Cyber and information security: have we all gone mad?

bert@hubertnet.nl / https://berthub.eu/

https://berthub.eu/cyber-mad/

Held at TU Delft, department of Technology, Policy & Management

We have now sunk to a depth at which restatement of the obvious is the first duty of intelligent ~~men~~ people - George Orwell.

A rousing quote. But I do think our cyber and privacy norms have now eroded so badly that it may be good to restate this obvious fact. In this presentation I don't just want to say things are terrible, but I would like to say things changed a lot, and we may not be aware enough of that. Either we are mad now or we were mad before.

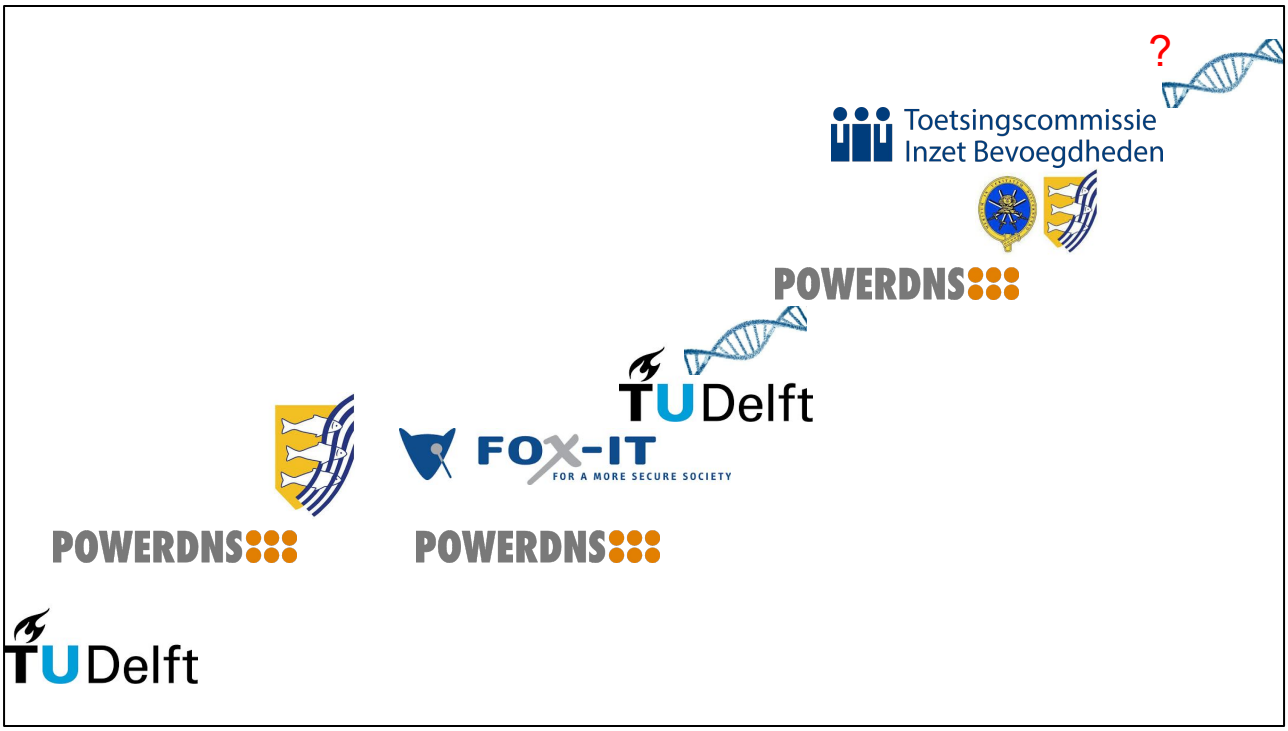
We have now sunk to a depth at which restatement of the obvious is the first duty of intelligent ~~men~~ people - George Orwell.

(or perhaps not! Can't find this quote anywhere! UPDATE! It has been found!)

Supposedly from "Facing Unpleasant Facts: Narrative Essays". But it is not in there! It is a good compilation though.
UPDATE: The quote is from George Orwell's review of Bertrand Russel's 1939 book "Russell's Power: A New Social Analysis". This review is worth reading: https://www.lehman.edu/faculty/rcarey/BRSQ/06may.orwell.htm

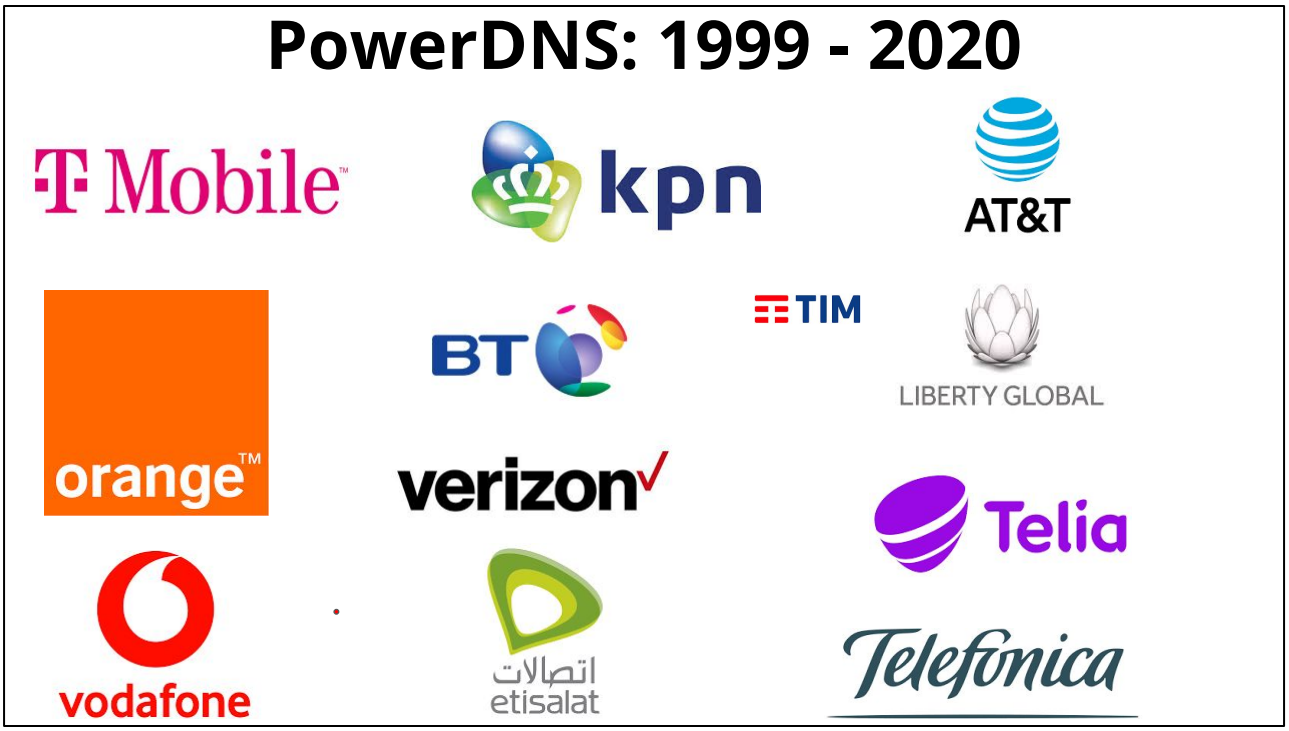
Credit:
James Lee
FormerIP
Wikipedia
Commons

https://en.wikipedia.org/wiki/Boiling_frog you will read everywhere that if you boil a frog slowly enough, it will not notice. Turns out we know exactly at which temperature different kinds of frogs become uncomfortable.



Things I have done - only interesting to put my (strong) claims on later pages in context. I failed in my studies of physics, launched an unsuccessful startup (PowerDNS), and when that did not go well joined Dutch intelligence & security agency AIVD. From there I went on to develop software for police and intelligence agencies, while PowerDNS went on. After Fox-IT I did DNA research in Delft again, and then focused on PowerDNS again. After that, I became a regulator of Dutch intelligence services for 2 years. During this time I managed to get my DNA paper published in Nat. Scientific Data.
https://www.nature.com/articles/s41597-022-01179-8

This committee that regulates the Dutch intelligence and security agencies is/was unique in that it employs technical specialists at the heart of a place that in most countries only features lawyers. If you work at a department that studies policy and technology, this should warm your heart!
https://www.politico.eu/article/intelligence-watchdog-bert-hubert-netherlands-hacking-cyber-law/ has some stuff on this committee.



For PowerDNS, I worked with people from a lot of different big telecommunication companies. There we also had to deliver highly secure but also very high performance solutions. Such solutions contained browser filtering preferences, which are very privacy sensitive.

Historical norm (1990s)

- Software could not talk to outside world:
  - No network
  - Often no internet
  - **Very strong** norms against "phone home"
    - https://en.wikipedia.org/wiki/Phoning_home (2008 page)
  - Would repeatedly ask for permission before even being allowed to check for updates
    - Let alone install them!
  - Sending out any kind of metrics or telemetry unthinkable

The phoning home page mentions that this is actually illegal! Not quite true probably, but it shows how we looked upon software talking to its masters back in 2008

Ownership

Norm was: software and hardware were very much 'owned' by the operator

Island culture

For better or worse

Additional norm: installing upgrades was a lot of work, strong dislike against having to install fixes all the time

I want to make it very clear that this is not a talk about how everything used to be better. This island culture was not good, for example. Lots of technology was only accessible if a company employed a ton of geeks. If you could not afford the geeks, no technology for you. So some things are actually better now.

The transition

Later:

- Phone home is good actually (warn user about updates)
- Nag about updates
- Perform updates silently

Metrics:

- Some metrics are good (crashes for example)
- No need to ask for basic metrics
- Optionally send out all kinds of metrics
- New normal, every click is logged w/o clear permission

For the last line, Spotify for example literally logs every click, scroll, pause, search or change in volume. And it never asked you about this.

Controversy about privacy issues [edit]

The Pentium III was the first x86 CPU to include a unique, retrievable, identification number, called Processor Serial Number (PSN). A Pentium III's PSN can be read by software through the CPUID instruction if this feature has not been disabled through the BIOS.

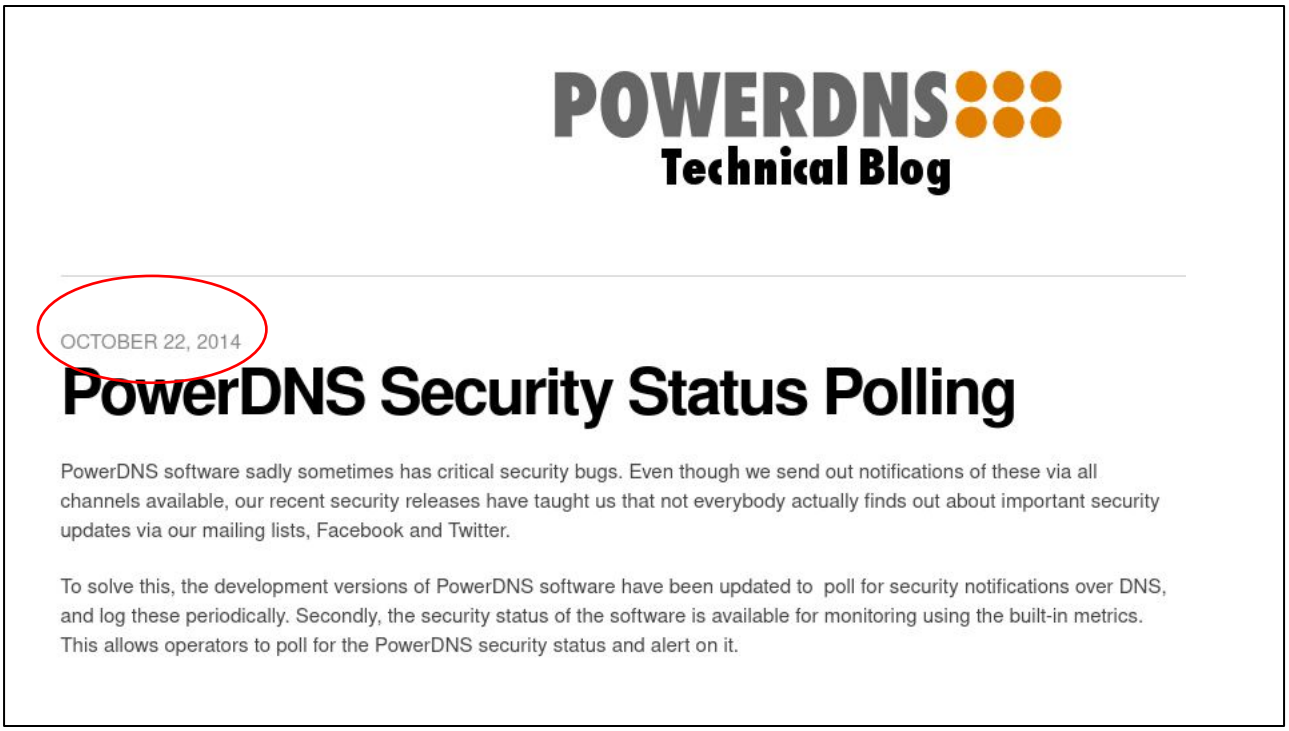
On November 29, 1999, the Science and Technology Options Assessment (STOA) Panel of the European Parliament, following their report on electronic surveillance techniques asked parliamentary committee members to consider legal measures that would "prevent these chips from being installed in the computers of European citizens."[20]

Intel eventually removed the PSN feature from Tualatin-based Pentium IIIs, and the feature was absent in Pentium 4 and Pentium M.

A largely equivalent feature, the Protected Processor Identification Number (PPIN) was later added to x86 CPUs with little public notice, starting with Intel's Ivy Bridge architecture and compatible Zen 2 AMD CPUs. It is implemented as a set of model-specific registers and is useful for machine check exception handling.[21]

2015

https://en.wikipedia.org/wiki/Pentium_III#Controversy_about_privacy_issues - if you remember one slide from this presentation, this is the slide to remember. It may be comforting to know that the 2015 'PPIN' can only be seen by the operating system. However, the operating system is free to relay this data to applications. And given how Windows 11 works, it will probably help you make this happen.



Even in 2014, PowerDNS had to very carefully ask the community if it was ok to “phone home” for security updates. Various Linux distributions promptly disabled this feature.

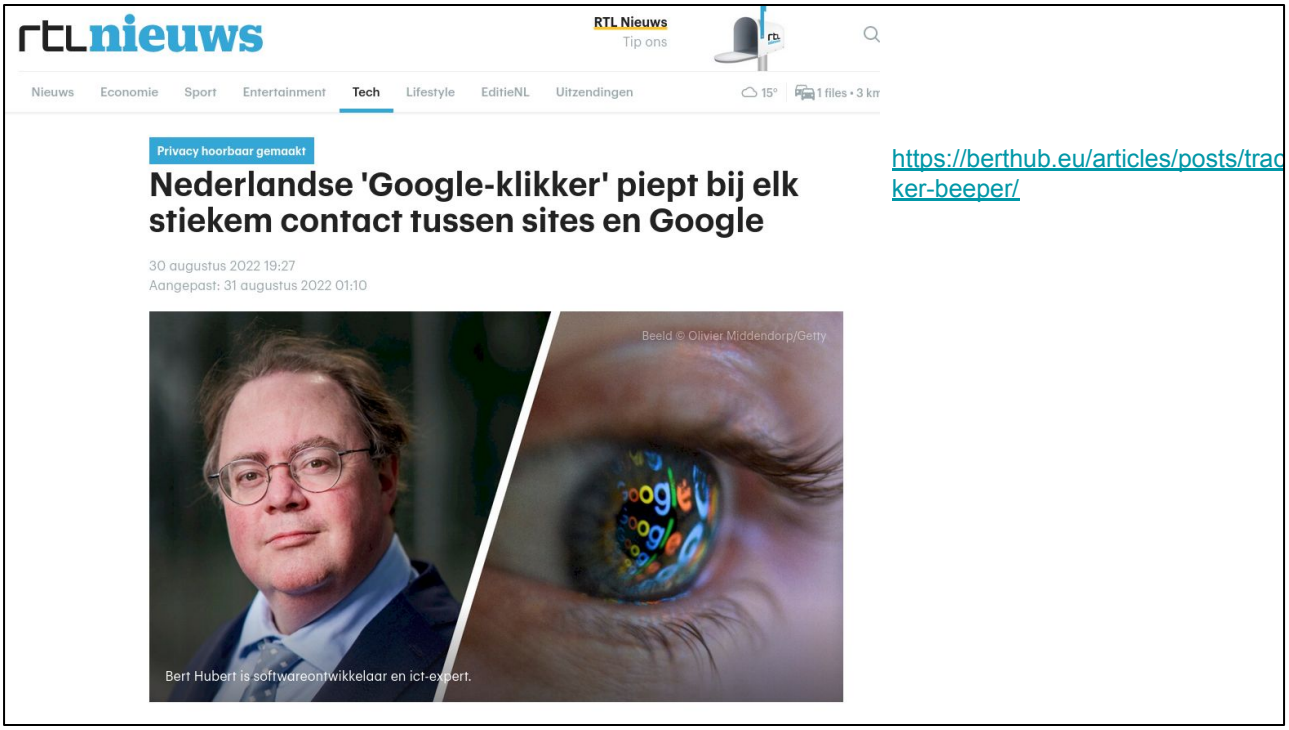
Procession

- 1999: A CPU can not leak its serial number
- 2000s: “Polling if there is a security update is **unacceptable**”
  .
  .
  .
- 2015: CPU serial number is not worth our attention
- 2022: It is entirely ok to log every click on the official government jobs site to Google
  - By default, no notification
- 2022: It is entirely ok for most banks to log every click to Google, including user information once logged in, to Google
  - Even after choosing ‘minimal tracking’

Both the Dutch government and banks do not find this a problem!!1! However, eventually it reached the right people, and something might happen now https://www.security.nl/posting/773126/Overleg+over+wenselijkheid+trackingcookies+op+Nederlandse+overheidssites?channel=rss

Credit:
James Lee
FormerIP
Wikipedia
Commons

https://en.wikipedia.org/wiki/Boiling_frog - the frog is a lot smarter than we are!



https://berthub.eu/articles/posts/tracker-beeper/

Click on the link to hear my little “Google Beeper” tool. It beeps everytime a packet goes to Google (but not to the Google cloud). Caught some international attention from Austrian and Belgian press too.

“Zero trust”

Software talks directly to its company

First fully encrypted

With decryption possibility (MITM proxy)

Then removed decryption capability (Certificate transparency/pinning)

Then removed **detection** capability

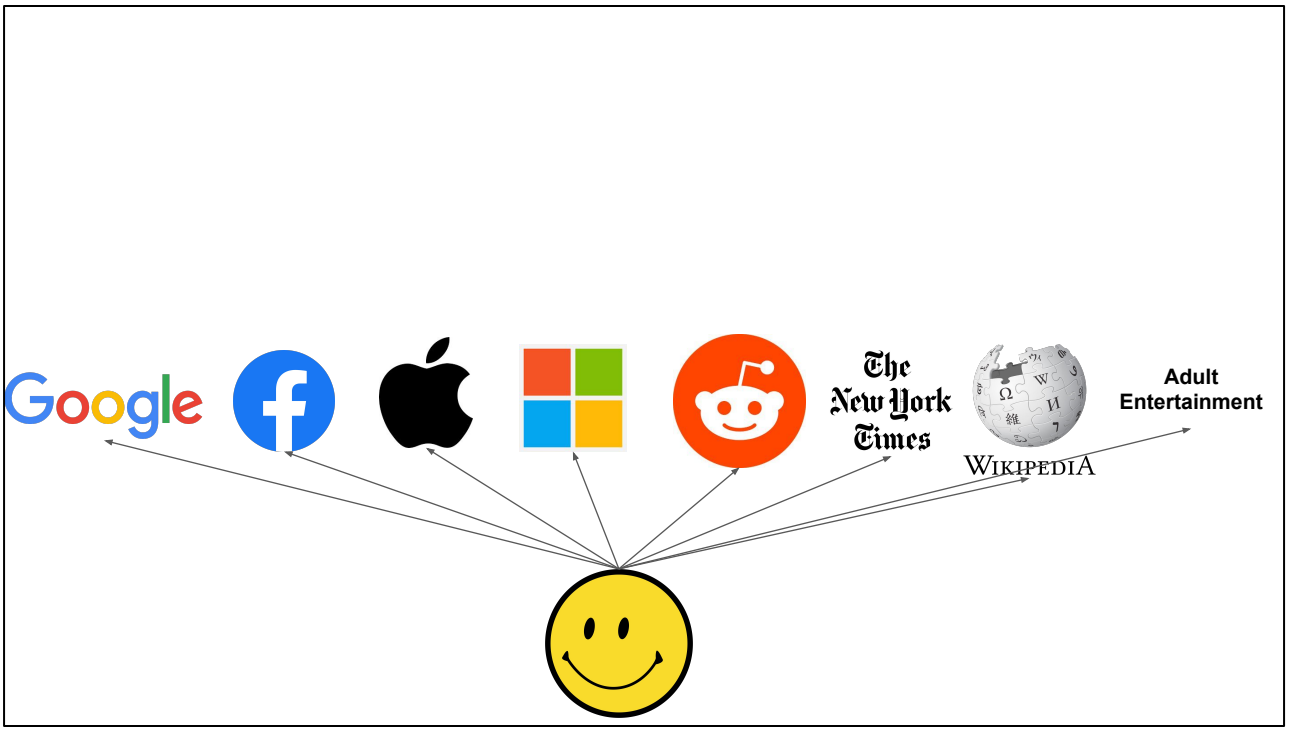
DoH / ESNI / ECH https://blog.cloudflare.com/encrypted-client-hello/

Your network is no longer your network! No idea what is happening there

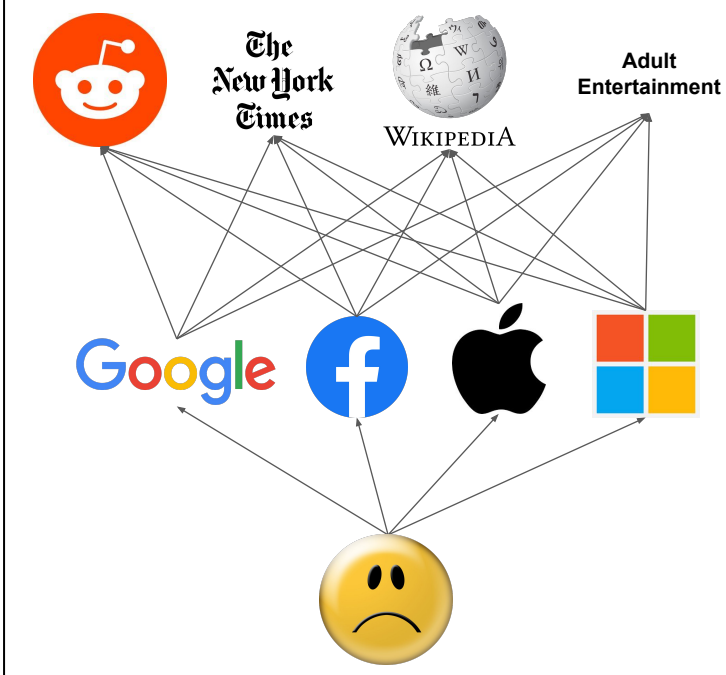
Need to hack your phone to find out what it is doing

https://www.tcd.ie/news_events/articles/study-reveals-scale-of-data-sharing-from-android-mobile-phones/

This transition is currently ongoing. The link to the work of Trinity College in Dublin is worth your while. Their research continues, and everytime Google feels really bad about what they discovered. Every time!



How you (think you) browse the internet today.



- VPN by Google One (US only)
- (Facebook Onavo)
- **Apple Private Relay**
- Microsoft Edge Secure Network

Everyone is now trying to put themselves between you and content providers. Apple is furthest along with this and has spent hundreds of millions of dollars on this project. Ostensibly this is all about your privacy, but little good has ever come from adding gatekeepers to a network.

The frog is now surely boiled

Procession

* Unacceptable and/or illegal
* Ask for permission
* **Nag** for permission
* No longer (explicitly) ask for permission
* But, you can still turn it off
* You can no longer turn it off
* But you can inspect what gets sent
* You can no longer inspect what gets sent, but you can see it happens
    * You can no longer determine that it happens
* **Company lies that it is not happening**

This appears to be a pretty universal schedule of how norms erode.

Windows 11

“**By default**, Windows 11 tracks your activities and sends the information to its advertising partners, who can then show you targeted ads. Your personal information is contained within something called an advertising ID – but this can be turned off if you know where to look”

The very basics, the actual operating system, is corrupt.

o_O - if the very bedrock of your computing already sells you out, what can you do?

A bit on security

The privacy situation is bad. But get a load of this.

Security

- (very) historical: you run **your own software** on your own hardware in your own building
- Longer norm: run someone else's software on your hardware, which you install and maintain yourself
- Slow shift to more and more external support

  .

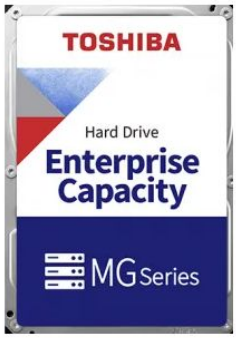
  .
- Absolutely unthinkable to run any kind of hardware on premise
  - "Do you also generate your own electricity?!"
  - "Or mine your own coal?!"

Again a huge transition. If you try to install a server at a modern company this is about as hard as trying to install a coal fired energy generator. Everything _must_ be in the cloud.

317 euros, 18 TB. Costs 1800 euros to transfer out of Amazon

Toshiba MG09 Series MG09ACA18TE - Vaste schijf

18 TB - intern - 3.5" - SATA 6Gbs - 7200 tpm -buffer: 512 MB



Belangrijke specificaties

Fabrikantcode	MG09ACA18TE
EAN	4260557511664
HDD omvang	3.5 "
HDD capaciteit	18000 GB
HDD rotatiesnelheid	7200 RPM
Interface	SATA III
Soort	HDD
Component voor	NAS

Bekijk alle specificaties

TOSHIBA

Artikelnummer: 4610472

317,23

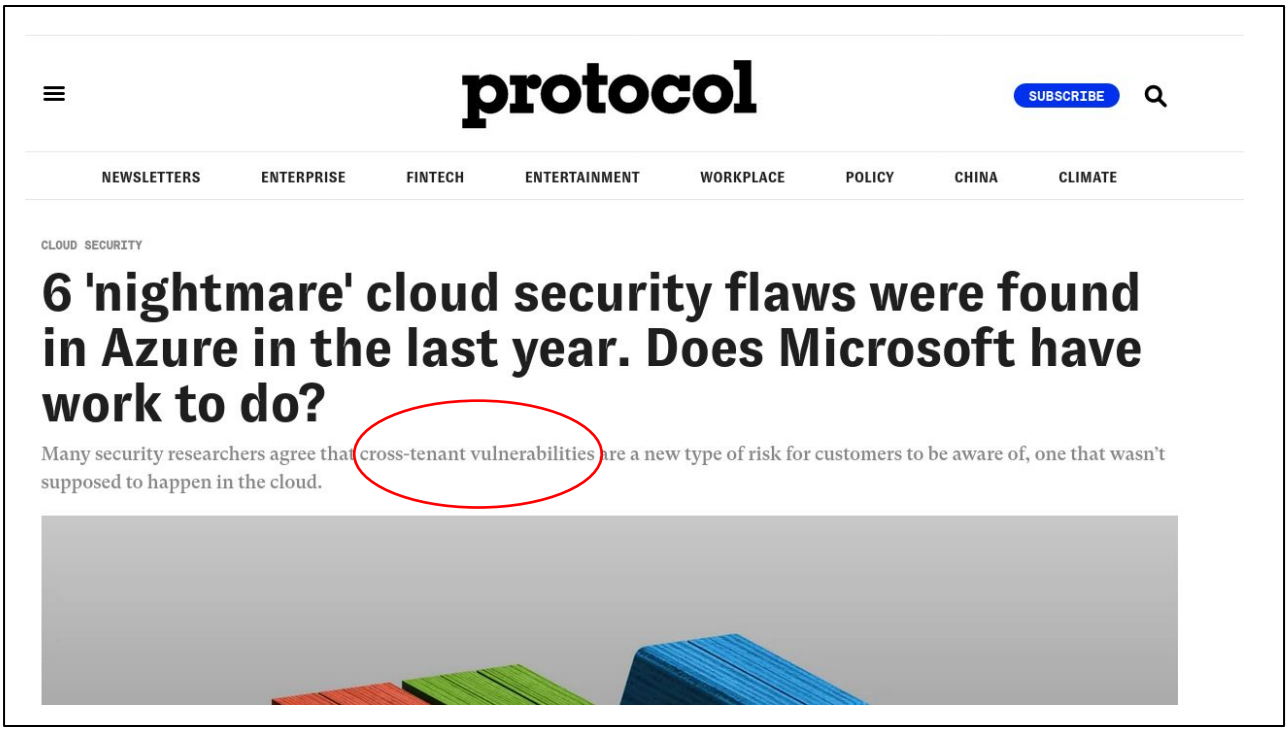
(€ 262,17 excl. 21% btw)

Volgende werkdag in huis

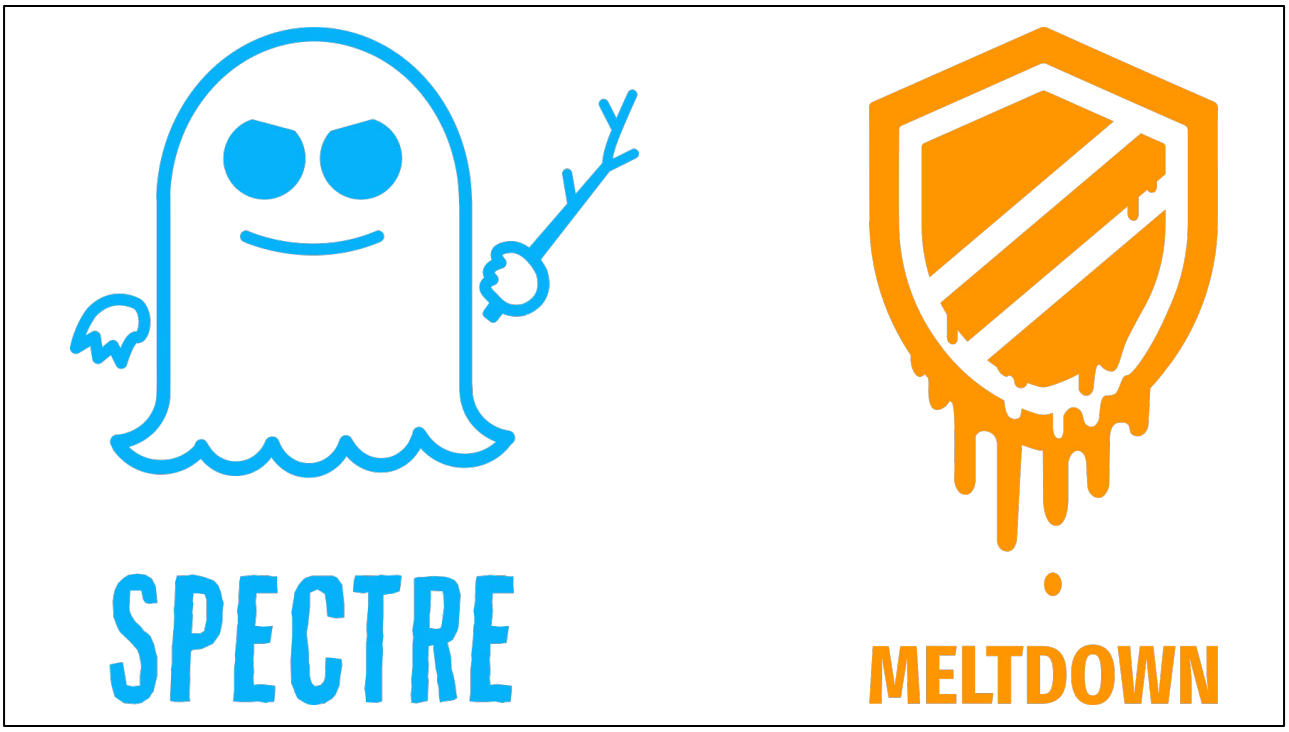
Raalte:
Leverancier:

- 1 +

This has consequences. Because the cloud is mandatory, it does not need to be cheap. You can buy this 18TB hard drive for 317.23 euros. But if you want to download the contents of this single drive from AWS, it will cost you 1800 euros. But apparently the hate for setting up a server and bandwidth is so huge they can get away with such pricing.



As another example, it is widely known among security professionals that the security of the Microsoft Azure cloud is balls. See for example https://www.lastweekinaws.com/blog/azures-terrible-security-posture-comes-home-to-roost/ - but clearly this does not matter to anyone. Azure is a very popular destination with big enterprise. Put all your secrets on there! The cognitive dissonance is so huge that news of Azure's terrible security is widely ignored. We'd rather not talk about it.

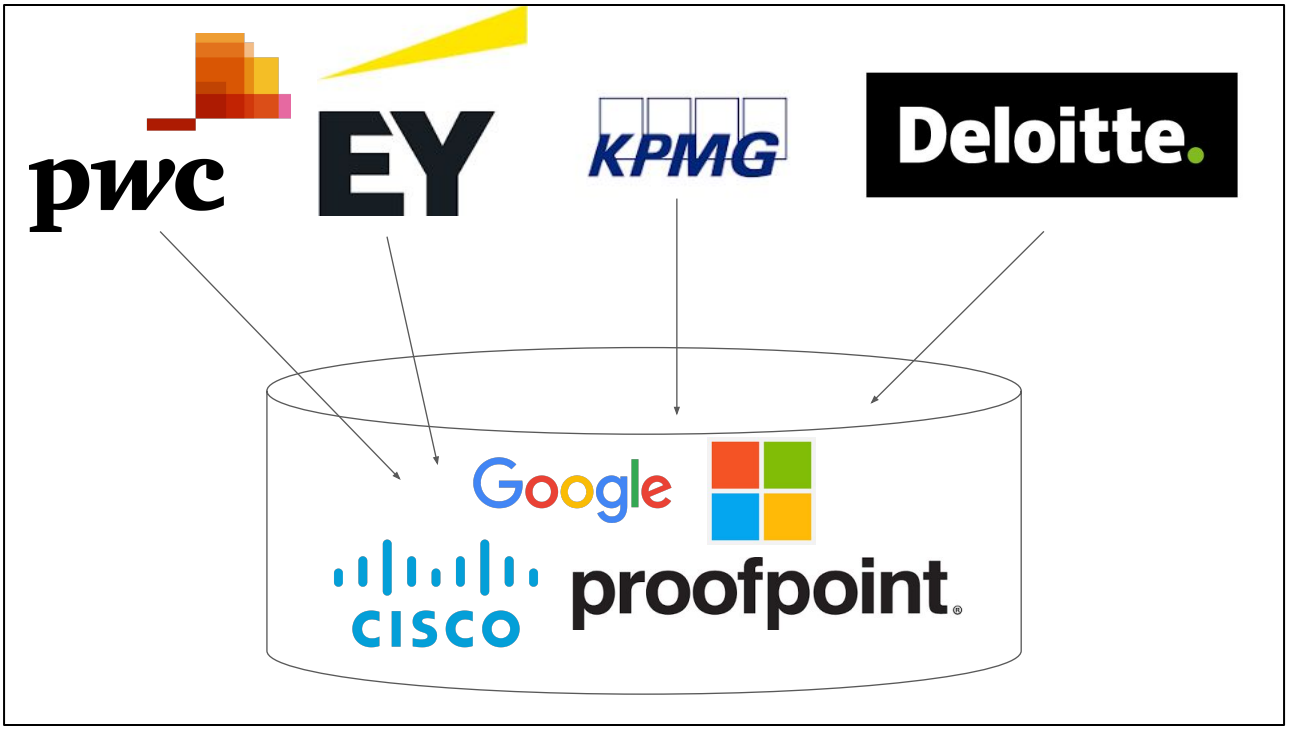


In 2018, we learned that if you share CPUs with other people, it is entirely possible to retrieve secrets from those other processes. Since 2018, the Spectre and Meltdown vulnerabilities have been joined by loads of additional ways of eavesdropping on other tenants. It appears fundamentally impossible to share CPUs among different users without leaking data. Yet we do not talk about this. See https://en.wikipedia.org/wiki/Side-channel_attack

Actually!

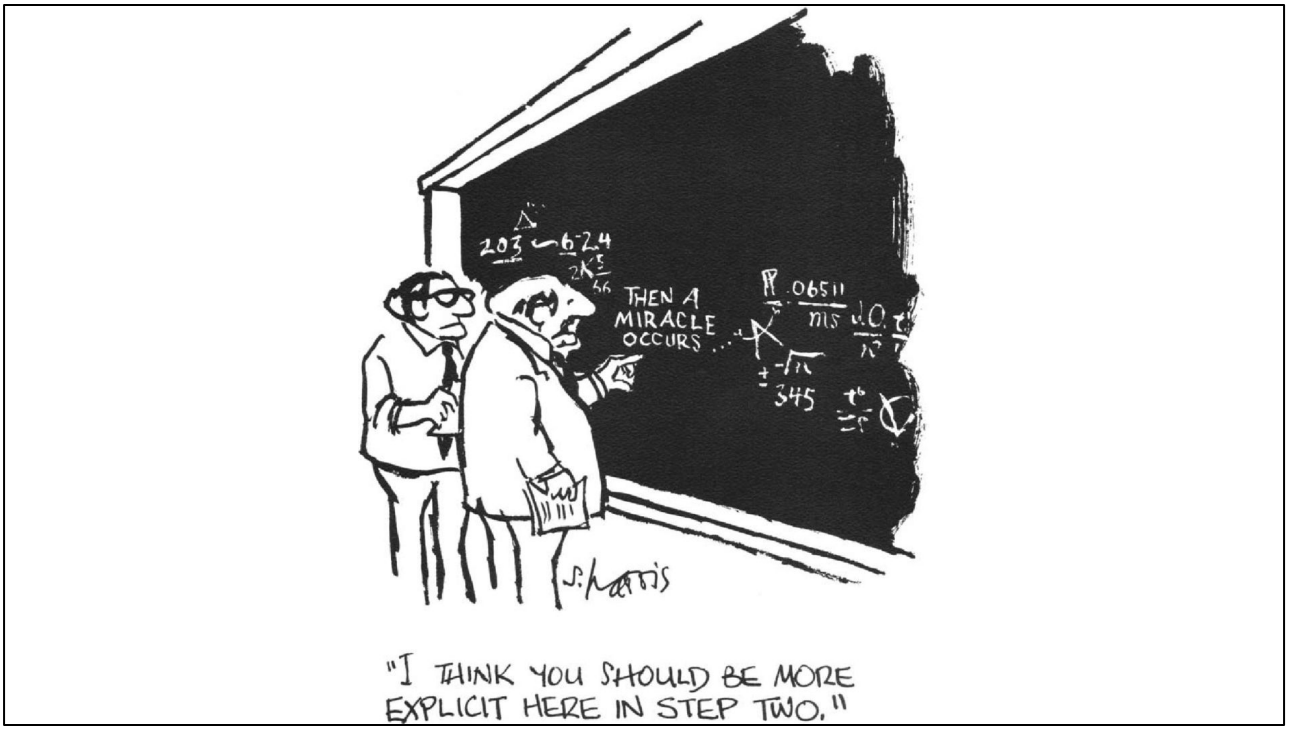
- Not only terrible to run on premise hardware
- You should not even be running software, far too dangerous!

However! Not only must you not run your own servers, you also can’t run software on rented servers. And indeed, if you install a random piece of software that can be reached through the internet, if you wait for a year, it is hacked.



These are “the big four”, they do the accounting for most of the world’s big companies and governments. They know everything. If they leak data, the results are terrible. All of them have decided to hand their email to Google or Microsoft. And all four of them have also added an additional spam filtering company that sees the plaintext of every email they receive. Their proprietary data therefore sits side by side with that of their biggest competitors.

You run software:	As-a-service provider runs software:
Not secure	**Secure**



So it might be true that a dedicated as-a-service provider could devote more attention to security. But so could you. The problem is now that any as-a-service provider is considered more secure than you are. But they are also a far more attractive target for hackers! We can't just call a whole class of companies secure-by-miracle

Some painful truths

- All common software now tracks what we do and reports on it by default
- Basically impossible to escape from this situation
- If you are a dysfunctional organization, your own on-premise efforts will not be good enough
  - Cloud may be the best you can do
- Securing software is very hard to do, especially if dysfunctional
  - As a service may be the best you can do
- Software is indeed terrible, the business model for good software is dead
  - “Only free software can afford to be good”
- Yet, even the most professional organizations have now given up
- We have globally accepted a terrible situation

Do note this slide - if you are dysfunctional enough, the cloud is way better than anything you could do!

Cyber and information security: have we all gone mad?

bert@hubertnet.nl / https://berthub.eu/

https://berthub.eu/cyber-mad/

Held at TU Delft, department of Technology, Policy & Management