the greatest risk since the hacker can easily be concealed. Equally though, do not neglect the physical security of your systems – there are countless examples where networks are compromised by cleaners, night porters and service engineers who just plug in to a spare network point or turn on one of the PCs.

In order to be secure, networked devices MUST use have a strong password and WIFI must use the *WPA* (Wireless Protected Access) security system. In buildings where multiple organisations share the same network cabling, they should be separated by means of VLANs to prevent users from one organisation directly accessing the network resources of another. VLAN capabilities are supported in network switching gear costing as little as £150.

Misuse of PC's

The last category of risk applies to the higher risk environments where unknown or un trusted users have access to PCs. Although it may not be immediately obvious, the mere fact of logging into a PC may grant them sufficient privileges to stop it from functioning properly. Malicious users could uninstall printers, change system settings, delete crucial files or install software that puts equipment and data at risk.

Preventing this kind of risk is all about 'locking down' the PCs such that those users are barred from these types of activity. No matter what *operating system* or environment you use, there are many forms of restricted account that can be applied to a given computer. If this is an area you are concerned about, seek support from a network specialist supplier.

Source: http://www.ictknowledgebase.org.uk/securingnetwork