

Mobile Security - Securing The Mobile User



Working while on the move opens up both users and the office network to all sorts of threats and dangers. We look at ways of combating those threats

The popularity of mobile working continues to grow in the UK, but many firms are still concerned about the security implications of investing in mobile devices for employees, according to new research released by Sony Ericsson.

The survey found that over half of the workforce now works away from the office at some point during the week and a further half said that this had increased in the last year.

However, while 82 percent of medium and large enterprises said they are prepared to invest in mobile devices for their staff to improve productivity, efficiency and employee motivation, roughly the same percentage said they have data and security concerns.

For the mobile user and the person who has to administer that user, there are a number of things to consider when it comes to security.

Connecting to the network

There are two different threats when you open up your network to the outside world; someone can steal the password and get into your network, or someone can eavesdrop on the connection and take the data without you or anyone else knowing, particularly if you're using a wireless connection in a shared space like a restaurant, coffee bar or airport lounge.

VPNs

The internet is a fantastic means of communication. However, it's a public network and any information that passes on it is open for anyone to see. To create a private network you either need to encrypt the data or use an internet service provider (ISP) and routers that allow you to do multiprotocol label switching (MPLS) connections. Encrypting the data and producing a virtual private network (VPN) using a dedicated device is the most practical, and cost effective, solution for most companies. A dedicated device is far faster and much more effective for creating VPNs, the hardware is optimised to enable encryption and decryption so your device isn't slowed down unduly, and you can have multiple VPNs open at any one time.

Two-factor authentication

A major concern of the VPN system is the need for authentication and the reliance on passwords to enable authentication. Studies continue to point to the ineffectiveness of passwords for securing

information. More than 60 percent of users, when given the ability to do so, continue to use the same passwords, according to Forrester Research.

A solution comes in the form of two-factor authentication. Strong authentication dramatically enhances network protection by requiring users to present a strong proof of identity before being granted access to protected resources

Two-factor authentication involves a PIN number that can be issued by an application run on a mobile phone or PDA, or produced on a small dedicated piece of hardware that is no bigger than a USB key, and a piece of personal information, such as a user's name or date of birth.

To make two-factor authentication work on a network, you need to add a solution that sits between the network and the user, and supply users with tokens.

There are two pieces to the solution; an authentication service that handles the passwords, and a service or device that provides the secure token. The authentication service plugs into the network and handles the management and verification of authentication requests and centrally administers authentication policies for the networks. The tokens produce a six-digit number that the user enters into the system along with their name to get entry to the VPN and the network.

Hardware theft

According to the latest Internet Security Threat Report from Symantec, businesses are not doing enough to protect against data losses from hardware theft. The report found that 54 percent of all data breaches that could facilitate identity theft were the result of the loss or theft of computers or data storage devices.

If the data on the device is not secure then you could lose the data to your competitor or you could be fined for breach of data protection laws and financial regulations. The Nationwide Building Society was recently fined £980,000 following the theft of a notebook containing customer data.

Physical devices that lock your notebook down, such as Kensington cables, are a way of deterring opportunists but won't deter a determined thief. Security is important to most businesses however it's not something you should just do as a one off, it's a constant spend.

As Forrester analyst and research co-author Bill Nagel explains: "We're trying to push people towards the idea of making security a proactive, business, process-based initiative, and if the spending levels out, it looks like people are listening to us."