

Top 10 Tips for a Safer 2010

30 Sep 09

2009 may have been the year of 'flying by the seat of your pants'-style IT security policies, but 2010 can be a safer year if a few simple steps are followed, suggests David Kelleher.

By **David Kelleher** .

(1) Limit network access to those who need it

In smaller and medium-sized businesses it's often the case that most people tend to be given full privileges and access to the network, and to devices that they do not need to do their job. Taking such liberties with security is asking for trouble.

While it's likely that your boss' recruitment skills are top notch and honest, trustworthy people have in fact been employed, as IT administrator and security specialist responsible for the organisation's network security, the granting of full privileges remains a risk that you do not want to take... just in case.

(2) Control the use of portable devices on the network

Endpoint security is another issue that is based on too much trust. Insider threats can often be the most harmful and the least likely to be protected against, merely because employees and management in a smaller or medium-sized business tend to have high levels of trust towards each other.

Network activity should be monitored and the use of portable devices on the network such as iPods and USB sticks ought to be forbidden as it's too easy for a disgruntled employee to steal confidential data without being noticed.

(3) Limit Internet browsing

End users often fail to realise the threats that they can be exposed to on the Internet so it's best to nip the problem in the bud and limit their browsing capabilities so as not to allow viruses and other threats to infiltrate the network.

The problems lie mainly with peer-to-peer sites and social networking sites such as Facebook whereby malicious links can be sent from a 'friend's' hacked account without one realising that the link leads to a harmful website that could download malware or some other threat onto the user's machine and then spread onto the network.

(4) Carry out regular audits on the network

Monitoring event logs and carrying out regular audits provides you with important information about the network and is, therefore, a beneficial task.

Unfortunately, this undertaking is also very tedious and time-consuming. However, when it comes to network security this is definitely a step that should not be skipped because of the crucial data that it provides.

Regular audits let you know what materials are available on the network, while log analysis permits you to better understand the way that resources are being used and how to improve their management.

(5) Ensure that systems are secure before connecting them to the Internet

While any computer can be taken out of the box and connected directly to the Internet, to do so is a major security blunder.

Before any computer is connected to an Ethernet cable or telephone line, anti-virus and anti-spam software must be installed as well as a program that prevents malicious software from being installed. Once these security features are installed and the machine is then hooked up to the Internet, it's critical that these security features are kept updated at all times to ensure protection from malware and viruses.

Operating systems are prone to security holes. Once a flaw is detected, it's usually exploited within a short time frame. Up-to-date security scanners ensure that the latest malicious software is detected immediately so that the appropriate patches can then be downloaded.

(6) Eliminate default accounts/passwords

This is a basic but very common mistake that's preyed upon by hackers. Leaving the default account name and password on test systems means that hackers can very easily infiltrate the network and take over. Names and passwords should be changed upon immediate connection to the network to avoid hacking.

(7) Always authenticate callers

Authenticating callers might seem like a redundant process for administrators when they can recognise the voice of the caller. However, giving out password changes or other confidential information over the phone without following a proper authentication process could lead to security problems that often cannot be traced back to their point of origin - thus they are that much harder to detect and deal with.

(8) Maintain and test back-up systems

Failing to maintain back-ups of the system is practically unheard of, but actually testing the back-ups and confirming that your disaster recovery plan actually works is another issue entirely.

First, proper back-ups must be created on a regular basis and kept in a safe place off site. If this step is being done then the next thing is to actually ensure that the back-ups work in case of an emergency.

Back-ups that don't work are of no use. The work that went into creating them has effectively been a waste of time. Having proper back-ups is far easier and cheaper than creating the data from scratch.

(9) Test your disaster recovery plan

Your disaster recovery plan is probably a work of art in theory and looks great all planned out on paper filed away in your disaster recovery folder, but how does it work in practice? Have you actually simulated a disaster situation where your back-ups need to be used in order to get your systems back up-and-running so that work can continue and loss of revenue is kept to a minimum?

Planning such a simulation to ensure that the organisation can get back on its feet using back-ups should an emergency occur is a critical step in security. A disaster recovery plan that fails when put into practice is just another disaster!

(10) Don't go it alone!

There's no shame in asking for help with the bigger tasks. Setting up the network on your own is something of a gargantuan task. Outside help should be sought if you don't have the experience or the skills as yet. Although employing external help may be costly, professionals will make sure that the job is done well.