The Mobile Workforce - The Weakest Link

Written by Magnus Ahlberg - MD of Pointsec Technologies Ltd

The use of handheld computers is expected to grow by more than 50 percent in the next few years. The Gartner Group forecasts that more than one billion handheld computers and mobile telephones with wireless network connectivity will be in use globally by 2003. This surge in the use of mobile devices will mean that companies must make sure that the mobile devices used by an increasingly mobile workforce do not become the weak link in their corporate security infrastructure.

While the Internet has revolutionized communication and business, mobile devices enable us to have any information, possibly even up to the minute, at our fingertips 24 hours a day. Companies have had to distribute mobile devices such as laptops, notebooks, handhelds and WAP phones just to remain competitive. Employees have driven many of these device rollouts, not IT, increasing the likelihood that the security implications and policies have not been investigated or implemented.

As the storage capacity of PDAs increases, so does the risk involved with using them. Most devices have at least 8MB of memory (Palm OS devices), and many have 32MB or more (PocketPC devices), many with the ability to add extra storage cards, which can hold up to 1GB. This storage capacity could easily allow for thousands of addresses, emails and notes, and as many of these extra storage cards are compatible with the latest laptops, it is easy to transfer other large files as well. The advantage is that this power makes the device extremely useful away from the office, and the low cost and simple setup make them appealing for a person to buy one and use for business.

With laptops and handhelds becoming ever more powerful, more people work “on-the-move,” placing increasing amounts of valuable and confidential data at serious risk of theft, sabotage, exploitation or damage to their professional integrity. Examples of stolen laptops containing either company or government (and sometimes both) confidential data that were unprotected are plentiful, from the CEO of a wireless communications company to an employee at the Ministry of Defense. A few are returned, but most are never seen again.

The number of handheld computers lost or stolen is directly related to the amount in use. IDC predicts that the global handheld market will explode in the next three years, from 12.9 million units in 2000 to over 63.4 million by 2004. If handheld computers become as popular as mobile phones, the amount of thefts could be astronomic. According to The Federation of Communication Services over 15,000 mobile phones are stolen every month in the UK alone.

As sales of handhelds increase, so do the number of connections to corporate networks posing a potential security breach. While companies spend billions of dollars a year on IT security systems, very little is invested in securing an increasingly mobile workforce and the devices they carry. While companies should have this area covered in their corporate security policy, in reality, very few have the necessary security solutions to ensure they are fully protected against breaches. According to the DTI Information Security Breaches Survey, 60% of organizations have suffered a security breach in the last 2 years, yet only one in seven have a formal security policy in place. Only 37% of organizations have undertaken a risk assessment where a systematic approach is taken to assess the security risks faced by the organization.

Even when mobile devices do have security mechanisms installed, users often try to circumvent them due to the time and "hassle" factor related to using them. This gives the illusion of security to the company, since they have deployed the security solution, likely making them more vulnerable, as they are “protected.”

There are many security vulnerabilities associated with mobile devices. Since usability is always more important than security when new technologies emerge, little thought is given to the potential vulnerabilities. However, when new technologies such as handheld and wireless devices enter the corporate world, security and central management become essential pieces of the integration plans for any deployment of the new devices. Obviously, PDAs follow the pattern of usability over security, and the lack of security as a central tenant to the design of these operating systems evident.

For example, the passwords on even the most recent Palm OS PDAs can easily be reverse engineered so that an attacker can determine the original password from the encrypted copy. The attacker could then use this to gain full access to the PDA, undetected.

Another potential weakness is that some of the debugging tools used for application development could be used to copy contents of the device without requiring any user authentication. Once copied, all the information stored on the device could be examined with the knowledge of the user.

While both of these methods require physical access to the device, there are other methods that do not. The methods not requiring physical device access will become more problematic as they are integrated into more devices. Currently the most prevalent of these methods are the short distance wireless communication protocols using IR (Infra Red), and Bluetooth. They have both been designed to communicate with other devices in close proximity, creating a link that can be used to "beam" information from one device to another.

The chief vulnerability in these protocols stems from the default setting on most devices; receive and store, and possibly even transmit, data automatically. This leaves open the possibility that someone will beam unwanted data. Even worse is the risk of someone beaming malicious code that, when activated, might send the information stored on the PDA (or other device) out to the Internet, where it could be further analyzed.

HotSyncing your Palm OS PDA may also open up security holes since a copy of all the information stored on the device is backed up on the computer. Any PDA that can HotSync with that computer would have a complete copy of the latest synced information transferred to the PDA. In an office environment where there are many handheld devices in use, someone could walk up to your computer with an empty handheld, press the HotSync button, and the HotSync program will "restore" all your information to the false handheld as the program thinks you are attempting to restore your device.

Another potential vulnerability is the 802.11 wireless communications protocol, which is becoming more popular for home and office use. The security of the wireless communications is handled by WEP, the Wireless Equivalent Protocol. The default encryption setting of WEP is generally weak (usually encryption is off), and leaves open a huge risk that someone with very inexpensive equipment (which could just be a single wireless network card) will either break the encryption (keys), or become another seemingly valid node on the network. Once on the network, the attacker is most likely behind the firewall, and can listen in to any communication that is going on in your network, including the non-wireless traffic.

While it is true that using software available from various vendors can solve many of these security vulnerabilities, the best way to ensure security is to have one integrated solution protecting against all these vulnerabilities.

So what can be done to secure the mobile workforce without losing the mobility?

8 STEPS TO SECURING YOUR HANDHELD

1. A security policy, specifically designed for handheld devices, needs to be put in place. This policy must be communicated to the workforce. Staff must be told about the security implications of mobile devices, and what action will be taken if this policy is ignored.
2. Fast and easy to use access control an encryption systems which can not be circumvented by the user should be put in place on all mobile devices.
3. Use dynamic passwords or certificates for secure remote access.
4. Perform an audit to determine who in the company is using a mobile device, and the owner of the device, i.e. whether the company or the employee owns the device.
5. Personal mobile devices should not be allowed to hold customer or company information unless protected by the company security system.
6. Use a centrally managed security product that is compatible with all the mobile devices and software versions the company uses.

7. Avoid using products that allow the user to make security decisions. All security decisions should be able to be controlled centrally to avoid user circumvention.
8. Make sure that if handheld devices are used, that the chosen security software protects all known security holes.

There are currently very few security devices available for handhelds and WAP phones as companies are only just now beginning to recognize the need to secure the devices of their mobile workers. However, last month Pointsec Mobile Technologies Ltd. introduced *Pointsec for Palm OS*, an access control and encryption product for mobile devices. This means organizations can have one security system to protect everything from handheld computers, laptops and desktops from unauthorized users. It allows user access to the device only after entering the correct password, and can offer further protection by encrypting data as needed. This recent introduction of a security solution for laptops and PDA's will put an end to embarrassing and potentially damaging leaks of information from the mobile devices used by today's mobile workforce.

Visit www.pointsec.com or email magnus.ahlberg@pointsec.com.