Bring Your Own Risk

On Your Own Device

Rene Graf & Enno Rey
{rgraf, erey}@ernw.de

Who we are

- Old-school network geeks, working as security researchers for
- Germany based ERNW GmbH
  - Independent
  - Deep technical knowledge
  - Structured (assessment) approach
  - Business reasonable recommendations
  - We understand corporate

- Blog: www.insinuator.net

- Conference: www.troopers.de
  (You obviously found that ;-)

Agenda

- Intro & "Device Lifecycle"
- Going through the Lifecycle
- Conclusions

The “mobile world” is getting crazy

The devices

Taipei

Eee Slate
ASUS

swissbit

iPad
ERNW
providing security.
Workshop in progress.
TROOPERS

Google
SAMSUNG

The operating systems

open-source experts from all over the world, Ubuntu is available in 24 languages and ready for download today.

It's open source.
Our global community is made up of thousands of people who want to help build the best open-source operating system in the world.

There are quite some flavors of mobile device usage out there!

There's the traditional way …

Corporate owned devices

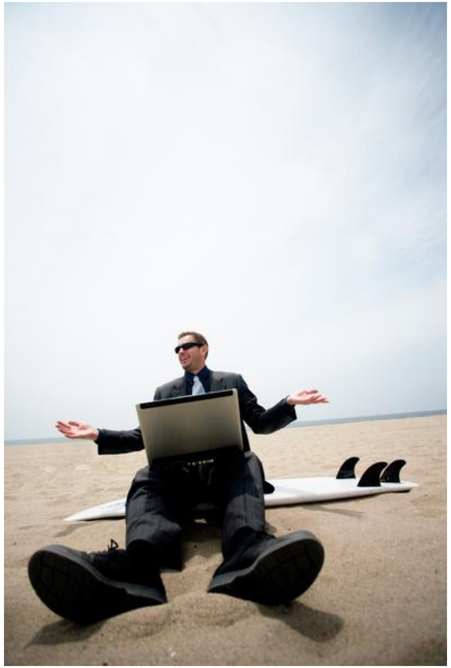
What We Actually See in the Wild

¬ Corporate device with corporate use only (o rly?).

- Will probably not work with all the "smart devices" out there.
- Still, some (organizations) try to.

Corporate owned devices

What We Actually See in the Wild



¬ Corporate device with private use allowed

- That’s what we actually see a lot out there.
- At least when “the new mobile devices” are “in place”.

Then, there are private devices

What happens when you do not support "these modern devices at all"?

The Reality

What We Actually See in the Wild

- People just bringing their devices in and connecting those to WLAN / EAS (or $SOME_BACKEND).
  - In quite some orgs any technically savvy user can do that.
  - Even seen, that users switch SIM cards from BB to $SMARTPHONE.
- Users forwarding $CORP_EMAIL to their gmail accounts, to open them while sitting on the couch with their (private) iPads...

You think that is not the case in your environment?

Ever had a look at your MS Exchange logs?

If you allow private devices

…

…

that would be called “Bring your own device” (BYOD).

And that´s what this talk is about!

Motivation

Why do this?

- FIRST: It's NOT about saving money!
- Enable users to "work with their favorite device"
- Make them "available in their free time" => That's evil ;-)
- Users have to carry only one device.
  - Btw. You can also achieve this by allowing private use of corporate devices.

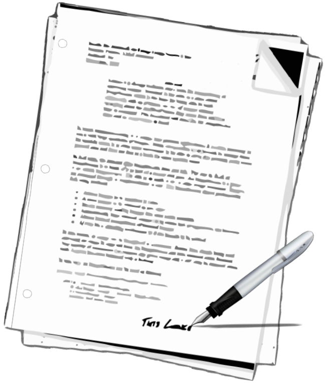
The Talk's Message on One Slide

- BYOD = fundamental paradigm shift
- When looking a at device's full lifecycle, it seems that in many BYOD discussions some risks might not be considered appropriately.
  - Just looking at container solutions (and AUPs, if at all) might not be sufficient.
- So, the goal of talk:

→ Enable you to get a better understanding of the risks associated with BYOD, and how to potentially mitigate them.

The Reality

- Organizations supporting BYOD often rely on container apps for data separation.
  - And maybe AUPs.



- Question is: Is that sufficient?

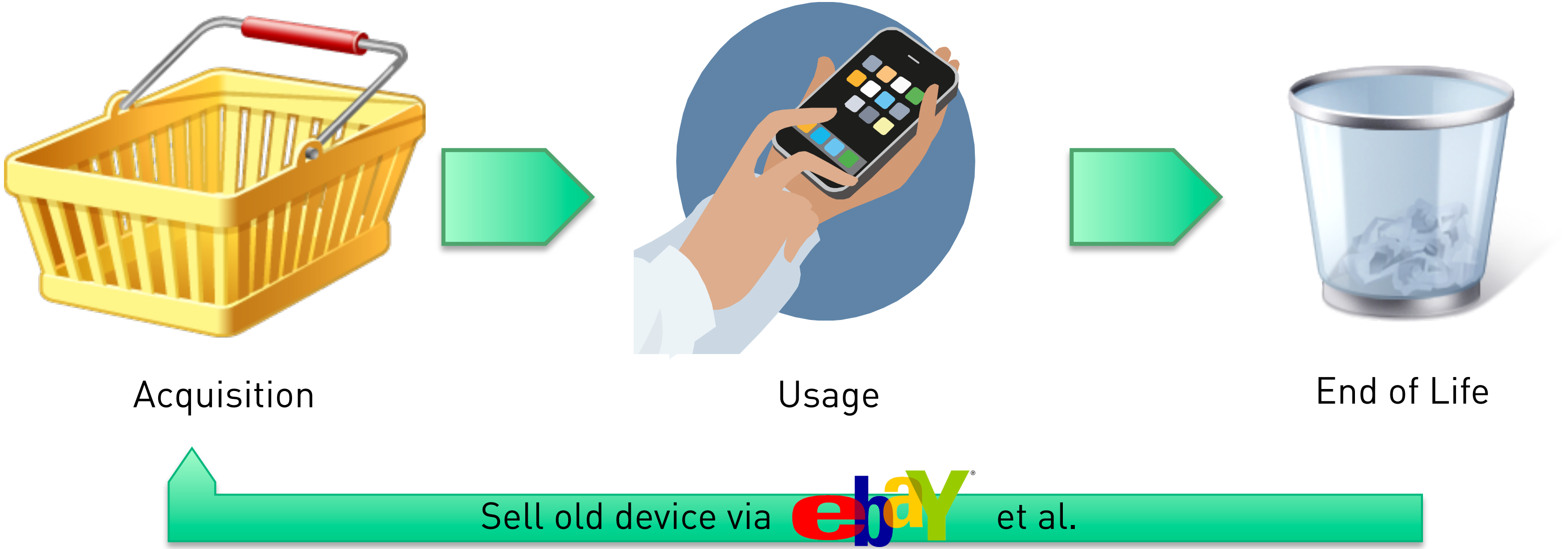
Just to make this clear

- We‘re not “against BYOD“.
  - Or container apps, for that matter.
  - And BYOD might be one of the fights you can‘t win anyway.

→ So we just want to cover some aspects that we think are often overlooked.

Let´s have a look at a typical MD´s lifecycle

Lifecycle



Acquisition

Usage

End of Life

Sell old device via ebay et al.

Three Angles

- How does $SOME_STEP_FROM_LC usually work with a "company managed approach"?
- How is it potentially performed in a BYOD world?
- What can go wrong, in BYOD world?

Initial Acquisition

Company managed device

- Careful selection of devices, based on their (well-understood?) features
- Supply chain to some degree “known and trusted“.
- Supply chain potentially covered by contracts.
  - At least as part of general T+C.

Initial Acquisition

BYOD

- A mess!
- Supply chain "unknown and potentially not trustworthy"

- Potentially no or weak legal/ contractual controls.

Initial Acquisition

What can go wrong?

A story from the field.

- Device “already low level compromised“ might not be “securable“, even with $CONTAINER.
- Do you trust that brand new iPad 3 you can win @Troopers? ;-)
  - BTW: 1729-6671-2834-5338-9309
- Or that “brand new smartphone prototype“ the VP of R&D just received at a fair trade in $SOME_EMERGING_MARKET?
- User buys device which no longer gets updates.

Initial Acquisition

What we suggest

- Take clear stance if jailbroken/rooted devices to be allowed within BYOD or not.
  - Might contradict "full liberal approach".
- User education on supply chain importance & issues.
- Try to govern supply chain ($ORG buys devices and gives those away)?
  - Will probably not work, for a number of legal or psychological reasons.
- $ORG gives user some money (as some bonus) to buy device
  - User may then by cheap ones $SOMEWHERE to "earn some money"

Device in Use

Company managed

- The device is mostly used for company purposes.
  - And secondly for private stuff (if allowed).

Device in Use

Company managed

¬ $ORG imposes the rules.

- How they are protected (Passcode)
- What restrictions are enforced.
- What backend services ([i]Cloud) may be used.

Device in Use

Company managed

- $ORG imposes the rules.
  - What software / apps are installed / prohibited.
  - Which platforms are allowed
    - iOS, Android, WP7, BB, ...

Device in Use

Company managed

- $ORG imposes the rules.
  - To what extend private use is allowed.
    - Who else may use the device
    - Which media content is allowed to store.

Device in Use

Company managed

- $ORG imposes the rules.
  - If, where and how the device syncs / backups its contents
  - iTunes, iCloud, Google Sync, ...

Data in Use

BYOD

- Majority of device use for personal/ private purposes.
  - Willingness to physically hand over device to other persons probably higher.
    - Can/should be addressed in AUP.
  - Willingness to forward emails to gmail account might (even) be higher.

Data in Use

BYOD

¬ User makes the rules.

- Or at least decides what $ORG may do with her device.

→ Ever tried prohibiting app installation ? ;-)

Data in Use

BYOD

- No restrictions regarding apps
  - User won't accept "Facebook denied"
  - User installs "whatever app she wants"
  - Majority of applications from $SOMEWHERE.

Data in Use

BYOD

- Users also probably won’t accept strong monitoring of his/her device.

  - Especially not the workers council.

Data in Use

BYOD

¬ User cannot be advised to perform certain steps (update, ...) as device is not owned by $ORG

- (can be locked out, but that's all)
- Also, try wiping the device of your boss cause of missing patches ;-)

Data in Use

BYOD

- Devices cannot be audited
  - would you let your private device be audited by $SOME_IT_GUY? ;-)

What can happen

- Device can get lost / stolen
  - Positively, if the user forgets his device somewhere, she might put more effort in getting it back (cause its her own asset / money)
  - So you wipe the device / container & replace the device, right?

What can happen

- Device can get lost / stolen
  - Oh, wait. It's the users responsibility to "get a new one".
  - Which might take some time, as users typically do not have replacement devices.
  - Which in turn leads to users not being fully "work ready" for a couple days.

What can happen

¬ Broken breaks down

- So you'll wipe it before sending it to repair, right?
- What if this is not possible anymore?
- If it's a VIPs device, you would probably just replace it and destroy the old one.
- If this is a private device, the user will send it back anyway.

What can happen

- And what about a replacement?
  - For private devices, this typically takes longer, as users do not have the "business flag".
  - What if the user has no money left to buy a new one? ;-)

What can happen

- And what about restoring data?
  - Ok, container solutions typically cover this by simply provision the device.
  - But if no container is used, users may not have access to a backup (home PC)
  - You also cannot backup users devices cause of privacy law limitations.
  - And as you do not want to have $ILLEGAL_MEDIA on $ORG systems.

What can happen

- Users private device gets compromised / infected.
  - And this device probably will contain corporate data / credentials within the backup (depending on the container solution)
  - Also certainly, some $CLOUD_SERVICE_CREDENTIALS are stored on this box (iCloud, ...)
  - Which in turn will probably hold backed up data.

What can happen

- User’s $CLOUD account gets compromised.
  - Which again possible contains corporate data.

What can happen

¬ Regarding cloud services …

- As you cannot forbid cloud usage.
- Some of them may affect corporate data, even if it is not allowed to use cloud services.
- Think of iMessage
  - cheap for international MSGs
  - If a users uses this service, this also affects corporate “SMS” messages (passwords and the like)

What can happen

- Malware infection
  - What would you do normally?
  - Investigate / analyze it forensically?
  - Well, the user decides if he/she gives the phone to you.

What can happen

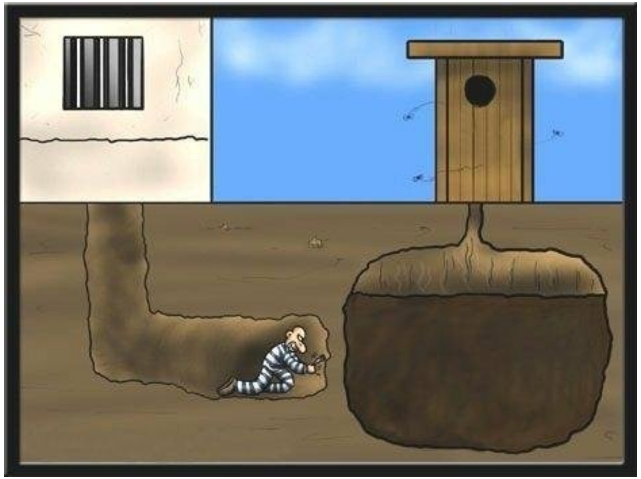
- User not ready for work
  - Regarding his/her data plan
  - If the users is roaming, he/she might not be willing to pay for roaming costs
    - And thus doesn‘t
  - Or users get locked due to unpaid invoice

What can happen

- User may press charges on $ORG
  - $ORG wiped device due to policy violation (Jailbreak, …)
  - Destroying users data (the pictures he took from some relative's marriage and was supposed to deliver them).

Data in Use

What can possibly go wrong?



¬ Container solutions might not provide the maturity you expect.

- Did you hear Dmitry's talk this morning, on password safes?
  - This might give an idea as for the overall maturity of security software in the mobile device space.
- In the course of a pentest we found a major flaw in a major solution.
  - On Android, under certain (not too uncommon) circumstances, temp-files stored outside container.

Data in Use

Our recommendations

- Good accompanying AUPs needed in case $container used.
  - No corp data ever to be handled outside container.
    - E.g. forwarded to gmail account.

- Evaluate (before project! ;-) if $USER_POPULATION is willing to accept restrictions of container.
  - I mean it´s VIPs…

- Perform own pentesting or ask for detailed security reports.
  - See above, whole space still a bit immature.

Don‘t Forget

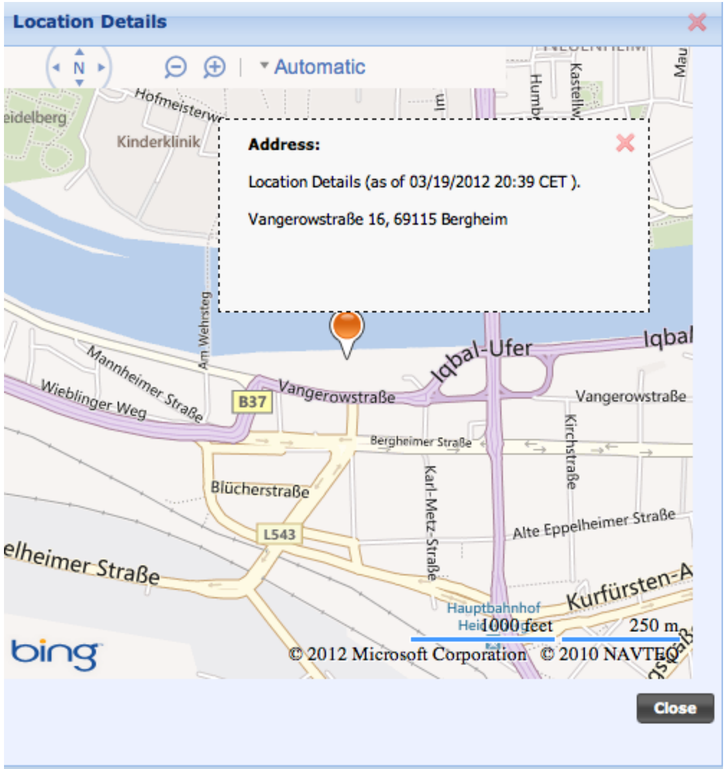
There Might be New Threats from the User‘s Perspective, Too

- User‘s private device can be located from company.
  - Which the workers council may not like that much ;-)
  - And the user neither.
- Think about:
  - $ADMIN likes $SECRETARY
  - And “by accident” shows up at the same bars.

Co workers location

A hotel? Oh, wait. Who else is there?

Or, what is he doing at my home?



Location Details

Address:

Location Details (as of 03/19/2012 20:39 CET).

Vangerowstraße 16, 69115 Bergheim

9826-2511-9934-5752-4666

End of life

Company owned

- $ORG takes them back.
- And [hopefully] decommissions them accordingly.
- Maybe, instead of selling them, $ORG destroys them.

End of life

BYOD

- User sells device on ebay
  - See our decommissioning newsletter
- Give to friends/kids/spouse
- Give to ERNW for hacking lab ;-)
- And probably asks to provision his new device after that (and then its too late to give advice).

End of life

What can possibly go wrong

¬ Data exposure

- $ORG getting bad press
- Nobody will ask if it was a private device, if $CONF_DATA shows up on the internet.

Conclusions

- Acceptable use policy
- Think about the _whole_ lifecycle.
- Separate private / business data
- Limit local data storage

There's never enough time...

THANK YOU...

...for yours!