jamk.fi

Third-party software patch management in Windows environments

Tuukka Tiainen

Master's thesis
November 2019
Technology
Master's Degree Programme in Information Technology
Cyber Security

Jyväskylän ammattikorkeakoulu
JAMK University of Applied Sciences

jamk.fi

Description

Author(s)	Type of publication	Date
Tiainen, Tuukka	Master's thesis	9.11.2019
		Language of publication: English
	Number of pages: 82	Permission for web publication: x

Title of publication

Third-party software patch management in Windows environments

Degree programme

Master's Degree Program in Information Technology, Cyber Security

Supervisor(s)

Kotikoski, Sampo

Lappalainen-Kajan, Tarja

Assigned by

Centero Oy

Abstract

The thesis was assigned to support the assignor's internationalization project. The main goal was to learn how organizations are involved in third-party application patch management. The second goal was to compare the solutions automating the third-party patch management.

To study the behavior and processes of organizations with patch management, the quantitative method was chosen. In practice, a web survey was selected to be the primary tool for gathering the data. The survey was carried out using two methods: namely, with all questions being mandatory and with all questions being optional. There were no real differences between the methods. The audience for the survey was a combination of the assignor's mail lists, LinkedIn members, related IT forums and JAMK cyber security students.

In addition to existing literature, the resulted in a base for proceeding with the comparison. Together they helped to select the crucial features and characteristics of automated tools for the comparison. Otherwise, the results were variable but still very much aligned with the existing studies. The results show that most of the organizations consider the third-party patch management very important and even critical; however, not all of them carry out the necessary actions to meet the risks. This was important knowledge for the assignor to proceed with their project to reach international prospects.

The research questions were answered. Nevertheless, the survey results raised up some important questions which could be studied with further research. The quantitative study complied with the existing studies rather well which means that the hypothesis was met. The reasons why some of the organizations stand out in a crowd would be interesting.

Keywords/tags (subjects)

Cyber security, patch management, third-party patch management, vulnerability

jamk.fi

Kuvailulehti

Tekijä(t)	Julkaisun laji	Päivämäärä
Tiainen, Tuukka	Opinnäytetyö, ylempi AMK	9.11.2019
		Julkaisun kieli: Englanti
	Sivumäärä 82	Verkkojulkaisulupa myönnetty: x

Työn nimi

Kolmannen osapuolen sovellusten päivitystenhallinta Windows-ympäristöissä

Tutkinto-ohjelma

Master's Degree Program in Information Technology, Cyber Security

Työn ohjaaja(t)

Kotikoski, Sampo

Lappalainen-Kajan, Tarja

Toimeksiantaja(t)

Centero Oy

Tiivistelmä

Työn toimeksiantaja tilasi tutkimuksen tukemaan heidän kansainvälistymishankettaan. Pääasiallinen tavoite oli oppia tuntemaan organisaatioiden tapoja toimia kolmannen osapuolen sovellusten päivitystenhallintaa. Toinen tavoite oli vertailla tuotteita, jotka automatisoivat kyseessä olevan päivitystenhallinnan.

Tutkimustavaksi valittiin määrälllinen tutkimus. Valitulla tavalla haluttiin tutkia tarkemmin organisaatioiden käyttäytymistä ja prosesseja liittyen kolmannen osapuolen sovellusten päivitystenhallintaan. Pääasiallinen työkalu määrällisen tutkimuksen läpiviemiseen oli web-pohjainen kysely, joka tehtiin kahdella tapaa. Kysymykset olivat molemmissa täysin samat, mutta toisessa kaikki kysymykset olivat pakollisia ja toisessa valinnaisia. Tapojen välillä ei kuitenkaan havaittu mitään merkittäviä eroja. Kyselyn kohdeyleisöksi valittiin toimeksiantajan olemassa oleva postituslista, joukko LinkedIn-käyttäjiä, sopivien IT-keskustelupalstojen jäseniä ja JAMK:n ylemmän ammattikorkeakoulututkinnon kyberturvallisuuden koulutusohjelman oppilaita.

Jo olemassa olevat tutkimukset yhdessä kyselyn tulosten kanssa mahdollistivat hyvän pohjan vertailua varten. Näitä tietoja hyödyntäen oli mahdollista valita vertailuun sopivat ominaisuudet ja piirteet. Muutoin kyselyn tulokset olivat melko lailla hyvin linjassa jo olemassa olevan kirjallisuuden kanssa. Tulokset osoittivat, kuinka organisaatiot pitävät päivitystenhallintaa tärkeänä asiana, mutta silti kaikki eivät kuitenkaan pidä asiasta huolta, kuten pitäisi. Tulokset antoivat tärkeää tietoa työn toimeksiantajalle liittyen kansainvälistymisprojektiin.

Vaikka määrällisen tutkimuksen tulokset olivat kohtuullisesti linjassaan olemassa olevan kirjallisuuden kanssa, heräsi tutkimuksen aikana jatkokysymyksiä. Erityisesti poikkeavat toimintatavat ja niiden syyt voisivat olla hyvä laadullisen jatkotutkimuksen aihe.

Avainsanat (asiasanat)

Kyberturvallisuus, päivitystenhallinta, haavoittuvuuksien hallinta, haavoittuvuus

Contents

Contents **1**

Acronyms **5**

1 Introduction **6**

2 Theoretical-conceptual starting points **7**

2.1 Software updating 7

2.2 Software vulnerabilities 8

2.2.1 Disclosure 9

2.2.2 Zero-day 10

2.2.3 Rating 11

2.3 Patch management 12

2.4 Patch management of third-party software 13

2.5 Patch management in organizations 14

2.6 Economic impact of using a patch management solution 16

2.7 Patch management process 17

2.8 Automated patch management solutions 19

3 Research **23**

3.1 Purpose 23

3.2 Objectives 23

3.3 Research questions 24

3.4 Risks 24

4 Implementation **24**

4.1 Research methodology 24

4.2 Data gathering and material sampling 25

4.2.1 Survey 26

4.2.2 Audience 27
4.2.3 Tools 29
4.2.4 Survey reachability 30
4.3 Analysis of data 31
4.3.1 Demographics 31
4.3.2 Vulnerability threats and risks 35
4.3.3 Current third-party patch management methods 38
4.3.4 Third-party patch management versus other cyber security controls 39
4.3.5 Awareness and usage on third-party patch management solutions ... 40
4.3.6 Patched applications 40
4.3.7 Patch management processes and solution features 42

5 Discussion 44

6 Comparison 48
6.1 The purpose of research questions 48
6.2 Categories 48
6.3 Compared solutions 53
6.4 Comparison in practice 55
6.5 Elaborating the comparison 58

7 Discussion 61
7.1 Results and theoretical framework 61
7.2 Further research 63

References 65

Appendices 68

Figures

Figure 1. Lifecycle of a vulnerability. 8
Figure 2. Development of availability for patches. 10
Figure 3. Maturity of patch management process. 16
Figure 4. The targeted job titles for InMail in LinkedIn. 28
Figure 5. The selected regions for respondents to be invited. 29
Figure 6. The final response amount of the two identical surveys. 30
Figure 7. Survey reachability. 30
Figure 8. Respondent countries with more than one respondent. 32
Figure 9. Job titles of the respondents. 33
Figure 10. Organization types of the respondents. 33
Figure 11. Industries of the responding organizations. 34
Figure 12. Number of different sized organizations. 35
Figure 13. Numbers of responses to vulnerability related questions. 35
Figure 14. Organizations consider the third-party vulnerabilities as a threat. 36
Figure 15. Answer percentages of cyber security risk assessment question. 36
Figure 16. Answers on question considering cyber security assessment. 37
Figure 17. Respondents answers to question regarding risk level of vulnerabilities. 37
Figure 18. Answers on current third-party patch management methods in organizations. 38
Figure 19. Survey answers considering most important security controls. 39
Figure 20. Respondents' awareness of third-party patch management solutions. 40
Figure 21. Respondents' answers on third-party application usage. 41
Figure 22. Reasons for not patching specific applications. 42
Figure 23. Answers considering the importance of patch management processes. 42
Figure 24. Respondents' opinions on importance of patch management tool features. 43
Figure 25. The distribution of different automated third-party patch management solutions. 46
Figure 26. Survey answers considering the importance of vulnerability monitoring. 51
Figure 27. Survey results on patch management features. 51

Figure 28. Survey results regarding enterprise readiness and package customizing. . 53
Figure 29. Selected third-party patch management solutions for the comparison. ... 55

Tables

Table 1. Utilization and number of vulnerabilities for the top priority applications. .. 49
Table 2. Third-party applications used in the comparison. 56
Table 3. Scoring system used in the review Excel sheet. 57
Table 4. Overview and overall scoring in the first iteration of the comparison. 58
Table 5. Balancing the scoring system. 59
Table 6. The maximum points were equalized to match 400 and the points were re-calculated accordingly. 59
Table 7. The final form of the scoring system for the comparison. 60

Acronyms

ACSC	Australian Cyber Security Centre
CERT	Computer emergency response team
CIA Triad	Confidentiality Integrity Availability
CIS	Center for Internet Security
CVE	Common Vulnerabilities And Exposure
CVSS	Common Vulnerability Scoring System
JAMK	Jyväskylän Ammattikorkeakoulu, JAMK University of Applied Sciences
PCI	Payment Card Industry
PCI DSS	Payment Card Industry Data Security Standard
SLA	Service Level Agreement
NIST	National Institute of Standards and Technology
NVD	National Vulnerability Database

1 Introduction

The aim of the study is to have a better understanding on the very specific subject of third-party software patch management. The concept third-party software in this case means extensively used and free software. Such widely known third-party software are e.g. Google Chrome, Mozilla Firefox, Adobe Reader and Oracle Java Runtime Environment.

The thesis is assigned by an organization with a strong will to go international. The assigner has a self-developed tool which automates the third-party patch management. Therefore, the thesis plays a big role in the internationalization project. The assigner defined a steering group for the thesis to follow its progress and to make sure that it is aligned with the original plans and goals.

The study is constrained to focus on researching the behavior in workstation environment within Windows operating system. The studied behavior and phenomena are opinions, processes and ways how organizations consider the subject. Equally important studied subjects are the automated tools and solutions for third-party software patching. After studying these subjects, the goal is to create a credible comparison of third-party software patch management tools. The comparison would greatly benefit the assigner itself from the developer point of view. On the other hand, the comparison and the knowledge it brings can be used to interact with existing customers and the future prospects.

Existing studies on third-party patch management strongly focus on its cyber security side. In addition, there are multiple well-known and highly considered cybersecurity frameworks which are unanimous on the matter that third-party patch management is a highly important process and a security control to have in place. The goal of the study is to find out if the organizations comply with these recommendations. Even though there are existing studies concerning the third-party patch management, not one of them focuses third-party patching so determinedly. On that note there is a demand for this specific subject.

2 Theoretical-conceptual starting points

2.1 Software updating

Systems, products, operating systems and software have a life cycle when they are professionally developed. This means that they receive different types of updates during the maintenance phase of the active life cycle.

Microsoft is known to be one of the largest software developers in the world. They have decades of experience updating operating systems and software for organizations and consumers. Microsoft has described a variety of different update types for software and operating systems. (Microsoft 2019)

- Critical update
- Definition update
- Feature pack
- Security update
- Service pack
- Update
- Update rollup
- Security-only rollup
- Monthly rollup
- Servicing Stack Updates

The list provides a picture of the complexity of the matter software updating can be. The types of the updates can be simplified into different categories. There are security updates and non-security updates. In addition to that, there are updates which introduce new features to the system and updates which fix bugs in the system. The updates can also be delivered individually, or in collections. (Microsoft, 2019)

More importantly it is clear that there are different purposes for updates. But what is the definition of a patch? There is a guideline for software versioning called Semantic Versioning 2.0.0. It explains a patch to be a software version which fixes a bug or bugs. For example there can be a software version 3.1.12 in a following format *MAJOR.MINOR.PATCH*. This means that it is the third major version of the software, it is the first minor revision of the software and it is now the 12th fix released to the software. (Preston-Werner n.d.)

Another good approach to explain a patch is to define it from a cyber security perspective. White describes a patch to be a permanent mitigation for a security vulnerability in a software. He also claims that patches are necessary to a functioning vulnerability management program. (White 2006, 3).

The different explanations for the concept of a patch show that it can mean different concepts to different individuals. The thesis focuses mostly on the cyber security side of the patches and how they are managed.

2.2 Software vulnerabilities

Wasserman from CERT Coordination Center (Cert CC) has described a vulnerability to be a flaw in software or hardware component. The flaw enables for an attacker to perform an action which would not be possible in a normal situation. Usually there is an impact strongly attached to a vulnerability. The impact can for example taking control of a computer, retrieving private information or causing harm to systems. (Wasserman 2016)

Vulnerability has a lifecycle. One way to introduce it is to divide it to eight stages which are creation, discovery, disclosure, correction, publicization, exploiting, disinterest and death. The stages are not always in the same order and some of the stages could occur simultaneously. The following figure shows how the number of exploitations changes in the different points of the lifecycle of a vulnerability. (White 2006, 13-14)

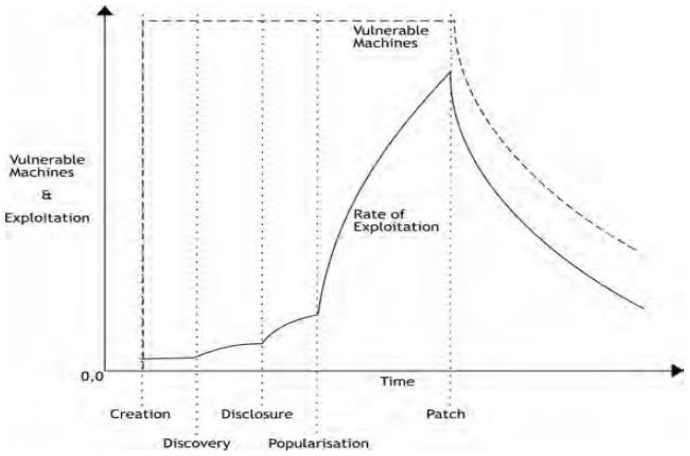


Figure 1. Lifecycle of a vulnerability.

2.2.1 Disclosure

Information on a vulnerability is usually reported publicly and/or to consumers of a vulnerable product. This process is called vulnerability disclosure. Depending on a vendor there is a variety of methods to do this. For example, it can involve a mailing list or a blog post. Cert CC recognizes a few different vulnerability disclosure philosophies: (Wasserman 2016)

- No disclosure
- Limited disclosure
- Full disclosure
- Responsible disclosure
- Coordinated disclosure

The difference of the disclosures is mostly based on the publicity of the information on vulnerability. In the full disclosure the reporter of a vulnerability makes the information public, which makes a vendor more likely to react and patch the vulnerability. Additionally, consumers can create mitigations for the vulnerabilities while waiting for the soon to be released patch. No disclosure means that all the information on the vulnerability is kept private. The reasons for this might be non-disclosure agreements or vendors protecting their secrets. Limited disclosure is something between the two of those. One major reason to do it this way is to slow down attackers from creating exploits and reverse engineering more information on the vulnerability. (Wasserman 2016)

Microsoft (Microsoft 2019) has their own exploitability index. It is used to assess different vulnerabilities for different products. One of the important assessed items are whether the vulnerability is publicly disclosed or not. Public disclosure naturally can also have greatly negative effects because it brings the knowledge to public. This knowledge can be used to create exploits.

Responsible disclosure is used when a reporter who discovers a vulnerability then reports it to a vendor and suggests a timeline for the full or limited disclosure. Usually this means that the reporter and the vendor work together to publicly disclose the vulnerability at the same time. There is a chance that vendor does not agree with the reporter's timeline or is disinterested for some reason. In that case, the reporter could publish the vulnerability information after the proposed timeline.

Coordinated disclosure is a synonym for the previously used term responsible disclosure. CERT CC prefers to use term coordinated disclosure. (Wasserman 2016)

According to Flexera (2018, 9), 86 per cent of vulnerabilities have a patch available on the same day as the disclosure took place. The percentage has improved over time, which is mostly because the researchers co-operate even more with different vulnerability programs and software vendors. Figure 2 illustrates the development of availability for patches.

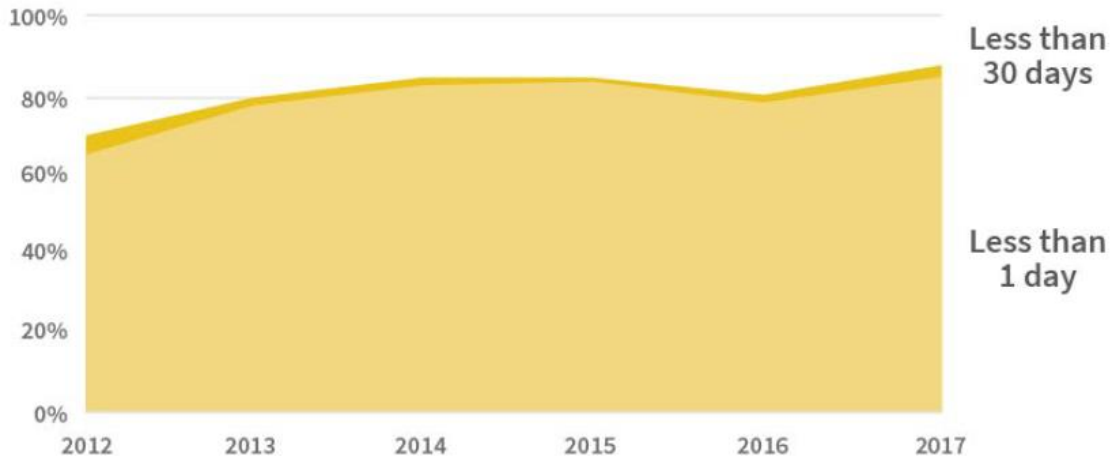


Figure 2. Development of availability for patches.

CIS Controls give a good example about new vulnerabilities and the parties usually involved in them. When a new vulnerability is reported, vendors and then attackers and defenders start a race. Software vendors try to fix the vulnerability and then deploy a patch. Meanwhile, the attackers try to deploy an attack and exploit the vulnerability. At the same time, defenders try to assess the risk, then test and finally install the patch. (Center for Internet Security 2018, 11)

2.2.2 Zero-day

If a vulnerability is just discovered and it is new information to the vendor, the industry calls it a zero-day vulnerability. It is possible that attackers have already exposed the vulnerability at this point. Nevertheless, the software vendor has had 0 days to fix the security flaw in the software. Now if there is an attack performed

using this specific vulnerability before vendor fixes it, then it is called a zero-day attack. (Symantec 2019)

In 2017 Flexera identified 19954 vulnerabilities. They monitor 55 000 applications, appliances and operating systems continuously. Only 14 out of all the vulnerabilities were zero-day exploits and they were used before a public disclosure. This means that there is almost always time to patch and mitigate before risk of exploitation drastically increases. (Flexera 2018, 4)

2.2.3 Rating

Vulnerability can be publicly known; it might be exploited and there is no fix for it available. This kind of a vulnerability is usually very critical. However, the publicity status and the exploitations status do not alone define the severity of the vulnerability. Software vendors can have their own definitions for the levels of severity and there are different rating systems for vulnerabilities out there. The most well-known vulnerability metrics system is the Common Vulnerability Scoring System (CVSS).

CVSS is a quantitative model to describe characteristics of vulnerabilities according to National Institute of Standards and Technology. The purpose of CVSS is to offer accurate and consistent information on vulnerabilities. Organizations urge to understand what kind of an impact a specific vulnerability can have on their systems. CVSS helps them calculate how severe and impactful a vulnerability can be. This information is critical when patching or some other kind of mitigation is planned and prioritized. (National Institute of Standards and Technology n.d.)

The current version of CVSS is 3.0. It is a complex metrics system and three different scores can be calculated with it. The higher the score is the more severe the vulnerability. The score categories are base, temporal and environmental. If all these scores are in use, then it is also possible to calculate an overall score for a vulnerability. The base score is the one used the most. For example, National Vulnerability Database (NVD) does not even offer temporal scoring. (Forum of Incident Response and Security Teams 2019)

The base score group describes the characteristics of a vulnerability. There are multiple exploitability metrics in the base score. They are attack vector, attack complexity, requirements of privileges and user interaction. For example, if an attack vector is network, it means that a vulnerability can be remotely exploited and does not require the attacker to be physically present. If the attack vector of a vulnerability is network instead of physical, the vulnerability gets a higher CVSS base score. The other exploitability metrics function in a similar way. The base score is not only calculated based on the exploitability, but also the possible impact of a vulnerability influences the score. The impact is based on the very well-known CIA principle. This means that the total impact is calculated on the possible effects on confidentiality, integrity and availability. (Forum of Incident Response and Security Teams 2019)

The temporal score, on the other hand, describes the current state of a vulnerability. It calculates the base score summing up current exploit techniques, remediation possibilities and how confident the reports are regarding the existence of a vulnerability. The environmental score can be used to calculate a score for a specific system or an IT asset. With the environmental score, CIA triad requirements can be set for the asset. The same characteristics which are in the base score can also be modified to be better suitable the specific system or asset. (Forum of Incident Response and Security Teams 2019)

2.3 Patch management

National Institute of Standards and Technology (NIST) has explained patch management extremely well. According to them, it is a process to keep systems and products up to date. There are different sub-processes in the patch management. It involves identifying, downloading, installing and verifying the software updates. (Souppaya & Scarfone 2013, 4)

Many different organizations claim that most of the attacks could be prevented by patching the systems. For example, Finnish cyber security vendor (F-Secure 2018) says that 80% of attacks could be prevented by keeping the operating systems and third-party software up to date. Cloud Management Suite also has given out a very

similar percentage in their document. According to them (Cloud Management Suite 2019), in April 2015 United States Computer Emergency Readiness Team published an alert which claimed that 85% of the attacks could be prevented by patching the operating system and third-party software as well.

Various security frameworks such as NIST Special Publication (SP) 800-53 and Payment Card Industry Data Security Standard (PCI DSS) recognize Patch Management as a critical part of cyber security controls (Souppaya & Scarfone 2013, 2)

Payment Card Industry is known for the security framework they provide. Their Software Security Framework sets some specific requirements for patch management. But in general, they require that all the systems must be appropriately patched against vulnerabilities. (Payment Card Industry 2019, 53)

2.4 Patch management of third-party software

Different software vendors have a different cycle for releasing security updates and patches. When it comes to workstations, the major operating system is Windows. Microsoft is very predictable for patches. It takes place every second Tuesday of a month. Oracle, on the other hand, tend to release patches every three to four months. Some vendors do have a similar patch cycle as Microsoft, and some do releases patches whenever there is a critical vulnerability in their products. (G DATA Software AG 2018, 6)

Security compliance and other goals set their requirements for consistent patching. Some patches for a variety of software can be harder to deploy and install. In addition, Gartner also talks about enterprise-ready patches. The default packages downloaded from software vendors are with default settings and might not be suitable because of the high standards of usability in enterprises. Especially repackaging the software can be a very time-consuming task. (Gartner 2017)

In some sense it can be much more complex matter to have a functional patch management process on third party software. Because there is a great variety of updating methods among the different application vendors, it is hard to keep them all updated manually. Flexera claims that there is no way for an IT administrator or

an end user to reliably do this all manually. Their latest report also shows that number of vulnerabilities documented in 2017 was all time high. It is extremely difficult to protect against the vulnerabilities without an optimized process. (Flexera 2018a, 11)

Flexera also delivers a top desktop apps document as a part of vulnerability review annually. It is also called top 50 portfolio consisting of an operating system, Microsoft applications and non-Microsoft applications. The majority as many 65% of vulnerabilities for this portfolio was for non-Microsoft applications. Still, these applications stand for only 33% of all the applications in the portfolio. This clearly shows that patching only the operating system is not enough by any means. (Flexera 2018b, 5-6)

2.5 Patch management in organizations

Sans Institute conducted a study on securing industrial control systems. There were different types and sizes of respondents. Organization size varied from under 100 employees to over 100 000 employees. One topic of the study considered patch management processes. 46% of respondents applied vendor-validated patches on a regular basis. On the other hand, 23% of the respondents did not patch at all or just added other layers of security controls to mitigate vulnerabilities. (Gregory-Brown 2017, 20)

BitSight (Bitsight 2017, 2) conducted their own research on more than 35 000 companies around the world from different industries in 2017. The research was at least partially inspired by WannaCry crypto locker outbreak earlier that year. The specific outbreak could have been avoided by patching the operating systems properly. The research has some interesting results to point out. 2 000 of the 35 000 organizations had over 50% of their computers running an outdated version of an operating system. Acting this way, it is three times as likely to face a data breach. Even in the Government sector, over 25% of the computers (Windows or MacOS) were running an outdated operating system.

Most of the computers (over 80%) were running MacOS. Even more outrageous fact is that 2 months before the WannaCry outbreak almost 20% of computers were

running Windows XP or Windows Vista. These operating systems have not been supported by Microsoft for a long time. Organizations do not upgrade and patch the browsers perfectly either. From 35 000 companies over 8 500 organizations had an outdated browser installed on at least 50% of their computers. (Bitsight 2017, 3)

Kaseya conducted a study on automated patch management (Kaseya, 2019). The results considering the different with operating system patch management and third-party patch management is surprising. 75% of the respondents did scan and patch for the operating system vulnerabilities but only 47% did the same to third-party vulnerabilities. What comes to timeframe of patching the critical vulnerabilities do maintain the same pattern. 65% of the respondents applied the critical patches for operating system within a month of the patch release. For the third-party patches the corresponding percent was 42.

Microsoft in collaboration with Securosis also conducted a study regarding patch management in 2009. The findings regarding the maturity of operating system patch management and third-party patch management were similar to the study of Kaseya. Also, back then in 2009 it seemed very normal that organization used multiple tools to manage third-party patch management. One of the key findings in the study was that results are relatively biased if the respondents considered patch management important. (Jones & Mogull 2009. 1)

The study also included questions on patching the WS (workstation) applications. Around 13% of the organizations did not have any third-party patch management. 30% of the respondents did manage patches in some sense but were lacking both policies and tools from the process. The patch management maturity is presented in

the Figure 3. (Jones & Mogull 2009. 8)

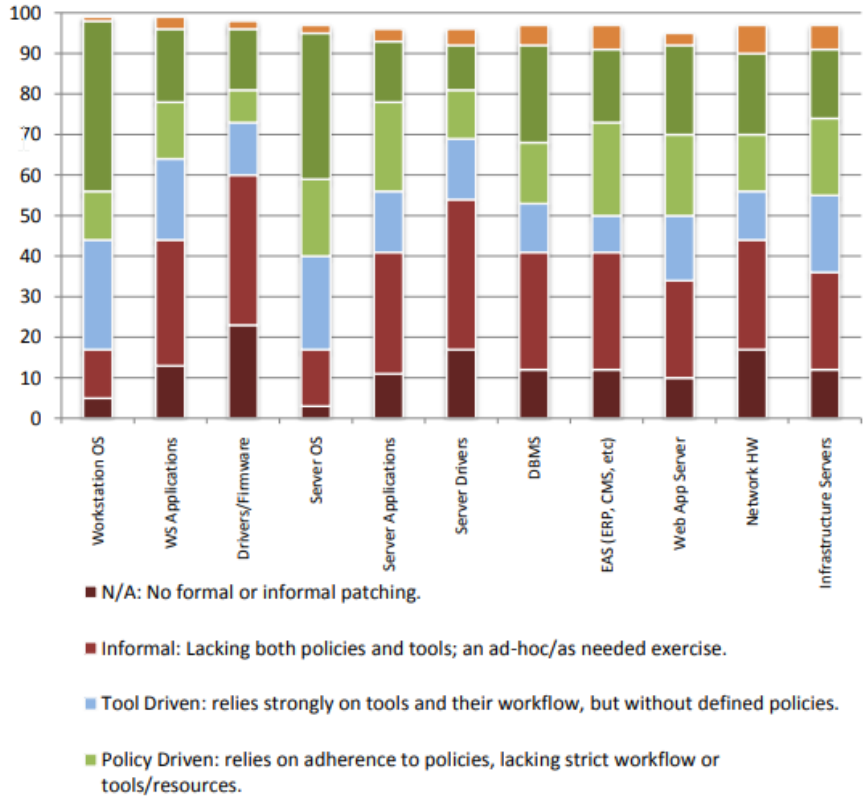


Figure 3. Maturity of patch management process.

2.6 Economic impact of using a patch management solution

Very well-known research organization Forrester conducted a study for a patch management vendor named Ivanti in 2008. The study was based on data of three-year term of using an automated patch management tool for third-party software. One of the key points was to compare economic impact whether an organization manages the patches or not. There were a couple of key findings based on quantitative research. Firstly, the studied organizations would have used drastically more time and resources and patch management it is done manually. For an example, an organization managing 50 000 endpoints estimated that it would require 5 times the resources if they were not using an automated patch management solution for the third-party software. (Forrester 2018, 1)

Keeping the endpoints up to date in a more efficient way was not the only advantage organizations identified. Validation of successful updating is highly regarded. A patch

management solution was estimated to take only a quarter of time forming necessary compliance reported instead of doing it manually. Combining these the examples customer with 50 000 endpoints was able to annually save resources compared to four and a half of full-time employees. For three years this translated to savings worth of $832 785. (Forrester 2018, 1)

One aspect of the study was obviously the effect on cyber security and what kind of an impact it has to risk management. Forrester used an unnamed cyber security framework provided by US government to assess the risks. An interviewed organization managed to reduce their high-risk items by 40% by implementing the third-party patch management solution. (Forrester 2018, 2)

2.7 Patch management process

The importance of patch management is undeniable; however, there is not just one correct way to manage patches. Organizations are different and so environment, systems, software and versions do vary. The Australian Cyber Security Centre, also known as ACSC, recommends organizations to assess the security vulnerabilities before applying the patches to them. They also list important matters to consider when a risk assessment on a vulnerability is conducted. At this point not only the vulnerability and its characteristics are important, but the exposed and impacted assets are to be considered as well. The following list holds key points which should be considered while assessing a vulnerability: (Australian Cyber Security Centre 2019, 1)

- Value and exposure of an asset can increase or decrease risk caused by a vulnerability.
- There might not be a patch released for a vulnerability or the patch might not resolve a vulnerability in full. It can increase the risk.
- A vendor can release a patch outside of a regular schedule. It might show that there is a zero-day vulnerability, or a vulnerability is publicly known.
- It might be possible that a vulnerability exploitation can be automated. This can also increase the risk level.
- There is often a possibility to mitigate a vulnerability in some other way. The mitigation can decrease the risk.

One aspect of the patch management is careful assessment, which means that an organization must have concrete knowledge on their environment. The organization must know their operating systems, software and which version they are running.

ACSC also recommends that a patch for a vulnerability should be scheduled depending on the assessed risk level for the vulnerability. This means that the higher the risk is the faster it should be patched or mitigated. However, on the opposite side of resolving the risk of vulnerabilities quickly is accessibility. For example, when a new patch is installed to a system, there is always a chance of something going wrong. There might be a bug or some other malfunction in the patch. Even though software vendors test their products and new patches thoroughly, they cannot test them in all different kinds of environments. Therefore, a customer should properly test a new software version or a patch in their environment and against their systems. (Australian Cyber Security Centre 2019, 2)

NIST acknowledges a similar matter with patching. There are issues that patching can cause. A patch might require a computer to restart, it can break the application itself or it can cause problems in other applications. Additionally, when devices can be more and more mobile, a valid patching strategy and tool should also cover these devices. (National Institute of Standards and Technologies 2013, 11)

German security company G DATA Software has an extensive guide on patch management. According to them, organization size has an impact on a patch management process. Usually small businesses do have different kinds of processes compared to enterprises. Enterprises have more business units and different systems, so patch management is usually a more complex task to handle. Small businesses do usually have a simpler organizational structure, systems and networking; however, they also have usually less manpower and dedicated personnel to handle specific IT matters such as patch management. Therefore, small and medium sized businesses are a very interesting target for cyber criminals. (G Data Software 2019, 7-8)

Since software update constantly, vulnerabilities are found, and the patches are continuously released the process to manage them must also be continuous. Different parties call this process vulnerability management, change management, patch management or something else. There are different terms; however, there are also different point of views and recommendations.

LabTech (2013, 6-7) opens a process which is also recognized by Microsoft. It is a six-step patch manage process.

1. Get informed on a vulnerability and a patch related to it.
2. Assess the risk and plan the patching.
3. Obtain the patch.
4. Test the patch.
5. Deploy the patch.
6. Validate the installation of the patch.

Another example of patch management policy is introduced in Special Publication of National Institute of Standards and Technologies. It contains similar key points as LabTech and Microsoft but there some other recommendations as well which are for a policy rather than for a process. They recommend deploying an enterprise-wide automated patch management solution. One key point is to inventory all the IT assets. According to them, it is also necessary to continuously test, and measure effectiveness of the organizations patch management program. (Mell, Bergeron & Henning 2005, 51)

2.8 Automated patch management solutions

Gartner has researched patch management solutions several times in the past. In 2003 they went through different characteristics that an automated patch management solution should have as listed below: (Nicolett & Colville 2003)

- Maintain an inventory of systems including operating system, software and versions.
- Track outdated and superseded patch and acknowledge patch dependencies.
- Inventory patches and classify the severity of vulnerabilities.
- Report which patches are needed on inventoried systems.
- Group managed endpoints.
- Distribute and install patches including roll-back feature.
- Support different operating systems and devices.
- Leverage and an existing patch management system.

White has studied this specific matter in his master's thesis. He used the list of characteristics of patch management solutions by Gartner and merged it with a similar list from his earlier study. Some terms were combined to make the list of characteristics simpler. This resulted a good and simple list of features which automated patch management list should include. The features are notification,

inventory management, vulnerability scanning, patch testing, patch distribution and reporting. (White 2006, 101-102)

There is also a more recent study on the matter by Gartner. It was published in 2017. One of their key findings was that different security roles require faster patching but on the other hand, IT operations still must ensure a stable environment during the whole patch management process. The current patch management tools can also vary because of different IT departments handling different technologies. Thirdly, it was found out that endpoints patching is managed better compared to applications and servers. (Gartner 2017)

Based on their findings, Gartner recommends replacing manual and homegrown scripts with an automated patch management tool. They have also found out that many organizations do have a patch management system for Windows operating system; however, it is not the same for Mac OS X and Linux. Patching non-Microsoft and non-Apple so-called third-party software is not organized very well either. Manual patching for desktop applications can be very time-consuming. Desktop administrator might struggle with manually repackaging and deploying the updates for endpoints. Gartner also recognized different type of solutions for managing patches. They are management suites for servers and endpoints, plugins that are integrated to management suites and stand-alone solutions. (Gartner 2017)

Gartner also has a description for the characteristics of a functional patch management solution. The solution must have complete inventory information on hardware, software and the software versions. The patches should also be in a catalog, which means that patches must be downloaded from a software vendor or from some other source and the solution must have a capability to detect whether the patch is needed in the environment or not. The solution must also detect if a patch or a version of operating system is superseded. As organizations have the need to assess the risk based on vulnerabilities, a patch management solution should have features to help with it. Such features could be relating vulnerabilities to Common Vulnerabilities and Exposure (CVE) and to proper Common Vulnerability Scoring System (CVSS). (Gartner 2017)

A proper patch management tool should also have good control over the patch deployment and installation. This means such things as controlling reboot, rollback feature, setting the maintenance window and other similar features. Validating is also a crucial part of a proper patch management process. Therefore, it is necessary to a patch management system to have proper reporting features to offer a good overall view on patch compliance on the systems. Gartner has also listed some key points and evaluation criteria for choosing a patch management solution. (Gartner 2017)

Vulnerability assessment should be included in a patch management solution, or there should be a possibility to integrate an existing vulnerability assessment tool to a solution. There are security configuration and compliance management features in some patch management solutions. These kinds of features can be very useful when an organization tries to follow internal security standards or some regulatory requirements. Controls over deployment and installation of patches are regarded highly important as well. Therefore, a patch management solution should include features for controlling reboots and pre- and post-installation actions. In addition, Gartner also recognizes store and forward feature to be important. It means that a patch could be deployed to a location and redistributed there locally. The endpoints should also be able to download a patch beforehand and install it on a specified later date. (Gartner 2017)

Scheduling the deployment and installation of patches is something a patch management solution should have control over. For example, Microsoft releasing their patches every second Tuesday of a month means that organizations might want to schedule deployments following the same cycle. Using Gregorian calendar means that if deployments are configured to take place for example every second Wednesday of a month, it is not always going to be the following day of Microsoft's patch Tuesday. Because of this, some patch management solutions should have advanced features for scheduling. (Gartner 2017)

Features and functionalities for general patch management solutions are important indeed; however, according to Gartner, patching third-party applications is also a very important process. The patch management solution should have clear indicators and a dashboard to show the most critical vulnerabilities targeted to third party

applications. The solution should also have a support for all the common applications. Additionally, the more the solution has information and metadata on patches the better. The metadata could help organizations to discover, prioritize and report patches. (Gartner 2017)

In addition, Gartner has introduced the term enterprise-readiness for third party patch management. It means the impact on accessibility and usability when new application versions are installed and patched. For example, this can be an ability to install new software versions silently or have an integrated auto updater of a software disabled to increase the enterprise-readiness. In that sense, the end user should be distracted as little as possible by a patch management solution and updating software. Other issues to improve enterprise-readiness can be disabled adware, end-user license agreement removed, and unnecessary shortcuts removed. Some patch management solutions also have a capability to use command line switches to further configure installing patches and new software versions. Furthermore, one considered matter when choosing a patch management solution is speed and SLA how fast third-party patches are available after a software vendor has released them. (Gartner 2017)

3 Research

3.1 Purpose

Patch management is regarded as one of the most important security controls by the cyber security industry. There are many studies conducted on it, but they are very general and do not deep dive into different parts of patch management so well. There are also many studies on vulnerabilities and organizations having outdated software. But the studies tend to refer patch management as whole package including operating systems and all the software.

The thesis is specifically planned find out characteristics and phenomena on third-party software patch management. The study is ordered by an organization which operates in the very industry and they have a product for automated third-party patch management.

3.2 Objectives

The organization has a strong urge to go international with their product. Therefore, there is a great need to understand different types organizations and how they handle the third-party patch management. Additionally, the organization wish to learn what are the competitors for their product. To study this topic, a market comparison for the automated patch management products was conducted as a part of the thesis. The comparison could clarify how do their product perform against the competitors and what are the strengths and weaknesses. It also gives a great opportunity to develop the product.

The purpose of the comparison is not just to give more insight to the organization which ordered it but also function as a utility for other organizations when they are evaluating and choosing a patch management product. Therefore, the comparison will be published in the web. The organization also plans to create a functional web site utility based on the comparison. This web application is supposed to be adjustable by users to give them more proper comparison scores with specific weighting they wish.

3.3 Research questions

There are two surveys used in the study. Questions in the surveys are the same but there are more required answers in the other one. The other survey has no mandatory questions at all. The research questions are formed in cooperation with the ordering organization and their steering group. The questions are targeted purely to learn on important matters which affect the plans to go international.

There are five research questions used to guide and delimit the study:

- How important is the third-party patch management regarded in organizations?
- How do organizations manage third-party software patches?
- Which automated third-party patch management tools are used in organizations?
- What are good characteristics of an automated third-party patch management tool?
- How are automated third-party patch management tools different?

The first four questions should get answers with the help of the survey. The fifth question is answered with the descriptive comparison.

3.4 Risks

To have a credible quantitative analysis there must be enough answers in the survey. Since the invites to the survey are sent via multiple platforms at least 50 organization hopefully answers. Less answers than that might result of lowering the confidence level and increasing the margin of error.

Another risk is related to the descriptive comparison and getting too subjective point of view. Viewing and studying the third-party patch management solutions must be objective. The comparison metrics must be as objective as possible, and they must be based on existing studies and analysis done on the survey results.

4 Implementation

4.1 Research methodology

In the thesis, both quantitative and descriptive comparison methods are used. Most of the research questions can be answered with a survey and a quantitative research. However, the nature of a product comparison requires more profound testing and

analysis which quantitative method cannot properly suffice. Therefore, descriptive comparison is also used in the thesis.

Because of the product comparison the study involves some exploratory characteristics as well. This is mandatory because all the compared products are not that familiar beforehand. Rautio (Rautio 2007) claims that while the knowledge on the compared objects increases it might be necessary to add new aspects to the comparison.

According to (Hantrais 1995) comparative research methods are widely used to explain and analyze for example differences across societies. It is also used to study on cross-national phenomena. This does not mean that descriptive comparison could not be used to study differences on automated patch management solutions. Rautio states (Rautio 2007) descriptive comparison can be used for example to study similar products created by different producers or designers. He also recommends that a wide study of literature should be done before moving to empirical comparison. This helps quite a lot with discovering all the necessary causal influences.

Shuttleworth (Shuttleworth 2008) describes quantitative research as an excellent method to prove or disapprove a hypothesis. Therefore, quantitative research is adequate for the thesis. The existing studies give a decent knowledge what to expect and with the help of the survey conclusions on the hypothesis can be made.

Survey study was selected to be the main method for gathering necessary data. Survey suited the study better than interviews for example. This is because one of the goals was to learn more on phenomena and characteristics related to third-party patch management in organizations. Fewer qualitative answers would not help the assignee organization to understand the desired matters well enough. Some reasons for this are the variety of organization and their subjective needs and points of views in patch management. Survey should get enough answers to cover different phenomena.

4.2 Data gathering and material sampling

The thesis process started with planning it alongside with internationalization project. The organization needed information on processes and tools related to

third-party patch management. It was certain very quickly that a survey was needed to take the whole project forward. The project included weekly meetings with the steering group where the survey and the thesis were only a part of it.

4.2.1 Survey

Advancing the thesis was only a small proportion of a weekly workload so most of the thesis-oriented work was planning for the survey. The most important matters to consider were audience and questions of the survey. The questions were very general in the start and different individuals in the steering group had their own ideas what should be surveyed. There were questions about workstation management, spending money on patch management and intentions to invest in an automated patch management product. These questions are understandable from a point of view of organization willing to go international.

However, the steering group understood gradually that the questions must be simple and self-explanatory. Instead of asking straight questions how to sell a product better to customers the steering group decided to ask questions about processes, habits and opinions on third-party patch management. When the course of survey was vaguely locked it was time to come up with the questions.

The demographics were obviously a category in the survey. In addition to compact personal information, country and job title were asked. More importantly the steering group wanted to know what kind of organizations will answer. Therefore, organization type, industry and number of managed windows workstations were a part of the survey.

Following the necessary demographic information, it was natural to move on the actual questions. The first set of questions considered application vulnerabilities and cyber security assessments in organizations. The set of four questions were linked to each other so if the respondent knew more and answered yes then an additional question was asked. For example, the respondent was asked on their opinion on application vulnerabilities being a threat to their organization. If they answered yes, then they were asked if their organization had conducted a cyber security

assessment to their organization. This way the respondents did not need try answer questions they might not know anything about.

One goal was to learn more on patch management processes and practices of organizations. Some specific questions were asked on that topic. Organizations were asked how they manage patching third-party applications. They were also asked to choose the most important security controls for Windows workstations. Third-party patch management was one of the options. One important aspect of the survey was to clarify which automated patch management solutions organizations use. Therefore, one of the multiselect questions asked which products organization use or they are familiar with.

Since the thesis focuses on third-party application and their patch management it was necessary to study the software usage. The respondents were asked which free third-party applications are used in their organization and if there are any applications which are not included in any patch management process. If there were any patch application excluded from patch management process the respondents had a chance to list the applications and state a reason for that.

The final part of the survey focused on studying how organization think on third-party patch management processes and features of automated third-party patch management solutions. The respondents were given a chance to define the importance of different patch management process on the scale of three from low to high. Questions for features of automated third-party patch management solution were asked in a matrix form on similar scaling as well.

4.2.2 Audience

The best audience for the survey would have been people who know how their organization manage third-party application patching. An ordinary person in an organization have might not have any knowledge on a specific IT process. The person can have an understanding that new software versions are installed to its endpoint from time to time. More importantly the ordinary personnel do not most likely understand the concept of vulnerability, cyber security assessment or how many endpoints their organization manages.

The optimal respondent would probably work in IT, cyber security or risk management. Therefore, it was mandatory to choose which were the channels to distribute the survey. Naturally all the existing contacts and customers of the organization were used. Additionally, it was decided to invite people to respond on different IT oriented forums. One of the used methods was to invite people to answer in a cyber security channel in Slack chat of JAMK.

As a fourth and as the most extensive way to reach potential respondents the steering group decided to use LinkedIn as a platform. LinkedIn gives an opportunity to choose target audience. Because it is the platform for social business networking, they have huge amounts of different job titles to choose from. 17 different job titles were chosen. The following figure (Figure 4) shows how the different target groups were chosen.

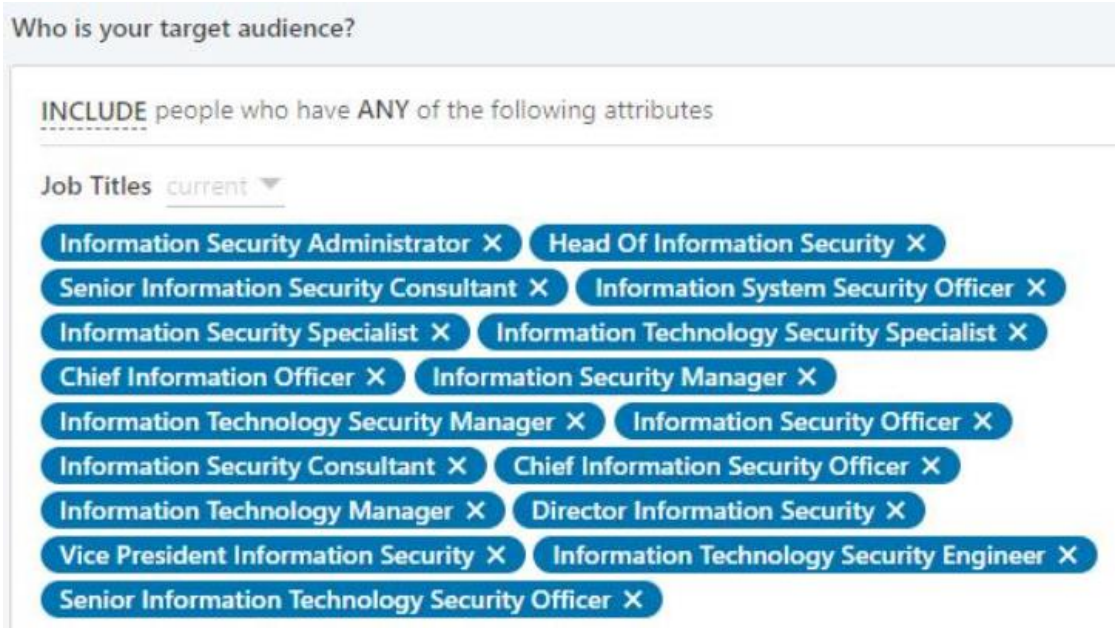


Figure 4. The targeted job titles for InMail in LinkedIn.

It was clear that most of the respondents with in-house methods such as mail lists and invitations in forums would result in mostly Finnish people. Therefore, it was necessary to reach international organizations as well. LinkedIn supports geographical targeting which was very helpful. Figure 5 shows the selected continents and regions where the potential respondents were sought.

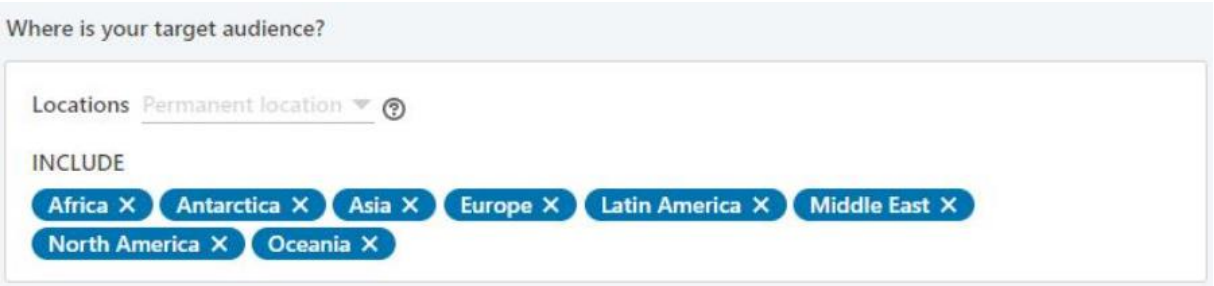


Figure 5. The selected regions for respondents to be invited.

4.2.3 Tools

Since the study is mostly quantitative and the objectives require answers internationally. That being the case a web survey was the most suitable tool to arrange the survey. At first, it was the plan to use Microsoft Forms as a platform to create the survey. However, it turned out have too limited features. The search for web survey tools resulted in finding one of those most used solutions, SurveyMonkey. A quick review assured that it had all the necessary features and functions to arrange the survey.

As said earlier, there were two surveys created with identical questions. The only difference between them was that all the questions in the first survey were mandatory, unlike the second where all the questions were set optional. The surveys were piloted with smaller groups to find out if they had crucial differences in the response rate, specific questions or overall. According to the pilot results of around 20 of each survey, there were no major differences between them. Therefore, it was decided to move on with both surveys. Figure 6 shows the final statistics after collecting the responses for about six months.

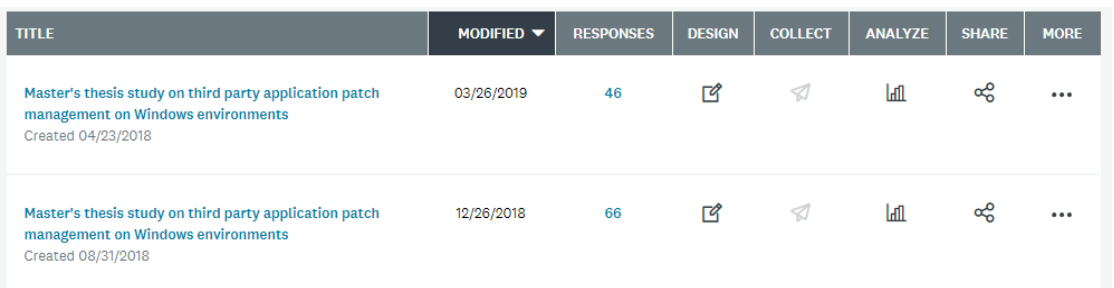


Figure 6. The final response amount of the two identical surveys.

4.2.4 Survey reachability

With the specific region and job title attributes the target audience size was between 2 to 2.1 million people according to LinkedIn. From the amount of over 2 million plausible participants the algorithms of LinkedIn chose 3 992 people. Additionally, the survey link was shared on 6 different IT oriented forums in web, sent to 3 811 existing customer or leads. Additionally, around 40 cyber security specialists studying at JAMK were invited to respond to the survey. Without a doubt, the two major methods to reach the audience were sponsored InMail in LinkedIn and the existing mailing list of the organization. Figure 7 represents the statistics how the audience was reached by using different methods.

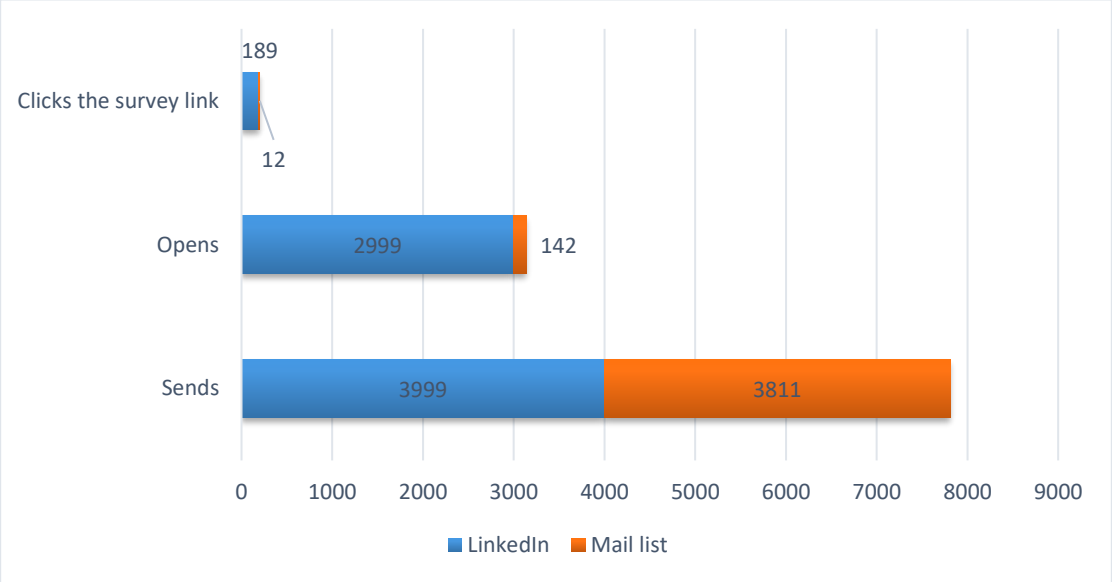


Figure 7. Survey reachability.

Carefully targeted mail advertising was much more effective. The results are significant when inspecting sent mail amounts to opened mails on both platforms. Even though the number of sends was very similar. The customers and prospects on the mail list consist mostly of people involved in information technology.

4.3 Analysis of data

Out of the estimated set of 3 200 reached people slightly over 200 decided to move to survey by clicking a link. From the 200 possible respondents 110 decided to participate in the survey.

4.3.1 Demographics

The respondents were asked to provide some personal information and basic information on their company. These questions were not mandatory; yet, the respondents were encouraged to provide at least an e-mail address if they wanted to receive a link to the thesis and the comparison later on.

Nevertheless, most of the respondents decided to answer the demographics questions. The total of 110 respondents answered the demographic questions in the following as follows:

- 98 provided the information on country.
- 105 answered the question about their job title.
- 102 gave out the information regarding the type of their organization.
- 103 answered how many workstations their organization manages

The responses came from 44 countries. The exact numbers of the countries are listed in Appendix 8. Additionally, Appendix 7 shows a more representative map-based chart. Most of the answers came from Finland due to the use of the mailing list of the assigner organization. Figure 8 shows the number of the responses per country if there were more than one respondent. 26 countries had only a single respondent.

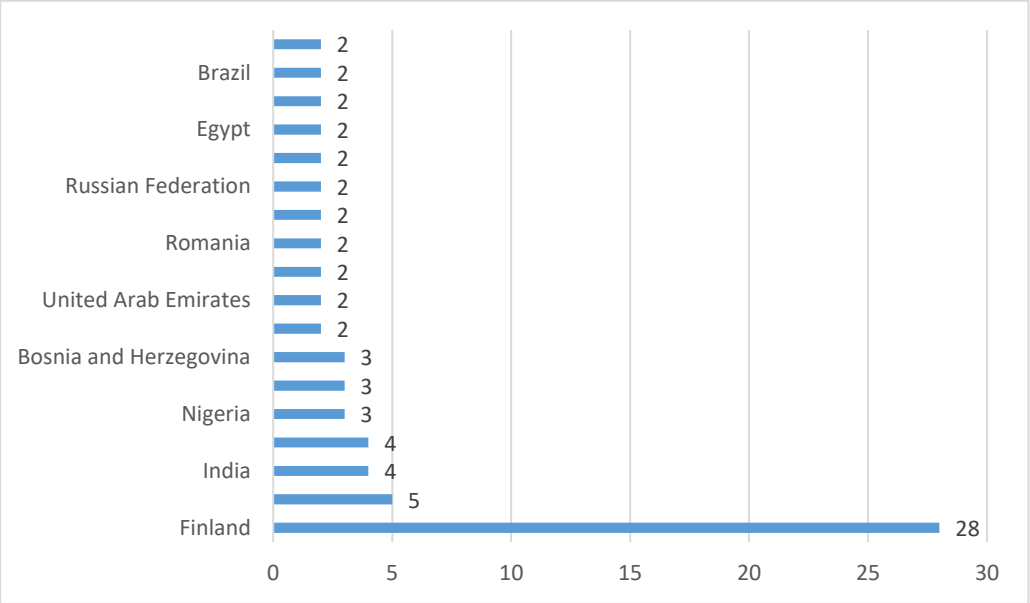


Figure 8. Respondent countries with more than one respondent.

The question regarding the job title had 7 options including so called other option and a possibility to input a custom job title. Some of the input job titles that were very similar, so they were merged to a single nominator. For example, an “IT officer” and a Finnish title “IT palveluvastaava” were merged to IT Manager. There were a few answers which can be regarded as a joke: IT overlord and Oddman. Those were removed from the demographic statistics because they would not have any productive impact on the study. Other unusual answers were musician and clinical psychologist. All the answered job titles are listed in Figure 9.

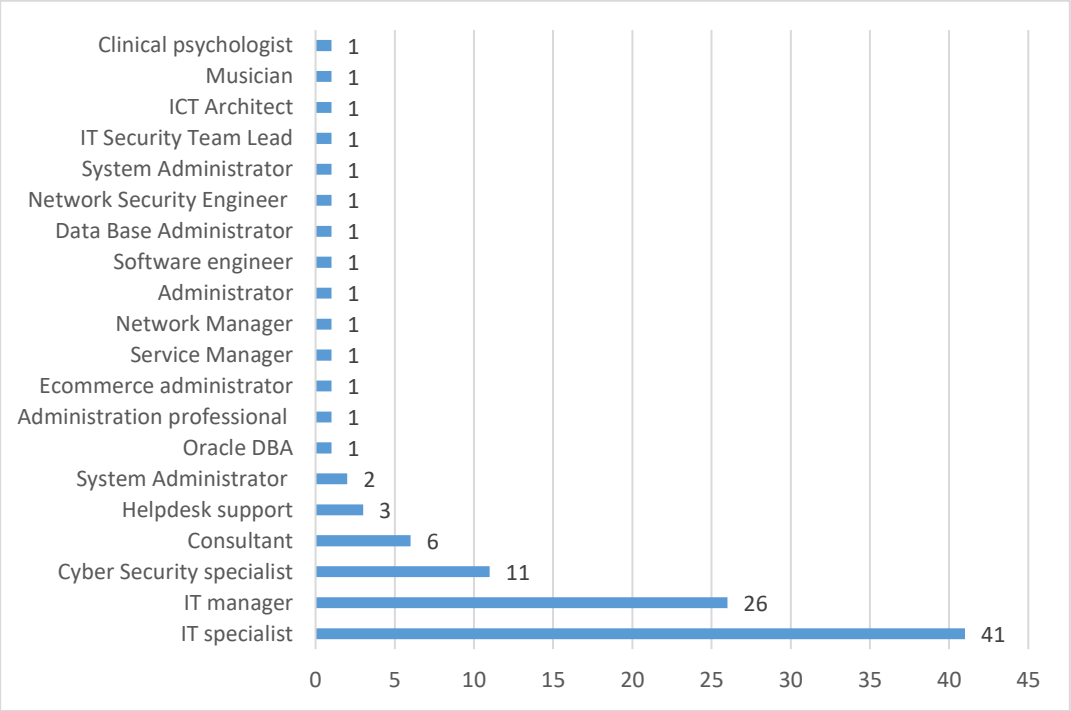


Figure 9. Job titles of the respondents.

The question about the organization types was very straightforward. Private sector was clearly the major organization type with 75 responses. Figure 10 shows that academic, non-profit and government were the minor organization types in the survey.

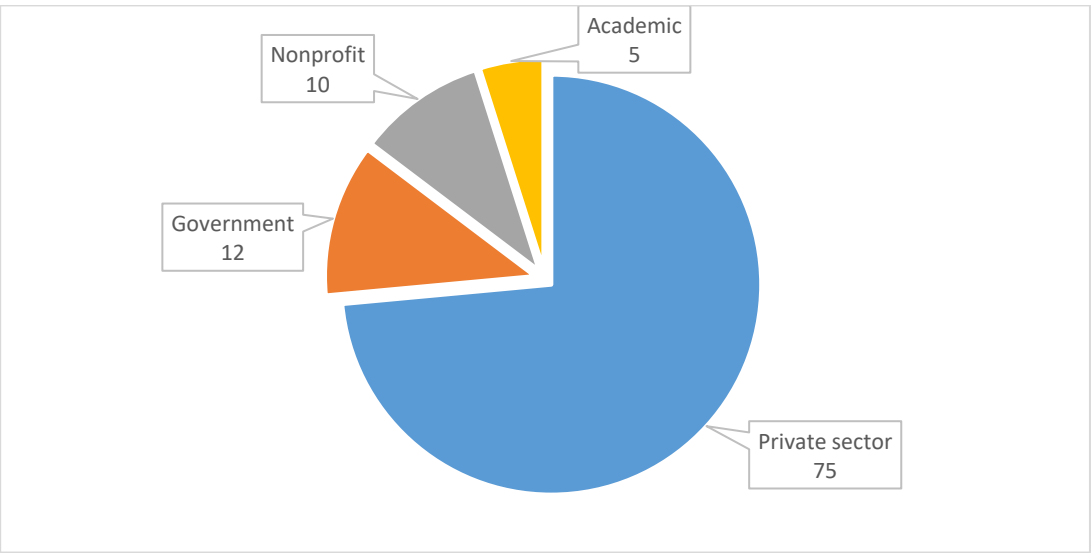


Figure 10. Organization types of the respondents.

The respondents were also asked about their organization's industry. The biggest industries to answer the survey were clearly telecommunications, technology, Internet and electronics. This most likely reason for this is the mail list and targeted job titles in LinkedIn consist mostly of IT professionals. Figure 11 lists all the responding industries.

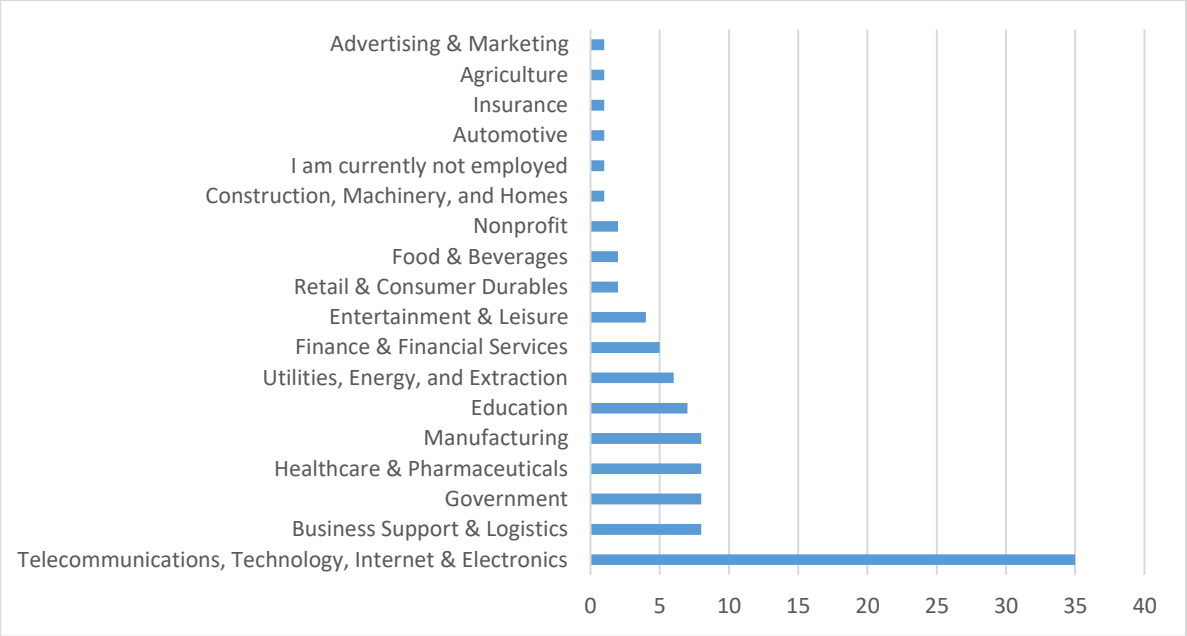


Figure 11. Industries of the responding organizations.

Another important demographic statistics is organization size in the manner of the number of workstations. Different sized organizations were very even when looking at the number of responses. The largest option for the number of workstations in the survey was 10 000+; however, there was an option for an even larger figure in which the respondents were asked to provide a number. Therefore, the organizations sizes varied from 25 000+ workstations to 1 – 10 workstations. Figure 12 lists all the sizes and their amounts.

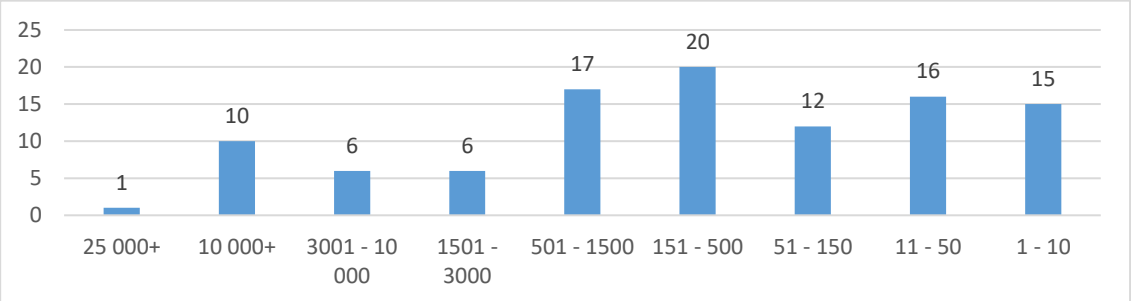


Figure 12. Number of different sized organizations.

4.3.2 Vulnerability threats and risks

After the basic demographic information, the customers were asked to answer four questions regarding vulnerabilities as well as threats and risks related to them. The questions were conditional, which means that if a respondent answered yes then a follow-up question was asked. The same rule applied to the first three questions regarding the vulnerabilities. The asked questions were the following:

- Do you think the vulnerabilities of third-party applications might be a threat to your organization?
- Has your organization conducted a cyber security risk assessment of your business?
- Have you included software vulnerabilities in the risk assessment?
- How high a risk does your organization consider third party application vulnerabilities to be?

The four vulnerability related questions were answered well. The response percentages for the questions were 96.4 %, 95.5 %, 54.5 % and 48.2 %. The decreasing per cent is because the questions were conditional. All the response percentages can be found in Appendix 10. Figure 13, on the other hand, shows how many answers there were regarding the vulnerability questions.

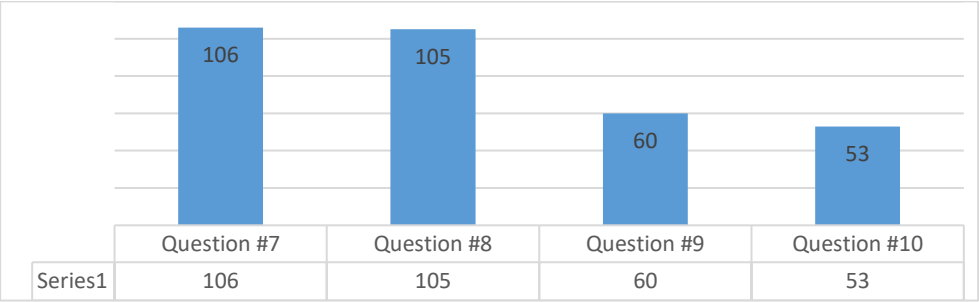


Figure 13. Numbers of responses to vulnerability related questions.

According to responses, the majority considered third-party software vulnerabilities to be a threat to their organization. The percentages of the opinions are represented in Figure 14.

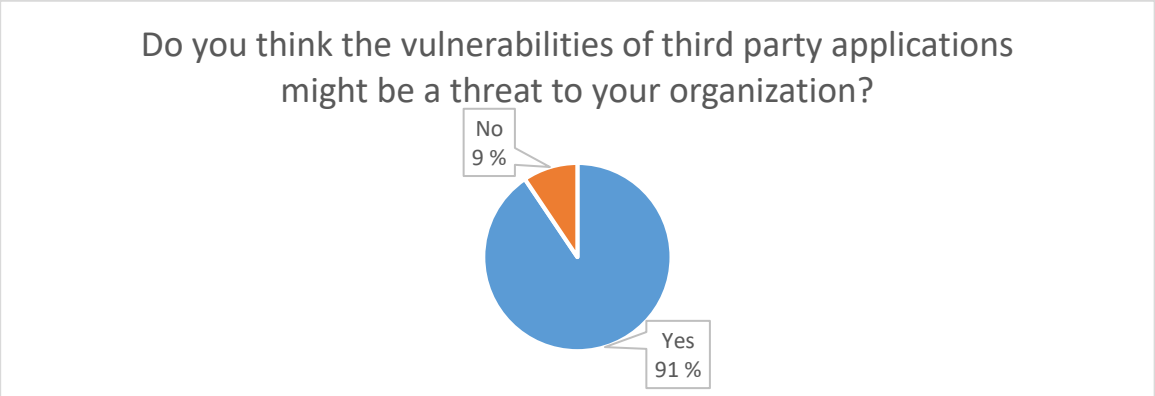


Figure 14. Organizations consider the third-party vulnerabilities as a threat.

The set of 96 respondents who answered yes were then taken to answer the next question regarding cyber security risk assessment. The rest who had answered “no” (10 respondents) to the previous question were then taken to question to question 11. The question regarding the cyber security risk assessment was given 3 options to answer: “no”, “yes” and “I do not know”. From the set of 96 respondents, 60 answered that their organization had conducted a cyber security risk assessment to their business at some point. 26 respondents answered “no” and 19 did not know whether a risk assessment had been conducted or not. The percentages of the answers are represented in Figure 15.

Figure 15. Answer percentages of cyber security risk assessment question.

If a respondent answered “yes” to the question, he/she was then taken to answer if his/her organization had included third-party application vulnerabilities in the cyber security risk assessment. Out of the set of 60, the majority had included the vulnerabilities of third-party applications to the assessment. In other words, 54 respondents answered “yes” and 6 answered “no”. Figure 16 shows the response percentages on the very question.

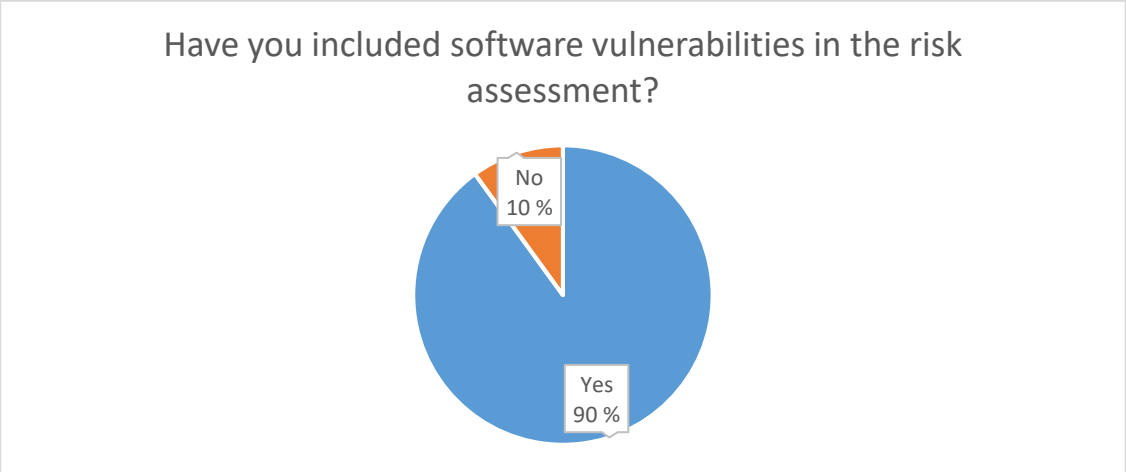


Figure 16. Answers on question considering cyber security assessment.

The majority that had included the vulnerabilities in the assessment were then asked about the risk level of the third-party application vulnerabilities. 7 of the respondents considered the risk to be critical. A larger number with 21 respondents answered that the risk level of the vulnerabilities is high. The slight majority with 22 respondents answered “medium”. Only three respondents considered the third-party application vulnerabilities to be only a low risk. Figure 17 presents the percentages of the answers.

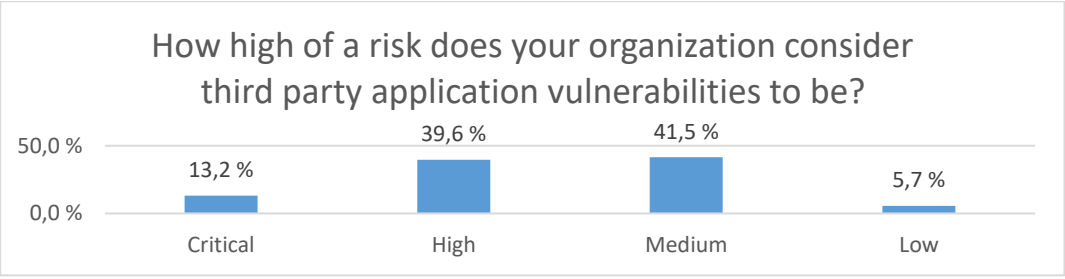


Figure 17. Respondents answers to question regarding risk level of vulnerabilities.

4.3.3 Current third-party patch management methods

There was a question on the current patch management methods and processes that the organizations have. The statements were the following:

1. Application patch management is automated by a patch management product or a remote monitoring and management solution.
2. IT manages the application patching individually on each endpoint.
3. IT uses a tool or a script to manage application patches.
4. Applications are considered to patch themselves automatically.
5. Third party application patches are not managed.
6. Users of the endpoints are responsible for patching the applications.

A small majority of 30 respondents answered that the third-party patch management of their organization is automated in some way. The second highest number of respondents (26) said that IT manages all the endpoints and their patch management individually. A tool or a script received the third highest number of responses (19). There were also some (6) organizations which considered the third-party application patch themselves successfully. With the similar number of responses, 6 organizations answered that third-party patches are not managed at all. The minority of 5 of the responding organizations answered that their end users are responsible for patching their own endpoints. Figure 18 states the exact percentual distribution of the answers.

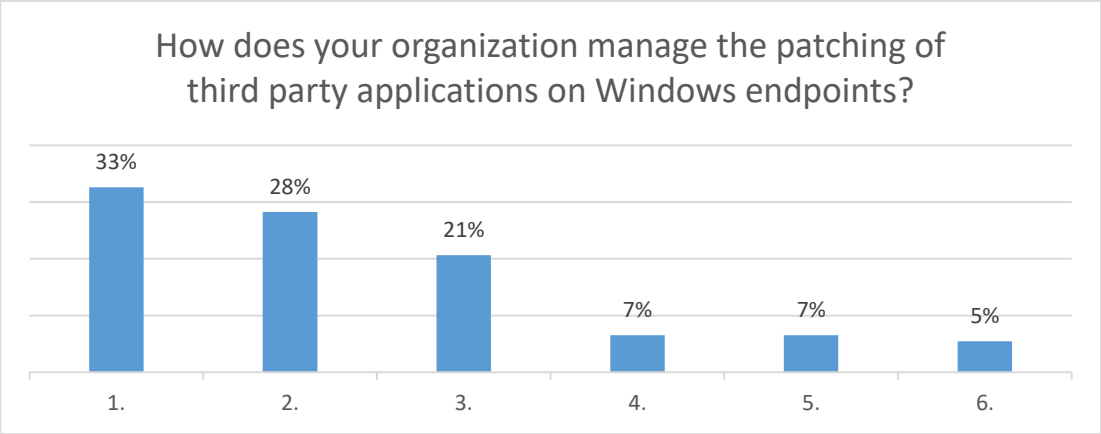


Figure 18. Answers on current third-party patch management methods in organizations.

4.3.4 Third-party patch management versus other cyber security controls

The respondents were asked to select the three most important security controls from five options. This means that all of the respondents could choose three options instead of just trying to think which one is the most important. The options for the statement were:

- Third party application patching (Keeping software such as Java, Firefox etc. up to date)
- Enforcing the principle of least privilege in operating system (Restricting regular users to not have administrator privileges)
- Software firewall (Windows firewall or additional software-based firewall in operating system)
- Operating system patching (Keeping the operating system up to date)
- Preventing the use of removable media (Disallowing USB-media connection for example)

The majority of respondents with 70 answers considered that operating system patch management is the most important cyber security control of these 5 alternatives. The second highest number of 55 respondents considered the least privilege policy to be the most important security control. The third most important security control was password policy with 41 answers. Software firewall and third-party patch management received both the same amount of 39 answers. Preventing use of removable media was regarded the least important security control. The answers are presented in the pie chart in Figure 19.

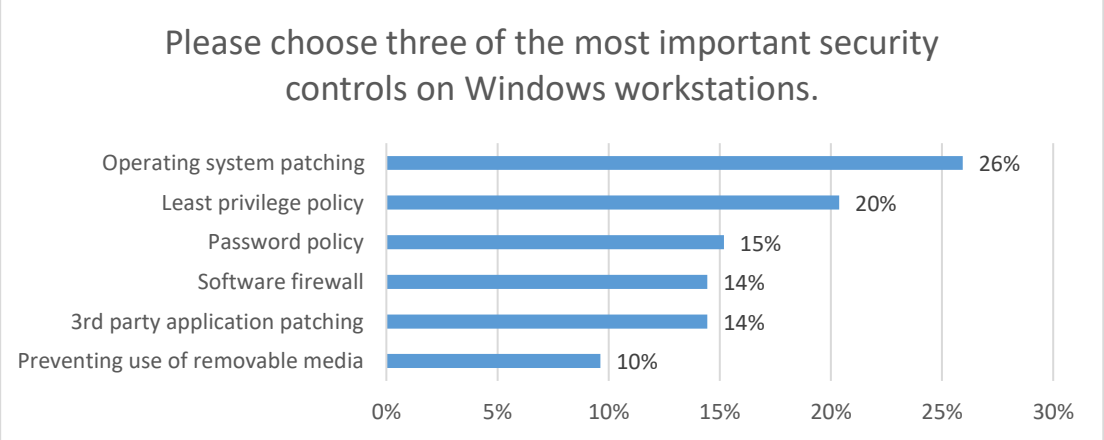


Figure 19. Survey answers considering most important security controls.

4.3.5 Awareness and usage on third-party patch management solutions

One of the most important objectives was to study the existing third-party patch management solutions. The survey included a question on patch management solutions used by organizations or which they are familiar with. The respondents had 21 patch management solutions to choose from and they were able to select multiple alternatives. The respondents were also given an option to provide any other patch management solution. Therefore, four more solutions were answered by the respondents. Because of the great amount of solutions, they are looked over in Figure 20.

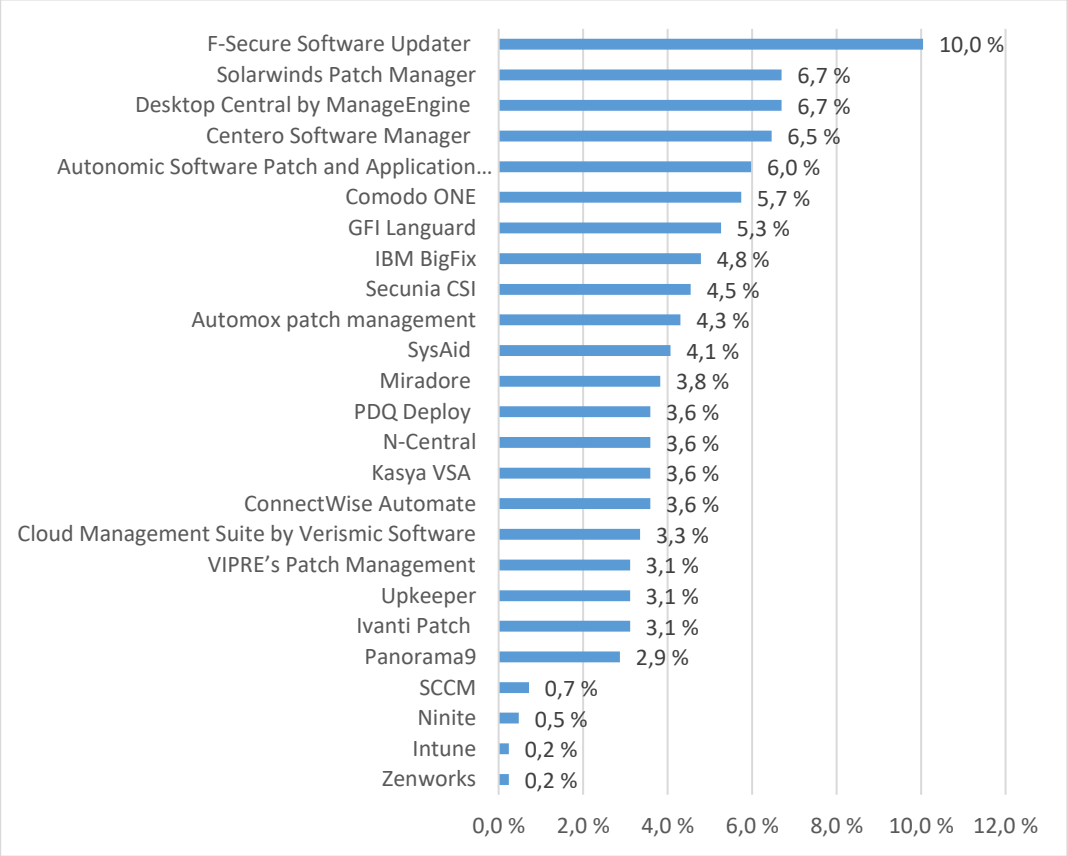


Figure 20. Respondents' awareness of third-party patch management solutions.

4.3.6 Patched applications

The respondents were asked to choose which applications they have within patch management process. There were 15 commonly used free Windows third-party

applications to select from. Figure 21 explains the distribution of third-party application usage.

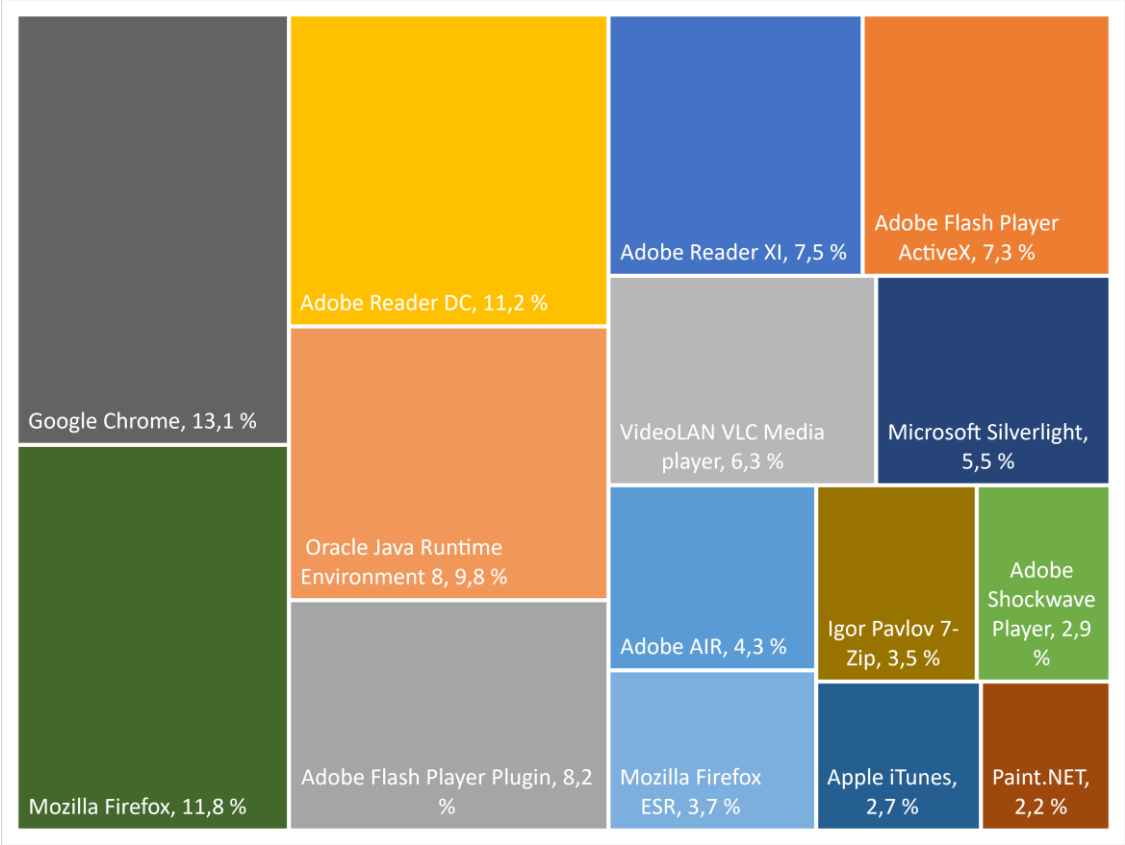


Figure 21. Respondents' answers on third-party application usage.

Instead of having only knowledge on patched applications, the respondents were also asked if they have any applications which are not included in the patch management process. If a respondent answered "yes" he/she had a chance to provide additional information on the reason behind it. The majority of almost 60 % answered that they have applications which are not included in the process. 40 % of the respondents answered the opposite.

Total of 20 respondents also considered their organization to have some applications not included in patch management provided an additional reason. The free answers were merged and a total of 9 different reasons was found. The answers and their numbers are listed in Figure 22.

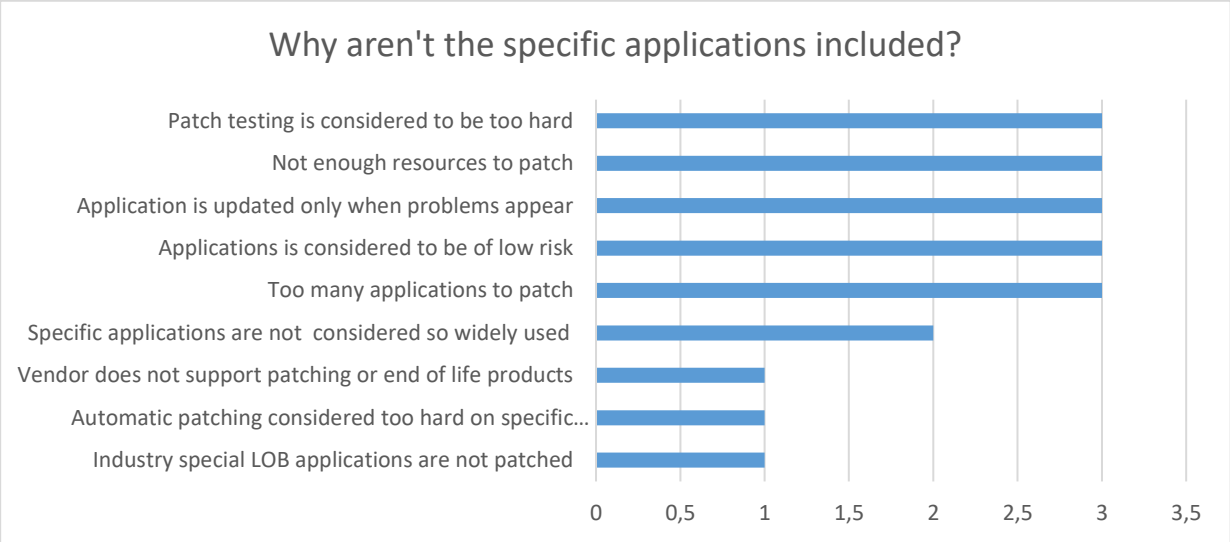


Figure 22. Reasons for not patching specific applications.

4.3.7 Patch management processes and solution features

The organizations were asked to define the importance of different patch management processes. The respondents defined the importance for eight patch management processes on low, medium and high scaling. The complex answers are presented in Figure 23

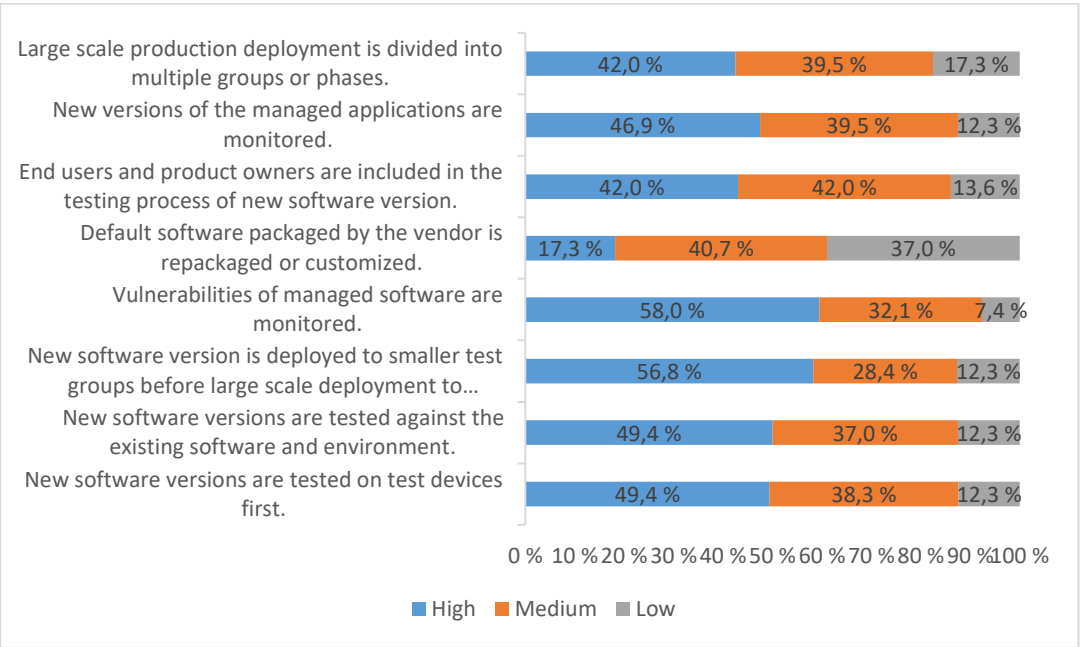


Figure 23. Answers considering the importance of patch management processes.

The last question of the survey had a very similar structure to the previous one. This time the respondents were asked to define the importance of automated patch management solution features. Figure 24 shows the distribution of the answers.

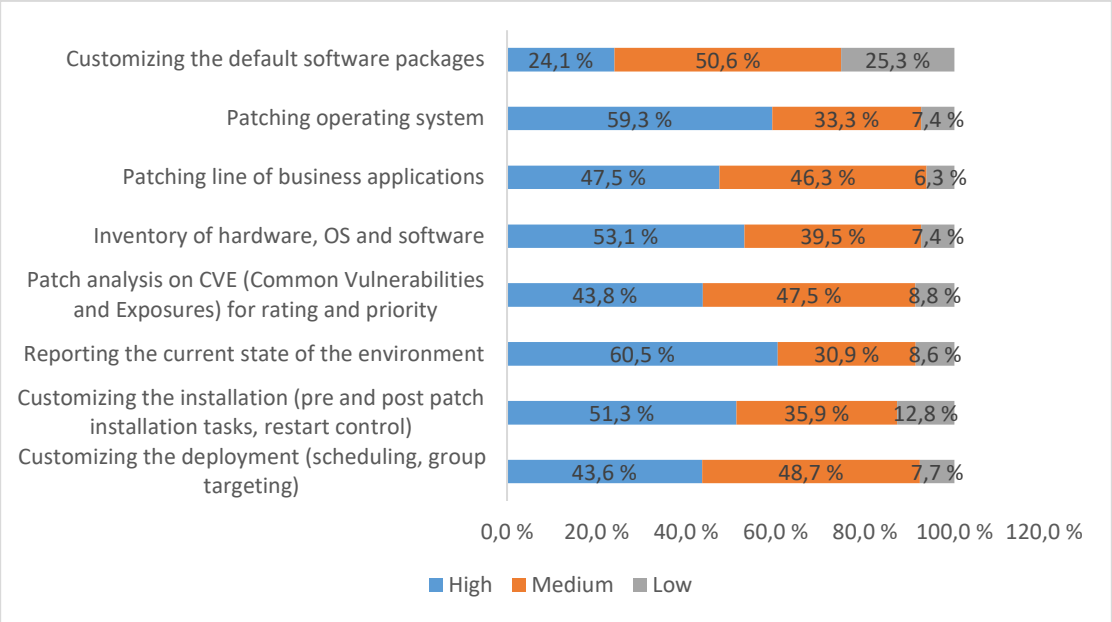


Figure 24. Respondents' opinions on importance of patch management tool features.

5 Discussion

When the results are walked through, one must understand that the respondents are individuals representing their organization. Therefore, some of the answers and opinions can be subjective and might not present the complete truth how the organization as a whole would answer the same questions. There are 110 respondents with 20 different job titles who participated in the survey. This means that all the respondents might not have all the necessary knowledge to perfectly reflect on the matters regarding the patch management of their organization. On the other hand, only 2 % of the respondents did not have an IT job at the time of answering; hence, the vast majority should have a basic understanding of simple IT technologies and cyber security controls including patch management.

The study aimed to find answers to five research questions. The first question in the survey (#7) dealt with the importance of patch management in organization. Therefore, a good part of the survey focused on vulnerabilities, and patch management was compared to other cyber security controls. As it was noted in chapter 4.3.2 of this study, the vast majority of respondents considered application third-party vulnerabilities to be a risk to their organization. The question itself is obvious and simple. Nevertheless, 9 % of the respondents do not consider vulnerabilities as a risk. There could be different reasons for the portion of respondents to think this way. Some might think that their IT environment is so secure and highly protected that there is no way that a software vulnerability could be a risk to them. A more probable reason could be ignorance of the great security risk of software vulnerabilities. In any case, it is very reassuring to discover that 91 % of the respondents do understand the risks of vulnerable applications.

The next question (#8) concerned cyber security assessments. It is understandable that 18 % of the respondents did not know if their organization has conducted one. Additionally, it is reasonable that a quarter of the organizations had not conducted an assessment. Even though slightly over a half of the respondents had conducted an assessment, it indicates something distressing about cyber security overall. Assessing risks and including cyber security to the assessment is a base for healthy IT management. One must understand that conducting a cyber security assessment

requires knowledge, time and human resources. Hence, there can be many reasons for an organization to neglect a process like this.

However, when organizations assess cyber security, they seem to include software vulnerabilities in the assements most of the time. The risk severity answers of third-party application vulnerabilities vary moderately. This shows that organizations and individuals think very differently about third-party software vulnerabilities. The same trend continues in answers considering the most important security controls. There were four security controls which are regarded to be more important than third-party application patching. At least there is a remarkable difference in the way how people think about operating system patch management versus third-party application patch management.

Even though the opinions vary on the importance of third-party patch management, still the majority of the organizations manage the patches by some method or process. The remaining organizations either do not patch at all or rely on users or the software to operate the patching. 59 % of the respondents had a third-party patch management solution in use. A quarter of the respondents did not have any third-party patch management solution in use or they were not familiar with any. The respondents were asked which solution they use. The distribution of usage in percentage is shown in Figure 25. These results answer the second and the third research question:

- How do organizations manage third-party software patches?
- Which automated third-party patch management tools are used in organizations?

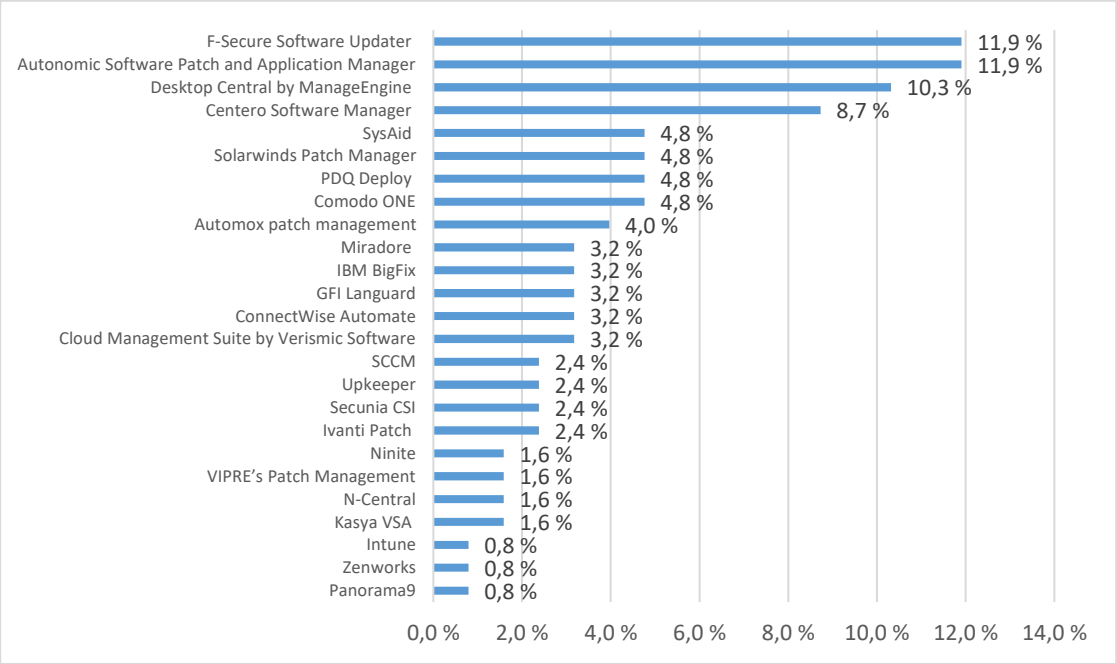


Figure 25. The distribution of different automated third-party patch management solutions.

The fourth research question was to find out the good characteristics of an automated third-party patch management solution. Two of the questions in the survey provided helpful information regarding the question. In addition to the existing theory on patch management solutions, the respondents put processes and features in order of importance in the survey. Only one out of eight patch management processes was not considered important by the respondents. According to the respondents, repackaging or customizing a default third-party application software is not an important process in patch management. On the scale of low, medium and high, there were no other obvious deviations; however, it could be said that three of the processes were strongly considered as of both high and medium importance. Those processes are the following:

- Large scale production deployment of the new software version is divided into multiple groups or phases.
- End users and product owners are included in the testing process of new software version.
- New versions of the managed applications are monitored.

The remaining processes were rather similarly valued. When going through the answers of the last question which considered the importance of patch management

solution features, there are two features which stand out. The respondents value features to patch the operating system and report the current state of the endpoint environment. Other than that, the respondents value the patch management features mostly of high and medium importance.

6 Comparison

From the assigner point of view comparison would be an extremely valuable asset for them. This would support both the marketing and development teams. The comparison evolved throughout the project, but the objective remained the same all along. In addition of creating a helpful comparison for the assigner, they also have a framework and process to evaluate additional solutions and make iterative comparison in the future.

6.1 The purpose of research questions

The purpose of the final research question was to understand the differences of the automated third-party patch management solutions. The comparison had been done twice earlier by the organization assigning the thesis. Unlike the earlier iterations of the comparison, it was supposed to be more objective and thorough this time. The criteria for the earlier comparison had been constructed with the knowledge of the employees of the organization.

Different from the previous comparisons, the criteria for it were formed on the basis of the existing theory and received responses from the survey. Additionally, the criteria were not locked before the evaluation of the solutions because new important criteria and features might appear. The comparison started by listing all the possible features of a patch management solution.

The steering group of the study also realized that it is not rational to try to rank the solutions from one point of view. Therefore, the known features were checked out and marked to the comparison worksheet. With this objective information, the future reader of the comparison can weigh out and focus on the chosen features.

6.2 Categories

There were 8 categories in the comparison: general information, security, vulnerability management, inventory and assessment, patch deployment, validating and compliance, enterprise readiness and solution deployment. The general category included basic information related solutions:

- Number of different third-party applications supported by the solution.
- Coverage on top priority applications based on usage and number of vulnerabilities.
- Price for organizations sized around 200 endpoints.
- Price for organizations sized around 2 000 endpoints.
- Price generally available in the web.
- Supported endpoint operating systems.
- Number of prerequisites.
- Capability to patch line of business applications.
- Capability to patch Windows operating systems.
- Option to test the solution independently.

The majority of the previous criteria is self-explanatory; however, the priority applications need further clarification. At first, the utilization of the well-known third-party application had to be resolved which was carried out by getting statistics from the organization that had assigned the study and from Vulnerability review 2018, Top Desktop Apps by Flexera (Flexera 2018). In addition, the third-party application utilization was studied in the survey as well.

With the help of these three sources it was possible to form a list of 11 most used applications. Then, the known vulnerabilities for the most used applications from the three previous years were verified from CVE Details (CVE Details 2019). The combination of vulnerabilities and utilization of the applications helped in choosing the top nine priority applications for patching. The utilization and the count of vulnerabilities are shown in Table 1.

Table 1. Utilization and number of vulnerabilities for the top priority applications.

Application	**Flexera ranking**	**Orderer ranking**	**Survey ranking**	**Vulnerabilities 2016**	**Vulnerabilities 2017**	**Vulnerabilities 2018**
Adobe Flash Player	1	1	3	266	71	26
Google Chrome	2	2	4	172	153	160
Mozilla Firefox	4	4	2	133	305	333
Adobe Reader	6	3	1	227	207	286

Oracle Java Runtime environment	5	5	5	37	69	53
Microsoft Silverlight	3	9	7	3	3	0
VLC Media Player	7	7	6	2	7	3
7-Zip	9	6	9	2	1	4
Adobe AIR	10	13	8	0	0	0

This set of software was then used when the hands-on comparison was performed. Because all the applications can have multiple different versions, different languages and bitness, they had to be chosen beforehand. 32-bit applications were used in the comparison and their language was English. In addition to this, the versions used were the second newest version of the software.

Another category in the comparison was security. Some features were taken into consideration based on the recommendations of NIST as stated (Souppaya & Scarfone 2013, 5) that users should not be able to negatively affect the patch management solution. The compared features were the following:

- Capability to prevent uninstallation of the agent of the solution on endpoint.
- Capability to prevent changes by an end user.
- Information on the software packages origin to track the validity and integrity of them.
- Capability to keep track on actions done within the solution by administrative users.

In the capability to prevent uninstallation of the agent, some properties were verified. Firstly, it was explored if a user can remove the agent of the solution from control panel. Secondly, it was checked if the user has a possibility to stop the agent service or do some similar negative actions.

Vulnerability management is a very important part of a functional patch management process. The survey indicates that the respondents consider vulnerability management to be high priority. Figure 26 displays a part of the responses on the question regarding the most important patch management processes.

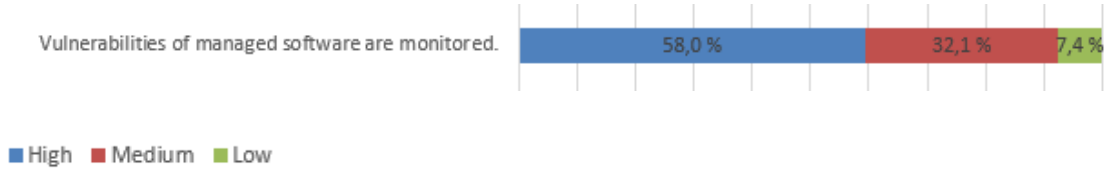


Figure 26. Survey answers considering the importance of vulnerability monitoring.

Gartner (Gartner 2017) identified features related to vulnerability management with a high priority. In addition to this, some other important features were compared:

- Monitoring vulnerabilities related to managed third-party applications.
- Capability to configure alerts on newly disclosed vulnerabilities.
- Severity rating for vulnerabilities.

These features are very self-explanatory; however, vulnerability rating capability was further inspected. It was reviewed for the type of the rating and how thorough the rating system was.

Both Gartner Gartner (2017) and NIST (Souppaya & Scarfone 2013, 6) have considered inventory and assessment of computers, software and software versions as a highly important feature. Therefore, these three features were reviewed in the third-party patch management solutions.

One of the more extensive categories was third-party application patch deployment which is one of the necessities to have in a patch management solution. This is also something that Gartner (2017) and NIST (Souppaya & Scarfone 2013, 11) recognize. The respondents of the survey consider features of this category mostly as both high and medium importance. Figure 27 shows the percentages on how respondents answered the questions regarding the priorities third-party application deployment.

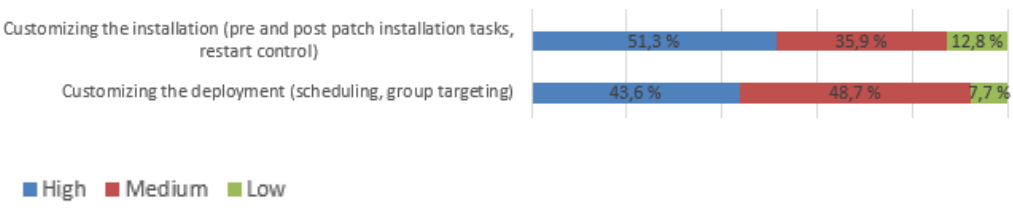


Figure 27. Survey results on patch management features.

The following features are included in the category:

- Configuring endpoint restart during the software update process.
- Option to run patch management in so called autopilot mode with minimal manual effort.
- Excluding specific applications in the software update process.
- Configuring the schedules of the software updates.
- Managing device and application groups in the solution.
- Creating and managing different policies for software updates.
- Installing specific software in fresh even if it is not installed on the endpoint yet.
- Informing an end user of the incoming software update
- Customizing the installation of a software with a custom package or installation parameters.
- Creating deployment rules based on the severity of the update.

If the deployment of the patches is a very important category of features, so is validating and compliance. NIST (Souppaya & Scarfone 2013, 16) states that organizations should also use other methods to confirm the installation of the patches. Additionally, LabTech (2013, 6-7) and Microsoft both recognize the fact that validating the installation of the patches is a necessity. There were three features included in this category:

- Endpoint reporting regarding the third-party software updates.
- Reporting on various patch management related information.
- Configuring reports to be automatic and scheduled.

The concept of enterprise readiness was introduced in chapter 2.7. This term was conducted by Gartner (2017) and it means the specific requirements for applications and patching. It is also something that the organization assigning the thesis highly regards in their solution. Although Gartner thinks in this way, the feedback received via the survey was not aligned with it at all. Figure 28 displays that the respondents consider enterprise readiness type of features mostly as being of medium importance.

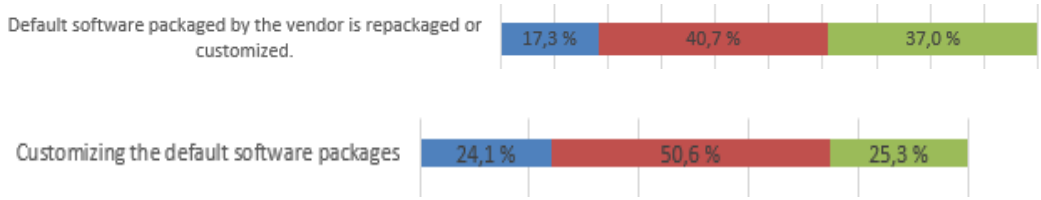


Figure 28. Survey results regarding enterprise readiness and package customizing.

Enterprise readiness category includes the following:

- Disabling unnecessary software shortcuts in the third-party applications.
- Installing a patch does not change any applications settings.
- Installing updates in total silence without interrupting an end user.
- Disabling integrated software update settings for third-party applications.
- Enrolling multiple endpoints simultaneously.

As an extra category it was decided that solution deployment could be included in the comparison. This means that consumed time, reliability and simplicity were metered. The features compared in this category were:

- Time it requires to deploy the solution
- Solution reliability.
- How easy it is to deploy the solution.

6.3 Compared solutions

There were three different types of patch management solutions included in the comparison. The majority of the products are cloud based standalone solutions which communicate to the end points with or without a client. Then there are quite many integration-based on-premises solutions out there. In addition to these, there can also be standalone solutions on-premises without any integration to existing systems.

All the existing solutions in the market could not be included in the comparison or could not be reviewed. At the time of planning the comparison, 23 different third-party patch management solutions were already known or could be found by searching web. The number would have been too high for the scope of this study. Therefore, the respondents were asked which solutions they have knowledge of and

what solutions they have in use. Out of the available solutions 9 were picked. The criteria for picking consisted of the following matters:

- Awareness and utilization of the solution.
- Every solution category requires at least 3 products to be compared.
- A trial for the solution must be easily available.

Autonomic software was quite a surprise in the sense of utilization level and the respondents' awareness of it. It is a very specific patch management integration to McAfee ePolicy Orchestrator. It was left out of the comparison because McAfee ePolicy Orchestrator does not seem like a widely used solution compared to SCCM or WSUS. Additionally, it was not feasible to get a proper environment and evaluation trial to test it out. Secunia CSI is also known as Flexera Software Vulnerability Manager after Flexera acquisitioned Secunia. This specific solution was not available for a trial even though the company were asked for one. Then there were many products with a very similar level of awareness and utilization. From this set of solutions three were selected because of various reasons. Shavlik was recently acquired by Ivanti and therefore many of the respondents might not recognize the otherwise very well-known third-party patch management solution on the market. Therefore, it was selected to the comparison as well. Automox and Cloud Management Suite were both cloud-based solutions and they had not been included in the earlier reviews, so it was natural to include them in the current comparison. The selected third-party patch management solutions are presented in black color in Figure 29.

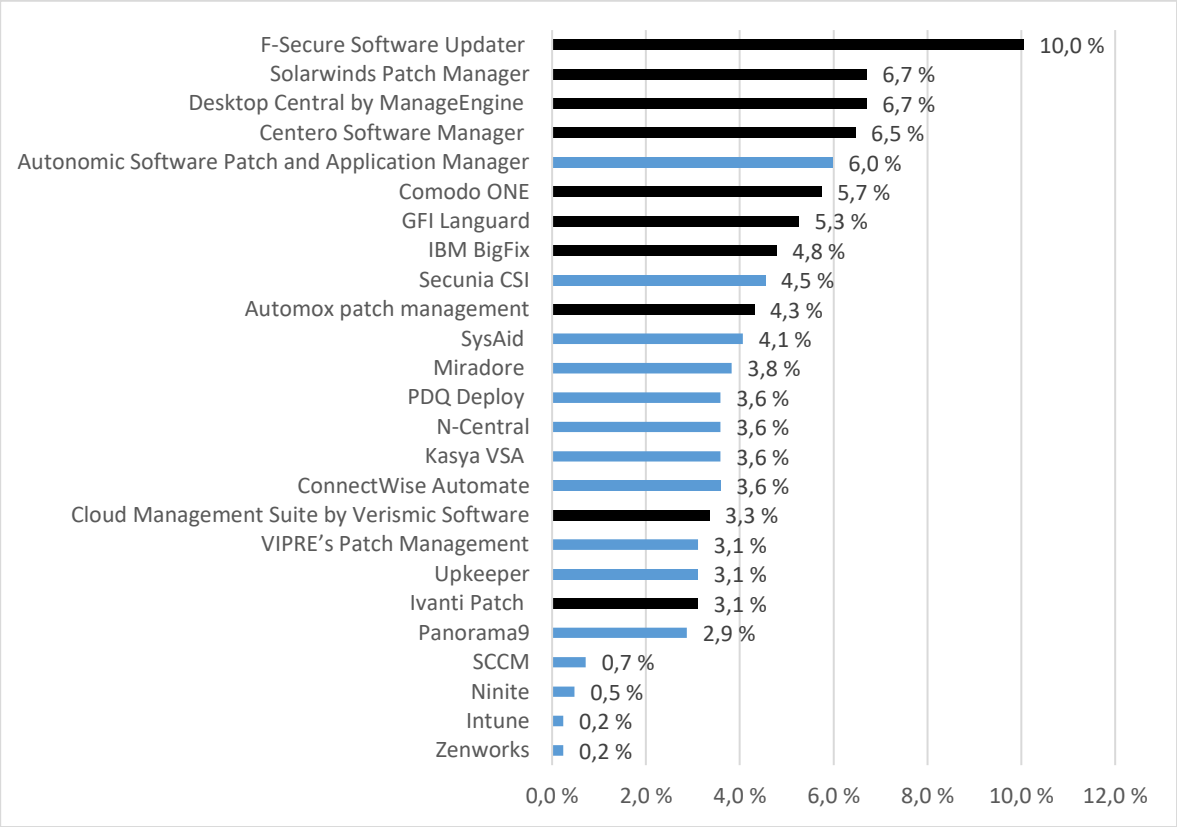


Figure 29. Selected third-party patch management solutions for the comparison.

6.4 Comparison in practice

The technical testing of the solutions took place in a virtual environment in Microsoft Azure. The on-premises solutions required some existing infrastructure. It was possible to test all the selected third-party patch management solutions with the following configuration:

- Windows Server 2016
- Windows Server Update Service -component
- System Center Configuration Manager
- Microsoft SQL -component
- Windows 10 build 1803

In addition to the server and client components, third-party applications were obviously required. The versions of the applications were the second latest or the third latest at the time of comparison. The final set of the applications were fine-tuned by dropping out two software. Google Chrome had to be excluded from the practical test because there is no way to disable the integrated automatic updates

reliably without Active Directory environment. Silverlight is also managed by Windows update client so it could also have been updated in an uncontrolled manner. The final set of the applications for the testing is listed in Table 2:

Table 2. Third-party applications used in the comparison.

Application	**Version**	**Bitness**	**Language**
7-Zip	18.06.00.0	x86	EN
Adobe AIR	31.0.0.96	x86	EN
Adobe Flash Player	32.0.0.114	x86	EN
Adobe Reader	19.010.20091	x86	EN
Mozilla Firefox	65.0.2	x86	EN
Oracle Java Runtime Environment	8.8.0.1910.12	x86	EN
VLC Media Player	3.0.4	x86	EN

All the solutions in the same category were tested similarly. The cloud-based standalone solutions were obviously really easy to deploy. All of them had a web-based admin portal where it one could download and agent and deploy it to an endpoint. When the agent was up and running it reported back to admin portal. Then it was tested if the solution patches the specifically selected third-party applications and if the other specified criteria come true or not.

Most of the focus and resources were targeted to reviewing the admin portals' cloud solutions and management software in on-premises solutions. Finding out the existence of features was the main purpose of the comparison. On-premises solutions were much more difficult to deploy than cloud solutions in overall. The cloud solutions took around an hour to deploy to a level they could be properly tested. Unlike cloud solutions, the on-premise solutions and their deployment varied a great deal. Deploying them took multiple hours. Apart from the solution category and how the basic installation and configuration was made, they were all reviewed in a similar manner.

1. Deploy the solution.

2. Go through the features of the solution in the management portal or software.
3. Patch the specified third-party application.
4. Validate the patching.

During the review of an individual patch management solution an Excel sheet worked as a support utility to a more accurate evaluation. The features and characteristics of a patch management solution were then scored individually. Table 3 shows 7 features from 2 different categories. There are 3 numeric values on the bottom, and the first of them is an initial score for a feature. Then there is a multiplier for the initial score and finally, the bolded value is a multiplication of the two earlier values. Now the final scores of the features were added for total score of the category.

Table 3. Scoring system used in the review Excel sheet.

	Security				Vulnerability management			
	2,00				1,50			
	Deny the solution uninstallation	Deny end user client changes	Trace the update package origin	Admin command audit log	Vulnerability monitoring	Alerts on vulnerabilities	Vulnerability rating	
	Capability to prevent uninstallation of the agent or solution on endpoint	Capability to prevent changes by an end user	Information on the package origin to track the validity	Capability to keep track on actions done within the solution	Capability to monitor vulnerabilities related to managed software	Capability to configure alerts on new vulnerabilities	Capability to show a rating for vulnerabilities	
	0,5 pts restrict users from Uninstalling the Agent from Control Panel, 0,5 pts restrict users from stopping Agent Service.	1 pts	0,5 pts download url, 0,5 pts update hash value or similar	1 pts	1 pts	1 pts	1 pts CVSS rating, 1 pts other rating	
	0,5	1,0	1,0	1,0	1,0	1,0	0,5	
	2,0	1,0	0,0	0,0	1,0	0,0	1,0	
	1,0	**1,0**	**0,0**	**0,0**	**1,0**	**0,0**	**0,5**	

After all the solutions were reviewed, the scoring was displayed in an overview sheet with category-based scores and total scores. Table 4 describes the overall scoring of the solutions.

Table 4. Overview and overall scoring in the first iteration of the comparison.

Solution	Annual price SMB	Annual price enterprise	Supported applications	General	Security	Vu ma
Maximum points						
F-Secure PSB: Software Updater	8400	84000	118	7,5	2,0	
Comodo ONE (Itarian)	Free	Free	368	8,5	1,5	
Automox patch management	8570	85700	14	8,5	1,5	
Cloud Management Suite	8308	55383	29	9,5	2,5	
Solarwinds Patch Manager	3055	12345	34	8,0	3,5	
Centero Software Manager	4800	12000	30	8,5	1,5	
Ivanti Patch for SCCM	19282	192824	118	8,5	2,5	
ManageEngine Patch Connect Plus	2397	23018	250	8,5	2,5	
GFI Languard	33600	240000	77	8,5	1,5	
IBM BigFix	N/A	N/A	21	6,0	1,5	
Cloud standalone						
On-premises integration						
On-premises standalone						
* Could not get 3rd party application updated on endpoints						

6.5 Elaborating the comparison

The steering group of the study and comparison was very satisfied with the initial version of the comparison; however, as the comparison proceeded further, many important questions were raised. One of the matters was the scoring system of the different features and how the different solutions performed on them. The steering group realized that instead of trying to rank the best overall patch management solution for everyone, it would be more feasible to build a tool for organizations for highlighting and balancing the scoring based on their needs. This decision meant that all current scoring systems had to be made more balanced. Instead of having a big difference between maximum points of categories they needed to be balanced. The initial version of the comparison sheet consisted of 8 categories and two of them were too vast and included many different features. Therefore, these two specific categories were broken down to three subcategories both like it is presented in Table 5. The largest categories were divided into smaller ones. All the categories also have a weight and maximum amount of points.

Table 5. Balancing the scoring system.

	E	F	G	H	I	J	K	L	M	N	O
		General						Application deployment			
	No. supported applications	Supported applications	Pricing, versaility and infrastructure	General features and piloting	Security	Vulnerability management	Inventory and assessment	Restart management	Deployment configuration	Installation specification	Validating and compliance
Weight		4	2	2	2	4	4	2	2	4	4
Max points		7	7	5	5	5	6	5	5	4	4

These changes created a solid base for a dynamic scoring system following adjustable weight and prioritization. The next observation on the comparison was that the maximum points of the categories still varied a great deal. It was decided that the maximum points should be even, so it would be much easier for customers to use the future comparison tool with the weight and prioritization they like. Therefore, the calculated points had to be adjusted in relation to maximum points. To make it happen, the maximum points of the categories needed proper multipliers to reach an integer of 420. The value 420 was used because it was the smallest possible integer for widening the points to same scale. The maximum points of the categories were 4, 5, 6 and 7 so the points of the categories were multiplied accordingly with values 105, 84, 70 and 60. After that, the points were divided with 420 and multiplying with 400 again to reach a nice and round maximum point of 400. The following Table 6 presents an example of the calculation in practice.

Table 6. The maximum points were equalized to match 400 and the points were re-calculated accordingly.

Leikepöytä | Fontti | Tasaus | Suojaus | Numero

G24 | =G7*60/420*400

	A	D	E	F	G	H	I
22	**Maximum points**			400,00	400,00	400,00	400,00
23	F-Secure PSB: Software Updater			200,00	114,29	160,00	160,00
24	Comodo ONE (Itarian)			200,00	114,29	240,00	200,00
25	Automox patch management			142,86	228,57	160,00	120,00
26	Cloud Management Suite			142,86	228,57	240,00	280,00
27	Solarwinds Patch Manager			200,00	85,71	240,00	280,00
28	Centero Software Manager			200,00	114,29	240,00	200,00
29	Ivanti Patch for SCCM			200,00	114,29	240,00	280,00
30	ManageEngine Patch Connect Plus			200,00	171,43	160,00	280,00
31	GFI Languard			200,00	114,29	240,00	120,00
32	IBM BigFix			142,86	28,57	240,00	200,00
33							

After the calculation the numbers were obviously too big and therefore the points and the maximum points of the categories were divided with 100. After this step the scoring system seemed to be understandable and even. The weight shown in Table 7

does not affect the points in any way for now but it is more of a default recommendation for customer when they start using the comparison tool based on this work.

Table 7. The final form of the scoring system for the comparison.

			General					
Solution	Annual price enterprise	No. supported applications	Supported applications	Pricing, versaility and infrastructure	General features and piloting	Security	Vulnerability management	Inventory and assessment
Weight			**4**	**2**	**2**	**2**	**4**	**4**
Maximum points			4,00	4,00	4,00	4,00	4,00	4,00
F-Secure PSB: Software Updater	84 000 €	118	2,00	1,14	1,60	1,60	1,20	0,67
Comodo ONE (Itarian)	Free	368	2,00	1,14	2,40	2,00	1,20	2,00
Automox patch management	85 700 €	14	1,43	2,29	1,60	1,20	1,20	2,00
Cloud Management Suite	55 383 €	29	1,43	2,29	2,40	2,80	1,20	0,67
Solarwinds Patch Manager	12 345 €	34	2,00	0,86	2,40	2,80	1,20	2,00
Centero Software Manager	12 000 €	30	2,00	1,14	2,40	2,00	0,00	2,00
Ivanti Patch for SCCM	192 824 €	118	2,00	1,14	2,40	2,80	1,60	2,00
ManageEngine Patch Connect Plus	23 018 €	250	2,00	1,71	1,60	2,80	1,20	2,00
GFI Languard	240 000 €	77	2,00	1,14	2,40	1,20	1,20	2,00
IBM BigFix	N/A	21	1,43	0,29	2,40	2,00	1,20	2,00

7 Discussion

The objective of the research was to study the phenomena regarding third-party application patch management for Windows operating systems in organizations all around the world. The purpose of the findings is to help out the assigning organization to plan for an internationalization of their business. The organization had started planning the business expansion project a year before initiating the study. The research was planned to be an important part of the internationalization project from the beginning. Therefore, the assigning organization allocated a commendable amount of resources towards it.

The following sections discuss how the existing theoretical framework and literature align. The discussion also raises up some interesting questions which could not be answered within the scope of the thesis. More importantly the discussion evaluates how the research questions are answered.

7.1 Results and theoretical framework

Windows third-party application patch management is not a very widely studied subject. One could say that it is only a single cyber security technical control among others. The patch management as a concept is more studied subject. Some of the existing studies included third-party patching as a part of them, which made it possible to have a sufficient theoretical starting point for the thesis. In addition to this, a few of the major actors in third-party patch management and cyber security had conducted decent studies considering specifically the third-party management.

With help of the existing theory and knowledge a set of question was created for the survey. Four out of the five research questions were studied with the help of the survey. The importance of the third-party patch management was not just a single question but rather a set of questions made to gain a better comprehension of the subject. Instead of asking solely about the importance for example with a specific scale of options, the questions targeted risks and vulnerabilities to businesses.

The survey provided a view on how the organizations see the problems and risks considering the subject. This surveyed data in addition with the question comparing

the importance of different cyber security controls including third-party patch management gave a comprehensive a base for answering the first research question. The findings of the study were biased regarding the importance of the third-party patch management. Neverless, so did the other existing studies show as well. It is clear that the well-known cyber security frameworks consider third-party patch management as highly important; however, not all the organizations do comply with that opinion.

The steering group of the assigning organization wanted to know how the organizations manage the third-party patching. This was a natural choice for a research question. A more linear approach was suitable for this question. Therefore, the respondents were given 6 options to choose from. The first half of the options meant that the third-party patches are actively managed in some way, and the three other options meant that the patches are not really managed. In other words, 21% of the organizations do not actively manage the third-party applications according to the survey, which is very similar to percentage (23%) reviewed in chapter 2.5 in this study. At least one existing study complied rather closely with the findings on the third-party patch management methods.

Based on the existing knowledge and the comparisons, it is certain that there are at least a dozen of solutions automatizing the third-party patch management. In addition of learning which solutions are used, the respondents were also asked which solutions they are familiar with. This question had multiple choices to answer with a chance to provide a custom answer. The number of custom options was very low, which means that the list of the solutions was sufficient. Therefore, the survey should provide an adequate answer to the third research question. Unfortunately, the answer cannot be compared to any existing data since there is none publicly available. Since the nature of the question is rather straightforward and simple, it could be strongly assumed that the answers are reliable and valid.

The fourth research question is the most abstract of these questions. There is no definite answer for it; however, now there is a list of important and good characteristics of a third-party patch management system. A great deal of the characteristics was found from existing publications and theory. This, in addition to the existing knowledge based on the earlier patch management comparisons, helped

out with forming a suitable list of characteristics for a product. The survey also played a remarkable role regarding this question because it gave the respondents´ perspective. Additionally, it could be said that the respondents represented a set of different organizations in this case. The abstract nature of the question makes it hard to evaluate its answers concerning their reliability and validity.

The last research question was very different compared to others. Qualitative study or existing literature would not help here because none exists. The steering group of the study wanted an objective and thorough comparison of the existing solutions. Therefore, the study answers the research question sufficiently, although the research question was by far the most difficult one to work with. The earlier comparisons were not academic studies. Nevertheless, obviously some ideas and working methods used could be the same. The single most important thought was not to try to find the single best patch management solution but instead, the patch management features were just divided into as small segments as possible. The solutions could then be compared among themselves piece by piece and one feature at a time.

During the planning phase of the thesis a quantitative research with some descriptive comparison seemed to be a sufficient method. Now, when inspecting the results, it still feels the same. The steering group was looking for a general view for the third-party patch management phenomena and behavior. Therefore, the statistic view of answers seemed a good fit. As stated in chapter 3.3, the survey was conducted in two parts. The questions were the same, but all the questions were mandatory in the second survey. Nevertheless, there were no real differences between these methods.

7.2 Further research

The results of the quantitative research raised up multiple intriguing questions but unfortunately, they could not fit into the scope of the study and would require some further development. Some of the interesting further research questions for the third-party patch management phenomena would be the following.

- How does the organization's size affect different behavior of third-party patch management?
- Why does the fifth of the organizations consider third-party patch management be such an unimportant matter.
- Why do the organizations prioritize the third-party patch management so lowly compared to other security controls?

The further research questions could be studied both utilizing both quantitative and qualitative methods. Therefore, a multimethod research would be a good fit. Some of the interesting behavior could be inspected further by using the surveyed results. For some of them, interviews with organizations would be the best way to proceed.

References

Australian Cyber Security Centre. 2019. *Assessing Security Vulnerabilities and Applying Patches*. Accessed on 22 May 2019. Retrieved from https://www.cyber.gov.au/publications/assessing-security-vulnerabilities-and-applying-patches.

BitSight. 2017. *A Growing Risk Ignored: Critical Updates, Exploring the prevalence of outdated systems and their link to data breaches*. Accessed on 26 May 2019. Retrieved from https://info.bitsight.com/bitsight-insights-a-growing-risk-ignored-critical-updates.

Center for Internet Security. 2018. *CIS Controls*.

Cloud Management Suite. 2019. *Avoiding Patch Doomsday: Best Patch Management Practices*. Accessed on 17 May 2019. Retrieved from https://www.cloudmanagementsuite.com/avoiding-patch-doomsday-whitepaper.

CVE Details. 2019. *The ultimate security vulnerability data source*. Accessed on 21 March 2019. Retrieved from https://www.cvedetails.com.

F-Secure. 2018. *Sales presentation for F-Secure Business Suite*.

Flexera. 2018. *Vulnerability review 2018, Global Trends, Key figures and facts on vulnerabilities from a global information security perspective*. Accessed on 22 May 2019. Retrieved from https://www.flexera.com/media/pdfs/research-svm-vulnerability-review-2018.pdf.

Flexera. 2018. *Vulnerability review 2018, Top Desktop Apps, Key figures and facts on vulerabilities affecting most common desktop applications*. Accessed on 22 May 2019. Retrieved from https://info.flexerasoftware.com/SVM-WP-Vulnerability-Review-2018-Desktop-Apps.

Forrester. 2018. *The Total Economic Impact™ Of Ivanti Security Solutions*. Accessed on 14 September 2019. Retrieved from https://rs.ivanti.com/white-papers/ivi-2188-forrester-tdi-security-solutions.pdf.

Forum of Incident Response and Security Teams (FIRST). 2019. *Common Vulnerability Scoring System Version 3.0 Calculator*. Accessed on 17 May 2019. Retrieved from https://www.first.org/cvss/calculator/3.0.

G DATA Software AG. 2018. *G DATA TechPaper #0271: Patch Management Best Practices*. Accessed 22 May 2019. Retrieved from https://www.gdatasoftware.com/fileadmin/web/en/documents/techpaper/G_DATA_TechPaper_Patch_Management_Best_Practices_English.pdf.

Gartner. 2017. *Technology Insight for Patch Management Tools*.

Gregory-Brown, B. 2017. Securing Industrial Control Systems. SANS Institute.

Hantrais, L. 1995. *Comparative Research Methods*. Department of Sociology University of Surrey. Accessed on 30 May 2019. Retrieved from http://sru.soc.surrey.ac.uk/SRU13.html.

Jones, J. & Mogull, R. 2009. *Project Quant Patch Management Survey Summary and Analysis of Results*. Accessed on 2 November 2019. Retrieved from https://cdn.securosis.com/assets/library/main/quant-survey-report-072709.pdf.

Kaseya. 2019. *2019 IT Operations Survey Results: Automated Patch Management Not Widely Adopted*. Accessed on 2 November 2019. Retrieved from https://www.kaseya.com/blog/2019/09/17/2019-it-operations-survey-results-automated-patch-management-not-widely-adopted/.

Labtech. 2012. *Patch Management Best Practices*. Accessed on 22 May 2019. Retrieved from https://2wtech.com/wp-content/uploads/2018/11/Patch-Management-Best-Practices.pdf.

Mell, P., Bergeron, T., Henning, D. 2005. *Creating a Patch and Vulnerability Management Program: Recommendations of the National Institute of Standards and Technology (NIST)*.

Microsoft. 2019. *Description of the standard terminology that is used to describe Microsoft software updates*. Accessed on 15 May 2019. Retrieved from https://support.microsoft.com/en-us/help/824684/description-of-the-standard-terminology-that-is-used-to-describe-micro.

Microsoft. 2019. *Microsoft Exploitability Index*. Accessed on 9 November 2019. Retrieved from https://www.microsoft.com/en-us/msrc/exploitability-index.

National Institute of Standards and Technology, NVD (National Vulnerability Database). *Vulnerability Metrics.* Accessed on 17 May 2019. Retrieved from https://nvd.nist.gov/vuln-metrics/cvss.

Nicolett, M., Colville, R. 2003. *Robust Patch Management Requires Specific Capabilities*. Accessed on 23 May 2019. Retrieved from https://www.bus.umich.edu/KresgePublic/Journals/Gartner/research/113700/113768/113768.pdf.

Payment Card Industry. 2019. *Software Security Framework: Secure Software Requirements and Assessment Procedures Version 1.0*. Accessed on 17 May 2019. Retrieved from https://www.pcisecuritystandards.org/documents/PCI-Secure-Software-Standard-v1_0.pdf?agreement=true&time=1558085082885.

Preston-Werner, T. *Semantic Versioning 2.0.0*. Accessed on 10 May 2019. Retrieved from https://semver.org/.

Rautio, P. 2007. *Comparative Study*. Accessed on 30 May 2019. Retrieved from http://www2.uiah.fi/projects/metodi/172.htm.

Shuttleworth, M. 2008. *Quantitative Research Design*. Accessed on 30 May 2019. Retrieved from https://explorable.com/quantitative-research-design.

Souppaya, M., Scarfone, K. 2013. *Guide to Enterprise Patch Management Technologies.* NIST Special Publication 800-40. National Institute of Standards and Technology. Accessed on 15 May 2019. Retrieved from http://dx.doi.org/10.6028/NIST.SP.800-40r3.

Symantec. *Zero-day vulnerability: What it is, and how it works*. Accessed on 18 April 2019. Retrieved from https://us.norton.com/internetsecurity-emerging-threats-how-do-zero-day-vulnerabilities-work-30sectech.html.

Wassermann, G. 2016. *What is Vulnerability Coordination?*. Carnegie Mellon University Software Engineering Institute: CERT Coordination Center. Accessed on 15 May 2019. Retrieved from https://vuls.cert.org/confluence/pages/viewpage.action?pageId=4718642.

White D. 2006. *Limiting Vulnerability Exposure through effective Patch Management: threat mitigation through vulnerability remediation*. Science of Rhodes University, Department of Computer, Degree Programme in Science.

Appendices

Appendix 1. LinkedIn demographics: job function

Name	Impressions	Clicks	Average CTR
Information Technology	3,676 (92.08%)	2,798 (92.65%)	76.12%
Engineering	386 (9.67%)	310 (10.26%)	80.31%
Operations	206 (5.16%)	140 (4.64%)	67.96%
Business Development	184 (4.61%)	151 (5%)	82.07%
Program and Project Management	169 (4.23%)	127 (4.21%)	75.15%
Support	143 (3.58%)	97 (3.21%)	67.83%
Military and Protective Services	122 (3.06%)	92 (3.05%)	75.41%
Sales	105 (2.63%)	71 (2.35%)	67.62%
Media and Communication	98 (2.45%)	71 (2.35%)	72.45%
Education	92 (2.3%)	67 (2.22%)	72.83%
Consulting	73 (1.83%)	51 (1.69%)	69.86%
Finance	73 (1.83%)	46 (1.52%)	63.01%
Administrative	59 (1.48%)	49 (1.62%)	83.05%
Marketing	56 (1.4%)	43 (1.42%)	76.79%
Arts and Design	55 (1.38%)	38 (1.26%)	69.09%
Human Resources	41 (1.03%)	25 (0.83%)	60.98%
Research	40 (1%)	28 (0.93%)	70 %
Community and Social Services	27 (0.68%)	19 (0.63%)	70.37%
Accounting	26 (0.65%)	21 (0.7%)	80.77%
Quality Assurance	22 (0.55%)	15 (0.5%)	68.18%
Entrepreneurship	16 (0.4%)	11 (0.36%)	68.75%
Legal	16 (0.4%)	11 (0.36%)	68.75%
Product Management	14 (0.35%)	12 (0.4%)	85.71%
Healthcare Services	14 (0.35%)	8 (0.26%)	57.14%
Real Estate	7 (0.18%)	3 (0.1%)	42.86%

Appendix 2. LinkedIn demographics: job titles

Information Technology Manager	822 (20.59%)	610 (20.2%)	74.21%
System Administrator	459 (11.5%)	347 (11.49%)	75.6%
Database Administrator	215 (5.39%)	167 (5.53%)	77.67%
Network Administrator	208 (5.21%)	150 (4.97%)	72.12%
Information Technology Administrator	179 (4.48%)	129 (4.27%)	72.07%
Information Technology Specialist	157 (3.93%)	118 (3.91%)	75.16%
System Manager	156 (3.91%)	100 (3.31%)	64.1%
Chief Information Officer	114 (2.86%)	87 (2.88%)	76.32%
Cyber Security Specialist	105 (2.63%)	83 (2.75%)	79.05%
Security Consultant	99 (2.48%)	67 (2.22%)	67.68%
Information Technology Security Specialist	91 (2.28%)	72 (2.38%)	79.12%
Information Technology System Administrator	78 (1.95%)	55 (1.82%)	70.51%
Oracle Database Administrator	74 (1.85%)	58 (1.92%)	78.38%
System Specialist	64 (1.6%)	45 (1.49%)	70.31%
Security Professional	55 (1.38%)	41 (1.36%)	74.55%
Network Manager	53 (1.33%)	41 (1.36%)	77.36%
Information Security Consultant	52 (1.3%)	47 (1.56%)	90.38%
Information Security Analyst	51 (1.28%)	29 (0.96%)	56.86%
Information Specialist	47 (1.18%)	27 (0.89%)	57.45%
Information Security Specialist	45 (1.13%)	35 (1.16%)	77.78%
Service Administrator	42 (1.05%)	32 (1.06%)	76.19%
Information Security Officer	42 (1.05%)	26 (0.86%)	61.9%
Network Specialist	40 (1%)	33 (1.09%)	82.5%
Linux System Administrator	38 (0.95%)	35 (1.16%)	92.11%
System Network Administrator	37 (0.93%)	30 (0.99%)	81.08%

Appendix 3. LinkedIn demographics: company industry

Name	Impressions	Clicks	Average CTR
Information Technology and Service	1,084 (27.15%)	842 (27.88%)	77.68%
Computer Software	281 (7.04%)	220 (7.28%)	78.29%
Computer & Network Security	261 (6.54%)	210 (6.95%)	80.46%
Financial Services	234 (5.86%)	185 (6.13%)	79.06%
Banking	200 (5.01%)	161 (5.33%)	80.5%
Telecommunications	165 (4.13%)	129 (4.27%)	78.18%
Internet	98 (2.45%)	71 (2.35%)	72.45%
Education Management	95 (2.38%)	72 (2.38%)	75.79%
Higher Education	93 (2.33%)	73 (2.42%)	78.49%
Government Administration	90 (2.25%)	63 (2.09%)	70 %
Oil & Energy	86 (2.15%)	69 (2.28%)	80.23%
Management Consulting	76 (1.9%)	61 (2.02%)	80.26%
Computer Networking	73 (1.83%)	46 (1.52%)	63.01%
Retail	66 (1.65%)	54 (1.79%)	81.82%
Insurance	66 (1.65%)	54 (1.79%)	81.82%
Hospital & Health Care	66 (1.65%)	39 (1.29%)	59.09%
Hospitality	60 (1.5%)	45 (1.49%)	75 %
Construction	59 (1.48%)	43 (1.42%)	72.88%
Security and Investigations	58 (1.45%)	41 (1.36%)	70.69%
Automotive	55 (1.38%)	41 (1.36%)	74.55%
Marketing and Advertising	54 (1.35%)	51 (1.69%)	94.44%
Consumer Goods	50 (1.25%)	39 (1.29%)	78 %
Electrical/Electronic Manufacturing	44 (1.1%)	33 (1.09%)	75 %
Defense & Space	44 (1.1%)	31 (1.03%)	70.45%
Outsourcing/Offshoring	43 (1.08%)	36 (1.19%)	83.72%

Appendix 4. LinkedIn demographics: job seniority

Name	Impressions	Clicks	Average CTR
Senior	2,510 (62.88%)	1,870 (61.92%)	74.5%
Entry	1,555 (38.95%)	1,219 (40.36%)	78.39%
Manager	400 (10.02%)	290 (9.6%)	72.5%
CXO	176 (4.41%)	139 (4.6%)	78.98%
Director	110 (2.76%)	84 (2.78%)	76.36%
Owner	69 (1.73%)	53 (1.75%)	76.81%
VP	44 (1.1%)	35 (1.16%)	79.55%
Partner	15 (0.38%)	11 (0.36%)	73.33%
Training	10 (0.25%)	5 (0.17%)	50 %
Unpaid	5 (0.13%)	3 (0.1%)	60 %

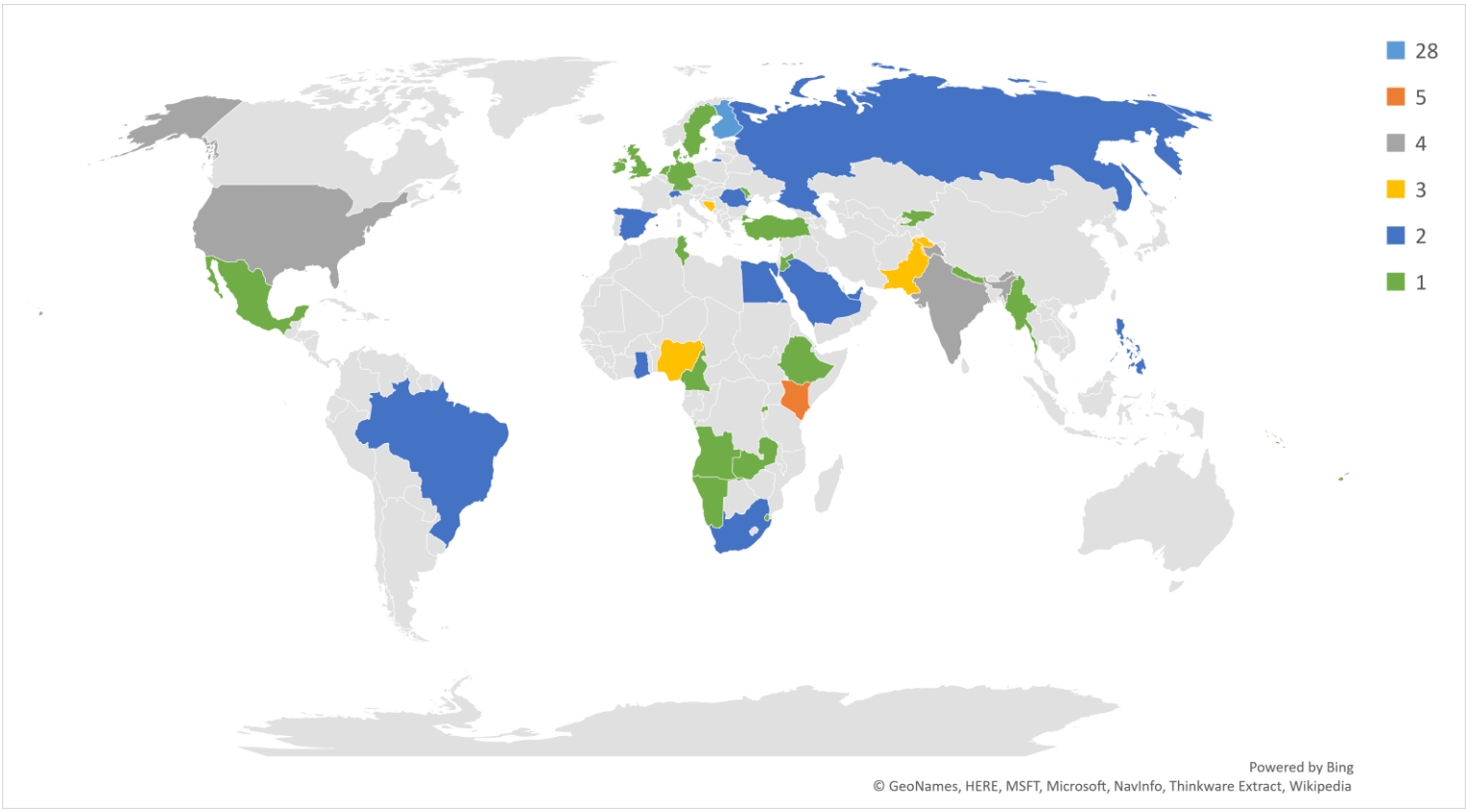
Appendix 5. LinkedIn demographics: company size

Name	Impressions	Clicks	Average CTR
10001+ employees	726 (18.19%)	547 (18.11%)	75.34%
1001-5000 employees	542 (13.58%)	420 (13.91%)	77.49%
51-200 employees	540 (13.53%)	393 (13.01%)	72.78%
11-50 employees	463 (11.6%)	362 (11.99%)	78.19%
201-500 employees	413 (10.35%)	322 (10.66%)	77.97%
501-1000 employees	248 (6.21%)	185 (6.13%)	74.6%
2-10 employees	189 (4.73%)	145 (4.8%)	76.72%
5001-10000 employees	186 (4.66%)	139 (4.6%)	74.73%
1 employee	37 (0.93%)	25 (0.83%)	67.57%

Appendix 6. LinkedIn demographics: country

Name	Impressions	Clicks	Average CTR
United States	336 (8.42%)	171 (5.66%)	50.89%
Brazil	216 (5.41%)	174 (5.76%)	80.56%
United Kingdom	160 (4.01%)	97 (3.21%)	60.63%
Pakistan	145 (3.63%)	131 (4.34%)	90.34%
Australia	131 (3.28%)	81 (2.68%)	61.83%
Philippines	130 (3.26%)	108 (3.58%)	83.08%
India	121 (3.03%)	81 (2.68%)	66.94%
Egypt	111 (2.78%)	94 (3.11%)	84.68%
Turkey	106 (2.66%)	82 (2.72%)	77.36%
South Africa	74 (1.85%)	55 (1.82%)	74.32%
Sweden	73 (1.83%)	45 (1.49%)	61.64%
Romania	67 (1.68%)	57 (1.89%)	85.07%
United Arab Emirates	64 (1.6%)	46 (1.52%)	71.88%
Israel	62 (1.55%)	52 (1.72%)	83.87%
Indonesia	59 (1.48%)	49 (1.62%)	83.05%
Poland	58 (1.45%)	43 (1.42%)	74.14%
Greece	54 (1.35%)	38 (1.26%)	70.37%
Saudi Arabia	52 (1.3%)	47 (1.56%)	90.38%
Mexico	51 (1.28%)	36 (1.19%)	70.59%
Sri Lanka	50 (1.25%)	46 (1.52%)	92 %
Jordan	47 (1.18%)	45 (1.49%)	95.74%
Other	47 (1.18%)	40 (1.32%)	85.11%
Italy	47 (1.18%)	34 (1.13%)	72.34%
Hungary	47 (1.18%)	34 (1.13%)	72.34%
New Zealand	47 (1.18%)	28 (0.93%)	59.57%

Appendix 7. The countries of the respondents on map.



Appendix 8. The respondents countries.

Finland	28
Kenya	5
India	4
United States of America	4
Nigeria	3
Pakistan	3
Bosnia and Herzegovina	3
Philippines	2
United Arab Emirates	2
South Africa	2
Romania	2
Spain	2
Russian Federation	2
Saudi Arabia	2
Egypt	2
Ghana	2
Brazil	2
Switzerland	2
Mexico	1
Rwanda	1
Namibia	1
Solomon Islands	1
Denmark	1
Republic of Moldova	1
Myanmar	1
Ethiopia	1
Netherlands	1
United Kingdom of Great Britain and Northern Ireland	1
Angola	1
Ireland	1
Kyrgyzstan	1
Tunisia	1
Cameroon	1
Fiji	1
Zambia	1
Turkey	1
Swaziland	1
Sweden	1
Andorra	1
Luxembourg	1
Maldives	1
Jordan	1
Germany	1
Nepal	1

Appendix 9. The survey

Master's thesis study on third party application patch management on Windows environments

1. Welcome to the survey!

The study
You have been asked to participate in a study conducted by Tuukka Tiainen, a candidate for a Master of Engineering in the Cyber Security program. The thesis is as an assignment from the current employer of the candidate, Centero Oy. Participating in the study will take about 10 minutes of your time.

All of the questions regarding this survey can be addressed to Mr. Tuukka Tiainen. Please contact via e-mail: tuukka.tiainen(at)centero.fi.

Study questions
We want to gather information on third party patch management. Here are some questions that we would like to have answered by way of this study.

1. How do organizations manage third party application patching?
2. How important is third party application patching considered?
3. What kind of processes and tools are involved in third party patch management?

Use of the survey data
The survey results data will be used in the master's thesis. In addition, Centero Oy will learn and develop their patch management solution based on the gathered information. The survey results will be analyzed, anonymized, and published with the findings, as a part of the master's thesis.

Personal information
We will also collect some personal information with the respondents' consent. The basic demographic information is collected at the start of the survey and answering the personal questions is optional.

Privacy and data collection
If you wish to learn about privacy policy of Centero, please follow the link provided.
If you wish to learn about data collection and privacy of Survey Monkey, you can find it here. More information on the security of Survey Monkey can be found in the security statement.

If you agree to our terms, please continue to the survey by clicking next.

Why we gather personal information?
If you wish to receive a link to the master's thesis and the patch management review, please fill in the personal information.

If you, on the other hand, wish to remain completely anonymous, just leave the personal information unanswered. In that case, unfortunately, we cannot reach out to you in order to send the study results.

1. Personal information

Name

Company

Email Address

2. Country

3. Job title

- IT specialist
- Cyber Security specialist
- IT manager
- Other (please specify)
- Manager
- Helpdesk support
- Consultant

As a part of the thesis research, we would like to study the differences among industries. Please let us know about your organization so that we can make even more accurate conclusions on third party patch management.

4. Organization type

5. Which of the following best describes the principal industry of your organization?

6. How many Windows workstations does your organization manage?

7. Do you think the vulnerabilities of third party applications might be a threat to your organization?

- Yes
- No

8. Has your organization conducted a cyber security risk assessment of your business?

- Yes
- No
- I don't know

9. Have you included software vulnerabilities in the risk assessment?

- Yes
- No

10. How high of a risk does your organization consider third party application vulnerabilities to be?

11. How does your organization manage the patching of third party applications on Windows endpoints?

12. Please choose **three** (3) of the most important security controls on Windows workstations.

- [ ] Enforcing the principle of least privilege in operating system (Restricting regular users to not have administrator privileges)
- [ ] Password management for operating system authentication (Forcing complex passwords and/or requiring password change after specific time)
- [ ] Software firewall (Windows firewall or additional software based firewall in operating system)
- [ ] Third party application patching (Keeping software such as Java, Firefox etc up to date)
- [ ] Operating system patching (Keeping the operating system up to date)
- [ ] Preventing the use of removable media (Disallowing USB-media connection for example)

13. Which third party patching solution or remote monitoring and management tools are you currently using and/or familiar with?

	In use	Familiar with
Automox patch management	☐	☐
Autonomic Software Patch and Application Manager	☐	☐
Cloud Management Suite by Verismic Software	☐	☐
Centero Software Manager	☐	☐
Comodo ONE	☐	☐
ConnectWise Automate	☐	☐
Desktop Central by ManageEngine	☐	☐
F-Secure Software Updater	☐	☐
GFI Languard	☐	☐
IBM BigFix	☐	☐
Ivanti Patch	☐	☐
Kasya VSA	☐	☐
Miradore	☐	☐
N-Central	☐	☐
Panorama9	☐	☐
PDQ Deploy	☐	☐
Secunia CSI	☐	☐
Solarwinds Patch Manager	☐	☐
SysAid	☐	☐
Upkeeper	☐	☐
VIPRE's Patch Management	☐	☐

Other (please specify)

14. Which widely used, frequently updated, and free third party applications are used in your organization

- [ ] Adobe AIR
- [ ] Adobe Flash Player ActiveX
- [ ] Adobe Flash Player Plugin
- [ ] Adobe Reader DC
- [ ] Adobe Reader XI
- [ ] Adobe Shockwave Player
- [ ] Apple iTunes
- [ ] Paint.NET
- [ ] Other (please specify the applications)
- [ ] Google Chrome
- [ ] Igor Pavlov 7-Zip
- [ ] Microsoft Silverlight
- [ ] Mozilla Firefox
- [ ] Mozilla Firefox ESR
- [ ] Oracle Java Runtime Environment 8
- [ ] VideoLAN VLC Media player

15. Are there any third party applications in your organization that aren't included in the patch management process?

Why aren't the specific applications included?

16. What are the applications without patch management?

17. How would you define the importance of the following patch management processes

	Low	Medium	High
New software versions are tested against the existing software and environment.	○	○	○
New software version is deployed to smaller test groups before large scale deployment to production.	○	○	○
End users and product owners are included in the testing process of new software version.	○	○	○
New versions of the managed applications are monitored.	○	○	○
Vulnerabilities of managed software are monitored.	○	○	○
Large scale production deployment of the new software version is divided into multiple groups or phases.	○	○	○
Default software packaged by the vendor is repackaged or customized.	○	○	○
New software versions are tested on test devices first.	○	○	○

18. How would you define the importance of patch management features?

	Low	Medium	High
Patching operating system	○	○	○
Patch analysis on CVE (Common Vulnerabilities and Exposures) for rating and priority	○	○	○
Inventory of hardware, OS and software	○	○	○
Reporting the current state of the environment	○	○	○
Customizing the deployment (scheduling, group targeting)	○	○	○
Patching line of business applications	○	○	○
Customizing the installation (pre and post patch installation tasks, restart control)	○	○	○
Customizing the default software packages	○	○	○

Appendix 10. Response percentage per question.

Question	Question #	Answers	answer %
Personal Information	Question #1	89	80,9 %
Country	Question #2	98	89,1 %
Job title	Question #3	105	95,5 %
Organization type	Question #4	102	92,7 %
Industry	Question #5	101	91,8 %
Number of workstations	Question #6	103	93,6 %
Do you think the vulnerabilities of third party applications might be a threat to your organization?	Question #7	106	96,4 %
Has your organization conducted a cyber security risk assessment of your business?	Question #8	105	95,5 %
Have you included software vulnerabilities in the risk assessment?	Question #9	60	54,5 %
How high of a risk does your organization consider third party application vulnerabilities to be?	Question #10	53	48,2 %
How does your organization manage the patching of third party applications on Windows endpoints?	Question #11	88	80,0 %
Are there any third party applications in your organization that aren't included in the patch management process?	Question #11.1	86	78,2 %
Please choose three (3) of the most important security controls on Windows workstations.	Question #12	88	80,0 %
Which third party patching solution or remote monitoring and management tools are you currently using and/or familiar with?	Question #13	82	74,5 %
Which widely used, frequently updated, and free third party applications are used in your organization	Question #14	87	79,1 %
Are there any third party applications in your organization that aren't included in the patch management process?	Question #15	86	78,2 %
Why aren't the specific applications included?	Question #15.1	26	23,6 %
What are the applications without patch management?	Question #16	33	30,0 %
How would you define the importance of the following patch management processes	Question #17	82	74,5 %
How would you define the importance of patch management features?	Question #18	82	74,5 %