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

Righard J. Zwienenberg
Senior Research Fellow
ESET, The Netherlands

Outline

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
- Conclusion

Introduction

The latest trend in the workplace is definitely BYOD: Bring Your Own Device.

In Businesses…

In Schools…

But….

PROS AND CONS OF BYOD

According to a recent *BT* survey 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.

PROS AND CONS OF BYOD

Advantages to BYOD:

- Devices are small and lightweight
- Easy to transport
- Have a battery life normally lasting a full workday
- Much cheaper to buy than a laptop
- Easy adaptation

PROS AND CONS OF BYOD

Disadvantages of BYOD:

- Manage the content.
- Updating
- Difficult to protect and outbound traffic is hard to monitor
- No multi-tasking
- Corporate-supported plug-ins often not supported.
- Applications for the different devices are not interchangeable

PROS AND CONS OF BYOD

Disadvantages of BYOD:

- VPN
- Easily stolen
- IPv6

DIFFERENT BYODS

Questions:

Should we allow BYOD at the work floor or any (professional) environment for that matter?

Can we (still) stop it?

Would you be able to…

Would you be able to spot this one?

Or would you be able to spot this one?

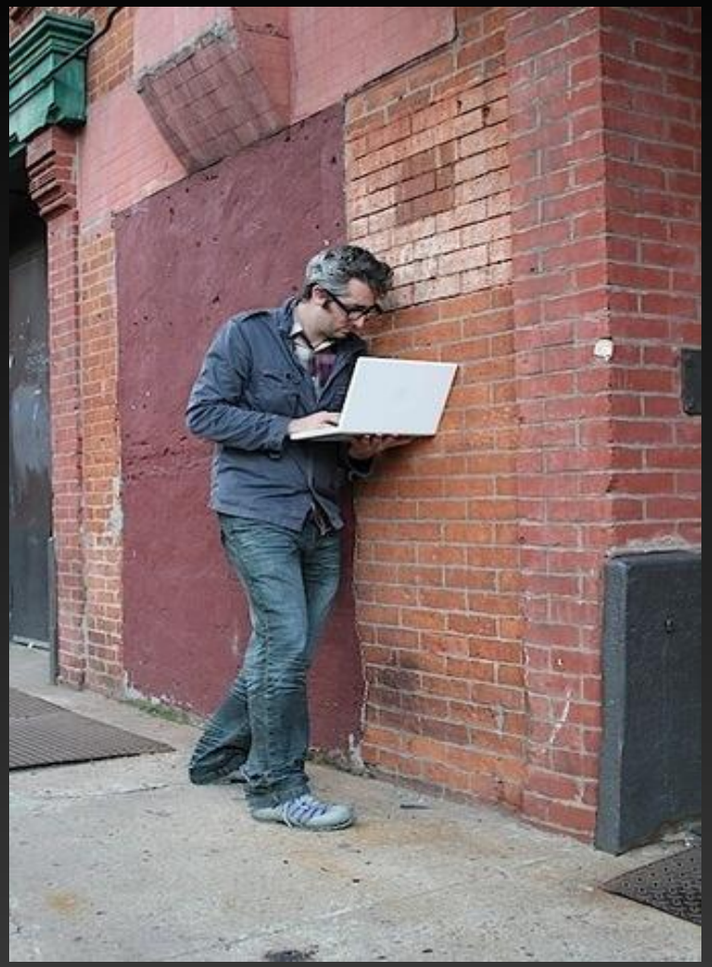
Or would you simply forget?

Or…

Or didn’t you spot it as it is lunchtime?

Or…

And then…



A joke? No fact!

GIZMODO

TOP STORIES

ART

Why Is There a USB Drive Sticking Out of This Wall?

Across New York, there are USB drives embedded in walls, buildings and curbs. The idea is to create an anonymous, offline file-sharing network in public space. The drives are completely public and anyone can plug in to drop and download files.

Seriously, you can plug the USB drive into your laptop. Like that guy right there.

It's part of an art project called "Dead Drops" by Aram Bartholl and I have to say, it's pretty awesomely creative. I mean, if I saw a USB stick stick out of a random wall, I'd be dying to know what's in there. I'd have to plug in. It'd also be interesting to see what people would anonymously share on the public drive, well, until some jackass decides to upload a virus to screw up everybody's computer. [Dead Drops via MAKE]

http://gizmodo.com/5677377/theres-a-usb-stick-in-my-brick-wall

And then…

What is included in the conference package at several conferences?

Banning USB Devices Is Not Realistic

So many “foreign Media”, so ,many devices!

eset

DIFFERENT BYODS: Smartphone

When connected to the USB port of a system, it can be used 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

DIFFERENT BYODS: Smartphone

When connected to the USB port of a system, it can be used as 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)

DIFFERENT BYODS: Smartphone

When connected to the USB port of a system, it can be used as 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

DIFFERENT BYODS: Smartphone

When connected to the USB port of a system, it can be used as a Bluetooth connection hub

DIFFERENT BYODS: Smartphone

When connected to the USB port of a system, it can be used as an infrared connection hub

DIFFERENT BYODS: Other

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…

STORAGE CARDS

- (Picture-playing) devices may have additional features, such as (for example) *Sony*'s *Personal Internet Viewer*.

STORAGE CARDS

Main feature:

- Displaying pictures stored in local memory

Additional features:

- Display pictures and movies stored on mass-media

What most people do not realize:

- These devices often have a small operating system using commonly available libraries.
- As the device is on the network, the possibilities there are endless (and worrying).

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.


21:06
Tue. Ma
Set Alarm
The Hague
18°C
RANDOM
refresh
Error loading pun
Update available
Control Panel Update
A software update is available. It may take 30 seconds or longer to install.
When would you like to install this update?
Now
Later
pun
Reversi
ARTILLERY
SONY


21:07
RANDOM
refresh
Update available
Control Panel Update
A software update is available. It may take 30 seconds or longer to install.
When would you like to install this update?
Now
Later
18°C
Reversi
SONY

From: Sony Electronics <support@info.sel.sony.com> Sent: Wed 05/09/2012 23:11

To: [redacted]

Cc:

Subject: dash(TM) Server Maintenance Advisory

Dear dash(TM) Customer,

We would like to inform you that we will be performing routine maintenance on our dash(TM) servers beginning Wednesday, September 5th at 7:30am PDT and ending at 7:30pm PDT. During that time, dash(TM) services will continue to function as normal, but you will not be able to register a new device, create a new dash account, or make changes to existing dash(TM) accounts, applications or services. If you have any issues with device you can contact Sony Customer Support at 866-918-2485 or visit our support website at www.sony.com/dashsupport. We thank you very much for your continued loyalty to dash(TM) and Sony.

Team dash(TM)

Sony Electronics

From: Sony Electronics <Sony-Electronics@sel-email.sel.sony.com> Sent: Mon 24/09/2012 23:40
To: [redacted]
Cc:
Subject: Important Notice Regarding Your Dash

View Web Page

SONY
make.believe

Dear Valued Sony Customer,

Thank you so much for your patience over the last week as we worked out a few issues on our dash™ servers. We sincerely apologize for the frustration and inconvenience this may have caused you

If you're still experiencing a problem on your dash, you can reboot it by removing and re-applying power, it should then work properly once it powers up. If you continue to experience an issue with the device, you are more than welcome to contact the Sony Customer Support team at 866-918-2485 or visit our support website at http://www.sony.com/dashsupport.

We thank you very much for your continued loyalty to dash™ and Sony.

Best Regards,

Team dash™

UPDATE THE FIRMWARE OR OPERATING SYSTEM

Corporate Security Team, it is impossible for them 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

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*.

WINDOWS TO GO

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 tunneling all communications, there is still the problem of the uncontrolled Internet itself.

WINDOWS TO GO

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.

IF WINDOWS IS NOT YOUR ENVIRONMENT

Why should you allow all these devices on your network?

Use a form of Device Control

Yes, you run the risk that e.g. a USB Flashdrive is lost “in public”

But… Encrypted when the data is exported, you only loose the device when it is lost

Why Device Control?

- Malware are specialized to infect through attached devices
- Control which port interfaces are available to users
- Avoids data leakage
- Monitor which files are copied out to portable media

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.

CONCLUSION

Update from BYOD to CYOD!

Choose Your Own Device

And just select the devices that you can manage, that allows corporate protection to be installed and that has updates.

Thank You!

If you have Questions,I may have Answers!

Righard J. Zwienenberg
Senior Research Fellow
ESET, The Netherlands

Email: righard.zwienenberg@eset.com
Twitter: @RighardZw