Research Project Title

Camilla Nadja Fleron {cafl@itu.dk}
Jonas Kofod Jørgensen {jkoj@itu.dk}
Supervisor: Oksana Kulyk {okku@itu.dk}

March 21, 2020

Course code: KIREPRO1PE

1 Abstract

Denmark is the most digitized country in Europe. However, IT security in Danish companies has not followed. Among other things, small and medium size businesses (SMBs) feel that the barriers to increasing IT security are the employees' lack of responsiveness to change and commitment to IT security (Monitor Deloitte for Erhvervsstyrelsen, 2018).

General Terms: *Security, Management, Policies, Human Factors.*
Keywords: *Security policies, security behaviour*

2 Introduction and motivation

According to the European Commission's Digital Economy and Society Index (DESI) of 2017, Denmark is the most digitized country in Europe. However, IT security in Danish companies has not followed the high digitization degree. Monitor Deloitte has made a status picture of the IT security level in Danish small and medium-sized businesses (SMB) this report shows that many companies have breached IT security and that even more are at risk. 39 per cent of SMBs have an IT security level that is considered inadequate to their risk profile (Monitor Deloitte for Erhvervsstyrelsen, 2018). Only 22 per cent of companies with 5-9 employees have a documented IT security policy. For every SMB in Denmark, it is only 36 per cent of them that have a documented IT security policy. [7].

2.1 Premise

2.2 Research Question

3 Background

In an increasingly tougher economic climate, organisations have to decide how to spend their resources most effectively to achieve their operational goals. To deliver effective IT security, one must not only understand the threats to an organisation, but how security fits into its business goals and processes... [7].

4 Best practices within IT-security and privacy

To be protected as an SMB it is important to know the best practices and be aware of the assets and the threats of the company. In the following we will list nine steps to develop good IT-security in the company. The list is highly inspired by the rapport *'Cyberforsvar der virker'* from Center for Cybersikkerhed and Digitaliseringsstyrelsen, 2017.

Out of the nine steps in the list, the first six are essential for any organization and should be known and prioritized. The actions in these first six steps could counter up to 80 per cent of cyberattacks. If the organization want a cyber defence, more optimally, they should implement all nine steps.

The 9 step-guide:

1. Cyber-security that work starts at the top of the organization
2. Understand assets and the corresponding cyber-threats
3. Define a security policy
4. Delegate technical responsibilities
5. Develop a response plan
6. Basic security rules of the company
7. Logging, monitoring and alarm
8. Test and analysis of IT-security
9. Further technical and organizational improvements

4.1 The 9 steps to build security that work

In the following, a complete description of the nine steps is presented. These nine steps describe a concrete, prioritized plan for how businesses can decrease the risk of cyber-attacks and remain calm even when an attack occurs. The nine step-guide focuses on the part of the overall information security work that can directly help reduce the risk of cyber-attacks. Other aspects of security, such as physical security are not mentioned [4].

1. Cyber-security that work starts at the top of the organization

- Top management is essential. If the CEO and other critical company directing people are prioritizing the security, the rest of the company will follow along. Beautement et al. (2008) presents a paradigm called the compliance budget which is used as: *"a means of understanding how individuals perceive the costs and benefits of compliance with organizational security goals"*. In other words, it is the amount of extra effort an individual is willing to make for no personal gain.
- The more security-minded an organization is the fewer conflicts concerning compliance will appear. Weirich and Sasse (2001) report that behavioural norms strongly influences the security behaviour of individuals and that most people strive to *"fit in"*. [8] If the company builds a positive and robust security culture, it will most likely reduce the friction and perceived cost of compliance [3].

2. Understand assets and the corresponding cyber-threats

- A vital point is to understand the assets and the corresponding cyber-threats of the organization. The company's employees must be aware of what it means if crucial information is changed, stolen or leaked. Or if the company's IT service is unavailable for a shorter or longer period.
- Make sure that employees are familiar with the most common cyber-attack methods. The employees should be aware of the risks from the first working day and kept up to date on the area throughout their carrier.

3. Define a security policy

- An important point is also to define and write down a security policy that everyone in the company understands, follows and actively supports. It helps to make it clear to everyone what rules the company has concerning security. So
- It is essential for the employees to know the attacker's methods and motivation in order to better understand the security policy of the company.

4. Delegate technical responsibilities

- The leaders in the organization must ensure that the right employees are assigned the right skills in the organization. Those responsible must ensure that the tasks are carried out by technically competent employees.
- One of these employee profiles is the system administrator.

5. Develop a response plan

- The organization must furthermore be able to handle a situation where a hacker has succeeded in breaking through the security measures. Managing such circumstance without panic is only possible with a well-functioning and a well-tested response plan. The response plan must clearly outline responsibilities and tasks in an unusual situation and contain contact information on the support that can be used if necessary.

6. Basic security rules of the company

- Any cybersecurity program should focus on the basic security standards before implementing any other technical measures. The organization should choose which programs to use based on their risk assessment.
- Employees should only have access to areas of the company that are necessary for performing their tasks. Domain rights for system administrators should be minimized as much as possible.

- If programs or operating systems no longer can be updated, the organization should prepare a plan for phasing out or isolating them. Continuing use of non-updatable systems involves high-security risk.

7. Logging, monitoring and alarm

- Successful attacks will occur, but they must be anticipated appropriately, detected and dealt with as part of the security when proactive efforts are insufficient. Logging with associated monitoring can detect and alarm the company. Proper logging increases the chance of investigating an attack, and the corresponding alarms make the company aware of any anomalies.

8. Test and analysis of IT-security

- Investigation of the security policy developed in step 3 should be an ongoing procedure. This investigation should test the effectiveness and whether the safety procedures work in practice for the employees.
- The state of the company's defence may be tested with simulated attacks, where observations on how quickly the organization discover and handle it. If the result does not meet the business requirements, corrective action should be taken.

9. Further technical and organizational improvements

- The final step is to introduce additional security measures spread across the entire IT environment, e.g. regarding the use and management of mobile devices and 2-factor-authentication.

4.2 Challenges with security in businesses

Security challenges within businesses are most often caused by human, rather than technological failure. Intuitively, one would think that the less tech-savvy are the sinners, but studies show that even users with technical skills such as system administrators and developers, often struggle to keep up with the complexity and workload created by the security mechanisms [3]. Weirich (2005) points out that when an individual is presented with a security task, he or she has a choice of

1. Complying and performing the required behaviour (at least try to do so)

   or

2. Attempting to bypass the task.

As Beautement et al. show in their 2008 study (The compliance budget: managing security behaviour in organisations) the results suggests that the decision - to comply or not, is the result of an internal cost/benefit assessment conducted by the individual. Quoting the authors: *"This does not mean individuals regard compliance with security behaviour purely as a cost: the participants in our study value security, both for themselves and for the organisation they work for."* [3]. Moreover, the study shows that security measures slow down productivity and are therefore often circumvent. However, most employees will comply as long as no additional efforts are required. The last example from the study, show that participants where wondering *"why they cannot run these things at night?"*. This highlights a lack of awareness and indicate potential conflicting goals at the organizational level, in this specific case the organizations desire to reduce energy consumption by closing down all systems at night versus effective security [3].

4.3 The IT-security culture is essential in SMBs

According to 10 out of 14 case interviews on SMBs conducted by Monitor Deloitte in 2018, employees' lack of knowledge about IT security is a barrier to the company's work with IT security. The lack of IT security knowledge reflects the employees' responsiveness to changes which affects IT security. These changes are necessary to increase the security level of the company. Especially changes which affect the employee's workflows and productivity are difficult to implement.

Companies also find that employees are not able to identify IT security threats to a sufficient degree. In this context, several companies cite the corporate culture as an underlying barrier to increasing the level of IT security in the company. Several IT executives believe it is necessary to work extensively on communication about IT security and potential IT security threats in order to make a positive IT security culture.

In this context, informal communication is a tool for creating the necessary cultural change, and 74 per cent of Danish SMBs also use oral communication with the workers in their work with IT security. The informal communication creates an increased understanding of IT security. This increased understanding makes the employees better know the importance of IT security and the consequences of inadequate IT security for the company. It is fundamental for the SMBs that the employees understand what IT security is, and it is, therefore, necessary to make IT security very tangible and something which is discussed. However, oral communication is often not enough, and it may, therefore, be necessary to follow up with more formalized measures so that IT security is also anchored in the company's processes and workflows [5].

5 The Study

To obtain an empirical basis for our research, we conducted five in-depth interviews in five different companies. The companies were ranged wide from healthcare products, Mobile games, Virtual reality, AI and security-help. We found the five respondents through the two authors connections. The interviewees had positions ranging from the part-time student worker to the CEO of the company. We chose diversity in the posts to receive different thoughts, ideas and experiences within the IT-security field. All participants had a university degree and at least one-year work experience.

The semi-structured interview is in many ways similar to an everyday conversation, though guided by an interview guide (Kvale og Brinkmann, 2009). The meeting is a planned but flexible interview with some research questions. The purpose is to gather nuanced answers and an in-depth understanding of the interviewee's perceptions. In the semi-structured interview, it is possible to change the order of questions, and it offers an opportunity to ask follow-up questions. These opportunities give the interviewer control over the conversation while allowing the respondent to answer freely. The advantage of the semi-structured interview is that the approach provides the respondent with the freedom to pursue particularly exciting topics that may arise along the way (Kvale og Brinkmann, 2009).

The interviews were exploring:

1. The tasks and responsibilities of interviewees,
2. Their companies IT-security policies and practices, and
3. Their attitude toward these.

5.1 Test of interview

Before conducting the interviews, we did a test of it. It is always a good practice to test the questions before conducting the interviews. The test gave us many clarifications, mostly concerning the interview-questions, the length of the session and to make sure the right questions were asked.

5.2 Anonymity

This study is conducted with respect for the participants privacy and anonymity. Thus, all collected recordings has been destroyed after transcription. Names of people and company has been anonymized. With respect to the participants privacy each participant was offered to review the transcript. GDPR?

5.3 Transcription

We recorded the interviews and made the transcription immediately after the meeting. The quick transcription is done so that the interview still is clear in the memory. This approach aims to reduce errors in the transcription. This research works with a relatively simple level of transcription, for example; Tone pitch and count on pauses are not included in the transcripts, as it is the meaning of the essence that is essential in this study.

5.4 An interview guide

An interview guide were sent to the respondents before the actual interview. This was done prior to make the respondents confident about the agenda, how many questions there would be, and what kind of questions they were gonna answer. Also IT-security policies within a company may be considered confident by the company, which make it even more important to emphasise the anonymity of the interview. By sending an interview guide beforehand also makes the answers of the respondents more considered. [1].

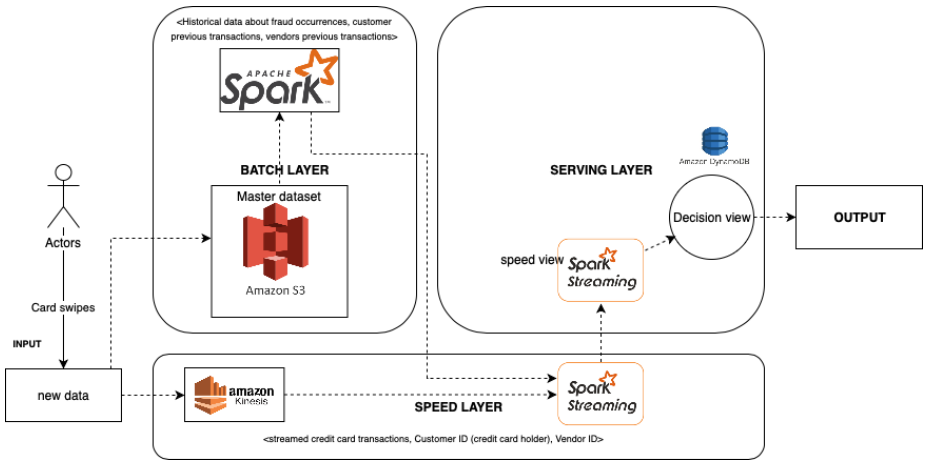

Figure 1: Lambda Architecture

Nulla nisi ligula, pulvinar sit amet lorem in, pharetra dapibus dolor. Interdum et malesuada fames ac ante ipsum primis in faucibus. Ut eget consequat lorem. Sed euismod auctor sodales [2].

5.5 Results

5.6 Highlighted interview answers

In this section, we present 4 key scenarios illustrating individuals' perceptions of security measures.

- first question
- second question

5.7 Analysis/findings

...4/5 did not have any security policy and 5/5 did not have any IT-security training. Everyone would like to have some kind of automated guidance about the best practices and weekly reminders about...

6 Proposal of an IT-security product

7 Discussion

8 Future work

Figure out the best possible solution and build the web-app.

9 Conclusion

This initial work have proven that a notification based product with a guideline of best practices would be of great help in SMBs. Because of this information we suggest that having a guide and a SMB it-security agreement in the company would be very beneficial. [6].

References

[1] Apache. *How Many Reduces?* URL: https://hadoop.apache.org/docs/current/hadoop-mapreduce-client/hadoop-mapreduce-client-core/MapReduceTutorial.html (visited on 12/29/2019).

[2] Apache. *Structured Streaming Programming Guide*. URL: https://spark.apache.org/docs/latest/structured-streaming-programming-guide.html#continuous-processing (visited on 12/30/2019).

[3] Adam Beautement, Angela Sasse, and Mike Wonham. "The compliance budget: managing security behaviour in organisations". In: (Jan. 2008). DOI: 10.1145/1595676.1595684.

[4] Center for Cybersikkerhed og Digitaliseringsstyrelsen. *Cyberforsvar der virker*. Jan. 2017.

[5] Monitor Deloitte for Erhvervsstyrelsen. *It-sikkerhed og datahåndtering i danske SMV'er*. Apr. 2018. URL: https://erhvervsstyrelsen.dk/sites/default/files/2019-03/it-sikkerhed_og_datahaandtering_i_danske_smver.pdf.

[6] Nathan Marz and James Warren. *Big data: principles and best practices of scalable real-time data systems*. Manning, 2015. ISBN: 9781617290343 1617290343. URL: https://www.amazon.de/Big-Data-Principles-practices-scalable/dp/1617290343.

[7] Apache Spark. *Spark Overview*. URL: https://spark.apache.org/docs/latest/ (visited on 12/27/2019).

[8] Dirk Weirich and Martina Sasse. *Pretty Good Persuasion: a First Step Towards Effective Password Security in the Real World*. 2001. DOI: 10.1145/508171.508195.