Portable Data Device Security

Over the past 12 months, we have touched on the potential threats that portable data storage devices such as USB flash disks and media players such as the Apple iPod can introduce to an organisation.

Awareness of these threats is growing at the moment and organisations are updating policy and technology to handle these threats. There are a number of specific issues that portable data storage devices of any type introduce. These include introduction of malware, breach of digital copyright legislation, theft of data from an organisation's information systems and potentially breaches of data privacy legislation.

Just as Information Security specialists are getting to grips with the different devices as outlined above, more new ones come along in slight disguise. There are a number of mobile phones available today that actually incorporate hard disk storage, and for those that don't, they provide memory card slots for storage space. This is due to the increased focus of the mobile phone as the portable mulitmedia centre with higher definition cameras and audio player support. These all need increased data storage areas and it is possible to use 4 Gigabyte cards in some, and soon we will have 8 and 16GB cards available.

As has been the case for a significant amount of time, people want to connect these phones to their PCs and synchronise their contacts, emails and calendars with the phone. This means that they are quite up to date even when not connected to the office. One of the downsides of this and the increased data storage available in phones is that this data storage area will often appear as an external hard disk to the operating system on the PC and thus available to copy data to and from. This is another example of a covert channel that can be used to get data in/out from an organisation through non-traditional means. It often happens that people use these devices at home and connect the phone to their home PCs which may not have adequate malware protection. It is also a very subtle and discreet method for a malicious employee to get information out of an organisation. This has been used when a competitor has poached a key employee and sweetened the package based on the amount of confidential information that the poached employee can take with them that would give competitive advantage to the new employer.

Again, it is absolutely vital that devices such as camera phones or digital cameras that are supplied to employees are not used to record, view or transfer digital content that is in breach of the policy. The apprpopriate policies should be updated to take account of these new risks and accepted by the employees to whom the devices are entrusted. This is particularly important in the situation where any inappropriate content stored or recorded on the device is in breach of legislation such as the Child Trafficking and Pornography Act 1998. Any incident that occurs involving such a breach would be very damaging to an organisation and it's brand and reputation.

Another major issue facing organisations that provide these devices to their employees is the disturbing frequency with which these devices are lost or stolen. In the past, this has usually been an inconvenience and financially of little reality but rarely treated with the same concern from a data loss perspective as a laptop would have been. Now, however, with the increased data storage capabilities and connectivity options to an organisations data, loss of mobile phones (and PDAs) must be treated in the same way.

It is possible to purchase the same type of security solutions for these mobile phones today as it for the existing laptops in many organisaitnos. These include full encryption of the data storage areas on the mobile phone, anti-virus software that can get Internet based signature updates, personal firewalls for the Internet connection and even Virtual Private Network (VPN) clients to connect to corporate networks via the Internet.

It is critical that an organisation reviews it policies in relation to the types of mobile phones it provides to staff as the current continuous upgrade cycle from the mobile operators means people will get these new features without specifically requesting them. Many organisations have usage policies for staff in place already when it comes to mobile phones, but most of these usually refer to the costs and charging of personal calls back to staff etc. They rarely outline acceptable usage from a content perspective, but should.

It is also important to determine if it is appropriate that these devices can get unrestricted access to all content on the Internet or whether it is more appropriate to route all Internet access via the organisation's own content monitoring suites of software. That way, enforcement of the organisation's policy can be implemented.

There is also the latest gadget syndrome. Many people are continually getting the latest and greatest technology in phones as a status symbol. When Apple release their long rumoured iPhone early next year, it will quickly become the corporate must-have fashion accessory. However, due to it's strong leaning towards being a portable media centre, the whole area of Digital Rights abuse will be centre-stage. Once again, if an organisation owns the phone, but provides it for use to the employee, and the employee copies their own legal CDs onto the device, the Copyright Act will have been breached. As has happened with style icons like the iPod in the past, the iPhone will also become a target for muggers and pickpockets, and with the theft of the device, so will go any organisationally sensitive data.

It is also a regular policy in many organisations to pass phones from one staff member to another, or even to pass them to another (possible a charity) when the phone is no longer required. However, many are not taking any precautions to protect the sensitivity of the data stored on the mobile phone. This could be everything from the SMS messages, phone contacts to calendar information and data stored on phone based memory. Appropriate secure data deletion tools must be used to prevent data breaches it the device is to be re-used and destruction of data when the device is no longer required.

Bottom line, if it's portable, can store data, gets connected to an organisation's PCs or network , it is a threat and the risk must be handled through appropriate policies, controls and enforcement points.

Rits Group Head Quarters
Information Security Centre
2052 Castle Drive
Citywest Business Campus
Co. Dublin
Ireland

Tel: +353 (0) 1 6420500
Fax: +353 (0) 1 4660468
Email: info@ritsgroup.com
Web: www.ritsgroup.com