Seminars, Challenges, Serious Games and Casus

Academic Year 2019-2020

Informative and analytic report of the third conference : *Good enough* security : the best we will ever have?

Conference presented by Miss Gwendolyn VAN AKEN and Mister Dieter VANDENBROECK.

Under the supervision of Mister Benjamin VAN DAMME, Mister Jonathan VAN GEEL and Mister Christophe DEBUT, *Seminars, Challenges, Serious Games and Casus* teachers.

Third year of bachelor report, in cybersecurity option, Hénallux.

16 December 2019.

Thomas Matis

Contents

1 Introduction 2

1.1 Presentation of the speaker(s) . . . 2

1.2 Presentation of the EY company . . . 2

2 Conference 2

2.1 The most secured company . . . 2

2.2 Equifax . . . 3

2.3 Security level needed . . . 3

2.4 Patch management . . . 3

2.5 Windows XP . . . 3

2.6 Problems with patching . . . 4

2.7 Business . . . 4

2.8 Q/A session . . . 4

3 Conclusion 4

4 Sources 5

1 Introduction

This conference will be talking about what level of security should you implemant based on the threat.
This is a non-technical topic but it is always interesting to hear a real-life work experience, as we are still students. We always talk about ideal security, and rarely about wether they should be implemented or not.
The purpose of the conference is to try to get us ready for reality.

1.1 Presentation of the speaker(s)

This conference has been presented by two speakers :

The first one is Mister Dieter VANDENBROECK, Manager Information Security at EY. He has graduated with a Distributed systems & computer networks (computer sciences) master's degree from KU Leuven.
He is currently managing and following up various information security risks that face many clients in the EMEIA region[1].
He talks Dutch, English and French.

Miss Gwendolyn VAN HACKEN, Manager IT Security, also at EY. She has graduated with a master's degree in commercial engineer in policy informatics from KU Leuven.
Her thesis was about the analysis of parking data by the use of Formal Concept Analysis.
She also speaks Dutch, English and French.

1.2 Presentation of the EY company

EY (Ernst & Young) is one of the Big 4 accounting firm (with Deloitte, KPMG and PWC).
It has four integrated service lines — Assurance, Advisory, Tax and Transaction Advisory Services.
Its headquarter is in London and provides worldwide services.
EY advanced his market presence in digital and strategic consulting, and is now in direct competition with the traditional *big three* companies : Bain, McKinsey and BCG.

2 Conference

2.1 The most secured company

The speaker started by asking a question to the assembly :
-> What is the most secure company ? Here is the answers we gave :

- The one that doesn't exist.
- Google, because they have the biggest data-centers in the world. They invest huge resource and they are number one so they have to invest in security so that they keep that position.

[1] Europe, Middle East, India and Africa

- Military : it depends in what country : For instance, Ukraine hasn't been successful lately. Governements aren't secure at all.

-> The speakers said that they would have expected :

- Fornox : the location where the whole gold of the US is stored.
- Black dolphin : a russian jail : they keep people from running away[2].

As cybersecurity students, we always think first in a **cyber**security way, where physical security is sometimes even more important. The example of fortnox should have came first in our mind.

2.2 Equifax

Equifax is a company that got completely hacked. They had a huge data breach where almost every credit card owner. They got breached because they forgot to apply a patch for the Apache Struts Vulnerability, while they patched everything else.
They lost 1.4 billion dollars from that breach, from legal fees to clients who quit.
2 years after, they have an even bigger capital than before the breach : the company lived on, only the data of their clients is still impacted.
We only know about this breach because of the congress and the house of commons did an investigation.
It's frightening that this kind of breach wouldn't have been known if the investigation was not done.

2.3 Security level needed

The speaker used a great analogy between security level we need and sharks in the water.
If you are in holidays on a stunning beach, and you would like to go for a swim, you should. Even if there are sharks in the water, the danger from a shark eating you is so weak that it is worth to go for a swim.
Furthermore, not all sharks are dangerous : not everyone on the internet is a threat.

2.4 Patch management

You don't immediately patch the vulnerability you find. The average timeline for a patch is 16 days.
There is an increase of 17% in know cyberattacks[3].
60% of the cyberattacks were linked to a non-patched vulnerability.

2.5 Windows XP

If you still use Windows XP, prepare for the worst. This is a nice quote : indeed, windows XP is no more supported as it ran end of life ten years ago, in 2009. We saw a graph on which was the most used Windows by end-users.
No surprise, first came Windows 10. Secondly came Windows 7, which will soon run end of life, in a month.[4]
The last one is Windows 8, behind windows XP.

[2] Well, they won't be able to run away *alive*

[3] This is a hard thing to evaluate, so we should take easy on this piece of information

[4] https://home.bt.com/tech-gadgets/computing/windows-7/windows-7-support-end-11364081315419

95% of Belgian banks use at least one or two outdated windows server.
ATM's use windows XP. The reason of this is because they first thought about the physical security of it. As they are isolated and there is a huge physical security behind it, they are not that much vulnerable.

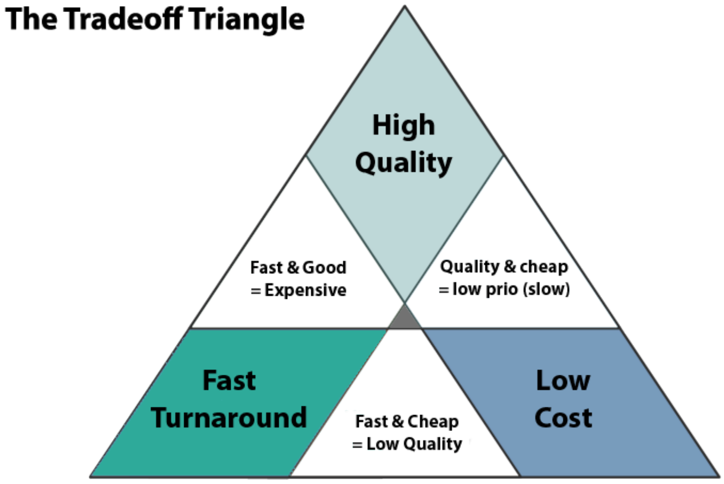
2.6 Problems with patching

Here are some issues with patching :

- The down time : you have to shutdown your systems for a certain amount of time.
- You have to test your patches before applying them.
- You have to keep some features running and sometimes cannot afford to take them down for a certain amount of time.

2.7 Business

You always have to talk business. Don't speak in technical terms and don't shot the IT impact but the business impact. This is a thing we will have to learn by doing.
For example, CBC in Czech Republic still uses pin as passwords for the bank accounts. This is not the most secure way but it is the most efficient for them.
You have to respect the trade-off triangle : High quality / low cost / fast turnaround.



2.8 Q/A session

What is your job at EY?
-> The jobs of both speakers were approximately the same : they are security managers, hey have projects that longs from 6 months to 2 years. They manage business. They are the one that give pieces of advice about security, but they do not implement them. They also talk about ISO level.

3 Conclusion

To conclude, it was an interesting point of view of the real-work life. It makes a huge difference with what we thought was security.

4 Sources

1. Linkedin :
   - Gwendolyn VAN AKEN
   - Dieter VANDENBROECK
2. websites :
   - EY
   - Big three
   - End of life windows 7
3. Pictures :
   - Trade-off Triangle