

Network Box white paper: Securing remote workers

Whether you allow your users to work from home, from the airport, or from anywhere else and remotely access resources on the company LAN, there are some important and serious security implications you need to consider to ensure that your remote workstations, laptops, and especially data, are properly protected.

In the case of home workers, the employee must use a VPN. The three most commonly used today are PPTP, IPSEC and SSL. IPSEC and SSL are the most secure, because they can use the highest security encryption – AES 256. SSL VPNs are becoming popular as they are more robust and flexible.

So, with the deployment of a VPN, the data can travel securely from the server in the office to the remote workstation. But when it gets to the workstation, it is unencrypted and can be written to the hard disk or to temporary files. When the user disconnects from the VPN, these files remain on the remote workstation unencrypted unless carefully purged by the user. If the information exchanged was confidential, that confidential data is now stored on a remote workstation over which you have no control.

When work is home and home is work

If this workstation is a home computer, it likely to be used by someone else in the house, someone who might join a peer-to-peer network, or browse to a website that will download a Trojan. Now those confidential files that were left over from the VPN session are being shared with millions of people, or stolen by the hacker who is controlling that Trojan.

This is not science fiction. It does happen, and a number of companies have suffered damage in terms of cost, reputation and image. Most companies don't consider whether the data that travels through the VPN will still be safe when it reaches the remote computer. But it is something that can seriously harm companies.

Perhaps the most obvious thing to do is not to allow your users to connect to the VPN using their home computer, over which you have no control. If you have telecommuters and you are in a position to enforce this, make sure that they use an employer-issued laptop and that you have full control over what's installed on it and how it is configured. Ensure that you have fully working and well updated antivirus and end point security on it.

Next, ensure that the user can't get to the Internet using that laptop unless connected through the VPN. There are plenty of software solutions on the market that allow you to do this. They will block direct access to the Internet unless the VPN is on. Then configure the VPN to redirect all traffic through the VPN itself, and on your VPN concentrator/firewall allow VPN to Internet traffic through a proxy that will scan this traffic for policy and viruses, as though that laptop were on your LAN.

It is important that the computer is not used by anyone other than the designated user. If they let their children free on the computer, it will most likely become infected. However, if your users are made aware of the potential risks to the company and possibly to their own

career, they will be less likely to indulge in such behaviour and will watch their employer-issued laptop more jealously.

If for any reason you are not in a position to issue laptops to your telecommuters but still want to allow them to work remotely, at least ensure that they are not allowed to have an administrative account, and limit what their account can see and do. This won't protect you completely, but at least should greatly reduce the risk of exposure. Demand that their remote PC be kept up to date with patches and AV signatures, and consider issuing an end point security license for that workstation, even though it will be installed on an asset that does not belong to your company.

Beyond the home and work place

If the remote user is connecting from a hotel or other remote place that is not their home, you run into another issue: the computer is connecting to a network that is not yours and so may be exposed to local attacks. A wireless connection at the airport is open to anyone who wants to connect. The downside of this is that your computer may end up in a large network, with other people you do not know. Therefore the possibility that someone with ill intentions may be connected to the same network is a real one. The most important thing to do in this case, and perhaps the only really serious protection you have, is to install end point security software on the laptop. This can intercept connection attempts, Trojans, unauthorized data transfer or similar issues. You should also advise your users to use strong passwords (see below), stay logged onto the wireless only for the time strictly necessary, and ensure they use a VPN when transferring confidential information. It would also be good practice to protect the laptop physically, because a high number of laptops are stolen every year. If you allow your users to check their mail remotely (by using Outlook Web Access for example), they should do this from their own laptop and not from a public computer, which could be infected with keyloggers, and is at the mercy of the next customer to use that workstation. The temporary files left on that computer during your user's session might contain data you do not want seen. These files are fully accessible to the next customer and to the administrators of that computer. This could lead to information being leaked, even though you have everything else well protected.

Whether your telecommuters are working from home or 'on the road', there are a number of options that are worth considering.

One very good way to protect potential data loss is to encrypt it. There are two ways to encrypt: you can encrypt the entire disk, or only certain file systems. The second option gives you more flexibility and allows for the recovery of the data should the OS become corrupted, but it can be easier for a hacker to decrypt. However, either one is a good solution to ensure that the data cannot be stolen. It is especially worth considering for laptops, which are unfortunately particularly prone to being stolen or lost.

Another option to limit your risks is to avoid data being transferred to the remote computer altogether. This is achieved by using thin client technology, such as Citrix. With this technology, the application runs on the server, the data is processed on the server and the data never leaves the server. What does leave the server is the graphic information to 'paint' the remote screen, which contains the data in 'visual' form but does not (usually) contain anything worth stealing. If it does, the data is usually kept in memory and is 'lost' when the client computer is turned off. There is some risk to files in the swap area but they will normally be quickly overwritten, deleting the information from the system.

Password protection

Earlier, we mentioned the use of strong passwords. Too many users still use birthdates, common names, names of pets and other easy to remember passwords. Unfortunately what is easy for us is often even easier for hackers. Here <http://www.whatsmypass.com/the-top-500-worst-passwords-of-all-time>, you will find the 500 most commonly-used passwords. If yours is one of them, you should change your password now. A strong password is critical to protecting your data, no matter where it is held. This particular issue is not restricted to roaming users, but of course it is more important for them, since they are more likely to have their computer stolen or hacked. You should encourage the use of complex passwords and change them regularly (but not too frequently, as frequently changing passwords results in users resorting to simple passwords so that they can remember them).

In conclusion, remember that all these rules and precautions apply to the IT department as well. We, IT people, have the tendency to think "it won't happen to me, I know better". And yet we are often the cause of the most grief to our company, because we have administrative accounts. We get cocky about our knowledge of IT and security and start believing that we are invulnerable. That often makes us the most suitable targets.

**For more information on securing your company network, visit
<http://www.network-box.co.uk>, or
call James Mackie on 0800 107 6098**

**To keep up with news from Network Box, see Simon Heron's blog:
<http://blog.network-box.co.uk>; or follow him on Twitter:
<http://www.twitter.com/networkbox>.**