BYOD: (B)ROUGHT (Y)OUR (O)WN (D)ESTRUCTION?

Righard J. Zwienenberg
ESET, The Netherlands

Email righard.zwienenberg@eset.com

ABSTRACT

Nowadays all employees bring their own Internet-aware devices to work. Employers and institutions such as schools think they can save a lot of money having their employees or students use their own kit. But is that true, or are they over-influenced by financial considerations? There are many pros and cons with the BYOD trend. The sheer range of different devices that might need to be supported can cause problems, not all of them obvious. The paper will list pros and cons, including those for Internet-aware devices that people do not think of as dangerous or even potentially dangerous. These devices are often 'powered' by applications downloaded from some kind of app store/market. The applications there should be safe, but are they? What kind of risks do they pose for personal or corporate data? Furthermore, the paper will describe different vectors of attack aimed at corporate networks and the risk of intractable data leakage problems: for example, encryption of company data on portable devices is by no means common practice. Finally, we offer advice on how to handle BYOD policies in your own environment and if it is really worth it. Maybe 'Windows to Go', a feature of *Windows 8* that boots a PC from a Live USB stick which contains Win8 applications plus Group Policies applied by the admin, is a suitable base model for converting BYOD into a Managed-by-IT device. Remember: BYOD isn't coming to us, it is already here and it is (B)ig, (Y)et (O)utside (D)efence perimeters!

Points to be discussed during the presentation:

- Pros and cons of BYOD
- Overview of all kinds of BYOD
- The apps problem on BYOD
- Potential attack vectors on and data leakage through BYOD
- Advice on BYOD and implementing an appropriate device management model.

INTRODUCTION

The latest trend in the workplace is definitely BYOD: Bring Your Own Device. Not only on account of the employees who regard this as a convenient way to read private email and to browse to (work-unrelated) sites at the office, and moreover as a way to work for their employer on a device they know really well, but the trend is also welcomed by many employers as they think it saves them money on hardware and training on operating the device. The same trend can also be seen in schools: the call for the use of the latest hardware is easily accommodated by allowing students to bring their own devices into school and allowing these devices access to the network. But it's far from clear whether these assumptions of increased convenience and/or a financial advantage in terms of reduced costs are really justified.

PROS AND CONS OF BYOD

According to a recent *BT* survey [1] 60% of employees are already using their own devices in the workplace, and the figure is expected to reach 82% within two years. While power users and employees in IT departments have led the trend, senior management and the Board have been following hard on their heels and are using their own devices on the corporate network, yet only 25% of them are aware of the security risks of BYOD.

Of course there are advantages to BYOD. In most cases the devices are small and lightweight, easy to transport, have a battery life normally lasting a full workday, and are much cheaper to buy than a laptop – especially if the initial outlay is funded by the employee rather than the company. The employees are likely to be more adept at using and working with their own devices, so they do not have to get used to a new device or environment and need little or no training.

But of course there are many disadvantages to this: it is difficult – if not impossible – to manage the content. Updating most often is done via the manufacturer, bypassing corporate QA and often relying on a third-party manufacturer to decide when and whether to apply updates and upgrades. The devices are difficult to protect and outbound traffic is hard to monitor. Using different applications at the same time (multi-tasking) is not possible and many corporate-supported plug-ins (*Flash*, *Silverlight*, etc.) are often not supported. Furthermore, the applications for the different devices are not interchangeable, so that work created on one device may not be usable on or even transferable to another.

It is also very unlikely that VPN Client software will exist for all the different devices that might be used within a single enterprise. Although corporate/sensitive data should never leave the corporate network, especially when no VPN software is available for the device, the risk of employees copying such data onto the device to have access to it while not in the office reveals the biggest disadvantage: theft. As the devices are usually small, they are easily stolen (and easily lost). If the device contains corporate/sensitive data, it is a small step to the information being stolen and misused.

And for the near future, it is just a question of how devices will handle IPv6 (if at all). IPv6 is coming fast, yet the number of devices that support IPv6 is still rather low.

DIFFERENT BYODS

The sheer range of different devices that can be brought into networks can bring about considerable complexity as regards the potential of the device for both functionality and compromise.

Some of the risks are more obvious than others. If we just look at smartphones as a common example, there are many features that can 'assist' a user once the device is connected to a USB port of the desktop. The connected device can serve as:

- An external storage device. And rather often as an external device twice over:

  - Once for storage in the smartphone's internal memory
  - Once more for the smartphone's external memory as (for example) a (Micro-)SD card.
- A modem when the smartphone set-up allows USB-connected devices to use the Internet via 3G (and with current call plans that is usually the default set-up, as it is convenient for everyone).
- A Wi-Fi relay station (an open hotspot), also called tethering, where devices without an Internet connection of their own can connect to a relay device that is connected to the Internet.
- A Bluetooth connection hub.
- An infrared connection hub (although in all fairness, infrared has not proved all that popular).

Other devices have less obvious 'features'. Some people like to take these kinds of devices into their working environment so as to make it feel more like home. Psychologically, a picture playing device may be useful… Or not… [2, 3].

STORAGE CARDS

Some picture-playing devices may have additional features, such as (for example) *Sony*'s *Personal Internet Viewer*. Besides displaying pictures stored in local memory, this device can also display pictures and movies stored on mass-media that can be connected to or inserted into the mass-storage port.

These devices often have a small operating system using commonly available libraries. If these libraries contain potential security holes, it may be possible to take over control of the device using specially crafted pictures. As the device is on the network, the possibilities there are endless (and worrying). Traversing the network, it may try to find open shares with access to interesting data, it may set up a backdoor, or start to serve as a small C&C server, a spam centre, and so on. And of course, as there is often no anti-malware available for the device, this will go unnoticed.

APPLICATIONS THAT CONNECT TO THE INTERNET

Lots of applications connect to the Internet, most often for innocent purposes such as retrieving details of the weather, or to (pre)view email in the inbox. These communications are usually carried as plain text, and tools like *WireShark* are able to view all the details (including passwords), and open the door to misuse of this information.

But devices that are able to connect to the Internet may also have the ability to run an application like *WireShark* themselves, storing all (or selected) corporate communications on the device to be taken outside the corporate perimeter.

UPDATE THE FIRMWARE OR OPERATING SYSTEM

Even if you have validated the device as being completely secure and confirmed that there is no scope for wrongful or inappropriate actions to be taken on or by the device, there may be a firmware update or operating system that brings new (undesirable) features to the device. These features can't be foreseen but can be catastrophic in their implications for security. It is not completely unlikely that mobile devices will start to use the now oh-so-popular public cloud. What if the device, for your convenience, is synchronizing all its data content automatically with the cloud? A nice feature if the device is broken or stolen and you want your replacement device to be identical and to have the same content as was present at the time the other device was lost or broken, but not so nice if the data is now accessible to a thief. Even if the device is PIN- or password-protected, some forensic software (and less legitimate code) is capable of gaining access in no time (by some form of jailbreaking, for example).

It is impossible for a corporate security team to know about *all* the new features introduced in *all* new operating systems, applications or firmware for *all* devices. Where, from a security point of view, one is normally well advised to make sure the latest update, patch and firmware is installed, this may not be the case for devices where the corporate IT team (or a team to which corporate IT is outsourced) is not completely familiar (or familiar at all) with the operation of the device and the software that runs on it.

WINDOWS TO GO

Windows 8 will include a new feature called 'Windows to Go' that allows corporate entities to create a full corporate environment including applications and utilities, booting from a USB drive. After the system has booted from the USB device, all corporate standards, policies and management tools are effective and enforced. This can make an employee's device as safe as any corporate desktop PC.

Windows to Go also comes with a few security precautions. To prevent a potential data leakage, if the USB key is removed, running processes will be frozen. If the USB key is inserted again within 60 seconds, the system will continue to work: otherwise it will perform a shutdown of Windows to Go to prevent sensitive data remaining displayed on the screen or stored in the memory. A Windows to Go USB key can also be protected by *BitLocker*.

Does Windows to Go mean that you are running no risk when your employee's personal device is booted from the USB device?

No, there still is a risk. Assuming that the Windows to Go environment has been set up correctly, so that a VPN is established to the office tunnelling all communications, there is still the problem of the uncontrolled Internet itself. While the corporate network is protected by a firewall, the personal device can also be used in unsafe environments, introducing other risks of compromise and infection. But of course that is no different from the case of any other corporate device that leaves the safe perimeter of the corporate network, such as a laptop that is connecting to the Internet in a hotel or at a hotspot.

CONCLUSION

For anyone thinking that BYOD is a problem for the (near) future rather than right now, here is your wake-up call: the

future is already here, including all the attendant risks. It is almost impossible to prevent people from bringing all kinds of devices into the workplace, short of the physical measures associated with state security agency buildings. Even wristwatches with cell-phone functionality (including Internet access) and also a USB-port already exist. It is time for you to take BYOD seriously and re-engineer your corporate policies around it. Integrating Mobile Device Management (MDM) inside your corporate IT management protocols is a must. Otherwise, sooner rather than later, you will find your corporate data exposed and misused.

REFERENCES

[1] http://www.blog.bt.com/LetsTalk/index.php/2012/05/research-shows-majority-of-it-managers-recognise-benefits-of-byod/.

[2] http://blog.eset.com/2007/06/23/open-item-attack-gadgets.

[3] http://blog.eset.com/?s=digital+photo+frame.