

Security, Availability, and Multiple Information Sources: Exploring Update Behavior of System Administrators

Christian Tiefenau and Maximilian Häring, *University of Bonn;*
Katharina Krombholz, *CISPA Helmholtz Center for Information Security;*
Emanuel von Zezschwitz, *University of Bonn, Fraunhofer FKIE*

https://www.usenix.org/conference/soups2020/presentation/tiefenau

This paper is included in the Proceedings of the Sixteenth Symposium on Usable Privacy and Security.

August 10–11, 2020

978-1-939133-16-8

Open access to the Proceedings of the Sixteenth Symposium on Usable Privacy and Security is sponsored by USENIX.

Security, Availability, and Multiple Information Sources: Exploring Update Behavior of System Administrators

Christian Tiefenau
University of Bonn

Maximilian Häring
University of Bonn

Katharina Krombholz
CISPA Helmholtz Center for Information Security

Emanuel von Zezschwitz
University of Bonn, Fraunhofer FKIE

Abstract

Experts agree that keeping systems up to date is a powerful security measure. Previous work found that users sometimes explicitly refrain from performing timely updates, e.g., due to bad experiences which has a negative impact on end-user security. Another important user group has been investigated less extensively: system administrators, who are responsible for keeping complex and heterogeneous system landscapes available and secure.

In this paper, we sought to understand administrators' behavior, experiences, and attitudes regarding updates in a corporate environment. Based on the results of an interview study, we developed an online survey and quantified common practices and obstacles (e.g., downtime or lack of information about updates). The findings indicate that even experienced administrators struggle with update processes as the consequences of an update are sometimes hard to assess. Therefore, we argue that more usable monitoring and update processes are essential to guarantee IT security at scale.

1 Introduction

"Keep your systems up to date" is one of the most popular pieces of advice that security experts give to end-users [33,55]. Supporting this, Khan et al. found that there is a correlation between not deployed updates and infected machines [35]. Systems can easily be hardened against vulnerabilities like Heartbleed [1] by applying updates. Regardless of that, many systems in the wild remain vulnerable for two years or more [57]. A prominent example of a situation where an update could have prevented severe data leakage is the Equifax breach [2], which occurred in 2017. Similar incidents seem not unusual as is reported by an industry report [42].

Related work studied user perceptions and experiences with system updates and found that the results are often not in line with current recommendations of experts from a security perspective. In most cases, concerns about functional issues or unexpected UI changes hinder individuals from updating their systems [63]. In addition, users often do not understand the importance of non-visual changes [63], as they come with security updates. In contrast to users who are responsible only for managing their own personal devices, system administrators are in charge of large and complex IT infrastructures while also being users. We argue that their update behavior can have severe implications at a much larger scale. Marconato et al. [43] observed the vulnerability life-cycle on different platforms and found that the time to patch and disclose vulnerabilities is decreasing. This finding can be applied to the Equifax breach and suggests that administrators are required to react in a timely manner.

Although general user concerns about system updates have been investigated in user studies, little light has been shed on the perspective of specific user groups (e.g., administrators or operators). Investigating administrators, Dietrich et al. [12] found that insecure configurations are often caused by institutional and individual factors, as well as time constraints. We assume that similar factors can have a negative impact on update processes. Administrators are often overworked [12], and updates are time-consuming. Secure systems, however, rely on updates and therefore, require regular attention by administrators. As the body of literature is still in an early state regarding administrators' update behavior, we follow an inductive approach to explore the processes and obstacles that administrators face when updating in a corporate context.

[1] http://heartbleed.com/, accessed 02/25/2020.

[2] https://www.theverge.com/2017/10/3/16410806/equifax-ceo-blame-breach-patch-congress-testimony, accessed: 11/20/2019.

Copyright is held by the author/owner. Permission to make digital or hard copies of all or part of this work for personal or classroom use is granted without fee.
USENIX Symposium on Usable Privacy and Security (SOUPS) 2020.
August 9–11, 2020, Virtual Conference.

Our contributions are as follows:

- We conducted **seven qualitative interviews to explore how administrators experience, perceive, and act during the update process**.
- We conducted an **online survey with 67 valid answer sets to test our observations on a larger scale.**
- We confirm that current **update processes and system factors tend to endanger IT security** and we discuss critical factors that need to be addressed to **support administrators**.

The results suggest that the update process differs among companies for various reasons. Administrators face a variety of obstacles in their update routines, e.g., downtime or hard-to-foresee situations, that often hinder them from performing updates in a timely manner. Overall, we argue that system administrators would benefit from more usable mechanisms, and that providing such mechanisms could effectively improve IT security at scale.

2 Related Work

Two areas of research are specifically important for our work: 1) studies about update behavior and 2) studies investigating the security behavior of expert users. In the following, we present lessons learned from both research areas.

2.1 Users' Update Behavior

According to security experts, keeping systems and software up to date is an important security recommendation [55]. However, users may not follow this advice for reasons that are not related to security [54], and only a minority of non-experts actually considers software updates an important security measure [33, 48]. It has been repeatedly shown that users often delay or even avoid updates [22, 47, 64].

Investigation of the root causes of such critical user behavior has become a very active field of research. Previous work revealed diverse reasons for avoiding updates. Many users think that updates are not important because the link to security aspects often is not obvious [15, 25, 45, 53, 63–65]. Furthermore, users are often afraid of functional changes (e.g., UI modifications) [7, 62–64] or fear making mistakes [22]. Inconvenience is an important factor as updates can cause interruptions and take time [45, 64, 65]. Finally, bad experiences with previous updates and negative online reviews hinder the installation of future patches [15, 45, 59, 62]. This problem seems self-perpetuating, because the frequency of security updates is influenced by the emergence of novel attacks and thus, cannot be controlled by the vendor alone [56]. However, high update frequencies can lead to further negative reviews [21, 52].

Several countermeasures for mitigating the problem of delayed updates have been proposed. As one straightforward solution, automatic updates [65] and silent updates [13, 56] have been deployed. Although such mechanisms are very effective in keeping software up to date, they often cause confusion and irritation as they hamper the user's understanding of what is happening on their machines [14, 65]. Furthermore, some users might have good reasons to refrain from performing certain updates [14]. Therefore, user-centered solutions, such as providing more information [44, 50, 58, 59] and designing better notifications [16, 17, 24], have been repeatedly suggested as complementary concepts to further increase compliance rates.

2.2 IT Professionals and IT Security

Recently, researchers have started focusing on security-related usability problems of specific user groups [2]. In contrast to security advocates [29] or security analysts [27], most of these people are not security professionals. They are often knowledgeable in a specific domain, related to IT. Several recent studies addressed the problems of software developers [1,3,4,40]. For example, Acar et al. [1,3] investigated available sources of information and how these sources influence code security. Gorski et al. [40] showed that software developers benefit from API-integrated security recommendations and that such usability-optimized concepts can significantly improve security [60].

Several human-centered studies with system administrators were published between 2001 and 2007. In 2001, Hrebec and Stiber [32] studied the mental models of system administrators and found that these experts often struggle to understand the complex systems that they need to manage. In addition, the study participants reported a lack of formal education and the desire to solve problems by themselves. Barrett et al. [6] found that system administrators often lack situational awareness. Haber and Kandogan [28, 34] and Botta et al. [10] observed the tools and work practices of security administrations and IT professionals. Their results show that security administrators perform a lot of different tasks and need various skills like pattern recognition or inferential analysis to perform these tasks. They proposed, that new classes of tools need to be developed to counter the ever increasing complexity of the systems and attack-vectors.

In contrast to this early work, a few recently published papers investigated more specific problems of system administrators. Fahl et al. [18] studied non-validating X.509 certificates and revealed that about 30% of the responsible webmasters misconfigured their web servers accidentally. Ukrop et al. [61] analyzed the corresponding warnings and found that rewording can help administrators to make better informed decisions. Krombholz et al. [37, 38] showed that the deployment process for HTTPS is far too complex and that administrators struggle with finding secure and compatible configura-

tions due to the lack of conceptual mental models. Dietrich et al. [12] investigated the administrators' general perception of misconfigurations and identified missing or delayed updates as one of the root causes of these problems.

There exists work that discussed update processes in companies [8, 9, 46, 64]. For example, Vitale et al. [64] performed three interviews with technical staff concerned with updates and found that these professionals prioritized security aspects and licensing issues over potential usability consequences. This finding confirmed previous findings [46] that in a corporate context, business needs rather than user requirements drive update decisions. In contrast, Blythe et al. [9] reported that employees often rely on "security experts" in the company to manage updates and often lack a feeling of responsibility. Finally, the update challenges of system administrators have been indirectly considered by various researchers who proposed automatic tools to improve the manageability of the update process (e.g., [5, 26, 39, 49]). However, none of these concepts have been evaluated in a user study.

Parallel to our work, Li et al. [41] published a closely related paper in which they studied US-based system administrators in a qualitative fashion. They as well researched the update process in companies and found several *pain points* within the process. In contrast, our interview sample was drawn from German companies, thus representing a different culture. Overall, our study confirms most of their findings. We will separately discuss our findings in comparison to Li et al.'s in section 5.5 in more detail.

3 Interview Study

Although recommendations for patch management have been published[3], we are aware of only one other study that systematically investigated the update behavior of system administrators [41]. Therefore, we started with an interview study to identify important factors of the problem space.

This interview study aimed to provide answers to the following research questions with an emphasis on administrators' perceptions, challenges, and tools they use in their update routines:

1. **How can the update processes be described, and what common patterns are there?**
   Administrators are usually paid professionals who are responsible for updating large and complex IT infrastructures. This raises the question, whether, and if so, where, system administrators' updates processes differ from end-users' processes [62].

2. **What issues and obstacles do professional administrators face in their update routines?**
   We specifically aim at understanding the problems of administrators and their perception of update processes. Identifying obstacles in relation to processes, tools, and environments is indispensable to define important directions for future work.

3. **How are administrators informed about updates, and which sources of information do they use?**
   Related work has indicated that the source of information can have a significant impact on software security [1, 20]. Thus, we aim at understanding how administrators gather information and what sources they use.

4. **What kind of tools do administrators use to manage system updates, and is there room for improvements?**
   As usable security researchers, we are specifically interested in the tools involved in the update process. We hypothesize that although some tools are used on purpose and other tools are unavoidable, such tools can either complicate or ease the process.

3.1 Study Design and Procedure

We conducted seven semi-structured interviews in June 2018 to explore the participants' opinions, thoughts, and experiences. Based on three pilot-study interviews, we refined the interview guidelines to balance between informing the research questions and supporting a flexible exploration of the problem space (i.e., leaving enough room to add further comments). The interview was structured into (1) general questions about the daily work routine of the participant, (2) general experiences with updates, (3) a more detailed assessment of specific aspects, and (4) additional comments. The guidelines are in Appendix B.

All but one interview were conducted by the same researcher. Both researchers are experts in computer science and spoke the same native language as the interviewees. After an introduction to the purpose of the study, the participants were asked to sign a consent form. All participants gave their consent to being audio-recorded. We conducted one interview in person and six via telephone. All interviews were held in German. During the interviews, the interviewee and the researcher were allowed to take notes. The interviews lasted between 34 and 67 minutes and ended with a short questionnaire that collected demographic information.

3.2 Recruitment and Participants

We did not restrict our invitations to administrators working with a specific operating system, infrastructure or type of update. The only criterion for inclusion was that participants had to be in charge of, or in contact with, any kind of updates. Personal contacts were used as entry points to larger organizations and asked to forward the announcement to their employers' IT department. Additionally, we directly

[3] https://www.infosec.gov.hk/english/technical/files/patch.pdf, accessed 02/25/2020.

approached representatives of medium-sized and large companies at CeBIT 2018, a large international computer expo[4].

In total, we recruited seven participants at companies that had an office based in Germany. All participants reported they were in charge of system administration, although they had various job descriptions and managed different types of systems. Table 7 in the appendix presents more details about the sample. All the participants were male. For ease of readability in the following sections, we assigned the participants random names.

3.3 Analysis

The interviews were transcribed, and coded by two researchers. We coded open answers inductively following the approach of Wertz, Charmaz et al. [66]. The two researchers categorized the data according to the research questions presented in Section 3. The first three interviews were coded in a batch to establish the first codebook. Each of the following four interviews was coded separately. Then, the conflicts were discussed, and new codes were added to the codebook. We calculated the combined Krippendorff's alpha [36] before (0.61) and after (0.98) the discussion phase for each interview. Our goal was to use the qualitative analysis solely as a first step and foundation for the following quantitative study. Therefore, we refrained from continuing with interviews until theoretical saturation [23] was reached.

3.4 Qualitative Results

In the following, we present the results from the interview study with respect to the research questions.

3.4.1 Update Processes

In Table 1, we present the sum of all extracted process phases, including all reported steps that were performed in these phases. Overall, the update process varied in time and structure among participants and tended to be variable even for individual administrators, depending on the software that needed an update. Cyril reported he worked in a client environment with Windows systems. He was concerned mainly with regular update cycles. Therefore, he was able to prepare for update events (e.g., briefing the team, allocating resources, allocating maintenance windows, and gathering information). Four out of seven participants reported they relied on fixed update cycles for client systems, although Zelko reported that this was not always possible in practice. In contrast, Lorenz, who worked at a smaller company, reported that employees at his company were responsible for their systems. When we discussed more specific software, the answers became more diverse. Milan usually builds packages to automate the distribution, but Markus tends to perform manual installations.

[4] https://www.cebit.de/, accessed 02/25/2020.

Although participants' responsibilities differed, we were able to identify common patterns in the update process. Most of these phases can be mapped to those of client users [62]. However, we identified three major differences:

Some administrators perform extensive testing before installing the update on a live system. For example, Julian utilized up to three stages. Zelko, who stated, that "[E]ven if there is a risk that the update breaks something, we install them timely", utilized two test stages. First, he tested the update with virtual machines that simulate the client landscape, and then he rolled out the updates for a small group of colleagues.

Updates are rolled out step by step. The participants reported that often not all systems are updated in one batch. This allows the administrators to minimize the number of misconfigurations once an update fails, but constraints on resources are also a reason for this. For example, Julian reported that the network would be used to capacity if all systems were patched at the same time.

The preparation step is structured and involves planning and research of resources and the allocation of time slots. Five participants explicitly reported they conduct online research before they install an update. In addition, Alexander told that important update decisions are often made in group discussions.

3.4.2 Obstacles

We identified various obstacles that hamper the administrators' task of performing updates. In Table 1, we connect and report obstacles to the phases of the update process. In the following, we discuss common obstacles in more detail:

Downtimes. The participants stated that downtimes are a serious obstacle in the update process which often cause delayed deployments. As soon as a reboot is necessary, and there is no redundant system, downtime is induced. Alexander gave anecdotal evidence of a mitigation strategy: Upgrading from Solaris 10 (which required significant downtime) to Solaris 11 (which supports near to hot-swap updates and an easy rollback) increased update frequencies from three times a year to once a week.

Dependencies. The participants reported patches that break dependencies usually delay the process. Although this may not be surprising, it highlights the problem of dealing with dependent systems that cannot be patched in time. Further dependencies are introduced as part of the infrastructure landscape. For example, some systems depend on other systems to be available at boot time (Markus). Assessing these dependencies and then following the right order makes the process highly complex. Another type of dependency is towards the vendor of the software or hardware. An example of this can be as trivial as no available patches, even if a vulnerability is public, as Lorenz reported for the Meltdown case.

High frequency and large files. Every update takes re-

Phase	Step	Obstacles
Information	Becoming aware	
	Further details	Unsatisfying communication with the publisher*
Deciding	Discussion	Stability (1); Risk of exploits (2); Performance (1); Priority (2); Missing expertise (1)
Preparation	Planning	Planning itself (3); Time of release (3); Communication (1); Missing documentation about the system and processes*
	Backup	
	Waiting for release	
	Obtaining the patch	Missing patches (1)
	Automating	
	Informing users	
Testing	Test system	Testing itself (1); Broken dependencies (4); Resources*; Frequency of updates*
	Pilot system	
	Problem solving with manufacturer	
Installation	Installation itself	Failure (2); Missing configuration options (1); Social pressure; System resources (2); Complexity (3); Missing tools (3); Heterogeneous system (6); Company structure (3); Impact on systems/users (2); Downtime (1); Installation method (manual/automatic) (1,1)
	User interaction	Waiting for users (1)
	Reboot	Reboot itself (3); Old/Slow hardware (1)
Post-Installation	Documentation	
	Testing/Monitoring	
	Troubleshooting	
	Reversing	Missing backup, failover, or redundancy*

Table 1: Overview of phases, steps, and obstacles. The number in brackets denotes the number of participants who mentioned this aspect in the interviews. *Additional obstacles were found through the questionnaire.

sources: for example, time, workforce, CPU, and data storage. Zelko reported that big update files, which are often a consequence of combining functional updates with security patches, can cause problems. To handle resource constraints, updates are rolled out in multiple but smaller batches (Julian).

Competing priorities. Similar to standard users, administrators' decisions to perform updates are influenced by various factors. Participants reported stability considerations, the risk of an exploit, and performance issues as influential aspects. The fact that some systems do not separate security and feature updates may intensify this situation. Finally, required resources are sometimes allocated to other processes that have higher priority. Alexander reported that "the decision [to update] is always based on the sum of available information". As mentioned in Section 3.4.1, group discussions are an important part of the process. However, the need for communication can also delay updates (Milan).

Human Factors. In addition to technological and structural constraints, the administrator faces other obstacles. Missing expertise or a lack of knowledge can lead to situations where administrators rely on third parties. In this regard, Lorenz acknowledged that he does not always know how to act correctly. Or as Markus put it, he has to trust the vendor that the classification of the patch is correct. System administrators have to trust the information they get from the software developer, vendor, or other source. Another factor we identified is social pressure, as Lorenz reported, "And you look like an idiot, when you kill a git server. [...] That chases me." Another aspect that makes updating harder for administrators was software which is managed by end-users. Such software is often installed without the knowledge of administrators and makes the update process more complicated because it is not integrated in standard processes.

3.4.3 Sources of Information

The participants reported they use various methods to inform themselves about security updates and vulnerabilities. Five out of seven participants reported they use third-party sources that were independent of the software publisher, such as popular news portals or blogs. This information is usually supplemented by publisher-related newsletters and specific mailing lists, such as the Ubuntu-security mailing list (Lorenz). Cyril mentioned specialized third-party services that push information about available patches. Others got more specific and

reported that they use tools like SCCM[5] or Nessus[6] which serve as sources of information.

3.4.4 Tools

The participants reported OS-integrated tools and special purpose tools that are used to update servers and clients and that serve as sources of information. The purpose of such tools ranged from monitoring systems (Julian) to complete automation of the update process, such as SCCM or WSUS[7] (Markus). Participants also named external services (e.g., Shavlik[8]) that test and pre-filter patches for companies. Although automation of update processes was an important goal for participants, it had not yet been fully implemented. Software that is not covered by such tools, meaning not integrated by default, has to be updated manually or integrated. This seems to be the case when the vendors or the operating systems differ (e.g., using Microsoft WSUS to update Adobe Flash Player). Although the integration is possible, it is connected to additional effort and is not always done (Markus), e.g., if it affects only a small group of clients (Milan). Concerning future developments, Lorenz was less optimistic and brought up that the time investment in tools that would ease the workflow was not a high priority.

3.5 Key Observations

We performed an interview study of administrators' update behavior. Based on the research questions, we were able to describe update processes, common obstacles, information retrieval, and the use of software tools. We extract a series of key observations to guide the construction of the quantitative study, following the interviews. Table 1 provides an overview of the process phases, tools, and obstacles that administrators face in their daily lives according to the participants. Table 2 presents nine key observations, which were formulated based on the qualitative findings and then categorized in three groups: "Update Process and Information," "Update Obstacles," and "Human Factors." In the next section, we report on a quantitative online survey which was performed to shed further light on the update behavior of system administrators.

[5] https://www.microsoft.com/en-us/cloud-platform/system-center-configuration-manager-features, accessed 02/25/2020.

[6] https://www.tenable.com/products/nessus/nessus-professional, accessed 02/25/2020.

[7] https://docs.microsoft.com/en-us/windows-server/administration/windows-server-update-services/get-started/windows-server-update-services-wsus, accessed 02/25/2020.

[8] https://www.ivanti.com/company/history/shavlik, accessed 02/25/2020.

ID	Observation
	Update Process and Information
U1	Online sources are an important source for administrators to get informed about updates.
U2	Small companies have no formal update process.
	Update Obstacles
O1	Performance considerations often hinder the installation of an update.
O2	Update-caused downtimes delay the installation of an update (e.g., reboots)
O3	Problems after the installation of an update on the live system are only a minor concern.
O4	Lack of information hinder the update process.
O5	User action (e.g., installing a software without the knowledge of the admin) can circumvent the update process and render it useless.
	Human Factors
P1	Administrators of big companies feel sufficiently trained.
P2	Administrators think that timely updates are important.

Table 2: Key observations based on qualitative results.

4 Quantitative Online Survey

Following the interviews, we performed a quantitative online survey. We created statements based on our observations in the interview study and developed an online questionnaire to quantify and enrich them.

4.1 Procedure and Structure

The recruitment process for the preliminary interview study indicated that system administrators are inherently short on time, and thus, minimizing the time to fill out the survey was indispensable to obtain a sufficient number of responses. Therefore, most of the questions were based on simple answer types, such as check boxes or rating scales. To further motivate participation, we offered an opt-in for a raffle of 3D prints. Every tenth participant had the chance to win a 3D-printed model of their choice. E-mail addresses were collected only for this raffle, stored separately, and deleted afterward. Twenty-three entered their contact email address of whom no one was interested in a print. After participants had given their consent to take part in the study, the survey started. Completion took about 10 minutes.

To support many different circumstances, we framed questions in a way that answers could be related to the current position or if not applicable, to the last position as system administrator. We started by collecting demographic data (e.g., age), personal information (e.g., years of experience), information about the work environment (e.g, their role, company size), and information about update processes (e.g., existence

ID	Statement	1	2	3	4	5	*	Plot	Median
O1	Performance considerations hinder the installation of an update.	24	27	7	9	0	0		2
O2	Downtimes caused by the update process hinder the installation of an update.	8	22	13	18	6	0		3
O4	A lack of information about the update hinder the installation of an update.	15	19	18	9	4	1		2
P1	I feel sufficiently trained as an administrator.	1	7	13	29	17	0		4

Table 3: Overview of the responses to statements regarding the frequency on a 5-point scale from "1 - Never" to "5 - Always" (* "Not sure") and their connection to the key observations.

ID	Statement	1	2	3	4	5	6	7	*	Plot	Median
O3	Post-installation problems in a live system are only a minor concern because they don't happen frequently.	8	9	8	5	12	16	9	0		5
O5	Users often install software without the knowledge of the administrator.	18	9	7	8	12	6	7	0		3
P2	Deploying security updates in a timely manner is important.	0	1	0	0	7	18	41	0		7

Table 4: Overview of the responses to statements regarding the attitude on a 7-point scale from "1 - Strongly disagree" to "7 - Strongly agree" (* "Not sure") and their connection to the key observations.

of formal processes). In the second phase, participants rated 1) the frequency of specific events using 5-point scales ranging from "1 - Never" to "5 - Always" and 2) indicated their agreement with different statements using 7-point scales ("1 - Strongly disagree" to "7 - Strongly agree"). The questions were presented in random order for each participant. The questions were chosen based on our observations and thus, examined the impact of obstacles (e.g., "Downtimes caused by the update process hinders the installation of an update"), human factors (e.g., "I feel that I am sufficiently trained as an administrator"), and information sources (e.g., selection of sources used). The questionnaire ended with an open-ended question about the biggest obstacles in the update process that we coded afterwards. The new categories are marked with an asterisk in Table 1.

To ensure the internal consistency of the collected data, we added an attention check based on the negation of one of these questions. Five participants, who answered both questions with a different polarity, were excluded from the evaluation.

4.2 Recruitment and Participants

To attract professional system administrators, we decided against using crowdsourcing platforms like Amazon Mechanical Turk. Instead, we reached out to community sites like Reddit and specialized forums. Additionally, we used Twitter and followed a similar approach as we did in the interview study. Posting in forums resulted in 66 answers, advertising on Twitter resulted in 67 responses, and using personal contacts in companies to spread the questionnaire contributed eight answers.

The English survey was active for 14 days in September 2018. During this time, the questionnaire was started 141 times and completed by 72 (51.1%) participants. As reported, five data sets were excluded from the analysis due to failed attention checks, resulting in 67 valid data sets. The participants' age ranged between 22 and 55 years. Fifty-eight of them were male, one female, three reported "Other" and five preferred did not specify their gender. More than 61% (41) work in European countries. The biggest group of the participants pool work in Germany (22), but we also received answers from other continents, like North America(19), Australia (2) or South America (1). Table 6 in the appendix provides an overview of the participants' demographics. The job-related education of our participants can be classified as "unspecified training," "vendor training," "self taught," and "experience at the job." Most of the participants worked in a team (39), 16 were a team leader, and 10 worked alone. In the following, we report on the data gathered by the questionnaire.

4.3 Results

In the following, the results of the online survey are presented structured by the main categories presented in Table 2. The observations from the interviews suggest that company size may have an influence on different factors. To assess this point, we divided the data sets in two groups: 34 companies with 250 employees or fewer were tagged as small and medium-sized enterprises (SMEs), and 33 companies with more than 250 employees were defined as large enterprises [11]. This was found to be a suitable comparison because post-hoc we had comparable group sizes. A controlled analysis of additional

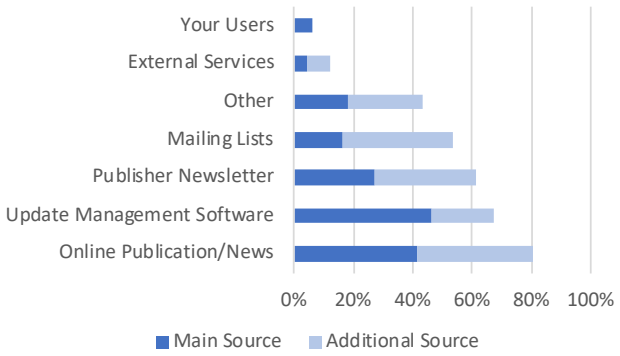


Figure 1: Distribution of information sources used by the administrators (n=67).

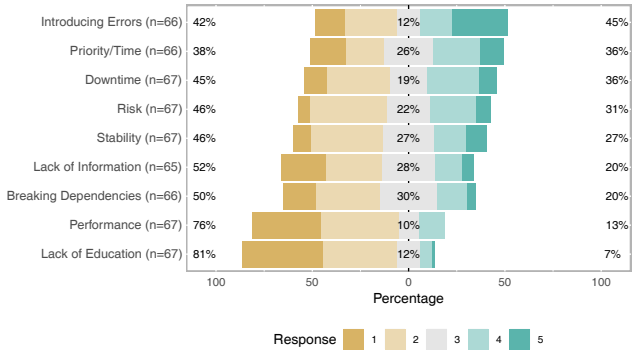


Figure 2: Frequency of considerations that hinder the installation of an update. The scale ranged from "1 – Never" to "5 – Always." Not included are "not sure" or missing answers.

factors was not feasible at this stage, and future work should consider other aspects (e.g., experience, type of systems, and team size). Tables 3 and 4 show the answers of the participants to the statement they were presented.

4.3.1 Update Process and Information

U1 Figure 1 presents the *sources of information* administrators use to learn about (new) updates. Most of the participants reported a median of three different sources. Third-party online publications are the most frequently used sources of information. They served as a source for 54 (81%) participants, and 28 of all 67 participants (42%) even declared them the main source of information. When focusing on the main source of information, we found that update management tools are essential for most administrators (46%). Fisher's exact test indicated no statistically significant differences between differently sized companies ($p = 0.2242$). Using an optional comment field, some administrators added other sources of information, such as vendors, the online community (e.g., Twitter), work experience, and active monitoring of systems. Due to the structure of the questionnaire, we cannot make statements about how the participants ranked the quality of those sources. We do not know whether they use one source to get informed about the occurrence of an update and then use another to capture details.

U2 To investigate the *existence of formal update processes*, we asked the participants if 1) "there is a written document," 2) "no document but an informal guideline," or 3) "no defined process" in their company. Twenty-eight (42%) participants indicated the existence of formal processes, 26 (39%) administrators had at least informal guidelines for performing updates, and 13 (19%) participants indicated that there are no predefined processes. A comparison of the use of formal, written update processes in differently sized companies revealed a statistically significant difference between large companies (57.6%) and smaller ones (26.5%), ($p = 0.0136$, $ratio = 3.769$, Fisher's exact test). This indicates that small companies make less use of formal update processes. The lack of such a process is not uncommon in our sample, as 10 out of 34 of the small companies did not report any kind of defined process.

4.3.2 Update Obstacles

Figure 2 shows the share of administrators who have faced specific obstacles during daily update routines. Quantifying the observations, we found that general risk assessments are known to most of the participants (94%) while deciding to deploy specific updates. Only four (6%) participants answered that they never considered assessing risks as an obstacle, while 63 agreed they did so at least sometimes.

O1 to O4 When asked about more specific obstacles, or risks, *stability considerations* represented the biggest issues that had been considered by 61 (91%) participants in the past. Similarly, 59 (88%) participants considered *downtime* as a specific obstacle. *Lack of information* (50, 77%), performance issues (43, 64%) and educational aspects (39, 58%) were the least prevalent obstacles in the sample. However, even those factors were considered by a majority of the participants. Finally, we performed Mann-Whitney U tests to investigate the impact of company size on the prevalence of obstacles: We could not find statistically significant differences [9].

Fifty-five percent seemed to agree that *problems after the installation of an update* are only a minor concern. However, eight participants strongly disagreed with the statement. Five

[9] stability considerations: $p = 0.814$, downtime: $p = 0.324$, lack of information: $p = 0.655$, performance issues: $p = 0.067$, educational aspects: $p = 0.752$, introducing errors: $p = 0.611$, risk considerations: $p = 0.415$, breaking dependencies: $p = 0.387$, priority: $p = 0.559$

Interval	
Hours to a day	11
Within a week	19
Within two weeks	8
Within one month	11
More than a month	9
No answer/no usable information (e.g., missing unit)	11

Table 5: Reported time intervals between the release of an update and deployment on all systems.

were undecided, and 25 (37%) disagreed in some way. To cover potential reasons for the answers, we assigned participants to two groups: those who do some kind of testing before installing updates on the live system ($n = 45, 67\%$) and those who do not ($n = 22, 33\%$). There was no statistically significant difference ($p = 0.2553$, Mann-Whitney U test) meaning that having a testing phase seems not to prevent all problems after the installation. Due to the sample size, we could not investigate if the company size is a significant factor in this regard.

O5 Another aspect in the interview study was the *user rights*. The agreement to the observation "Users often install software without the administrators' knowledge" was diverse. Although there was a tendency to disagree, as can be seen by the low median (3), there were also seven strong agreements. We found no statistical significance that would have supported our assumption that IT companies may have a different distribution on this than non-IT companies.

4.3.3 Human Factors

P1 Seventeen (25%) administrators reported that they always *feel sufficiently trained* for dealing with updates. However, 50 (74.6%) participants already faced situations for which they did not feel sufficiently trained. An evaluation of the impact of the administrator's company size indicates that administrators at large companies ($Median = 4$) more often feel sufficiently trained than their colleagues at smaller companies ($Median = 4$), Mann-Whitney U test: $U = 358.0, p < 0.01$, two-sided.

P2 Finally, all administrators (except one) somewhat agreed that *timely updates are important*. The self-reported time span between the release of an update and its installation can be seen in Table 5. While some participants reported deploying updates within a day, there were nine cases where updates needed more than a month. Optional comments given by the participants supported the findings that downtime, complexity, and dependencies are common reasons for such delays.

4.3.4 (Missing) Distinction between Security- and Feature-Updates

The interviews revealed that security- and feature-updates are often hard to distinguish. While we did not ask for the share of security-related patches in our interviews, the survey participants reported that 56% (ranging from 5-100%) of the overall updates involved security-related ones.

5 Discussion and Implications

Our work identified multidimensional problems that should be addressed by multiple stakeholders (e.g., software vendors or the companies themselves). In this section, we reflect on our results, provide actionable recommendations for these stakeholders and suggest directions for future research. We acknowledge that many aspects reported in this paper may seem like "common sense". With this work, we add to the scientific evidence in this very broad area with several factors that influence the update process and directions for further research and discussion.

5.1 Security Implications

Our results are in line with Li et al. and show that even professionals cannot always deploy updates in a timely fashion. This can be a security issue since outdated systems are often vulnerable to exploits. The administrators we asked were aware of this problem and agreed that deploying updates in a timely manner is important. However, we found that external factors such as compliance with company-specific rules, inflexible processes and communication overhead (e.g., leadership approval) still delay updating in practice. Future work needs to take a more holistic view and investigate technical and social factors in the update process. We need to understand which people are involved in these processes and how their communication can be supported. In addition, we need to develop approaches to better communicate the urgency of specific patches as today, the rating is often not clear [42].

5.2 Update Process

The results showed that the update processes of system administrators are diverse and complex. Although the update processes of administrators can be matched to the end-user phases [62], the identified phases differ in the details. In particular, gathering information and discussing update decisions were identified as important but time-consuming steps. As many administrators reported they make decisions in group meetings, we raise the question of how individual administrators can be supported in their decision-making process. The preparation process takes time and involves extensive testing. Although the testing processes were handled differently, they usually involved multiple iterative stages. This indicates that

administrators have to go through the whole update process multiple times. Two findings were primarily interesting: 1) Many companies lack formal processes, and 2) the update process is highly complex and lacks automation. The insights into this process provide important directions for future research and immediate action items for software vendors, such as the following:

- Formal processes seem to be more frequently used in large companies. Whether formal processes help to reduce the burden of decision-making and ease the overall process should be researched; that is, in what way they influence the update process (e.g., can well-defined responsibilities speed up the decision and do they lead to more and faster updates?) and where possible trade-offs can be expected (e.g., decreased complexity versus more time needed).
- The high number of iterative steps must be supported, e.g., with automation approaches. Thus, it is important to understand which phases of the process are critical and which parts can be effectively supported by tools.
- A possible approach for improving the process could be to connect more effectively virtual teams of administrators who share similar responsibilities and manage similar systems. Supporting such concepts with feasible tools can quickly lead to shared knowledge of best practices and experiences resulting in a better overview of the effects updates have on their systems. We hypothesize that especially smaller companies would profit from that.

5.3 Obstacles

The findings indicate that administrators face severe obstacles that often hinder them from performing timely updates. In line with Dietrich et al.'s work [12], the findings show that the problems administrators face are diverse and interconnected. Corresponding to Hrebec and Stiber's findings [32], individual-related factors, such as negative and positive experiences with updating, as well as education, come into play. The findings provide a baseline for future research questions and immediate action items for software vendors, such as the following:

- Due to the highly diverse landscape of large-scale systems, future research should further explore contextual factors and different populations of administrators. Differentiation of the various types of administrators could help to better categorize participants and understand their diverse problems and challenges. Related to this point, the check of the external validity of the research would benefit from better differentiation of types of administrators. However, a practicable taxonomy for this is still missing.
- Software development should focus on reducing downtime and providing rollback mechanisms that encourage administrators to take the risk of potential negative effects on availability.
- Researchers and software vendors should investigate on how to provide reliable information and accurate documentation of the effects of an update and occurring problems right in the moment and at the place the update is going to be installed.

Therefore, we hypothesize that supporting administrators' situational overview will have positive effects on timely updates. Finally, minimizing consequences by providing reversible updates, or just updates that have very small effects, could furthermore help administrators to update. As an example, dynamic software updates (DSU) [31] seems like a promising technique to contribute to this area and could be evaluated from this perspective.

5.4 Coping Strategies

As a consequence of facing obstacles, system administrators have developed a diverse set of coping strategies. Although the degree of usage varied among participants, an important countermeasure against the growing complexity is the use of tools that monitor update processes and support to (partly) automate installations. Because administrators expressed the desire for more automation, the findings emphasize the importance of the area of research that deals with the development of such concepts [5, 26, 39, 49].

To cope with the problem of limited resources combined with growing package sizes, the participants started to divide update processes into multiple batches. This can have the advantage of allowing more feedback loops and of reducing the load on the network. However, at the same time, this process increases the number of required iterations for single patches. Although we argue that the footprint (e.g., resources needed to roll out), especially of security updates, should be minimal, this may not always be possible.

Based on the findings, we provide the following recommendations to support existing coping strategies and for the development of novel solutions:

- Hot swap functionality and small-sized patches which enable administrators to estimate the impact of the installation on their systems, have the potential to further ease the update processes.
- Update management tools should better support the integration of third-party software.
- Administrators' coping strategies are still not sufficiently understood. Thus, researchers should focus on systematically investigating different coping strategies for various obstacles, identify desirable behavior and analyze in which way the human aspect contributes to this.

5.5 Comparison to Results by Li et al. [41]

As mentioned in Section 2, a thematically similar publication emerged independently while we were working on this research. Li et al. published a study on system update processes among US American system administrators, identifying an update process that was very similar to ours [41].

The Update Process

While Li et al.'s process emerged entirely from their interview response data, our update process was informed by theoretical work by Vaniea et al. [62]. This could explain minor differences such as the separate testing phase we introduced to highlight the difference to the end-user process. Despite this difference, overall, we consider the identified processes to be very similar. In alignment with their findings, we can confirm that in the information-phase, administrators use multiple sources to derive information about updates. We didn't find any statistical difference in the number of sources used between administrators working in different companies (big vs small) in our sample. Li et al. reports on the frequency of the used sources and that three quarter of their participants used security advisories or direct vendor notifications. In our data, 81% informed themselves using online publications and 63% relied on publisher newsletters. We can add that despite having multiple sources (median=3), our population uses update management tools as their main source followed by online resources.

Both works identified the deciding-phase. We can match most of our identified obstacles to the reported factors of Li et al. With a slightly different perspective, we can add an additional reported obstacle that focuses more on the administrator executing the process than the update: missing expertise.

We can support Li et al.'s finding that testing is an important phase in the process and we encountered the same approaches: "Staggered deployments" and "Dedicated testing environments". As 83 of 102 (81%) of their survey participants included some form of testing, a slightly smaller, but still the major, part of our participants 45/67 (67%) reported the same.

As for the remaining two phases, our works differed in focus. While Li et al. extensively discussed the method of deployment (automatic vs. manual) and the decision of when to deploy in the deployment phase, our work concentrates on the obstacles the administrators face in this phase. For the post-installation phase, their work presents the ways in which administrators deal with update issues, while we report on the frequency of the occurrence of such issues (O3) in Section 4.3.2.

Obstacles in the Update Process

Li et al. identified challenges faced by administrators within this update process that can be categorized as: (1) obtaining relevant information about relevant updates and deciding, (2) preparing, testing and deploying updates in a timely fashion, (3) recovering from update-induced errors, and (4) organizational and management influence [41]. Our identified obstacles (cf. Section 3.4.2) are in line with these obstacles. Li et al.'s work reports that identifying the relevant information in an update can be a challenging task. We can confirm this (O4) and show that this was mentioned by 77% of our participants.

Automation can help to deploy updates sooner and more frequently. Li et al. have found several obstacles such as dependency and compatibility considerations or host heterogeneity as factors that have an influence on update deployment. In addition to those, we have found additional ones such as missing tools or performance considerations in our data set. Table 1 provides a summary of our findings that assigns the problems to the phases in which they occur.

In general, while their work reveals the existence of those problems, we can complement these problems with the frequency of the problems that our survey participants stated. Li et al. report that the recovery of updated-induced errors is a problem that we can enrich with the fact that this seems to be of mixed importance (O3). This could indicate that this is a context-dependent factor, and a more detailed research must be undertaken in this regard.

Also, Li et al.'s work reports on the existence of organizational oversight that hinders or delays updates in some cases. We can also find this problem and show that this, among stability and risk considerations, is of more importance than factors such as performance considerations.

Demographics

While both Li et al.'s and our study are very similar in methodology, they differ in a key point: the recruited sample. Li et al. sampled only US-based administrators, while we recruited our interview-study population from Germany and our survey participants were mostly (41 of 67) European-based. Despite work culture in the US and Europe (e.g. in Germany [19,30,51]) being distinctively different (stemming from cultural differences in education, law, and professional socialization, among others), both studies report similar findings. We are thus in the fortunate situation to not only have our methodology and findings independently validated within a close distance in time, but also to confirm that the phenomena we identified are relevant across both US and European system administrators.

On interpreting the independently compiled findings, we have an indication that the system administration process is not as susceptible to cultural differences (at least in Western societies) as other fields of work. This might be connected to the rather globalized nature of IT infrastructure. Both participant pools used similar software, e.g., SCCM or WSUS (cf. Section 3.4.4). It is reasonable to assume that the technical challenges are similar. Comparing both papers, we could not

find any differences that originate in individual or organizational factors. If this can be confirmed in further studies within different countries such as China (the largest producer of IT hardware and systems[10]), Estonia (the often considered "most advanced" country within the EU in terms of digital transformation[11]), or Qatar (the largest economy in the Middle East according to GDP per capita [12]), this would significantly widen the recruitment possibilities for future studies within the field of system administration.

6 Limitations

The population we refer to as administrators is inherently diverse in terms of responsibilities, education, and previous experience. Depending on the size of a company, administrators have different responsibilities and work either in isolation or in larger teams. Furthermore, the security requirements depend on the types of products and services a company offers. Also, there is no unified career path for administrators, and one must not necessarily have a degree or certificate of any kind to become an administrator. Because of all these aspects, the results are not generalizable and thus applicable other populations of administrators with different demographics or training. The participants in the online survey were mainly from Europe and the United States. In these regions, technical staff like administrators are predominantly male which is why the sample was heavily biased in terms of gender. Due to our recruitment strategy for the quantitative study, the sample potentially suffered from self-selection bias, as was likely also due to the completion rate (51.1%) of the survey. Regarding our questionnaire, we did not ask the participants about their current employment status. This could result in answers from people that worked as an administrator previously and are now in a different position. However, due to the mentioned self-selection bias we think that the participants are still somehow active in this area. Also, we did not collect information about the systems and software, the administrators were in charge of. Because of this, we cannot report possible existing differences between, e.g., different operating systems or widespread versus niche software. The analysis is based on self-reported data, and thus, participant reports are highly subjective. We have no reason to believe that social desirability and recall bias are uncommonly strong in the sample because the interviews and related work showed that administrators tend to admit that they do not know about everything [32]. However, this must be taken it into account, especially when talking about risk, obstacle perception, and individual perception (e.g., P1). Finally, the qualitative interviews provided useful insights but did not reach saturation (cf. [23]). However, the potential lack of saturation is alleviated as the qualitative analysis was primarily used as an exploratory first step to build hypotheses. The answers to the free-text questions on the questionnaire did not bring up many new topics which make us confident that the most common real-world problems were covered. But, although several different issues were covered, we make no claim for completeness.

[10] https://www.mckinsey.com/~/media/mckinsey/featured%20insights/china/china%20and%20the%20world%20inside%20the%20dynamics%20of%20a%20changing%20relationship/mgi-china-and-the-world-full-report-june-2019-vf.ashx

[11] https://www.wired.co.uk/article/estonia-e-resident, accessed 11/21/2019.

[12] https://www.cia.gov/library/publications/the-world-factbook/rankorder/2004rank.html, accessed11/21/2019.

7 Ethical Considerations

Our institution located in central Europe does not have a formal IRB process for this type of study but has a series of guidelines to follow. According to these guidelines, we limited the collection of personal information as much as possible and collected data separately from contact information. Furthermore, all the processes complied with the European General Data Protection Regulation (GDPR). As the administration of services in a corporate environment is a sensitive topic, we did not collect detailed information about the companies' infrastructures. In addition, participants were explicitly given the chance to drop out at any time during the study. Finally, we emphasized the option to skip questions that participants preferred not to answer.

8 Conclusion and Future Work

This work contributes a mixed-methods study that revealed how administrators incorporate security updates in their daily work routines, what obstacles they experience, and what coping strategies they apply. We found that even experienced administrators find it hard to predict the direct consequences of applying an update and are heavily concerned about potential downtimes. Another interesting observation was that administrators often rely on information that is not provided by the (software) vendor but by online media or by their peers, who often face similar struggles. Among other things, the findings imply that there are aspects that vendors can influence such as, e.g., provide sufficient documentation or more granular updates, which can help to motivate administrators to update and support them in the update process.

Based on the insights presented in this paper, we recommend the following topics for future work: (1) Investigate current established formal processes and evaluate their effectiveness in supporting timely updates. (2) Create computer-supported solutions that enable better communication between administrators and in this way, enhance the transfer of knowledge. (3) Design and evaluate feasible tools that support situational awareness, e.g., by helping administrators to find out about relevant updates and provide them with the information they need.

9 Acknowledgements

We thank Karoline Busse for their support in the interview study and valuable input on the discussion. Also, we thank Jennifer Seifert for her help with the sociologial theory. Finally, we want to thank Matthew Smith, Frank Li and the anonymous reviewers that helped with their constructive feedback to improve this work.

References

[1] Yasemin Acar, Michael Backes, Sascha Fahl, Doowon Kim, Michelle L. Mazurek, and Christian Stransky. You Get Where You're Looking for: The Impact of Information Sources on Code Security. *Proceedings - 2016 IEEE Symposium on Security and Privacy, SP 2016*, pages 289–305, 2016.

[2] Yasemin Acar, Sascha Fahl, and Michelle L Mazurek. You are not your developer, either: A research agenda for usable security and privacy research beyond end users. In *Cybersecurity Development (SecDev), IEEE*, pages 3–8. IEEE, 2016.

[3] Yasemin Acar, Christian Stransky, Dominik Wermke, Charles Weir, Michelle L Mazurek, and Sascha Fahl. Developers need support, too: A survey of security advice for software developers. In *Cybersecurity Development (SecDev), 2017 IEEE*, pages 22–26. IEEE, 2017.

[4] Hala Assal and Sonia Chiasson. Security in the software development lifecycle. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 281–296. USENIX Association, 2018.

[5] Rekha Bachwani, Olivier Crameri, Ricardo Bianchini, and Willy Zwaenepoel. Mojave: A recommendation system for software upgrades. In *MAD*, 2012.

[6] 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.

[7] Ofer Bergman and Steve Whittaker. The cognitive costs of upgrades. *Interacting with Computers*, 30(1):46–52, 2017.

[8] John M. Blythe and Lynne Coventry. Costly but effective: Comparing the factors that influence employee anti-malware behaviours. *Computers in Human Behavior*, 87:87 – 97, 2018.

[9] John M Blythe, Lynne M Coventry, and Linda Little. Unpacking security policy compliance: The motivators and barriers of employees' security behaviors. In *SOUPS*, pages 103–122, 2015.

[10] 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.

[11] The commission of the european communities. Commission recommendation of 6 May 2003 concerning the definition of micro, small and medium-sized enterprises, 2003.

[12] Constanze Dietrich, Katharina Krombholz, Kevin Borgolte, and Tobias Fiebig. Investigating system operators' perspective on security misconfigurations. In *Conference on Computer and Communications Security (CCS'18)*, 2018.

[13] Thomas Duebendorfer and Stefan Frei. Why silent updates boost security. *TIK, ETH Zurich, Tech. Rep*, 302, 2009.

[14] W. Keith Edwards, Erika Shehan Poole, and Jennifer Stoll. Security automation considered harmful? In *Proceedings of the 2007 Workshop on New Security Paradigms - NSPW '07*, page 33, New York, New York, USA, 2008. ACM Press.

[15] Michael Fagan and Mohammad Maifi Hasan Khan. Why do they do what they do?: A study of what motivates users to (not) follow computer security advice. In *Twelfth Symposium on Usable Privacy and Security ({SOUPS} 2016)*, pages 59–75, 2016.

[16] Michael Fagan, Mohammad Maifi Hasan Khan, and Ross Buck. A study of users' experiences and beliefs about software update messages. *Computers in Human Behavior*, 51:504 – 519, 2015.

[17] Michael Fagan, Mohammad Maifi Hasan Khan, and Nhan Nguyen. How does this message make you feel? a study of user perspectives on software update/warning message design. *Human-centric Computing and Information Sciences*, 5(1):36, Dec 2015.

[18] Sascha Fahl, Yasemin Acar, Henning Perl, and Matthew Smith. Why Eve and Mallory (Also) Love Webmasters: A Study on the Root Causes of SSL Misconfigurations. In *Proceedings of the 9th ACM Symposium on Information, Computer and Communications Security*, ASIA CCS '14, pages 507–512, New York, NY, USA, 2014. ACM.

[19] Thomas Faist. The volume and dynamics of international migration and transnational social spaces. 2000.

[20] F. Fischer, K. Böttinger, H. Xiao, C. Stransky, Y. Acar, M. Backes, and S. Fahl. Stack overflow considered harmful? the impact of copy amp;paste on android application security. In *2017 IEEE Symposium on Security and Privacy (SP)*, pages 121–136, May 2017.

[21] Marvin Fleischmann, Miglena Amirpur, Tillmann Grupp, Alexander Benlian, and Thomas Hess. The role of software updates in information systems continuance â an experimental study from a user perspective. *Decision Support Systems*, 83:83 – 96, 2016.

[22] 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, 2016.

[23] Jill J. Francis, Marie Johnston, Clare Robertson, Liz Glidewell, Vikki Entwistle, Martin P. Eccles, and Jeremy M. Grimshaw. What is an adequate sample size? Operationalising data saturation for theory-based interview studies. *Psychology and Health*, 25(10):1229–1245, 2010.

[24] Alisa Frik, Serge Egelman, Marian Harbach, Nathan Malkin, and Eyal Peer. Better Late(r) than Never: Increasing Cyber-Security Compliance by Reducing Present Bias. In *Workshop on the Economics of Information Security (WEIS)*, page 20, Insbruck, Austria, 2018.

[25] Steve Furnell. Vulnerability management: not a patch on where we should be? *Network Security*, 2016(4):5 – 9, 2016.

[26] Jonathan Gallagher, Robin Gonzalez, and Michael E Locasto. Verifying security patches. In *Proceedings of the 2014 international workshop on privacy & security in programming*, pages 11–18. ACM, 2014.

[27] John R. Goodall, Wayne G. Lutters, and Anita Komlodi. I know my network: Collaboration and expertise in intrusion detection. In *Proceedings of the 2004 ACM Conference on Computer Supported Cooperative Work*, CSCW '04, pages 342–345, New York, NY, USA, 2004. ACM.

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

[29] Julie M Haney and Wayne G Lutters. "it's scary... it's confusing... it's dull": How cybersecurity advocates overcome negative perceptions of security. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*. USENIX Association, 2018.

[30] Norbert Hedderich. Three Approaches to Qualitative Content Analysis. *Global Business Languages: Vol. 2 , Article 14*, 2:162–172, 2010.

[31] Michael Hicks and Scott Nettles. Dynamic software updating. *ACM Trans. Program. Lang. Syst.*, 27(6):1049–1096, November 2005.

[32] Dennis G. Hrebec and Michael Stiber. A survey of system administrator mental models and situation awareness. *Proceedings of the 2001 ACM SIGCPR conference on Computer personnel research - SIGCPR '01*, pages 166–172, 2001.

[33] Iulia Ion, Rob Reeder, and Sunny Consolvo. "... no one can hack my mind": Comparing expert and non-expert security practices. In *SOUPS*, volume 15, pages 1–20, 2015.

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

[35] Moazzam Khan, Zehui Bi, and John A. Copeland. Software updates as a security metric: Passive identification of update trends and effect on machine infection. In *MILCOM 2012 - 2012 IEEE Military Communications Conference*, pages 1–6. IEEE, oct 2012.

[36] Klaus Krippendorff. Reliability in content analysis: Some common misconceptions and recommendations. *Human Communication Research*, 30(3):411–433, jun 2004.

[37] Katharina Krombholz, Karoline Busse, Katharina Pfeffer, Matthew Smith, and Emanuel von Zezschwitz. "If HTTPS Were Secure, I Wouldn't Need 2FA"-End User and Administrator Mental Models of HTTPS. *To appear in the IEEE Symposium on Security & Privacy, May 2019*, 2019.

[38] Katharina Krombholz, Wilfried Mayer, Martin Schmiedecker, and Edgar R. Weippl. "I Have No Idea What I'm Doing" - On the Usability of Deploying HTTPS. In *26th USENIX Security Symposium, USENIX Security 2017*, 2017.

[39] Mika Latimer. Trace-weighted binary comparison for software update management, 2017.

[40] Peter Leo Gorski, Luigi Lo Iacono, Dominik Wermke, Christian Stransky, Sebastian Moeller, Yasemin Acar, and Sascha Fahl. Developers Deserve Security Warnings, Too On the Effect of Integrated Security Advice on Cryptographic API Misuse. 2018.

[41] Frank Li, Lisa Rogers, Arunesh Mathur, Nathan Malkin, and Marshini Chetty. Keepers of the machines: Examining how system administrators manage software updates.

In *Proceedings of the Fifteenth USENIX Conference on Usable Privacy and Security*, SOUPS'19, pages 273–288, Berkeley, CA, USA, 2019. USENIX Association.

[42] PONEMON INSTITUTE LLC. COSTS AND CONSEQUENCES OF GAPS IN VULNERABILITY RESPONSE, 2019.

[43] Geraldine Vache Marconato, Vincent Nicomette, and Mohamed Kaâniche. Security-related vulnerability life cycle analysis. In *7th International Conference on Risk and Security of Internet and Systems (CRiSIS-2012)*, pages 1–8. IEEE Computer Society, 2012.

[44] Arunesh Mathur, Josefine Engel, Sonam Sobti, Victoria Chang, and Marshini Chetty. "they keep coming back like zombies": Improving software updating interfaces. In *SOUPS*, pages 43–58, 2016.

[45] Arunesh Mathur, Nathan Malkin, Marian Harbach, Eyal Péer, and Serge Egelman. Quantifying users' beliefs about software updates. *CoRR*, abs/1805.04594, 2018.

[46] Huoy Min Khoo and Daniel Robey. Deciding to upgrade packaged software: a comparative case study of motives, contingencies and dependencies. *European Journal of Information Systems*, 16(5):555–567, 2007.

[47] Andreas Möller, Florian Michahelles, Stefan Diewald, Luis Roalter, and Matthias Kranz. Update behavior in app markets and security implications: A case study in google play. In *Research in the Large, LARGE 3.0: 21/09/2012-21/09/2012*, pages 3–6, 2012.

[48] James Nicholson, Lynne Coventry, and Pamela Briggs. Introducing the cybersurvival task: Assessing and addressing staff beliefs about effective cyber protection. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS 2018)*, pages 443–457. USENIX Association, 2018.

[49] Jon Oberheide, Evan Cooke, and Farnam Jahanian. If it ain't broke, don't fix it: Challenges and new directions for inferring the impact of software patches. In *HotOS*, 2009.

[50] Srivatsan Parthesarathy, Reiner Fink, Sean L Flynn, and Ray Sun. Software update notification, 2002. US Patent 6,353,926.

[51] Heike Pethe. *Internationale Migration hoch qualifizierter Arbeitskraefte*. DUV.

[52] Rahul Potharaju, Mizanur Rahman, and Bogdan Carbunar. A longitudinal study of google play. *IEEE Transactions on computational social systems*, 4(3):135–149, 2017.

[53] Elissa M Redmiles, Sean Kross, and Michelle L Mazurek. How i learned to be secure: a census-representative survey of security advice sources and behavior. In *Proceedings of the 2016 ACM SIGSAC Conference on Computer and Communications Security*, pages 666–677. ACM, 2016.

[54] Elissa M Redmiles, Amelia R Malone, and Michelle L Mazurek. I think they're trying to tell me something: Advice sources and selection for digital security. In *Security and Privacy (SP), 2016 IEEE Symposium on*, pages 272–288. IEEE, 2016.

[55] R. W. Reeder, I. Ion, and S. Consolvo. 152 simple steps to stay safe online: Security advice for non-tech-savvy users. *IEEE Security & Privacy*, 15(5):55–64, 2017.

[56] Armin Sarabi, Ziyun Zhu, Chaowei Xiao, Mingyan Liu, and Tudor Dumitraş. Patch me if you can: A study on the effects of individual user behavior on the end-host vulnerability state. In *International Conference on Passive and Active Network Measurement*, pages 113–125. Springer, 2017.

[57] Symantec. Internet Security Threat Report. *Network Security*, 21, 2016.

[58] Yuan Tian, Bin Liu, Weisi Dai, Lorrie Faith Cranor, and Blase Ur. Study on user's attitude and behavior towards android application update notification. *Usenix, Menlo Park, CA*, 2014.

[59] Yuan Tian, Bin Liu, Weisi Dai, Blase Ur, Patrick Tague, and Lorrie Faith Cranor. Supporting privacy-conscious app update decisions with user reviews. In *Proceedings of the 5th Annual ACM CCS Workshop on Security and Privacy in Smartphones and Mobile Devices*, pages 51–61. ACM, 2015.

[60] Christian Tiefenau, Emanuel von Zezschwitz, Maximilian Häring, Katharina Krombholz, and Matthew Smith. A usability evaluation of let's encrypt and certbot: Usable security done right. In *Proceedings of the 2019 ACM SIGSAC Conference on Computer and Communications Security*, CCS '19, pages 1971–1988, New York, NY, USA, 2019. ACM.

[61] Martin Ukrop, Lydia Kraus, Vashek Matyas, and Heider Ahmad Mutleq Wahsheh. Will you trust this tls certificate? perceptions of people working in it. In *35rd Annual Computer Security Applications Conference (ACSAC'2019)*. ACM, 2019.

[62] 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, San Jose, CA, USA, May 7-12, 2016*, pages 3215–3226, 2016.

[63] 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. ACM, 2014.

[64] Francesco Vitale, Joanna McGrenere, Aurélien Tabard, Michel Beaudouin-Lafon, and Wendy E. Mackay. High costs and small benefits: A field study of how users experience operating system upgrades. In *Proceedings of the 2017 CHI Conference on Human Factors in Computing Systems*, CHI '17, pages 4242–4253, New York, NY, USA, 2017. ACM.

[65] Rick Wash, Emilee Rader, Kami Vaniea, and Michelle Rizor. Out of the Loop: How Automated Software Updates Cause Unintended Security Consequences. In *10th Symposium On Usable Privacy and Security (SOUPS 2014)*, pages 89–104, Menlo Park, CA, 2014. USENIX Association.

[66] F.J. Wertz, Kathy Charmaz, L.M. McMullen, Ruthellen Josselson, R. Anderson, and Emalinda McSpadden. *Five Ways of Doing Qualitative Analysis: Phenomenological Psychology, Grounded Theory, Discourse Analysis, Narrative Research, and Intuitive Inquiry*. 01 2011.

Appendix

A Questionnaire

Information & Consent

Hello, we're Usable Security researchers from BLINDED and our mission is to make your challenges with system updates easier. As a first step, we need to understand your experiences and struggles with software updates in a corporate environment. We conducted interviews with seven colleagues of you and condensed interesting themes. This short questionnaire will take about 10 minutes to answer . We know that your time is precious, which is why every tenth participant gets a 3D-print of a model of her/his choice (max. 3x3x3cm and a reasonable model). If you are interested in this form of compensation just leave us your email address in the commentary field at the end. This email address will be stored separately from your answers and will only be used to communicate about your compensation. Please read all questions and instructions carefully. All of your answers will be checked, and your survey may be rejected in the case of inconsistent answers. Your data will be collected and processed in anonymized form, so that no connection to your person can be made. You can stop participating in this study at any time. If you have any questions please contact us via email.

*1. I have read and understood the information provided above and consent to take part in this study.

- I consent
- I do not consent

Demographics & General

*2. How old are you?
Text-input field
3. What ist your gender?
Text-input field
4. In what country do you work?
Text-input field
*5. For how many years have you worked as a professional system administrator?
Text-input field

Job information

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. Instead, if you do not currently work as an administrator, please answer these questions about the last company at which you worked as an administrator.

6. Is this company an IT company (software/hardware development, hosting, ISP, ...)?

- Yes
- No
- Other (please specify): *Text-input field*

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

- My primary responsibility was system administration
- My primary responsibility was not system administration, but I spent at least 20% of my time on system administration
- My primary responsibility was not system administration, but I spent between 1% and 19% of my time on system administration
- 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?
Text-input field
9. What is your main task as a system administrator? If it is the same as in the previous answer, please answer: same.
Text-input field
10. What kind of systems do you administer?

- Clients (e.g. workstations)
- Servers
- Mobile Clients (eg. tablet, smartphone)
- Other (please specify): *Text-input field*

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

- less than 10 employees
- up to 50 employees
- up to 250 employees
- more than 250 employees

12. Do you work in a team?

- Yes, as a team leader
- Yes, as a team member
- No
- Other (please specify): *Text-input field*

*13. What kind of job related education did you receive? (e.g. training, certificate, university)
Text-input field
14. Which of the following statements best describes the security-related training you have received concerning system administration?

- I received security-related training for system administration at that company
- I did not receive security-related training for system administration at that company, but I have received such training at a previous company or school
- I have never received security-related training for system administration

Update Process

Please be reminded that we do not collect or store identifying information. In the following we are interested in your honest opinion.
15. Among all software updates you install for operating systems or any other software running on systems, approximately what percentage do you estimate are **security** updates?
Slider [0-100]
16. Within your job as a system administrator, how much effort does it take you to keep the software on your systems up-to-date?
7-point Likert scale from "1 - Nearly none" to "7 - Nearly all my capacity"
17. What pre-deployment steps do you take before installing an update on a live system?

- We install it on a test system.
- We install it on a small number of production systems before deploying it to all systems or to everyone.
- We install it directly on all production systems.
- Other (please specify): *Text-input field*

18. What is the share of security related updates in relation to all updates (in %)?
Slider [0-100]
19. Which of the following statements best describe the update process in the company?

- There is a written document, that formally describes the steps in the update process.
- There is no written document but an informal guideline that is followed in the update process.
- There is no defined update process.

20. What is the typical time-span between the release of an update to the installation in a normal update process?
Text-input field
*21. Please indicate how often the following situations occur:
Table of the following questions, with a 6-point Likert scale from "1 - Never" to "5 - Always" and the option "Not sure", per question.

- I feel that I am not sufficiently trained as an administrator.
- I think of work- related consequences when doing tasks that have, in case of a failure, an impact on my company (e.g. downtime of a service that everyone uses).
- I feel personally responsible for keeping the software on my systems up-to-date.

22. Please indicate how often the following situations occur:
Table of the following questions, with a 6-point Likert scale from "1 - Never" to "5 - Always" and the option "Not sure", per question.

- Stability considerations hinder the installation of an update.
- Risk considerations hinder the installation of an update.
- Performance considerations hinder the installation of an update.
- Priority/time considerations hinder the installation of an update.

- Software updates are prevented because of other software (e.g. dependencies).

23. Please indicate how often the following situations occur:
Table of the following questions, with a 6-point Likert scale from "1 - Never" to "5 - Always" and the option "Not sure", per question.

- System stability considerations are irrelevant to the installation of an update.
- The risk of breaking dependencies hinder the installation of an update.
- A patch that is known to introduce errors hinder the installation of an update.
- Downtimes caused by the update process hinder the installation of an update.
- Lack of information about the changes an update introduced hinder the installation of an update
- Lack of education and knowledge hinder the installation of an update.

24. Please indicate how much you would agree/disagree with the statements.
Table of the following questions, with a 7-point Likert scale from "1 - Strongly disagree" to "4 - Undecided" to "7 - Strongly agree", per question.

- Deploying security updates in a timely manner is important.
- Post-installation problems in a live system are only a minor concern because they don't happen frequently.
- Users often install software without the knowledge of the administrator.

25. Who makes the decision whether to update or not?

- My team.
- Myself.
- My colleague(s).
- My supervisor.
- None of the above, please specify: *Text-input field*

26. Please indicate how often the following situations occur:
Table of the following questions, with a 6-point Likert scale from "1 - Never" to "5 - Always" and the option "Not sure", per question.

- I feel sufficiently trained as an administrator.
- I can oversee the impact an update would have on our systems.
- I can oversee the impact of a failed update on our system.
- I can oversee the security impact of updates on our systems.

Source and Tools

*27. What sources do you use to get information about current system updates?

- Online publications/news (e.g. cnet.com, Hacker News, heise,...)
- Update management software
- (Software) Publisher newsletters
- External services (e.g. a company that is contracted to inform you)
- Mailing lists
- My users
- Other (please specify): *Text-input field*

*28. What ist your main source to get information about current system updates?

- Online publications/news (e.g. cnet.com, Hacker News, heise, ...)
- Update management software
- (Software) Publisher newsletters
- External services (e.g. a company that is contracted to inform you)
- Mailing lists
- My users
- Other (please specify): *Text-input field*

29. Please explain your previous answer:
Text-input field

Thank you!

30. What do you think are the biggest obstacles in the update process?

Text-input field

31. Thank you for your participation! If you have any further comments for us: Don't hesitate to use the textbox!

Text-input field

32 . If you are interested in the 3D model print just leave your email in this field. We will only use this mail for the communication and will not link it to your answers.

Text-input field

B Interview Guidelines

Questions to explore

1. What does the update process look like?
2. What obstacles are there?
3. Who is involved?
4. What is his/her personal experience and assessment?

Introduction

1. How long has he/she done the job? What is the training? What is he/she doing on a daily basis?
2. What are the systems?
3. Does he/she work in a team?
4. What is the scope of his/her actions?
5. What tools are used?

General update process (or a specific update story)

1. How does he/she come in contact with updates?
2. What is the time frame and the process?
3. What tools are used?
4. Who is involved?
5. Where does the information come from?

(Optional) A second story

1. How does he/she come in contact with updates?
2. What is the time frame and the process?
3. What are the tools?
4. Who is involved?
5. Where does the information come from?

End

1. Do they have a fixed update policy?
2. Are there any feelings connected to new updates or the installation?
3. Is he/she aware of potential impacts of not installed update/failures of the installation? (Are there stories?)
4. Are there wishes concerning the process/tools?
5. Questionnaire

C Demographics

Survey demographic data

n	**67**	
Gender	1	Female
	58	Male
	3	Other
	5	Not specified
Location	19	North America
	41	Europe
	7	Rest of the world
Age	**22 – 55**	
Statistics	$md = 34, mn = 34.5, sd = 7.8$	
Experience	**0.1– 30.0** years	
Statistics	$md = 10.0, mn = 11.1, sd = 7.0$	
Company	34	IT-related
	29	Non IT-related
	4	Other
Company Size	4	≤ 10
	15	$10 < x \leq 50$
	15	$50 < x \leq 250$
	33	> 250
Role	50	Full-time admin
	11	Not primary, but $> 20\%$ of time
	6	Not primary, but $< 20\%$ of time
Administered Systems	28	Clients
	63	Servers
	14	Mobile
	13	Other

Table 6: Demographic data from the online survey.

Interview demographic data

Pseudonym	Gender	Position/Task	Age	Exp. (Years)	Team size	Supervised Machines
Markus	M	Administrator	25–35	6	7	300–350 clients, 150 virtual servers
Lorenz	M	Update management	25–35	2	n/a	5 servers
Cyril	M	Administrator	25–35	6	15	10,000 virtual, ca. 100 physical
Milan	M	Help desk	25–35	2.5	12	600 clients, number of servers
Zelko	M	Administrator	25–35	10	2	16 physical, 35 virtual, 80 clients
Alexander	M	Update management	> 35	23	5	26 physical, 170 instances
Julian	M	Management	> 35	29	20	n/a

Table 7: Interview participants.