What does this Update do to my Systems? – An Analysis of the Importance of Update-Related Information to System Administrators

Florin Martius
University of Bonn
martius@uni-bonn.de

Christian Tiefenau
University of Bonn
tiefenau@cs.uni-bonn.de

Abstract

Installing updates is one of the most commonly advised topics in cyber-security. While this is already important for end-users, it is of even higher importance for system administrators: They are responsible for a large number of computer systems, and delaying or missing an update can result in many vulnerable machines. The likelihood of exploitation is reduced when updates are installed in a timely manner. One factor that can hinder the decision to update is a lack of demanded information that can prevent the evaluation of the impact of the patch on their systems. This work takes a look at update release notes of four software vendors and presents data from five interviews and two surveys that aimed to understand the importance of the possible information such a release note can contain. We found that the most important information to system administrators consists of the purpose, dependencies and known issues in a release note. Besides this, they tend to read updated-related information of manual updates more often than those of automatic updates.

1 Introduction

The deployment of updates is necessary to keep a computer system secure against known vulnerabilities. In May 2017, a cryptoworm called *WannaCry* infected hundreds of thousands of Windows computers. The vulnerability exploited by the ransomware was known to Microsoft before, so Microsoft released a patch to fix it. However, Microsoft did not highlight the criticality of the flaw and as a consequence, a lot of machines were not updated [10]. This enabled the worm to infect a large number of machines. The worm caused damage that is estimated to be ranging up to hundreds of billions of dollars [6].

While the update-topic is already well researched with respect to end users [4, 16, 17], recent studies begin to also observe another user group that has to deal with the topic, namely administrators [11, 15]. They are responsible for a large number of computers, keep them up to date and so, play a big role in hindering malicious software. Precise information about the update, for example information about dependencies, help the administrators in their decision on whether and when to update. Prior work showed that lack of information hinders this learning phase and is a barrier to the update process [11, 15] Thus, a further investigation into the aspect of the provided and considered information is of interest.

In this paper, we analyze which information administrators consider to be necessary as part of their assessment. Therefore, we conducted five interviews and two surveys that should answer the following questions:

- Where do administrators obtain information related to updates?
- What information is relevant for the decision whether or not to update?
- How do administrators compensate for a lack of information?
- What are the differences in handling security and feature updates?

Our study revealed that release notes are the main source for learning about an update. When they are considered to be insufficient, our participants also referred to online forums and blogs. We identified the purpose, dependencies and known issues as most important information of release notes to system administrators. Our study results show that administrators install security updates in a by far more timely manner than feature updates. For that reason, we recommend decoupling feature updates from security updates.

USENIX Symposium on Usable Privacy and Security (SOUPS) 2020.
August 9–11, 2020, Virtual Conference.

2 Related Work

2.1 End User Studies

A lot of research has been done on investigating end user update behavior. Several studies found that one of the primary reasons observed for users not to update is that they are not aware of security benefits updates entail [5, 13, 16, 17]. According to that, common belief states that functioning software does not have to be updated but only software that is not working properly [13, 17]. Vaniea et al. found that many users do not know that the software running in the background is actually in use, e.g. Java, and end users will only update software they do use [17]. Fear of undesired functional changes caused by bad experiences with past updates are another reason for users not to update [5, 8, 17]. The occurrence of bugs in new updates is also a barrier to update, as stated by Ion et al. [8] and Mathur et al. [13].

2.2 System Administrator Studies

Even though the behavior of end users related to updates has been researched thoroughly, only recently, researchers started to analyze that of administrators. There exist few studies related to system administrator's handling of updates. While researching this topic, Li et al. [11] and Tiefenau et al. [15] followed the same approach: Both papers combined conducting qualitative interviews with performing a quantitative survey. Li et al. [11] found learning about updates to be a fundamental part of the update process. The learning process is hindered by decentralized information, so administrators have to use several methods to gain information from different sources [11, 15]. Both works observe that some software vendors do not differ between feature and security updates which makes it hard for administrators to distinguish between them. Li et al. state that there is no reliable source to gather all information that is demanded by administrators [11]. They suggest bundling and standardizing information to gain higher outreach. They also pointed out that obtaining information is time-consuming and causes delays in deploying the update which may leave the computer system vulnerable. In line with these recent findings, Barrett et al. found that system administrators often lack situational awareness [2]. To counter the increasing complexity of the systems, most of the administrators use tools [11, 15] that also have been subject of research by Haber, Kandogan and Botta et al. [3, 7, 9]. They proposed that new classes of tools need to be developed to counter the ever-increasing complexity of the systems and attack-vectors.

2.3 Update Release Notes

When administrators perform updates, collecting information about the update is the first important step [11, 15]. One way to do so is by reading the provided update release notes. Moreno et al. analyzed 1,000 of those by hand. As a result, they stated that fixed bugs are by far the most frequent item included in the release notes. Other common information includes new code components, new features and modified code components [14]. Abebe et al. observed there are three different styles in writing release notes: New features, bug fixes and improvements [1]. By now, there are no standards [1] or guidelines on writing release notes.

3 Qualitative Interviews

We wanted to understand how the information in release notes gets processed by administrators. Therefore, we conducted five semi-structured interviews with system administrators from German companies. All of our participants were full-time administrators with more than 20 years of experience. We asked our participants (1) where they get informed about updates, (2) what information is relevant for the decision whether or not to update, (3) how they deal with a lack of information and (4) about differences in handling security and feature updates. The interviews were conducted either over the phone or in person and lasted between 10-55 minutes. All interviews were recorded and transcribed. We coded the interviews by creating an affinity diagram found in the appendix. To this end, one researcher extracted key messages to virtual sticky notes, arranged similar statements together and sorted them into groups.

In alignment with related work, we found that there are obstacles for administrators learning about updates. Four administrators reported bad experience with past updates due to incomplete or incorrect release notes. All participants agreed that they install feature updates only when necessary. Before the installation, they want to know the purpose and the main changes to infer the reason why this update is important. In addition, dependencies and requirements are key information. In particular, P2 stated: *"I would include how the update should be installed, [...] the improvements [...], what it does and what was fixed. These three details are mandatory for an update. Unfortunately, they are not always included."*

All of our respondents mentioned that security updates get installed as soon as possible, contrary to feature updates that will only be applied if necessary. When the information provided within the release notes appears insufficient to our interviewees, they primarily search for information on the internet or contact the vendor.

4 Analysis of Update Release Notes

In order to find out what kind of information matters to system administrators, we wanted to get an understanding of which components can exist in update release notes. To this end, we analyzed release notes of five broadly used software types that administrators may deal with. We picked that software our

interview participants told us they are using. These were the Apache2 (web-server), Microsoft Windows, Red Hat Enterprise Linux, Debian (operating systems) and GitLab (version control software). We derived information from 15 release notes of those software and generated a classification based on the codification of Moreno et al. [14]. Table 1 presents the types of information sorted in groups, while a check indicates whether or not a release note of this vendor provides the according information. As already obtained by Abebe et al. [1], no standards exist for writing release notes. In line with this, our analysis showed different approaches in providing update-related information: While some vendors like GitLab distinguish between security updates, bug fixes and feature updates, others like Apache or Microsoft release unspecified updates containing security updates or bug fixes as well as new implemented features. We observed that every release note contained a release number and most of them contained the date the update was released and the purpose of the update. Changes in the environment were never stated, dependencies only once.

5 Quantitative Survey

To quantify the importance of several information types as seen in Table 1, we created an online survey based on our previous findings. As the results of our interviews suggest that well written release notes can help system administrators in understanding the impact of the update, we wanted to know what specific kind of information is relevant to system administrators. Therefore, we asked our participants to rate the importance of the different information types in our survey. After conducting a first survey in February 2020 with 41 participants, we improved the questionnaire and conducted a second survey with 16 participants in May 2020.

5.1 Structure

Both surveys consisted of four topics of which the first three ones were based on the surveys of Li et al. and Tiefenau et al. [11, 15]. First, we asked about the participants' demographics, followed by a section about job-related information such as the company size or for how long they have been working as an administrator. Third, we asked general questions about update-related information that should answer which sources administrators use to collect information and how a lack of those pieces of information influences the update process. The last part of our survey aimed at obtaining how useful specific parts of update-related information are to the administrators. This part contained the types of information presented in Table 1 and was grouped by this classification.

We conducted a second survey because the first one revealed two areas of improvements that we wanted to investigate further: (1) First, to understand the differences in reading release notes between automatic and manual updates, we asked the participants to state how often they read release notes depending on the update type. In addition, we added a slide bar where participants could state the percentage of automatic updates. (2) Second, we rephrased some questions and displayed the values of the answer options[1] of the Likert scales, to help the administrators rate the given statements. Additionally, we offered the respondents the option not to answer these questions. The second questionnaire can be seen in the Appendix.

5.2 Participants

We recruited the participants by distributing a link to an online survey on Reddit[2], Twitter[3] and Computerbase[4]. Before the survey began, we presented information about the purpose of the study to the participants and moreover explained that their participation was voluntary and they were not compensated. The first survey was started 84 times which resulted in 43 (51.2%) complete responses. We removed incomplete responses. Two survey responses were excluded due to inadequate and obviously false responses: One participant filled out the open-ended questions with nonsense answers, another stated having experience of 99 years by the age of 33. This left us with 41 valid entries.

Thirty-nine participants started the second survey which led to 17 (44%) valid entries. After the sanitation of the data, we were left with a total of 58 completed questionnaires. Table 2 shows the demographics of our participants in both surveys. The age ranged from 18 to 60 years with a mean of 33.5 years (sd=9.73). The population was mostly male-dominated (98%). All participants came from Western countries: The majority were located in the US (27) or Germany (19). The remaining were spread over the UK (3), Canada (2), Argentina, Australia, Finland, the Netherlands, New Zealand and Switzerland (1 each). As stated before, we included a question in our second survey concerning the share of automatic updates, which the administrators face. This share ranged from 0% to 99% with a mean of 65.1% and a standard deviation of 29% as depicted in Figure 1.

5.3 Results

We asked how much time our respondents are able to spend on learning about an update. The answers were divided into two groups of nearly the same size: While 47% of both surveys accumulated stated having no or too little time, 53%

[1] "Not useful at all", "Slightly useful","Moderately useful","Very useful","Extremely useful" instead of "1 - not useful at all","2","3","4","5 - highly useful"

[2] https://www.reddit.com/r/sysadmin/comments/gvw22r/study_survey _relevance_of_updatedrelated/, accessed: 06/19/20

[3] https://twitter.com/chrizzlz/status/1222463199833919488, accessed: 06/19/20

[4] https://www.computerbase.de/forum/threads/professionelle-systemadministratoren-fuer-studie-gesucht.1903976/, accessed: 06/19/20

	Vendor Type:	Apache Unspecific	Debian Feature/Security	GitLab Security	GitLab Feature	GitLab Patch	Microsoft Security	Microsoft Unspecific	Red Hat Security	Red Hat Feature	Red Hat Patch
general	Release Date		✓	✓	✓	✓	✓	✓	✓		✓
	Release Number	✓	✓	✓	✓	✓	✓	✓	✓	✓	✓
	Note Number										
	Note Date		✓	✓		✓	✓	✓	✓		✓
	Purpose of the Update		✓	✓	✓	✓	✓		✓	✓	✓
summary	Fixed Bugs	✓		✓		✓		✓		✓	✓
	Still Existing Bugs										
	Steps to Reproduce Bug	✓				✓					
	Involved Components	✓	✓		✓	✓	✓	✓		✓	✓
	Changed Environment										
	Known Issues						✓	✓		✓	
	Closed Vulnerabilities	✓	✓	✓			✓		✓		
	Risk Qualification			✓			✓		✓		
	Added Feature	✓	✓		✓					✓	
impact	Removed Feature	✓	✓								
	Modified Handling of a Feature	✓	✓		✓					✓	
	Advertising Information							✓			
changes	Added Files	✓	✓			✓		✓		✓	
	Removed Files	✓	✓			✓				✓	
	Changed Files	✓	✓			✓	✓	✓	✓	✓	
manual	Prerequisites		✓			✓	✓	✓	✓	✓	
	Dependencies		✓								
	Update Delivery						✓	✓		✓	
	Installation Manual itself	✓				✓	✓	✓	✓	✓	✓
	Third party										
other	Documentation of Features	✓			✓					✓	
	CVE	✓	✓			✓	✓				
	Software Testing	✓		✓		✓					
	Disclaimers									✓	
	Support Contact Information		✓						✓		✓

Table 1: Classification of information and approaches of vendors.

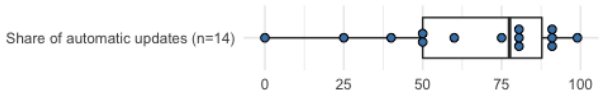


Figure 1: Relative share of automatic updates as stated by the participants.

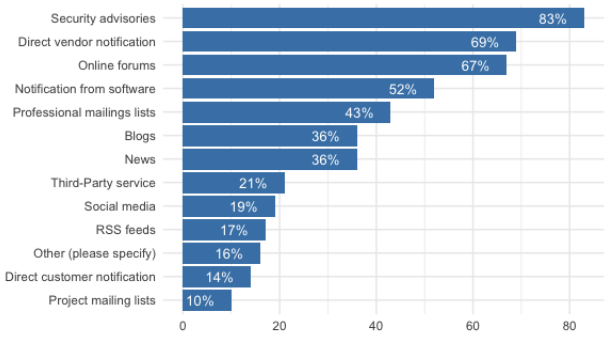


Figure 2: Sources of Information reported by the participants ordered by the number of occurrences.

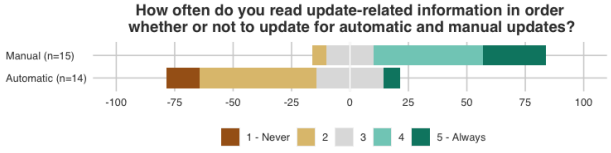


Figure 3: Overview of the responses to the frequency how often participants read release notes on a 5-point scale from "1 - Never" to "5 - Always" based on the update type.

mentioned having sufficient time or more time than needed. Figure 2 shows that our participants reported that they mainly discover an available update by security advisories, direct vendor notifications and online forums, which is in line with findings of Li et al. [11]. We observed our respondents are not likely to read update-related information of automatic updates: 65% stated they never or rarely read them. In contrast, update-related information of manual updates is read frequently by our respondents: 72% stated they always or very often read them, 21% mentioned to do so sometimes. Sixty-one percent of our participants stated there is sometimes or more often a lack of information, 68% mentioned that a lack of information increases the effort to update. To compensate missing information, 46% stated they always or very often look for additional information not given by the vendor. Doing this, almost every participant (98%) uses online forums. Blogs (74%) and Security-advices (65%) were frequently marked

Survey #		1	2
n		41	17
Age in Years		20-60	18-58
	mn	34.75	30.41
	sd	8.95	11.04
Gender	Female	1	0
	Male	40	17
Location	USA	23	4
	Germany	9	10
	Other	9	2
Experience in Years [5]		0.5-25	1-25
	mn	10.46	6.06
	sd	7.25	5.96
Company	IT-related	13	6
	Non IT-related	24	9
	Other	4	2
Company Size	x≤10	2	1
	11≤x≤50	5	2
	51≤x≤100	9	1
	101≤x≤500	16	7
	501≤x≤2000	0	2
	x>2000	9	3
Administered Systems	Clients	32 (78%)	13 (72%)
	Servers	40 (98%)	15 (88%)
	Mobile	21 (51%)	6 (33%)
	IoT	7 (17%)	5 (28%)
	Other	6 (15%)	7 (39%)

Table 2: Demographic data of our participants.

answers, too.

The most useful information stated by our respondents are: The purpose of the update (95% in the first survey / 82% in the second), prerequisites (95% / 77%) and known issues (95% / 88%), followed by fixed bugs (91% / 70%), closed vulnerabilities and dependencies (85% each / 71% and 85%). In contrast, information that fewer than 20% specified as very or extremely useful, are as follows: Disclaimers are identified as the least useful information, with only 11%/12% of respondents highlighting them as useful. Advertising information for the support level as well as the date of the release note is mentioned second, with only 12%/20% of respondents marking them as a decision-making tool. Although a large percentage of respondents found the number of the release note to be less useful than the note date. Here, we also had participants who reported that the date is very or extremely useful (15%/36). Results of the entire types of information are listed in Table 3 that can be found in the Appendix.

6 Discussion

The study with system administrators identified that some types of information are more relevant than others. In this section, we will discuss and evaluate the results.

6.1 Implications

Our results show that update-related information support administrators in the updating process. The survey indicates that the purpose and major changes such as fixed bugs are key information which coincides with our interview results. We infer that the administrators use these kinds of information to rate the urgency and the necessity of an update. The following types of information, that are especially useful for our respondents, are dependencies and prerequisites to install the update. This suggests that administrators need to be aware of the requirements, like a mandatory restart, in advance to be able to schedule the deployment of the update. Similarly, missing necessary dependencies delay or even hinder the update process since the administrator must execute further steps like updating third-party software. This fact may explain why our study revealed that release notes of automatic updates are read rarely, contrary to manual updates: Automatic updates check dependencies and prerequisites automatically, so the administrator does not have to ensure to fulfill all requirements to install the update.

Known issues provide information about possible bugs that may occur after installing the update. Our participants stated known issues as similarly helpful as the purpose or prerequisites of the update. However, they are a different kind of information than the update-related information stated before, as they do not communicate intentional changes the update entails and also, assessing these issues beforehand is hard. By knowing about bugs before they occur, the administrator can evaluate whether the bug might impinge the system and then either decide to update or refrain from the deployment of the update until this issue gets fixed.

As a fact, an update may impact the *support-level*, which means the administrator's handling with the software, or the *end-user-level* which describes the end user's handling with the software. We observed differences in the rating of the usefulness of information related to the impact of those two handling levels, since our respondents stated changes on the end-user level to be more important as on support level. These results indicate that administrators are aware that end users do not like rapid UI changes and want to prevent users from those.

As our study obtained administrators install feature updates in a less timely manner than security updates, we follow the

[5] Experience as system administrator

recommendations of [5, 11] in decoupling security patches from bug fixes or feature updates. This procedure has the advantage of allowing the administrators to close vulnerabilities without having to deal with undesired changes. In particular, P2 stated that they let two weeks pass after the update release in order to give the vendor time to improve the update and other users exploring problems with it.

6.2 Comparison to End User Behavior

We identified several similarities and differences between administrators and end users in processing updates. As a similarity, P3 reported a bad experience with past updates, stating that a key feature was removed due to an applied update. The same frustration was found for end users who stated similar bad experiences with past updates [8, 17]. Also, the fact that some end users expect bugs in recently released updates [8] or wait a certain period of time before deploying the update due to expected bug fixes [16] could be observed in our interviews: P2 explained exactly the same method in dealing with feature updates. Similar to how all of our interviewees mentioned different handling between feature and security updates, Mathur et al. [12] observed that end users are more likely to install a security update than a feature update. Another similarity can be found in the way of gathering update-related information: Like almost half of our survey participants who stated that they look for additional information not given by the vendor, Vaniea et al. [16] found that some end users also searched for additional information, for example by consulting family and friends.

A noticeable difference is the general handling of updates. While several user studies observed that many end users did not understand the benefit of updates [5, 8, 13, 16, 17], all of our interviewees agreed that updating is important. This finding coincides with a comparison study between experts and non-experts, which has been conducted by Ion et al. [8], stating experts do know that updating is one of the best measures to maintain security. Considering Mathur et al. [12] obtained knowing the purpose benefits the update decision of end users, our results suggest this is also the case for system administrators.

6.3 Limitations and Future Work

Our results rely on the responses of our study participants. The update behavior of an administrator depends on many factors, like, e.g., education, company size or experience. As our surveys had only a small number of participants with non-representative demographics, the results are not generalizable to all system administrators. In fact, all of the entire interviewees were employed in German companies with more than 250 employees. The respondents of our survey are mainly located in the US or Europe. In addition, we stress that a limited number of interviews cannot cover the whole spectrum of opinions. Besides, our recruitment strategy might enhance bias. For example, it should not surprise that participants recruited in online forums tend to use online forums as a source to gather update-related information. Due to our small sample of analyzed release notes, our analysis of update-related information may not be complete.

Future studies could investigate a larger number of administrators or another population such as other nationalities or different company sizes. Another approach is going further in detail about how exactly the update decision is made. We noticed that a large percentage of administrators do not have sufficient time to learn about an update, thus evaluating several representations of release notes in order to develop suitable standards that can save the administrators time are an interesting topic to look at.

7 Conclusion

Learning about updates is key part in the updating process of administrators. We did a mixed study combining qualitative interviews with quantitative online surveys to get an insight in this learning stage. Our study obtained that a lack of information can hamper the update process, which is in line with prior studies on system administrators [11, 15]. In the process of getting information, administrators read the update release notes of manual updates more often in contrast to information of automatic updates. We noticed that the key information for system administrators consists of the purpose, dependencies and known issues of an update.

References

[1] Surafel Lemma Abebe, Nasir Ali, and Ahmed E. Hassan. An empirical study of software release notes. *Empirical Softw. Engg.*, 21(3):1107–1142, June 2016.

[2] Rob Barrett, Eser Kandogan, Paul P. Maglio, Eben M. Haber, Leila A. Takayama, and Madhu Prabaker. Field studies of computer system administrators. In *Proceedings of the 2004 ACM conference on Computer supported cooperative work - CSCW '04*, page 388, New York, New York, USA, 2004. ACM Press.

[3] David Botta, Rodrigo Werlinger, André Gagné, Konstantin Beznosov, Lee Iverson, Sidney Fels, and Brian Fisher. Towards understanding it security professionals and their tools. In *Proceedings of the 3rd symposium on Usable privacy and security*, pages 100–111. ACM, 2007.

[4] Sadegh Farhang, Jake Weidman, Mohammad Mahdi Kamani, Jens Grossklags, and Peng Liu. Take it or leave it: A survey study on operating system upgrade practices. In *Proceedings of the 34th Annual Computer Security*

Applications Conference, ACSAC '18, page 490–504, New York, NY, USA, 2018. Association for Computing Machinery.

[5] Alain Forget, Sarah Pearman, Jeremy Thomas, Alessandro Acquisti, Nicolas Christin, Lorrie Faith Cranor, Serge Egelman, Marian Harbach, and Rahul Telang. Do or do not, there is no try: User engagement may not improve security outcomes. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 97–111, Denver, CO, June 2016. USENIX Association.

[6] Dan Goodin. Nsa-leaking shadow brokers just dumped its most damaging release yet. https://arstechnica.com/information-technology/2017/04/nsa-leaking-shadow-brokers-just-dumped-its-most-damaging-release-yet/, April 2017. accessed on 2020-01-31.

[7] Eben M. Haber and Eser Kandogan. Security administrators: A breed apart. *Soups USM*, 2007.

[8] Iulia Ion, Rob Reeder, and Sunny Consolvo. "...no one can hack my mind": Comparing expert and non-expert security practices. In *Proceedings of the Eleventh USENIX Conference on Usable Privacy and Security*, SOUPS '15, page 327–346, USA, 2015. USENIX Association.

[9] Eser Kandogan and Eben M Haber. Security administration tools and practices.

[10] Sean Michael Kerner. Wannacry ransomware attack hits victims with microsoft smb exploit. https://www.eweek.com/security/wannacry-ransomware-attack-hits-victims-with-microsoft-smb-exploit, May 2017. Accessed: 2020-01-30.

[11] Frank Li, Lisa Rogers, Arunesh Mathur, Nathan Malkin, and Marshini Chetty. Keepers of the machines: Examining how system administrators manage software updates for multiple machines. In *Fifteenth Symposium on Usable Privacy and Security (SOUPS 2019)*, Santa Clara, CA, August 2019. USENIX Association.

[12] Arunesh Mathur, Josefine Engel, Sonam Sobti, Victoria Chang, and Marshini Chetty. " they keep coming back like zombies": Improving software updating interfaces. In *Twelfth Symposium on Usable Privacy and Security (SOUPS 2016)*, pages 43–58, 2016.

[13] Arunesh Mathur, Nathan Malkin, Marian Harbach, Eyal Peer, and Serge Egelman. Quantifying users' beliefs about software updates. 01 2018.

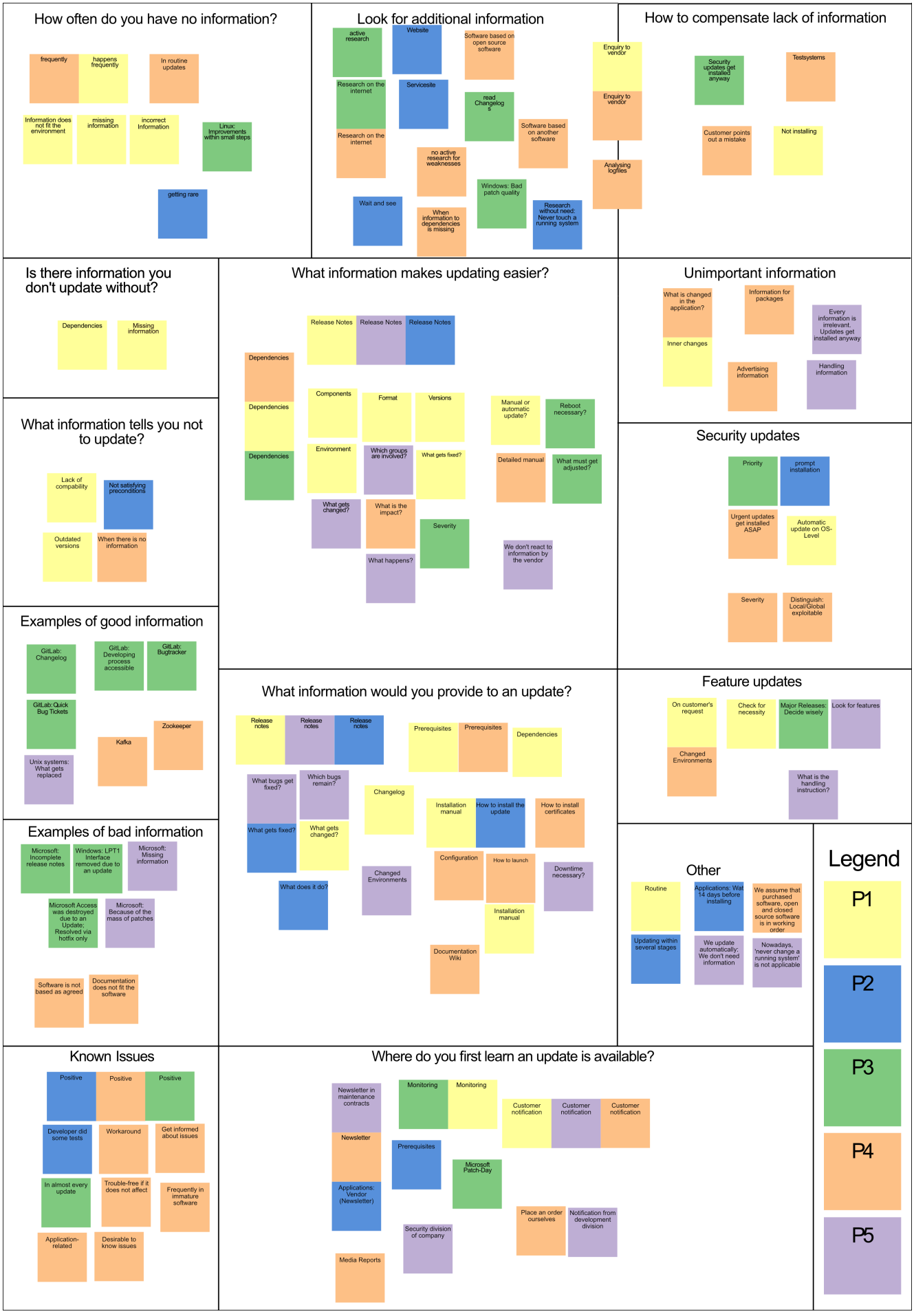
[14] Laura Moreno, Gabriele Bavota, Massimiliano Di Penta, Rocco Oliveto, Andrian Marcus, and Gerardo Canfora. Automatic generation of release notes. In *Proceedings of the 22nd ACM SIGSOFT International Symposium on Foundations of Software Engineering*, FSE 2014, page 484–495, New York, NY, USA, 2014. Association for Computing Machinery.

[15] Christian Tiefenau, , Maximilian Häring, and Emanuel Krombholz, Katharina von Zezschwitz. Security, availability, and multiple information sources: Exploring update behavior of system administrators. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*. USENIX Association, August 2020.

[16] Kami Vaniea and Yasmeen Rashidi. Tales of software updates: The process of updating software. In *Proceedings of the 2016 chi conference on human factors in computing systems*, pages 3215–3226, 2016.

[17] Kami E Vaniea, Emilee Rader, and Rick Wash. Betrayed by updates: how negative experiences affect future security. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, pages 2671–2674, 2014.

A Affinity Diagram


How often do you have no information?
frequently
happens frequently
In routine updates
Information does not fit the environment
missing information
incorrect Information
Linux: Improvements within small steps
getting rare
Look for additional information
active research
Website
Software based on open source software
Research on the internet
Servicesite
read Changelogs
Research on the internet
Software based on another software
no active research for weaknesses
Wait and see
When information to dependencies is missing
Windows: Bad patch quality
Research without need: Never touch a running system
Enquiry to vendor
Enquiry to vendor
Analysing logfiles
How to compensate lack of information
Security updates get installed anyway
Testsystems
Customer points out a mistake
Not installing
Is there information you don't update without?
Dependencies
Missing information
What information tells you not to update?
Lack of compability
Not satisfying preconditions
Outdated versions
When there is no information
What information makes updating easier?
Release Notes
Release Notes
Release Notes
Dependencies
Dependencies
Dependencies
Components
Format
Versions
Environment
Which groups are involved?
What gets fixed?
What gets changed?
What is the impact?
Severity
What happens?
Manual or automatic update?
Reboot necessary?
Detailed manual
What must get adjusted?
We don't react to information by the vendor
Unimportant information
What is changed in the application?
Information for packages
Every information is irrelevant. Updates get installed anyway
Inner changes
Advertising information
Handling information
Security updates
Priority
prompt installation
Urgent updates get installed ASAP
Automatic update on OS-Level
Severity
Distinguish: Local/Global exploitable
Examples of good information
GitLab: Changelog
GitLab: Developing process accessible
GitLab: Bugtracker
GitLab: Quick Bug Tickets
Kafka
Zookeeper
Unix systems: What gets replaced
What information would you provide to an update?
Release notes
Release notes
Release notes
Prerequisites
Prerequisites
Dependencies
What bugs get fixed?
Which bugs remain?
Changelog
What gets fixed?
What gets changed?
Installation manual
How to install the update
How to install certificates
Configuration
How to launch
Downtime necessary?
What does it do?
Changed Environments
Installation manual
Documentation Wiki
Feature updates
On customer's request
Check for necessity
Major Releases: Decide wisely
Look for features
Changed Environments
What is the handling instruction?
Examples of bad information
Microsoft: Incomplete release notes
Windows: LPT1 Interface removed due to an update
Microsoft: Missing information
Microsoft Access was destroyed due to an Update; Resolved via hotfix only
Microsoft: Because of the mass of patches
Software is not based as agreed
Documentation does not fit the software
Other
Routine
Applications: Wat 14 days before installing
We assume that purchased software, open and closed source software is in working order
Updating within several stages
We update automatically: We don't need information
Nowadays, 'never change a running system' is not applicable
Legend
P1
P2
P3
P4
P5
Known Issues
Positive
Positive
Positive
Developer did some tests
Workaround
Get informed about issues
In almost every update
Trouble-free if it does not affect
Frequently in immature software
Application-related
Desirable to know issues
Where do you first learn an update is available?
Newsletter in maintenance contracts
Monitoring
Monitoring
Customer notification
Customer notification
Customer notification
Newsletter
Prerequisites
Microsoft Patch-Day
Applications: Vendor (Newsletter)
Place an order ourselves
Notification from development division
Security division of company
Media Reports

B Survey

1. Welcome and thank you for your participation in our research study!

   The goal of our study is to analyze and understand the impact of update-related information and how it helps you in your decision to deploy the update.

   Therefore, we built this short survey based on previous interviews and findings. Please answer the following questions based on your experience and knowledge. Your data will be collected and processed in anonymized form, in a way that no connection to your person can be made. The study should take you around 5-10 minutes to complete and your participation is voluntary. You can withdraw at any point during the study, for any reason, and without any prejudice. If you would like to contact the Principal Investigator in the study to discuss this research, please e-mail martius@uni-bonn.de.
   By clicking the button below, you acknowledge that your participation in the study is voluntary, you are 18 years of age, and that you are aware that you may choose to terminate your participation in the study at any time and for any reason.

   (a) I consent.

   (b) I do not consent.

2. How old are you?
   Free response

3. What is your gender?
   Free response

4. For how many years have you been working as a professional system administrator?
   Free response

All of the questions on this page refer to a specific company. If you currently work as an administrator, please answer these questions about your current company. If you do not currently work as an administrator, please answer these questions about the last company at which you worked as an administrator.

5. Is this company an IT company?

   (a) Yes

   (b) No

   (c) Other (please specify)
   Free response

6. In what country is this company?
   Free response

7. Which of the following statements best describes your role in this company?

   (a) My primary responsibility was system administration

   (b) My primary responsibility was not system administration, but I spent at least 20% of my time on system administration

   (c) My primary responsibility was not system administration, but I spent between 1% and 19% of my time on system administration

   (d) I did not perform system administration at that company

8. In a few words, what would you consider as your main task in the company you are working at?
   Free response

9. What is your main task as a system administrator? If it is the same as in the previous answer, please answer: same
   Free response

10. What kind of systems do you administer?

    (a) Clients

    (b) Servers

    (c) Mobile Clients

    (d) Internet of Things

    (e) Other (please specify)
    Free response

11. How big is the company you work at as a system administrator?

    (a) Less than 10 employees

    (b) 11 - 50 employees

    (c) 51 - 100 employees

    (d) 100 - 500 employees

    (e) 501 - 2000 employees

    (f) More than 2000 employees

12. How many machines/devices do you manage?
    Slide bar from 0 to 1000+

13. How many updates do you run on the systems that you administer per week?
    Slide bar from 0 to 500+

14. What pre-deployment steps do you take before installing an update on a live system?

    (a) We install it on a test system.

    (b) We install it on a small number of production systems before deploying it to all systems or to everyone.

    (c) We install it directly on all production systems.

(d) Other (please specify)
Free response

15. What kind of job related education did you receive? (e.g. training, certificate, university)
Free response

16. Where do you find out about an available update? (Check all that apply)

(a) Online forums
(b) Security advisories
(c) Blogs
(d) News
(e) Social media
(f) RSS feeds
(g) Professional mailing lists
(h) Project mailing lists
(i) Direct notification from vendor
(j) Direct notification from customer
(k) Third-Party service
(l) When the software pops up a notification
(m) Other (please specify)
Free response

17. Please indicate the percentage of automatically applied updates in relation to all applied updates:
Slide bar from 0 to 100

18. How often do you read update-related information (including the installation manual) in order whether or not to update for automatic and manual updates?
Table of the following questions, with a 7-point Likert scale from '1 - Never' to '5 - Always' and the options 'Does not apply' and 'Prefer not to answer'

(a) Automatic update
(b) Manual update

19. Please indicate how often the following situations occur:
Table of the following questions, with a 7-point Likert scale from '1 - Never' to '5 - Always' and the option 'Prefer not to answer'

(a) There is a lack of update-related information.
(b) Lack of information increase the effort to update.
(c) I look for additional information not given by the publisher.

20. Where do you look for additional information (Check all that apply)

(a) Online forums
(b) Security advisories
(c) Blogs
(d) News
(e) Social media
(f) RSS feeds
(g) Professional mailing lists
(h) Enquiry to the vendor
(i) Other (please specify) *Free response*

21. Please rate the subjective time available to you to learn about an update:
Table of the following statement, with a 6-point Likert scale from '1 - No time' to '5 - No time restrictions' and the option 'Prefer not to answer'

(a) Time to learn about an update

The following questions refer to the usefulness of specific update-related information. We want to find out how these factors support you in your decision whether or not to update a machine/device/software.

22. Please rate the usefulness of the following general information-related information:
Table of the following statements, with a 6-point Likert scale from '1 - Not useful at all' to '5 - Extremely useful' and the option 'Prefer not to answer'

(a) Release Date
(b) Release Number
(c) Note Number
(d) Note Date
(e) Purpose of the update

23. Please rate the usefulness of the following release-notes-related information:
Table of the following statements, with a 6-point Likert scale from '1 - Not useful at all' to '5 - Extremely useful' and the option 'Prefer not to answer'

(a) Fixed bugs
(b) Still existing bugs
(c) Steps to reproduce bugs
(d) involved components
(e) Changed environment (if necessary)
(f) Known issues
(g) Closed vulnerabilities
(h) Update severity (i.e., critical, moderate..)

An update can have an impact on support-level (i.e., for you) and/or on end-user-level. Please answer the following questions that address these two factors.

24. Please rate the usefulness of the following support-impact-related information
    Table of the following statements, with a 6-point Likert scale from '1 - Not useful at all' to '5 - Extremely useful' and the option 'Prefer not to answer'
    (a) Added feature
    (b) Removed feature
    (c) Modified handling of a feature
    (d) Advertising information (i.e. more colorful)

25. Please rate the usefulness of the following end-user-impact-related information
    Table of the following statements, with a 6-point Likert scale from '1 - Not useful at all' to '5 - Extremely useful' and the option 'Prefer not to answer'
    (a) Added feature
    (b) Removed feature
    (c) Modified handling of a feature
    (d) Advertising information (i.e. more colorful)

26. Please rate the usefulness of the following changelog-related information:
    Table of the following statements, with a 6-point Likert scale from '1 - Not useful at all' to '5 - Extremely useful' and the option 'Prefer not to answer'
    (a) Added files
    (b) Removed files
    (c) Changed files

27. Please rate the usefulness of the following installation-manual-related information:
    Table of the following statements, with a 6-point Likert scale from '1 - Not useful at all' to '5 - Extremely useful' and the option 'Prefer not to answer'
    (a) Prerequisites (i.e. reboot necessary)
    (b) Changed/Added/Removed dependencies
    (c) Update delivery (zip-file, binary..)
    (d) Installation manual for the update itself
    (e) Installation manual for required third-party software

28. Please rate the usefulness of the following other information:
    Table of the following statements, with a 6-point Likert scale from '1 - Not useful at all' to '5 - Extremely useful' and the option 'Prefer not to answer'
    (a) Documentation of added or modified features
    (b) Disclaimers
    (c) Support contact information

29. Please rate the usefulness of properties of known issues:
    Table of the following statements, with a 6-point Likert scale from '1 - Not useful at all' to '5 - Extremely useful' and the option 'Prefer not to answer'
    (a) Knowing about possible bugs before they occur
    (b) Having a workaround for bugs
    (c) Knowing that a bug does not impinge our system

30. What else do you want us to know about update-related information not mentioned in the survey?
    Free response

C Survey Results

Information	Survey	1	2	3	4	5	*	**Median**
Release Date	1	2	6	10	6	17		4
	2	1	5	2	3	6		4
Release Number	1	4	14	13	7	3		3
	2		2	6	4	5		4
Note Number	1	6	17	12	4	2		2
	2	1	2	8	3	3		3
Note Date	1	6	12	18	3	2		3
	2	1	1	10	3	2		3
Purpose of the Update	1		1	1	5	34		5
	2		3		5	9		5
Fixed Bugs	1		2	2	6	31		5
	2			5	5	7		4
Still existing Bugs	1		4	6	13	18		4
	2		1	5	4	7		4
Steps to Reproduce Bug	1	1	8	14	14	4		3
	2		5	4	5	3		3
Involved Components	1		2	14	16	9		4
	2		1	3	8	5		4
Changed Environment	1		4	10	13	14		4
	2		3	2	5	6	1	4
Known Issues	1		1	1	12	27		5
	2			2	6	9		5
Closed Vulnerabilities	1		2	4	9	26		5
	2		1	4	4	8		4
Risk Qualification	1	1	4	11	8	17		4
	2		2	5	3	7		4
Added feature *(Support-Impact)*	1	1	1	9	14	16		4
	2		4	5	4	4		
Removed feature *(Support-Impact)*	1	1	1	7	12	20		4
	2		1	4	4	8		4
Modified handling of a feature *(Support-Impact)*	1		2	12	16	11		4
	2		1	3	9	4		4
Advertising information *(Support-Impact)*	1	14	19	3	3	2		2
	2	9	4		2	1	1	1
Added feature *(End-User-Impact)*	1		3	7	15	16		4
	2		2	5	4	6		4
Removed feature *(End-User-Impact)*	1	1	5	6	7	22		5
	2			3	8	6		4
Modified handling of a feature *(End-User-Impact)*	1	2	3	8	11	17		4
	2		1	3	9	4		4
Advertising information *(End-User-Impact)*	1	14	3	12	6	6		3
	2	4	7	3	2		1	2
Added files	1	3	3	13	9	13		4
	2	1	4	3	5	2	2	3
Removed files	1	3	4	12	11	11		4
	2	1	4	1	6	3	2	4
Changed files	1	3	2	14	10	12		4
	2	1	3	4	5	2	2	3
Prerequisites	1		1	1	8	31		5
	2		2	2	1	12		5
Dependencies	1	1		5	10	24	1	5
	2		1	1	4	10	1	5
Update delivery	1		7	15	13	6		3
	2	1	4	3	5	4		4
Installation manual itself	1	1	5	10	11	14		4
	2	1	1	6	4	5		4
Third party	1	3	7	6	10	15		4
	2		1	7	4	5		4
Documentation of features	1	1	2	6	13	17	2	4
	2			5	7	5		4
Disclaimers	1	13	14	8	1	3	2	2
	2	6	4	5	1	1		2
Support contact information	1	1	8	18	8	4	2	3
	2	1	8		4	4		2

Table 3: Overview of the responses to the information-type on a 5-point scale from “1 - Not useful at all” to “5 - Extremely Useful” (* “Prefer not to answer”) separated into the two surveys due to the different wording of the question.