Explore your case – Case 3: Technical Security Analysis for Small Businesses

Author: Peter

Responsible: Peter

Description: <https://learnit.itu.dk/mod/page/view.php?id=186399>

|  |  |  |  |
| --- | --- | --- | --- |
| Version | Change | Author | Date |
| 0 | Added ChangeLog (change me) | Peter | 22/09 |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |
|  |  |  |  |

**Context and Motivation**

Small businesses are increasingly using technology for different parts of their enterprise. This poses security risks to the business owners as well as their customers, as cyber-criminals view these companies as increasingly attractive targets. Due to the nature of their scale, however, these small businesses have very limited resources and budgets for cyber-security measures. Apart from just financial limitations, small businesses have trouble safe-guarding themselves due to issues presented in some of our additional material (Hall et al. 2021):

* Research and data relating to cyber-security is usually derived or obtained from non-representative, larger enterprises and is not translatable (ibid. 3-4).
* Many cyber-incidents are “symptom-less” to the normal user and only detectable via active traffic monitoring that few small businesses can afford (ibid. 5).
* Current cyber-security solutions favor larger organizations as they have historically been the targets of famous cyber-incidents and are ideal customers (ibid. 6)
* Cybersecurity measures cannot be copy-pasted from larger business to smaller ones. (ibid. 6)
* Proper cyber-security solutions rely on separate testing environments, requiring “substantial technical knowledge, time and ongoing maintenance” which is unfeasible for smaller businesses. (ibid. 6)
* Smaller businesses’ move towards cloud infrastructure renders traditional cyber-security products, such as general network scanning, unsuitable (ibid. 7)
* Mixed-use devices are common in small business, which makes the intrusive qualities of MDM software undesirable (ibid. 7)
* Lack of human resources with technical knowledge, “The small IT budgets of small businesses do not cover the salary of an IT administrator” (ibid. 7)
* Cyber-security assessment *cannot* be done effectively by a novice (ibid. 8)
* Many small businesses are short-lived and do not focus on processes in the inception and survival stages of the company (ibid. 8)
* Non-technical small business owners feel a low sense of control in relation to the complexity of cyber-security, possibly leading to inaction (ibid. 8)

**Existing Research and Products**

Some researchers have taken an interest in the cybersecurity issues of small businesses in recent years. This includes research for Australian small business needs (Hall et al. 2021) and analyses of different security approaches to cyber security in smaller systems (Zvereva and Loshchenko 2022, Bada and Nurse 2019). The research is not exactly extensive, as is also highlighted and criticised by Hall et al., but it does exist, and solutions are sorely needed.

Apart from traditional anti-virus services, platforms such as [vanta.com](https://www.vanta.com/) focus entirely on compliances, trust building and risk assessment. Optimally, a one-stop security offer would incorporate both considerations in one.

**Idea contribution**

We want to provide an automated digital security assistant that checks the customers system for possible insecurities. As highlighted in some of the research, the app would have to both check for technical vulnerabilities in the system, but also serve as a form of educational tool for the user, as many cyber-attacks are of a social nature such as phishing attacks. Most current options on the market consist mostly of anti-malware software which neglects the user education. The assistant would need to be usable by technical novices and accommodate many different system setups, as there is no de facto way of doing IT at a small business level. The assistant helps users comply with relevant data protection and security regulations of our targeted regions (TBD).

**Bibliography**

Bada, Maria and Jason Nurse. 2019. *Developing cybersecurity education and awareness programmes for small- and medium-sized enterprises (SMEs)*

Hall, Joanne, Asha Rao and Tracy Tam. 2021. *The good, the bad and the missing: A Narrative review of cyber-security implications for australian small businesses.*

Loshchenko, Vitaly and Olga Zvereva. 2022. *Integrated approach to cybersecurity of a small-sized business system.*