

PDA & Smart Phone Business Security Impact



By Marc Froemelt

“These well-connected, poorly-defended devices are fast becoming a lucrative attack target, putting business data and networks at risk.”

Last year a new breed of worms exploited Bluetooth and MMS to reach mobile wireless devices, commonly carried by business executives, racking up toll charges, destroying stored data and resetting infected devices. These well-connected, poorly-defended devices are fast becoming a lucrative attack target, putting business data and networks at risk.

We will investigate business options for securing mobile wireless endpoints like smart phones and PDA's. Specifically, we'll examine the security measures that can be employed to lock down PDA's and smart phones that are used for business.

Market researchers have been predicting explosive growth in mobile device adoption for years. And last year that growth did finally happen; in fact, global shipments of mobile devices, including PDA's and smart phones jumped 75% between the 3rd quarter of 2004 and the 3rd quarter of 2005. Most analysts expect mobile device sales to grow even faster in 2006, a forecast which is prompted in part by expansion of high-speed networks services, such as EV-DO.

Although many mobile devices are now being purchased by individuals, business use of PDA's and smart phones is still expanding. According to a 2005 survey conducted by Nokia, nearly 1 in 4 executives now use PDA's for business. In fact, the workforce that is most likely to carry these mobile devices are those that require ready access to business data, like corporate email, meeting schedules,

contacts, or even instant messages. This growth results in more and more corporate data being placed at risk by these mostly unmanaged and unsecured mobile devices.

Mobile viruses and malware are increasing in frequency and impact, spurred by business adoption and use of targeted mobile devices. This exposes corporate data networks whenever these mobile devices connect, wirelessly or through cradled synchronization, to access corporate data.

Redefining the Network Perimeter

PDA's and smart phones are increasingly tethered to company resources through a myriad of connectivity options:

- Serial/USB port desktop synchronization
- Personal area networks (IrDA, Bluetooth)
- Wireless wide area phone networks (CDMA, GPRS, 1xRTT, EV-DO)
- Wireless local area networks (802.11, WiFi)
- Wireless metropolitan area networks (802.16, WiMax)

In the past, most PDA's and smart phones were used primarily used to connect to the public internet, to browse the web, or to access a personal mailbox. However, as mobile workforces have grown and

companies have opened private networks to permit internet-based remote access for travelers and teleworkers, this access has become pretty common through VPN (Virtual Private Network) gateways, web portals and internet-based servers like Microsoft OWA (Outlook Web Access).

Furthermore, the advent of WiFi and Bluetooth, now common on most mobile devices, means that these PDA's and smart phones can now be connected to access points, wireless printers and other nodes that are inside a company network. Finally, with all the buzz about wireless, it can be easy to forget that those USB connections used to synchronize PDA's and smart phones with desktops PC's actually connect to the corporate network perimeter.

Mobility Benefits and Risks

Regardless how that connection is accomplished, once a mobile device is connected to an enterprise resource, it does become an integral part of your company network. These mobile devices can boost business productivity by providing anytime/anywhere access to corporate data and enterprise applications. Employees find it easier to get work done, even from locations that otherwise might impose unproductive down-time.

However those benefits are accompanied by new challenges. Every mobile endpoint that is used for business requires some degree of IT management. For example, company-owned devices must be inventoried, provisioned and tracked. Every mobile device that accesses your company network and contains business data, including PDA's and smart phones owned by employees,

must be secured to prevent loss or compromise of data.

Ignoring Risk is not an option

To many companies make the mistake of ignoring PDA's and smart phones. They may realize that employees buy mobile devices on their own, but may take the view that those devices are not business computers, hence not requiring IT supervision. The problem with burying your head in the sand is that PDA's and smart phones are used for business, creating hidden risks that may go unnoticed until a security compromise occurs.

For instance how many of us accidentally leave a phone or PDA in a public location, like a taxi, plane or restaurant?¹ How many of us forward company email to a personal mailbox that we then check over an unsecured public wireless hotspot? These situations are actually quite common and can expose confidential company data.

Conclusion

Of course there are many security measures that can be used to secure mobile devices, but without company guidance many workers are either unaware of these risks or unwilling to spend their own time and money to secure their devices.

Hence companies are better off acknowledging business use of mobile devices, educating work forces about mobile threats, and deploying measures to mitigate the associated business risk.



¹ Pepperdine survey of US professionals: 24% lose at least one PDA

http://www.pdatoday.com/more/A1460_0_1_0_M/

Marc Froemelt is a Consultant with Schooley Mitchell in Atlanta
www.schooleymitchell.com/mfroemelt
678.528.6689
mfroemelt@schooleymitchell.com