Evolution of Password Expiry in Companies: Measuring the Adoption of Recommendations by the German Federal Office for Information Security

Eva Gerlitz
Fraunhofer FKIE

Maximilian Häring
University of Bonn

Matthew Smith
University of Bonn, Fraunhofer FKIE

Christian Tiefenau
University of Bonn

Abstract

In 2020, the German Federal Office for Information Security (BSI) updated its Password composition policy (PCP) guidelines for companies. This included the removal of password expiry, which research scholars have been discussing for at least 13 years. To analyze how the usage of password expiry in companies evolved, we conducted a study that surveyed German companies three times: eight months ($n = 52$), two years ($n = 63$), and three years ($n = 80$) after these changed recommendations. We compared our results to data gathered shortly before the change in 2019. We recruited participants via the BSI newsletter and found that 45% of the participants said their companies still use password expiry in 2023. The two main arguments were a) to increase security and b) because some stakeholders still required these regular changes. We discuss the given reasons and offer suggestions for research and guiding institutions.

1 Introduction

Password composition policies (PCPs) aim to increase account security. Yet, research has shown that individuals often devise strategies to deal with PCPs to make them less unpleasant, resulting in insecure passwords [26, 52]. One specific element of PCPs that leads to user frustration while not improving the strength of passwords much is password expiry, which forces users to choose a new password on a regular basis [26, 46, 55]. The removal of this requirement has been discussed by academic research for at least 13 years now [28], but has not been fully implemented by the industry [22, 42].

USENIX Symposium on Usable Privacy and Security (SOUPS) 2023.
August 6–8, 2023, Anaheim, CA, USA

National institutions, such as the National Institute of Standards and Technology (NIST) in the United States of America or the Federal Office for Information Security (BSI) in Germany, are possible facilitators in transferring academic findings into industry practice. These institutions offer recommendations concerning authentication and password policies in particular. Regarding password expiry, NIST removed its suggestion to enforce a regular password change in 2016, and the German BSI followed in 2020.

To understand at what speed such a changed recommendation is implemented in the industry, and especially what problems hinder adoption, we conducted three surveys (2020, 2022, 2023) with German companies after the BSI changed its recommendations. Our survey was based on that of Gerlitz et al. [22], who surveyed German companies in 2019, just before the change mentioned above.

We surveyed the authentication system in use, including detailed questions about the password policy, especially password expiry. We recruited our participants via the BSI newsletter, thus, focusing on companies likely interested in IT security topics.

We found that the number of participants whose companies use a regular password expiry decreased in a statistically significant way from 2019 to 2023. But with 45%, the number of participants whose companies use it is still high. Several of those participants whose companies still use password expiry stated that it is used to increase security, because they do not have the capability to implement the suggested alternative mechanisms as recommended by the BSI, or because someone still requested the change. We discuss these reasons and their implications and offer recommendations for future work and national institutions.

Summarized, our key contributions are:

- We document the progression of authentication processes (PCPs and alternative mechanisms) in German companies over the course of 3.5 years.
- We present reasons why companies do not or cannot comply with the recommendations regarding password

expiry and alternative checks for account compromise.

- We offer suggestions and recommendations for researchers and national institutions.

2 Related Works

In this section, we summarize the published knowledge about the current state of authentication on websites and in companies. We present research that focused on the basis for deciding on these authentication systems and PCPs, and then give a short overview of current academic advice on how PCPs should look like and summarize the current guidelines of NIST and the BSI. We conclude by presenting areas in IT security for which the best practice has changed at some point in time to understand the pace at which such changes can be expected to be implemented.

2.1 Status of Authentication and Basis for Decision

In this section, we look at the current state of authentication in companies and websites and present a paper that looked into the decision process on PCPs.

In 2019, Gerlitz et al. [22] surveyed 83 participants responsible for the authentication process in companies at the time of the study. The authors sought details of their authentication system, such as the type of methods employees can use to log in to their accounts and the PCP in use. The authors found that all companies allowed or demanded passwords for authentication. Most companies specified a minimum length, required specific character classes, and used password expiry for employee passwords. However, when looking at the details of these three components, the actual implementation varied. The most common policy was used by seven companies and required at least eight characters for the password, at least three character classes, and a password expiry of 90 days. Only two participants explicitly mentioned not forcing their employees to change their passwords regularly. Back then, the BSI still recommended password expiry. We build upon this work by replicating the study up to three years later and comparing the results.

In 2022, Hypr, a company aiming for passwordless authentication, conducted interviews with 500 IT decision-makers within financial services organizations in Europe and the United States of America. They found that 32% use 2FA for their employees, while 22% use only the username and password [27].

Research has also looked into password policies on websites and compared them to recommendations by scientists and official institutions. At the beginning of 2019, Gautam et al. [20] extracted and analyzed the password composition policies of 270 websites with the highest ranks in ten different countries. They compared the policies to the recommendations of NIST and found that only around 40% followed the recommended minimum length of 8 or more characters, while more than 70% had an unnecessary maximum length requirement. Two-thirds did not enforce certain character classes and thus followed the recommendations.

Lee et al. [33] analyzed 120 of the most popular websites in 2021 and compared the password policies to current best practices from academia: blocking common passwords, requiring specific character classes, and using a password meter to provide feedback on the security of a password. They found that 60% of the websites do not prevent the usage of the most common passwords at all, and a further 15% seem to use a very limited blocklist, thus still allowing many easy-to-guess and leaked passwords. Contrary to recommendations, 45% of the websites required specific character classes. Only 19% used a password meter of any sort. Interestingly, the authors capture 73 distinct password policies among the 120 websites.

Another paper closely related to our study is that of Sahin et al. [42]. They interviewed eleven website administrators to understand what considerations impact the PCPs they employ and what challenges they face when doing so. The authors found that administrators often face design challenges, competing interests, and deployment challenges. We build upon their work by a) recruiting a larger sample and b) focusing on security professionals within a company. In a professional context, accounts not only hold personal information about a user but might also give access to sensitive company internals. We believe the behavior of decision makers might be influenced by the fact that not only the company's reputation is at stake but also company secrets. This way, it is possible to compare issues in different sectors.

2.2 Current Advice on Password Components

Over the last few years, several researchers have experimented with different elements often seen in password policies, trying to understand their implications on usability and security [25, 30, 45, 49]. Currently, the best combination seems to be one of a minimum length requirement combined with a minimum strength requirement (policies that require the password to exceed a strength threshold) or, if the latter is not possible, a carefully configured blocklist [49].

For a long time, it was recommended that users change their passwords regularly for two reasons: first, if the passwords were ever leaked, chances were high that the list was already outdated when an attacker got access to it. Second, attackers would need more time or computing power to brute force passwords before they were changed. For the latter, 90 days were often seen as a reasonable trade-off that would make it impossible for attackers to guess the passwords in time but still be usable enough for users [48].

The usability part has since then been studied several times, finding that users have trouble recalling new passwords and

find forced password updates annoying [9, 26, 28, 46].

Apart from usability, studies also show that password expiry does not seem to offer the security benefit it was thought to have, and many people simply modify the accounts' current password or reuse a password from another account [8, 26, 46, 55].

While several official recommendations included a regular password change in the past, this has changed now. Instead, other mechanisms should be implemented that check for a compromise, as summarized in the next section.

2.3 Institutional Recommendations Regarding Password Composition Policies

In Germany, where our survey was sent out, the BSI "is the National Security Authority and the chief architect of secure digitalisation in Germany" [17]. Once a year, it publishes an updated version of its IT-Grundschutz Compendium [14], which "offers a systematic approach to information security that is compatible with ISO/IEC 27001" [14]. The BSI additionally hands out implementation hints for some subsections, e.g., for identity and access management, including authentication [16]. Regarding PCPs, the guidelines in the compendium are quite vague and state that "Passwords MUST be sufficiently complex so that they are difficult to guess. Passwords MUST NOT be so complex that users cannot utilise them regularly with a reasonable amount of effort. [15][1]" The implementation hints are more specific and recommend not using words from the personal or work environment and comparing the passwords to lists of leaked passwords. It also suggests combining complexity and length requirements (e.g., 8-12 characters + 4 character classes or 20-25 characters + two character classes).

While in 2019, the compendium included a passage stating "The passwords SHOULD be changed at appropriate intervals" [13], this has changed at the beginning of 2020. Since then, users should only be prompted "to change their passwords with a valid reason. Changes based on the passage of time alone SHOULD be avoided. [15]" Instead, mechanisms must be implemented to detect compromised passwords, e.g., detecting parallel logins from different systems or locations. Only in case these alternative mechanisms cannot be implemented should a regular change be considered [16].

In 2020, the BSI also changed their wording concerning complexity requirements (from "[the organization] MUST specify that only passwords of sufficient length and complexity are to be used [13]" to "Passwords MUST be sufficiently complex so that they are difficult to guess. [15]"), and added a paragraph about two-factor authentication ("[the organization] MUST consider whether passwords are to be used as the sole authentication method, or whether other authentication features or methods may be used in addition to or instead of passwords [15]").

Companies do not have any legal obligation to apply the IT-Grundschutz. Yet, it is one way to implement ISO 27001 in order to get certified [14]. There are several reasons for companies to do this, e.g., reputation, risk calculation, and compliance. Certification is valid for three years, while there are yearly audits [18]. Therefore, changes to the compendium should be implemented in the industry at the latest after three years.

The US American equivalent of the BSI, NIST, recommends that user-chosen passwords should at least be eight characters long and shall be compared "against a list that contains values known to be commonly used, expected, or compromised" [24], e.g., passwords from previous leaks, dictionary words, repetitive or sequential characters, and context-specific words. Since 2016, the recommendations have advised against requiring periodical changes [23]. Instead, verifiers "SHALL implement controls to protect against online guessing attacks" [24], such as risked-based authentication using IP addresses, geolocation, and browser metadata.

2.4 Speed of Adopting Recommendations

After a recommendation is released by, e.g., institutions like NIST, or research, adoption takes time [3, 7, 11, 36] as the people in charge of implementing it are unaware of the recommendation [36], have no time [34, 50], or do not have the necessary knowhow [36]. In many IT security-related topics, technology has changed over the years, and with it, the knowledge of what is secure or usable secure.

To understand how fast the knowledge about best practices takes to reach those in charge of using this information, we highlight this process for two examples: deprecated hashing algorithms and HTTPS.

2.4.1 Deprecated Hashing Algorithms

One security-related area that encounters constant changes in recommendations is hashing. Algorithms get deprecated because they were found to be broken [47] or key lengths have to be increased due to the rising computing power [37]. In 2008, it became clear that MD5 was broken [47] and should thus not be used for storing passwords. Despite this being public knowledge for more than ten years now, some developers are still unaware of this fact. In a 2019 study, Naiakshina et al. [36] asked freelance developers to implement the password storage functionality for a website. Over 20% of the participants used MD5 (18% even stored the passwords in plain text/Base64 encoded). Danilova et al. [10] asked participants to review the program code and included insecure password storage (such as MD5). Only 36% pointed out this problem, and one even mentioned MD5 as a hash algorithm to improve

[1] At the time of writing, the English version of the 2023 version has not been published. The quotes are taken from the English translation of the compendium from 2021. The quoted passages of both German versions are identical.

security. Ntantogian et al. [38] investigated the default password hashing scheme of 25 content management systems and web application frameworks in 2018. MD5 was the default hashing scheme for around 27% of the analyzed CMS. This problem can also be seen when looking at the database of "Have I been pwned" [3]: around 30% of the datasets that included passwords and were breached in 2021 or 2022 used MD5 for password hashing; in 2020, it was 20%.

2.4.2 HTTPS

In 2015, the W3C Technical Architecture Group encouraged the use of HTTPS instead of HTTP [53]. At this point, only around 32% of all pages visited by Firefox browsers supported HTTPS. Around that time, Let's Encrypt was founded and, for the first time, enabled server owners to acquire TLS certificates for free [44]. The updated recommendations, in combination with the easier access to certificates, led to the fact that, in 2022, seven years later, the percentage of servers that supported HTTPS grew to nearly 80% [11], and most (79,8%) of the web servers specifically allow only HTTPS-connections [54].

Even though 80% is the majority, this, in turn, also means that one-fifth of the servers still do not support TLS-secured connections. This can be due to compatibility reasons or an administrator's incorrect mental model of the technology [7, 31].

3 Methodology

We conducted three online surveys recruiting through the BSI mailing list, one in October and November 2020, the second in February and March 2022, and the third in January 2023. The questionnaire and data for 2019 were provided by Gerlitz et al. [22]. For easier readability, we will refer to the surveys and datasets as follows: PCP19 for data presented by Gerlitz et al. [22] that was conducted in 2019, PCP20 for data collected at the end of 2020, and PCP22 and PCP23 for data collected at the beginning of 2022 and 2023.

3.1 Research Questions

The following research questions and hypotheses guide our analysis:

- **RQ1**: How did the authentication system within companies change over the years?
- **RQ2**: How did the usage of a maximum age develop over time after the BSI changed its recommendations in 2020? For this, we had the following hypotheses:
  - ***H1***. *The total number of companies using password expiry decreased from 2019 to 2023.* This hypothesis is built on the fact that the BSI dropped their recommendation for using a regular password expiry. Only in case alternative mechanisms, such as checking for parallel logins from different systems or locations, cannot be implemented should a regular forced change be considered. We performed one Fisher's exact test, including all participants who made a statement about their password expiry.
  - ***H2***. *For companies that use password expiry: The time range after which a password is required to be changed increased between 2019 and 2023.* We assumed that not all companies could implement alternative checks to remove password expiry entirely. We hypothesized that even if a company cannot remove the password expiry requirement, it would adapt to the BSI recommendation to increase the time intervals between enforced changes. We performed one Wilcoxon rank-sum test and included all participants who used a password expiry and also mentioned a specific time range.
  - ***H3-6***: *Company characteristics or the use of certain policy elements influence whether the companies use a password expiry in 2023.* Factors like time, money, or flexibility could influence adopting the changed recommendations in a company. We, therefore, performed four Fisher's exact tests based on different company characteristics like their size (H3) or whether it belongs to critical infrastructure[2] (H4). We also tested if the usage of checks for password compromises (H5) or if the last change of password policies was before or after 2020 (H6) influenced password expiry usage.
- **RQ3**: What reasons do participants have to still use password expiry?
- **RQ4**: How do companies check for compromised accounts, or what hinders them from implementing such checks?

3.2 Survey Design

The survey consisted of five blocks, as presented in the following paragraphs. Each questionnaire differed slightly from the one before, adapting to new situations and gathering further insights. The survey is given in Appendix A, including annotations highlighting differences between the years.

[2] "Critical infrastructures are organizations or facilities with important significance for the state community, the failure or impairment of which would result in lasting supply bottlenecks, significant disruptions to public safety or other dramatic consequences." Translated from the Federal Office of Civil Protection and Disaster Assistance [39].

Account per Employee and Login The participants were asked whether their company makes use of a centrally-managed account for each employee (Q1[3]), what services it can be used for (Q3a), what authentication methods can be used (Q3b, Q3c), and if two-factor authentication is possible (Q4).

Passwords The password part was shown to all participants who indicated the employee account is secured with passwords. If a company did not have such an account, all questions concerned email passwords. We asked the participants for their password policy (and encouraged them to provide a copy of it, Q6) and for elements allowed or forbidden in the password (Q16, Q17). The participants could indicate how the policies impact the security and usability of the overall authentication system and how often problems occur (Q26 - Q28). Extending the original questionnaire of Gerlitz et al., we also asked the participants whether there are additional specifications for particular user groups (Q18) and when and why the policy was changed last (Q22-Q25). Additionally, the changes in the BSI recommendations were brought up, and the participants were asked whether they looked into the changes and adapted their policy based on them (Q29, Q30). In 2023, we added further open-ended questions to understand if and why a company uses password expiry and how accounts are checked against a compromise (Q8 - Q14).

Biometric Authentication and Hardware Token All participants who indicated that the employee account could be unlocked using biometric authentication or a hardware token were asked for details (which biometric authentication is used (Q34) and whether the token supports FIDO2[4] (Q39)). Similar to the password part, they were asked for their perceived influence of the biometric authentication and token on the security and usability of the authentication system and the frequency of problems (Q35-Q37, Q40-Q42).

Passwordless We added one open-ended question in PCP23 asking for the general sentiments towards passwordless authentication (Q44).

Demographics In the final part, the participants were asked for details about themselves and the company they work for. In PCP19, this included the total number of employees working for the company (Q52) and the number of employees working on IT security topics full-time (Q54). From PCP20 on, the participants were also asked for the sector (Q47), the country the headquarters of the company is located (Q51), whether it can be seen as Critical Infrastructure (Q48), as well as the position of the participant (Q55), and their years of experience (Q56). In all years, the participants indicated their satisfaction with the overall authentication system (Q59). From PCP20 on, they could also suggest that they participated in the survey the previous year (Q58), which only two people reported in PCP22.

[3]The notation Qx references to the corresponding question in our questionnaire.

[4]"Authentication standards based on public key cryptography for authentication" [1]

3.3 Ethics

Our university's Research Ethics Board approved the study, and we adhered to the German data protection laws and the GDPR in the EU. Participants had to consent to their data being used for research before the study began, and we included the option "I don't want to state" for all questions. Participants could drop out at any point in time. The study included multiple open-ended questions. If a participant's answer contained deanonymizing information (e.g., their company name), we deleted it before we continued the analysis.

3.4 Recruitment and Demographics

Participants were recruited through the official newsletter sent by the BSI. Everyone responsible for authentication in a company was invited, and participation was voluntary and not compensated. In this, we followed the original approach by Gerlitz et al. [22], who recruited participants in the same way between September and October 2019. In the latest run in 2023, which also included the highest number of questions, participants took a median time of 16 minutes to finish the survey.

Table 4 and Table 5 in Appendix B show the participants' demographics and their company characteristics.

3.5 Data Quality

We eliminated all incomplete answers from our analysis, as well as one participant whose answers to open-ended questions indicated that they did not understand the questions correctly in PCP19. We further removed the response of one participant whose self-reported role does not clearly include being able to work on the company's authentication in the dataset of PCP20.

Gerlitz et al. [22] not only recruited over the newsletter but also used additional channels to distribute their survey. When comparing the results, we included only those answers by participants recruited through the newsletter for internal validity. To keep the samples as similar as possible, we included only those companies using employee accounts in our analysis. After this filtering, the datasets consisted of 54 (PCP19), 52 (PCP20), 63 (PCP22), and 80 (PCP23) answers. Due to the slightly different filtering, we included fewer participants in our comparison than reported by Gerlitz et al. [22], who reported the data of 83 participants.

All numbers for this filtering process are given in Table 3 in Appendix B.

3.6 Data Analysis

Over the years, the questions in the survey slightly changed. However, all questions for which we compared the results between the years were identical.

3.6.1 Coding

One of the open-ended questions was identical in all years and asked for the password composition policy in use (Q6). Answers for these questions from PCP20 and PCP22 were coded by two authors using the code book that Gerlitz et al. created for PCP19. For this step, we included all the complete answers that we received and merged answers from both years, such that during the coding process, the year in which the answer was given was not known to the coders.

First, both authors coded 31 answers to check for a similar understanding of the code book and then coded additional 31 responses to calculate the inter-coder agreement. After that, each coder then coded half of the answers.

To date, most research on password composition policies has focused on minimum length, password expiry, the number of required character classes (complexity), as well as blocklists (see Section 2.2). To gain a complete overview of these components in the PCPs described above, we decided to code the participants' answers that did not mention their minimum length, password expiry, complexity, or a blocklist as 'not mentioned.'

We had 29 codes and used Recal2 [19] to calculate the inter-coder reliability. For all codes, the reliability lies in the range of (0.47, 1) with a weighted mean of 0.98. Table 6 in Appendix B shows the codes, their occurrences, and the code-specific ICR.

Since we noticed that the answers given for Q6 were very straightforward and did not leave much room for interpretation, the other open-ended responses that we analyzed (Q6 of PCP23, Q8/Q12: Reason for using password expiry, and Q14: How do compromise checks happen or why are they not used of PCP23) were coded by one of the researchers. Two authors discussed all codebooks and answers that were ambiguous.

We proceeded the same way for answers given for the "other"-option in multiple-choice questions. All citations from these answers in this paper are translated from German.

3.7 Limitations

This work needs to be interpreted in light of the following limitations: Even though we recruited the participants through the BSI newsletter and clearly stated who the survey is aimed at, we cannot be sure that only the responsible employee took part. From PCP20 on, participants were asked what position they held. Except for one, all participants who specified their role indicated working in a position with detailed domain knowledge about the company's authentication system (see Table 5). Yet especially for bigger companies, we cannot rule out that only one member of the IT security team took part in the survey. We checked for duplicates in the company characteristics in combination with the given PCP but could not identify any identical entries.

All data are based on self-reports, and participants might have forgotten to include elements, especially for the password composition policy. We tried to counter this by asking them to copy and paste their policy.

Using the newsletter sent by the BSI for recruitment may have caused that in our samples, the participants are a) already interested in security topics and news and b) an even more interested subgroup, as those are more likely to read the study invitation and follow it. We discuss the possible implications in Section 5.3.

Over the years, the survey was adapted, and questions were added. This could have caused participants to be in slightly different states of mind when answering questions. However, we took care to include new questions only after similar questions were already asked and included page breaks.

The survey for PCP22 contained minor improvements mentioned above, as well as an additional question about the reason for the existence of a password expiry that was not recommended by the BSI anymore at this point. After the newsletter inviting participants for PCP22 was sent and 36 participants had already completed it, we noticed that the questionnaire for PCP20 was handed out by mistake that did not include the changes and the additional question. We still decided to switch to the improved survey since we were confident that the additional insights from the new questions outweighed the minimal risk of receiving different answers due to the slightly modified questions.

4 Results

In this section, we present the findings of our survey. The changes between the years of the used authentication systems within companies are presented in Section 4.1 (RQ1). The usages of password expiry (RQ2) are summarized in Section 4.2. In Section 4.3 (RQ3), we present the reasons participants gave for using a password expiry, and Section 4.4 (RQ4) summarizes how companies currently check whether accounts are compromised and what issues hinder them in implementing checks.

4.1 RQ1 - Evolution of Authentication Systems

This section considers the evolution of authentication methods and password composition policies between 2019 and 2023.

4.1.1 Possible Authentication Methods

Figure 1 shows the percentage of participants per year who stated that their company offers their employees to authenticate using passwords, biometric authentication, and hardware tokens, independent of their usage as the primary or secondary factor. The use of authentication methods apart from passwords has risen steadily over the last few years. In 2023 for the first time, two companies indicated that their company does not use passwords. All numbers can be found in Table 2 in Appendix B.

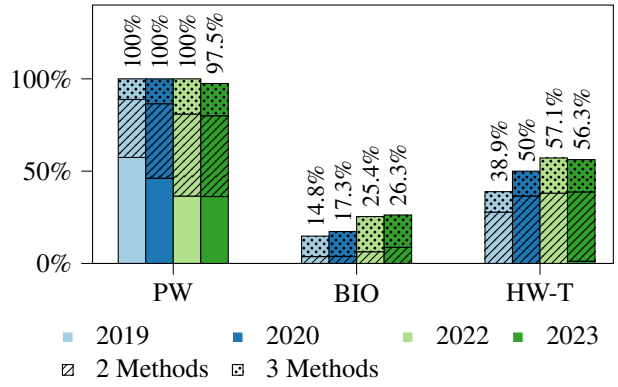

Figure 1: Percentage of participants that indicated that their company enables authentication using passwords (PW), biometric authentication (BIO), or hardware token (HW-T). Using authentication methods other than passwords rose steadily over the years. The bars also indicate the number of companies using one, two, or three authentication methods. Biometrics are seldom used as secondary factor alone.

If participants indicated that more than one authentication method could be used, they were asked whether these methods needed to be used in combination (two-factor authentication). Starting in PCP20, participants who mentioned only one method were additionally asked whether there is any possibility for two-factor authentication. The number of those requesting 2FA also increased, at least between 2019 and 2022: 22.2% of the companies that participated in 2019 required two-factor authentication – 32.7% did so in 2020, 55.6% in 2022, and 51.2% in 2023.

4.1.2 Usage of Password Components

Participants were asked to indicate their current password policy (Q6). This question text included the example, "e.g., at least x characters, new password needs to be selected after x days," and participants were encouraged to provide a copy of their policy. In PCP23, we also explicitly asked for password expiry in a separate question that was shown after a page break after Q6.

Figure 2 shows the development of the complexity, password expiry, and minimum length from PCP19 to PCP23. There is a slight increase in the number of participants who mentioned that their company requires all four character classes to be used in the passwords. While NIST advises against such complexity requirements, the BSI currently includes complexity requirements in their implementation hints (see Section 2.3).

The figures also show a trend towards longer passwords and larger time ranges before the passwords expire, e.g., the number of companies that require a password change every 90 days decreased from 33.3% in 2019 to 6.2% in 2023, while those who explicitly mentioned not using password expiry rose from 1.9% in 2019 to 22.5% in 2023. In 2023, 10.0% of the participants did not include any information about password expiry in the open-ended response but disclosed they actually use a password expiry in the question explicitly asking for it (Q11). We further explore the details of password expiry in Section 4.2. The concrete numbers of companies using a certain minimal length, complexity, and password expiry are shown in Table 6 in Appendix B.

We also looked at the most common combination of password expiry, a required minimum length, and complexity for each year and show the results in Table 1. The most common combination in PCP19 and PCP20 (minimum length of 8 characters, enforcing three character classes, and using a password expiry of 90 days) was not used by any participant in PCP23.

Summary for RQ1 From 2019 to 2023, the companies our participants worked for offered more authentication methods next to passwords, and the number of participants whose companies require 2FA rose by almost 20 percentage points. Looking at PCPs, it is now more common than in 2019 to require longer passwords (12 or even 14 characters) and to refrain from using password expiry.

4.2 RQ2 - Password Expiry

As detailed in Section 2.3, the BSI advises against a forced frequent change of passwords. Instead, companies should run analyses on whether a user account is compromised. This could, for example, be done by checking for parallel logins from several systems or locations. A regular change should only be considered if such checks are impossible.

While the development of the days after which a password change is required is given in the previous section, this section investigates H1 and H2, and we take a closer look at company characteristics that may indicate the use of password expiry (H3-6).

Since we wanted to dive deeper into the analysis of password expiration, we added an additional closed question about password expiry in PCP23 to double-check the open-ended general PCP question.[5] When comparing the numbers from

[5]We added a page break to ensure participants would not be influenced.

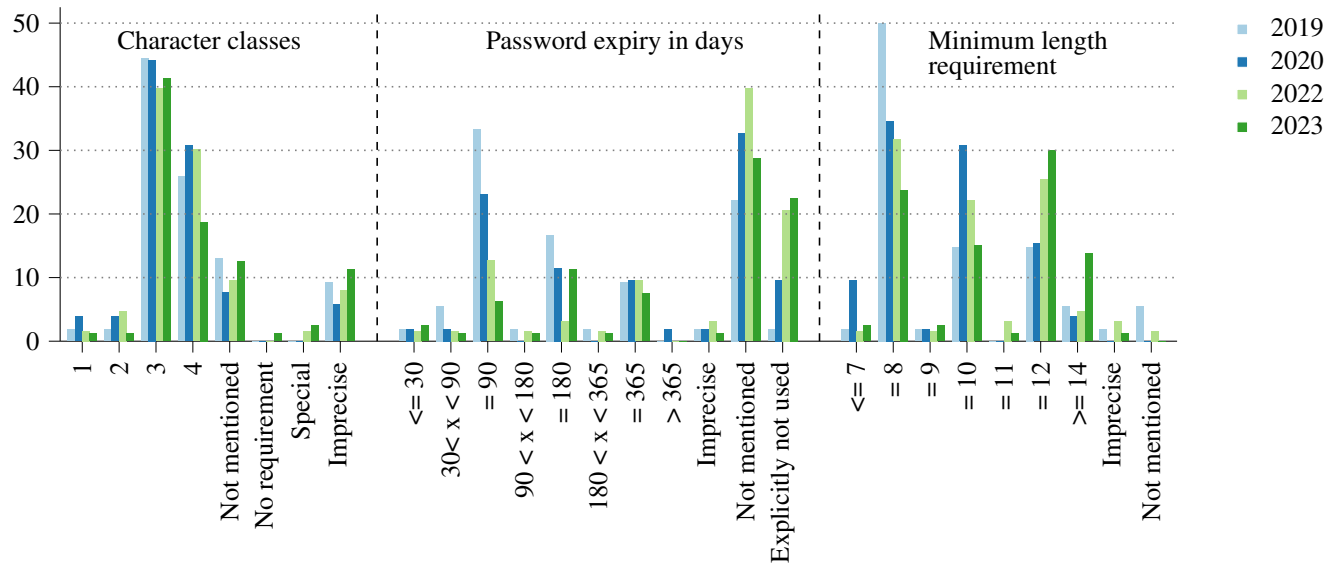

Figure 2: Overview of the required number of character classes that need to be covered in the user's passwords, number of days after which a user is requested to change their password (password expiry), and required minimum length in 2019, 2020, 2022, and 2023. Y-axis shows percentages. Answers from Q6. Findings: **1) Character classes:** Participants whose companies require at least three character classes either mentioned certain classes or allowed a password as long as any three classes were used. There are no big differences between the years. In their implementation hints, the BSI gives examples that include enforcing several character classes (see Section 2.3). **2) Password expiry:** The number of companies using password expiry of 90 or 180 days decreased from 2019 to 2023, and more participants explicitly mentioned not to use password expiry in 2022, following the BSI recommendations. **3) Minimum length:** Requiring passwords with at least 10, 12 or 14 characters is more common in 2023 than it was in 2019, where most PCPs asked for at least eight characters.

the closed question to the open-ended answers, we noticed that ten percentage points fewer participants mentioned password expiry in the open-ended question than in the closed question (35.0% vs. 45%). It is interesting to note that 10% did not think to mention password expiry when describing their policy.

While we cannot say this for sure, we think it is likely that there has been a similar amount of underreporting in the previous years. But to be on the safe side, when we compare PCP23 to previous years, we use only the open-ended data, so the comparisons are made based on the same measurement instrument, i.e., we only use the 35.0% that were captured the same way as in PCP19.

However, we believe 45% to be more accurate and use it wherever applicable.

4.2.1 RQ2 - H1

We hypothesized that the *total number of companies using password expiry decreased from 2019 to 2023.* To investigate this question, we performed two Fisher's exact tests based on answers given to Q6. The tests are based on slightly different assumptions: For the first one, we only included those participants who explicitly said something about their password expiry: either mentioning a time span or indicating they do not use one. In PCP23, 26.9% of those participants who did not mention a password expiry in the open-ended question (Q6) later stated one in the closed question specifically asking for it. The results show a statistically significant difference between the results from 2019 ($n_{exp19} = 39$, $n_{noexp19} = 1$) to 2023 ($n_{exp23} = 28$, $n_{noexp23} = 18$): $p_{(19,23)} = 0.00$, OR = 25.07.

For the second test, we included all participants and assumed that not mentioning expiry is the same as not having one. In PCP23, this was true for 73.1% of those who did not mention password expiry in Q6. This test also shows a statistically significant difference between the results from 2019 ($n_{exp19} = 39$, $n_{noexp19} = 13$) to 2023 ($n_{exp23} = 28$, $n_{noexp23} = 44$): $p_{(19,23)} = 0.00$, OR = 4.71.

This suggests that within three years after the change, there has been a shift towards the new recommendations.

4.2.2 RQ2 - H2

We further hypothesized that *for companies that use password expiry: The time range after which a password is required to be changed increased between 2019 and 2023.* For this analysis, we included only participants who used password expiry. We excluded all participants who gave no clear answer about the length of their password expiry (e.g., only stating that there is a password expiry but giving no numbers.) We

Expiry (days)	Min. Len	Complexity	2019	2020	2022	2023
90	8	3	5	4	3	0
90	8	4	4	3	1	0
90	10	3	3	1	1	0
180	8	3	3	0	0	2
180	8	4	1	3	0	1
Not mentioned	8	3	2	1	4	2
Not mentioned	8	4	3	3	3	2
Not mentioned	12	3	0	3	1	5
Not mentioned	12	4	2	2	6	2
Explicitly not	12	3	0	0	1	4

Table 1: Number of times a certain policy was mentioned in 2019, 2020, 2022, and 2023. The more participants mentioned their company uses a policy, the darker the cell is shaded. A PCP is included in this table if it appeared at least 3 times in at least one year. While the most common policies in 2019 included a password expiry, this trend has shifted in 2023, where the most commonly mentioned policies do either not mention regular password rotation or explicitly state not to use one.

performed a Wilcoxon rank-sum test for which we included 38 answers from 2019 and 27 from 2023. Figure 2 showed a trend towards fewer companies that enforce a password change after 90 or 180 days, and this theme was also picked up in the open-ended responses: "Jumping to unlimited passwords takes time because technical change and culture change take time. We went from 90 days to 1 year." Yet, the tests did not show a statistically significant result ($p_{(19,23)}$ = 0.131, $Z_{(19,23)}$ = -1.511).

4.2.3 RQ2 - H3-6

Finally, we were interested in whether *company characteristics or the use of certain policy elements influence whether the companies use a password expiry in 2023.* We conducted four Fisher's exact tests to analyze the impact of the following variables on the existence of a password expiry: company size (<500, >=500), critical infrastructure (no, yes), last policy change (before BSI changes, after BSI changes), and technical measures that check for account compromise (no, yes). We used data from the open-ended response (Q6) and the explicit question asking for password expiry (Q11) for these tests. Taken together, 45% of the participants mentioned that their company uses a password expiry in 2023.

After correcting the results using a Bonferroni-Holm correction, none of the tested factors remained to have a statistically significant impact on the existence of password expiry. The contingency table for all tests is given in Table 9 in Appendix B.

Summary for RQ2 Over 40% of the participants stated that their company still uses password expiry in 2023, although this is statistically significantly less than in 2019. None of the characteristics for which we tested differences in the use of password expiry showed a statistically significant result.

4.3 RQ3: Why do Companies Require a Regular Password Change?

Thirty-six participants in PCP23 and nine in PCP22 answered why their company uses password expiry.

Apart from this explicit question, some participants included a reason for using password expiry in their open response to Q6.

In the following, we present the most commonly mentioned themes. The coding table is given in Table 7 in Appendix B.

Increase Security In 2023, 17 participants said their company uses a password expiry for security reasons. Half of them stayed vague and stated "[password expiry] gives *some* security" or "improvement of password security." The remaining eight mentioned more specific reasons, e.g., "Because after a year, the risk of misuse of the PW through reuse with other, potentially corrupted services, is too great."

In 2022, two participants stated their company uses a password expiry to get rid of lost ($n = 1$) or leaked passwords where employees did not follow the recommended change after being notified about the leak ($n = 1$).

Still Demanded Another commonly mentioned reason was that someone or some regulation demands a password expiry. Four participants stated their CEO or internal policies require this regular change, "[...] contrary to the recommendation of the IT sec [department]" or because of "inertia in our security standards." Three participants mentioned that customers or the customers' compliance requires regular changes, and five participants mentioned official requirements, e.g., "Official (in my eyes outdated) requirements in handling officially classified data." The latter two reasons were also mentioned in previous years.

No Alternatives A small number of participants (Four in 2023, one in 2022) use password expiry because they have "No other method implemented yet" or because "there is currently no other technical solution." We look deeper into these alternatives in Section 4.4.

Best Practice Some participants (Two in 2023 and two in 2022) stated that password expiry is best practice or recommended by the BSI. One participant stated: "[We] consider it wrong not to change [the password] regularly." This was already a theme in 2022, so we asked in 2023 whether participants perceived a regular change as best practice before asking why password expiry was used. This question was affirmed by 23.1% of the PCP23 participants.

Currently Changing We also saw participants (One in 2023 and one in 2022) who stated they were currently in the

process of eliminating password expiry. One mentioned: "The auditor still has to be convinced."

4.4 RQ4: How do Companies Check for Compromised Accounts and What Hinders Them?

The BSI specifies that mechanisms must be implemented to detect compromised passwords (see Section 2.3). So, we were interested in the mechanisms companies use or whether they have problems implementing them. We included this question in the PCP23 survey, and 66 participants answered it. The coding table is shown in Table 8 in Appendix B.

Of those 66 answers, 36 participants said their companies use technical solutions to check for password or account compromises, whereas 25 do not. In three cases, the participants gave no clear answer, and in two cases, checks are not used consistently for all systems (e.g., used for SSO, but not for AD).

Those who use checks most often do so by checking against databases of leaked passwords ($n = 8$) or by using tools that check for anomalies within the system or during logins ($n = 16$).

The absence of technical checks was most often explained by missing resources (time, financial, or human resources) ($n = 7$), by structural and organizational issues ($n = 5$), or because the technical solution was not straightforward ($n = 9$). One participant mentioned a "conflict with the works council." Specific problems mentioned were that third-party tools are needed or behavior-based detection tests lead to several false positives in the past.

Three participants questioned the possibility of checking for compromises in general: "It is not clear to us how to check if a [password] is 100% not compromised."

Additional ($n = 2$) or alternatively ($n = 4$) to technical checks, some participants stated their companies encourage their employees to check for a compromise themselves.

Summary for RQ3 and RQ4 Companies still use password expiry in 2023, mainly to increase IT security or because another entity required it. Technical measures that check for account compromise were often not implemented because of missing resources.

5 Discussion

We conducted three surveys over three years to understand how password composition policies evolve. We found that companies now require passwords to have more characters than in 2019 and found significantly fewer participants whose companies rely on password expiry. When specifically asking for the reason for still using expiry in PCP23, we found IT security to be one of the leading explanations.

This section discusses the reasons why companies still use password expiry, draws connections to related work, and gives recommendations for future work and policymakers.

5.1 Password Expiry and IT Security

The BSI started advising against password expiry at the beginning of 2020. With this, they finally followed scientific work, a full decade after it showed the usability of password expiry to be a problem [9, 28, 46]. In our study, four participants explicitly mentioned that employees wrote passwords down when they had to change them regularly, and the company thus got rid of this requirement.

Nonetheless, in the latest survey run in 2023, still, 45% of the participants stated that their company forces regular password changes from their employees. Several of them (17) argued for an improvement in IT security, confirming the findings of Sahin et al. [42]. In the following, we discuss these reasons and evaluate whether this situation is problematic.

Compensation of Technical Issues We found cases where password expiry was used to compensate for other technical issues. One participant mentioned using expiry to get rid of old hashing algorithms, one referred to a maximum password length of eight that was set by the system, and a third explained that MFA was not yet implemented for all accounts. It can make sense to keep password expiry to bridge the time until new technologies are implemented (as mentioned in the latter example). However, accepting all the drawbacks that regular password changes bring because of a legacy system that itself can be a security risk seems like a missed opportunity: Instead of adopting to constraints of a system, system administrators could argue that they need a new and more secure system that can fulfill the updated recommendations. However, we must acknowledge that business constraints can make this difficult.

Initiate Password Development The most commonly used arguments for password expiry concerned initiating the development of passwords, i.e., making sure that a password is not in use anymore when an attacker gets access to it and reducing the problems that come with password reuse by, e.g., decoupling the employee account from private accounts for which the employee used the same password.

Both of those arguments sound reasonable in theory, especially as credential stuffing attacks (where an attacker tries to log into accounts by using passwords associated with that user in leaks) made up almost a third of all attacks across the Arkose Labs network [32] and more than 12 billion leaked login combinations are public by the time of writing in 2023 [3].

However, estimating the real security benefit of such changes is hard. Studies indicated that many individuals simply modify a previous password when being forced to change it [26, 55]. This makes it easy for an attacker to guess the new password if they have access to a previous one, especially

when considering advanced attacks where not only the password that is included in leaks is used but also variations of it (e.g., following the approach by Pal et al. [40]). Yet, simple attacks that use exactly the same password as found in leaks might be prevented.

Further, many attacks, e.g., data theft, do not require much time, and according to a study by Agari, 50% of the credentials were used within twelve hours after they were compromised [6]; thus, requiring password changes every month will likely not prevent many attacks.

If persistence is the goal, attackers will attempt to create further footholds so that losing access to the first account does not lock them out.

And while the results from a survey study by Habib et al. [26] indicate that users do not seem to choose weaker passwords when updating them compared to creating new ones, Adams and Sasse [5] argue that a regular password change could lead users to create very simple passwords. On a larger scale, it is unclear whether users' strategies for initially creating the password differ, depending on whether they know they will have to change it soon or can keep it for a longer period.

What is clear is that physical password handling differs depending on whether passwords need to be changed frequently or not: Habib et al. [26] saw a statistically significant increase in storing the main workplace password in the web browser when password expiry was in use. Depending on the details of this (usage of a browser password manager, behavior concerning device locking when leaving the desks, etc.), this might have a positive or negative impact on security. Similarly, if users are also more likely to write down their passwords on sticky notes, physical access to a workspace would be a problem. Yet, unobserved access to a workspace might come with several other risks anyway, such as being able to insert a physical key logger (even though this involves more planning than simply using the password from a sticky note).

Adding "Some" Security The uncertainty of how much security is actually added was also present in the answers, where participants associated password expiry with "*some* security". While it can be reasonable to use every opportunity, even the small ones, to increase IT security, people nowadays already have to deal with many security mechanisms in their work environment (e.g., authentication, secure messaging, physical access control). Removing those requirements that are very time-consuming [9], and can even be replaced by technical checks, thus seems like a good idea.

5.2 Further Reasons for Delayed PCP Updates

In this section, we discuss arguments for using password expiry apart from increasing IT security.

Alternative Mechanisms Cannot be Implemented One participant in 2022 mentioned that their company is not able to remove the requirement for a regular change because of "inadequate control mechanisms to detect compromise." In 2023, participants mentioned technical reasons, e.g., that third-party tools are needed, current tools lead to too many false positives, or that, in general, the implementation of such checks is "too complex."

This problem can also be seen in other security-related areas, such as deploying updates, where systems are not updated because of legacy software that is known to be incompatible with up-to-date environments [34, 50].

The area of these alternative mechanisms remains to be studied in more detail. Further reasons for some companies not being able to use checks that indicate a password compromise need to be identified. One paper that has already studied these alternative mechanisms was published by Markert et al. [35]. The authors studied administrators' understanding of risked-based authentication. They found that their participants struggled with the meaning of the given risk levels and the configuration interface in general.

Depending on further findings, it might be helpful if the BSI, or any institution with a similar influence, could publish additional information about the available alternatives and how they can be implemented. At the point of writing, the suggestions concerning alternative mechanisms in the current implementation hints are very vague: "For example, logging and the corresponding evaluation of log files can be used to determine whether there have been unusual accesses or hacking attempts. Special security products are also available for databases, operating systems, web servers, and other applications."[6]

Looking at the area of HTTPS, the increase in its usage was not only sparked by a changed recommendation but also because there was a new and very easy way to follow it (see 2.4).

Inertia Participants pointed to the necessity to follow requirements that still demand regular change, e.g., federal offices or the PCI (Payment Card Industry Data Security Standard). In some cases, internal security standards require the use. As pointed out in Section 2.4 and also mentioned by the participants, changes take time to reach every stakeholder, and one participant mentioned the word *inertia*.

The problem of contradictory guidelines can appear whenever multiple institutions publish different recommendations for the same topic. In these cases, administrators must decide which guidelines to follow or how to combine them.

No Knowledge About Change and Misconceptions Many technical news portals, e.g., [41, 43] and newspapers, e.g., [12, 29] reported the removal of password expiry in the new BSI

[6] Translated from the German implementation hints [16]

recommendations. However, we still encountered one participant who stated that this is recommended by the BSI. In 2020, 25% of the participants mentioned being unaware of the BSI changes published eight months earlier while being subscribers to the newsletter. This phenomenon can also be seen in other areas (see section 2.4).

We noticed misconceptions about how checks for account compromise happen and potentially problematic views toward security in general. One participant, e.g., stated that passwords need to be shared with third-party tools for compromise checks. Although this might be the case for some checks, there are solutions that circumvent this problem [2].

Another participant mentioned that it is never 100% sure whether a password is compromised. While this is true for almost any other security-related topic, it should not lead to not using compromise checks at all.

Here, efforts such as the Let's Hash website of Geierhaas et al. [21] can help by providing participants with a programming aid that supports developers in securely implementing password storage. It seems beneficial to further go this route and offer code-fulfilling recommendations such as from the BSI, NIST, or OWASP. While such a website is a good starting point, the people implementing the recommendations still need to be made aware of such platforms and that their knowledge is not up to date.

Processes Need to be Observed Depending on the size and structure of a company, changing the PCP can require potentially complex processes and involve multiple parties. In our sample, we found cases where the CEO was involved in creating the PCP. While we do not know the whole picture, we sometimes assume a clash of very different goals. A CEO of a small company stated: "From our point of view, the management is responsible for the guidelines and not the IT admins." In another case, the CEO of a company required password expiry, even though the security department advised against this. In cases like this, non-technical explanations of why something should or should not be used from the IT perspective might help to convince decision-makers without deep technical background and help to mediate between different stakeholders.

Apart from this decision process, a new policy has to be included in the systems. Several participants indicated they use Microsoft's Active Directory for authentication. It would be interesting to ascertain whether and how the usage of central software positively affects processes in general. This way, and in combination with secure defaults, the processes might be improved in simplicity, speed, and security, as has already been seen in other areas [4, 51].

Arguments for Change and Prioritization One of the most commonly mentioned reasons why checks for password compromise are not implemented are missing resources, i.e., time, money, or human resources.

If decisions need to be made for prioritizing tasks, low-priority tasks are often postponed, and other stakeholders must be convinced that allocating time for this is a good idea. For this reason, the arguments for a change that impacts usability more than security need to be good. Official recommendations could explain their rationale behind decisions, perhaps even beyond the security topic. That way, decision-makers have a better overview, and it might be easier to understand and communicate possible implications.

5.3 Sample and Recruitment Bias

We recruited over the newsletter sent by the BSI, thus focusing on companies interested in security-related topics, either out of an employee's personal interest or because their company has to follow specific guidelines. The latter might be the case for the 13.8% in our sample (PCP23) that indicated their company can be seen as critical infrastructure and for those 27.5% who indicated their company is certified with a certification relevant for IT security (6.2% indicated both). Yet, the effect of such a security focus is unclear and could lead to two very distinct outcomes: either following recommendations very closely or using every opportunity to increase security, even if the measures taken are questionable in terms of improving security.

6 Conclusion

In 2020, the BSI changed its guidelines regarding password composition policies and removed the advice to include password expiry. Instead, they recommend only enforcing a change if a password is compromised.

We conducted three survey studies after the guideline change to understand how fast and well these suggestions are implemented and what problems might hinder an adoption.

We found that fewer companies require a regular password change ofter the years (72.2% in 2019 to 45% in 2023). Participants who still use a regular expiry explained this with security improvements and additional guidelines by other institutions they must follow. Alternative checks were often not implemented because of missing resources or because of technical hurdles. We believe that it might be helpful if decision-makers were supported with more precise information about these alternatives than what is currently included in the guidelines given by the BSI.

Acknowledgments

We thank the Werner Siemens-Stiftung (WSS) for their generous support of this project. We thank Julia Angelika Grohs, Bilal Kizilkaya, Charlotte Theresa Mädler, and our anonymous reviewers for their help and feedback.

References

[1] FIDO2 - FIDO Alliance. https://fidoalliance.org/fido2/, No year given. Accessed: May 26, 2023.

[2] Have I Been Pwned: API v3. https://haveibeenpwned.com/API/v3, No year given. Accessed: May 26, 2023.

[3] Have I Been Pwned: Pwned websites. https://haveibeenpwned.com/, No year given. Accessed: May 26, 2023.

[4] Sigstore. https://www.sigstore.dev/, No year given. Accessed: May 26, 2023.

[5] Anne Adams and Martina Angela Sasse. Users Are Not the Enemy. *Commun. ACM*, 42(12):40–46, December 1999.

[6] Agari. Anatomy of a compromised account. https://www.agari.com/resources/guides/anatomy-compromised-email-account, No year given. Accessed: May 26, 2023.

[7] Devdatta Akhawe, Johanna Amann, Matthias Vallentin, and Robin Sommer. Here's My Cert, so Trust Me, Maybe? Understanding TLS Errors on the Web. In *Proceedings of the 22nd International Conference on World Wide Web*, WWW '13, page 59–70, New York, NY, USA, 2013. Association for Computing Machinery.

[8] Sonia Chiasson and Paul C Van Oorschot. Quantifying the security advantage of password expiration policies. *Designs, Codes and Cryptography*, 77:401–408, 2015.

[9] Yee-Yin Choong, Mary Theofanos, and Hung-Kung Liu. United States Federal Employees' Password Management Behaviors - a Department of Commerce case study. Technical Report NIST IR 7991, National Institute of Standards and Technology, April 2014.

[10] Anastasia Danilova, Alena Naiakshina, Anna Rasgauski, and Matthew Smith. Code Reviewing as Methodology for Online Security Studies with Developers - A Case Study with Freelancers on Password Storage. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pages 397–416. USENIX Association, August 2021.

[11] Let's Encrypt. Let's Encrypt - Stats. https://letsencrypt.org/stats/, 2022. Accessed: May 26, 2023.

[12] FAZ. Nicht immer wieder das Passwort ändern. https://www.faz.net/aktuell/wirtschaft/bsi-verabschiedet-sich-vom-regelmaessigen-passwort-wechsel-16616730.html, 2020. Accessed: May 26, 2023.

[13] Federal Office for Information Security (BSI). IT-Grundschutz Compendium - Final Draft, 1 February 2019. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi-it-gs-comp-2019.pdf?__blob=publicationFile&v=1, 2019. Accessed: May 26, 2023.

[14] Federal Office for Information Security (BSI). BSI - IT-Grundschutz. https://www.bsi.bund.de/EN/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html, 2021. Accessed: May 26, 2023.

[15] Federal Office for Information Security (BSI). IT-Grundschutz Compendium - Final Draft, 1 February 2021. https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Grundschutz/International/bsi_it_gs_comp_2021.pdf?__blob=publicationFile&v=4, 2021. Accessed: May 26, 2023.

[16] Federal Office for Information Security (BSI). Umsetzungshinweise zum Baustein: ORP.4. Identitäts- und Berechtigungsmanagement. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Umsetzungshinweise/Umsetzungshinweise_2021/Umsetzungshinweis_zum_Baustein_ORP_4_Identitaets_und_Berechtigungsmanagement.pdf?__blob=publicationFile&v=1, 2021. Accessed: May 26, 2023.

[17] Federal Office for Information Security (BSI). BSI - Organisation and structure. https://www.bsi.bund.de/EN/Das-BSI/Organisation-und-Aufbau/organisation-und-aufbau_node.html, No year given. Accessed: May 26, 2023.

[18] Federal Office for Information Security. Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz. https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Zertifikat/ISO27001/Zertifizierungsschema_Kompendium.pdf?__blob=publicationFile&v=1, 2019. Accessed: May 26, 2023.

[19] Deen Freelon. ReCal2. http://dfreelon.org/utils/recalfront/recal2/, No year given. Accessed: May 26, 2023.

[20] Anuj Gautam, Shan Lalani, and Scott Ruoti. Improving Password Generation Through the Design of a Password Composition Policy Description Language. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 541–560, Boston, MA, August 2022. USENIX Association.

[21] Lisa Geierhaas, Anna-Marie Ortloff, Matthew Smith, and Alena Naiakshina. Let's hash: Helping developers with password security. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 503–522, Boston, MA, August 2022. USENIX Association.

[22] Eva Gerlitz, Maximilian Häring, and Matthew Smith. Please do not use !?_ or your license plate number: Analyzing password policies in german companies. In *Seventeenth Symposium on Usable Privacy and Security (SOUPS 2021)*, pages 17–36. USENIX Association, August 2021.

[23] Paul A. Grassi. Publish#1. https://github.com/usnistgov/800-63-3/commit/3fb942e2f795f681155144d06933db28f29278e0#diff-c10a8efb34bad3a0b9a47880106e0f255f5f866f12fdcccbd73b7338ea82d301, 2016. Accessed: May 26, 2023.

[24] Paul A Grassi, James L Fenton, Elaine M Newton, Ray A Perlner, Andrew R Regenscheid, William E Burr, Justin P Richer, Naomi B Lefkovitz, Jamie M Danker, Yee-Yin Choong, Kristen K Greene, and Mary F Theofanos. Digital identity guidelines: authentication and lifecycle management. Technical Report NIST SP 800-63b, National Institute of Standards and Technology, Gaithersburg, MD, June 2017.

[25] Hana Habib, Jessica Colnago, William Melicher, Blase Ur, Sean Segreti, Lujo Bauer, Nicolas Christin, and Lorrie Cranor. Password creation in the presence of blacklists. In *Workshop on Usable Security (USEC) 2017*, page 50, 2017.

[26] Hana Habib, Pardis E. Naeini, Summer Devlin, Maggie Oates, Chelse Swoopes, Lujo Bauer, Nicolas Christin, and Lorrie F. Cranor. User behaviors and attitudes under password expiration policies. In *Fourteenth Symposium on Usable Privacy and Security (SOUPS) 2018*, pages 13–30, Baltimore, MD, August 2018. USENIX Association.

[27] Hypr. Report: State of Authentication in the Finance Industry 2022. https://get.hypr.com/state-of-authentication-in-the-finance-industry-2022, No year given. Accessed: May 26, 2023.

[28] Philip G. Inglesant and Martina A. Sasse. The True Cost of Unusable Password Policies: Password Use in the Wild. In *Proceedings of the SIGCHI Conference on Human Factors in Computing Systems*, CHI '10, page 383–392, New York, NY, USA, 2010. Association for Computing Machinery.

[29] Jurik Caspar Iser. Bundesamt hält regelmäßigen Passwortwechsel nicht mehr für notwendig. https://www.zeit.de/digital/datenschutz/2020-02/bsi-empfehlung-passwort-wechsel, 2020. Accessed: May 26, 2023.

[30] Patrick G. Kelley, Saranga Komanduri, Michelle L. Mazurek, Richard Shay, Timothy Vidas, Lujo Bauer, Nicolas Christin, Lorrie F. Cranor, and Julio Lopez. Guess again (and again and again): Measuring password strength by simulating password-cracking algorithms. In *2012 IEEE Symposium on Security and Privacy*, pages 523–537. IEEE, 2012.

[31] 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. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 246–263, 2019.

[32] Arkose Labs. 70% Increase in Fraudulent Account Registrations Puts Digital Accounts in the Crosshairs, Arkose Labs Reports. https://www.businesswire.com/news/home/20210805005657/en/70-Increase-in-Fraudulent-Account-Registrations-Puts-Digital-Accounts-in-the-Crosshairs-Arkose-Labs-Reports, 2021. Accessed: May 26, 2023.

[33] Kevin Lee, Sten Sjöberg, and Arvind Narayanan. Password policies of most top websites fail to follow best practices. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 561–580, Boston, MA, August 2022. USENIX Association.

[34] 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)*, pages 273–288, Santa Clara, CA, August 2019. USENIX Association.

[35] Philipp Markert, Theodor Schnitzler, Maximilian Golla, and Markus Dürmuth. "As soon as it's a risk, I want to require MFA": How Administrators Configure Risk-based Authentication. In *Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022)*, pages 483–501, Boston, MA, August 2022.

[36] Alena Naiakshina, Anastasia Danilova, Eva Gerlitz, Emanuel von Zezschwitz, and Matthew Smith. "If You Want, I Can Store the Encrypted Password": A Password-Storage Field Study with Freelance Developers. In *Proceedings of the 2019 CHI Conference on Human Factors in Computing Systems*, CHI '19, page 1–12, New York, NY, USA, 2019. Association for Computing Machinery.

[37] NIST Special Publication 800-57 Part 1: Recommendation for Key Management. https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-57pt1r5.pdf, 2020. Accessed: May 26, 2023.

[38] Christoforos Ntantogian, Stefanos Malliaros, and Christos Xenakis. Evaluation of password hashing schemes in open source web platforms. *Computers & Security*, 84:206–224, 2019.

[39] Federal Office of Civil Protection and Disaster Assistance. Kritische Infrastrukturen - BKK. https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/kritische-infrastrukturen_node.html, No year given. Accessed: May 26, 2023.

[40] Bijeeta Pal, Tal Daniel, Rahul Chatterjee, and Thomas Ristenpart. Beyond Credential Stuffing: Password Similarity Models Using Neural Networks. In *2019 IEEE Symposium on Security and Privacy (SP)*, pages 417–434, May 2019.

[41] Dieter Petereit. BSI rät jetzt von regelmäßigem Passwort-Wechsel ab. https://t3n.de/news/bsi-raet-regelmaessigem-ab-1249147/, 2020. Accessed: May 26, 2023.

[42] Sena Sahin, Suood Al Roomi, Tara Poteat, and Frank Li. Investigating the Password Policy Practices of Website Administrators. In *2023 2023 IEEE Symposium on Security and Privacy (SP) (SP)*, pages 1437–1454, 2023.

[43] Jürgen Schmidt. Passwörter: BSI verabschiedet sich vom präventiven, regelmäßigen Passwort-Wechsel. https://heise.de/-4652481, 2020. Accessed: May 26, 2023.

[44] Seth Schoen. Let's Encrypt Brings Free HTTPS to the World: 2015 in Review. https://www.eff.org/de/deeplinks/2015/12/lets-encrypt-project-comes-fruition-2015-review, 2015. Accessed: May 26, 2023.

[45] Richard Shay, Saranga Komanduri, Adam L. Durity, Phillip S. Huh, Michelle L. Mazurek, Sean M. Segreti, Blase Ur, Lujo Bauer, Nicolas Christin, and Lorrie Faith Cranor. Designing password policies for strength and usability. *ACM Transactions on Information and System Security (TISSEC)*, 18(4):13, May 2016.

[46] Richard Shay, Saranga Komanduri, Patrick G. Kelley, Pedro G. Leon, Michelle L. Mazurek, Lujo Bauer, Nicolas Christin, and Lorrie F. Cranor. Encountering Stronger Password Requirements: User Attitudes and Behaviors. In *Proceedings of the Sixth Symposium on Usable Privacy and Security (SOUPS '10)*, pages 1–20, New York, NY, USA, 2010. Association for Computing Machinery.

[47] Alexander Sotirov, Marc Stevens, Jacob Appelbaum, Arjen K Lenstra, David Molnar, Dag Arne Osvik, and Benne de Weger. MD5 considered harmful today Creating a rogue CA certificate. In *25th Annual Chaos Communication Congress*, number CONF, 2008.

[48] Nick Summers. Do you really need to change your password every 90 days? https://blog.1password.com/should-you-change-passwords-every-90-days/, 2022. Accessed: May 26, 2023.

[49] Joshua Tan, Lujo Bauer, Nicolas Christin, and Lorrie F. Cranor. Practical recommendations for stronger, more usable passwords combining minimum-strength, minimum-length, and blocklist requirements. In *Proceedings of the 2020 ACM*

SIGSAC Conference on Computer and Communications Security, CCS '20, page 1407–1426, New York, NY, USA, 2020. Association for Computing Machinery.

[50] Christian Tiefenau, Maximilian Häring, Katharina Krombholz, and Emanuel von Zezschwitz. Security, availability, and multiple information sources: Exploring update behavior of system administrators. In *Sixteenth Symposium on Usable Privacy and Security (SOUPS 2020)*, pages 239–258. USENIX Association, August 2020.

[51] 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, page 1971–1988, New York, NY, USA, 2019. Association for Computing Machinery.

[52] Blase Ur, Fumiko Noma, Jonathan Bees, Sean M. Segreti, Richard Shay, Lujo Bauer, Nicolas Christin, and Lorrie F. Cranor. "I Added'!'at the End to Make It Secure": Observing Password Creation in the Lab. In *Eleventh Symposium On Usable Privacy and Security (SOUPS) 2015*, pages 123–140, Ottawa, July 2015. USENIX Association.

[53] W3C. W3C TAG: Securing the Web. https://www.w3.org/2001/tag/doc/web-https, 2015. Accessed: May 26, 2023.

[54] W3Techs. W3techs: Historical yearly trends in the usage statistics of site elements for websites. https://w3techs.com/technologies/history_overview/site_element/all/y, 2022. Accessed: May 26, 2023.

[55] Yinqian Zhang, Fabian Monrose, and Michael K. Reiter. The security of modern password expiration: An algorithmic framework and empirical analysis. In *Proceedings of the 17th ACM conference on Computer and communications security*, CCS '10, pages 176–186, New York, NY, USA, 2010. Association for Computing Machinery.

A Survey

The used survey was adapted to new situations over the years. To indicate that a question was included in a year, we will use the following taxonomy:

- †, if a question was part of the original questionnaire by Gerlitz et al. [22] in **2019**.
- ⋆, if the questions was included in **PCP20**.
- ◇ for questions included in **PCP22**.
- ▽ for questions included in **PCP23**.

If no year is specified, the question was asked in all versions of the survey.

Accounts

- Q1 Is there a company-wide account per user, that is managed centrally? (e.g., for logging into the workstation, communication platform, email or the like.)
  Yes / No
- *Q2*$^{\triangledown}$ Which user management do you use? (e.g. Microsoft Active Directory)
  [Free Text]

If Q1 equals yes:

- Q3a What can this account be used for? (Multiple answers possible.)
  Email / Workstations / Communication platform (SharePoint, Slack, etc.) / VPN into corporate network / Access to shared corporate data (e.g., Active Directory) / Other: [Free text]

`< Page break >`

- Q3b Which methods can be used to log in? Please check the applicable.
  Password or PIN / Biometrics (e.g., Fingerprint, Face recognition) / Hardware Token (e.g. Smartcard, Token, Smartphone) / Device Certificates$^{\diamond}$
- Q3c Is there any other method in use that is not listed?
  Yes, the following: [Free text] / No

If more than one method is listed in Q3b:

- Q4a You stated, that there are several methods in use that enable your employees to log in. Are the methods used in combination (e.g., 2FA)?
  Yes, the methods are used in combination (2FA) / No, the employees can choose one of the methods / Other: [Free text]/ I do not know / I do not wish to make a statement

If only one method is listed in Q3b:

- *Q4b*$^{\triangledown}$ Do you make use of any kind of two-factor authentication?
  Yes, using the following techniques: [Free Text] / No / I do not know / I do not wish to make a statement

`< Page break >`

Passwords

You stated that there is no company-wide account with which the employees can log into several services.
The following questions regard the email accounts of your employees and their passwords (Webmail, IMAP, POP3, etc.).
Or
You stated, that your employees use passwords/PINs to log in. The following questions regard these passwords/PINs.

- *Q5*$^{\dagger\star\diamond}$ How are passwords handled?
  *Users can choose them themselves / Passwords are created by a system, and users **cannot change** them / Passwords are created by a system and **need to be changed** by the user*$^{\star\diamond}$*/ I don't want to make a statement / Other: [Free text]*
- Q6 What specification (also called password policy) do passwords need to fulfill (e.g., at least x characters, new password needs to be selected after x days, etc.)

  This question is the main focus of our research. Please be as detailed as possible. If possible and allowed, please copy your specification into the following text box. At this point, we want to remind you, that the data is managed anonymously. It will not be possible to identify your company.
  [Free text]

- Q7 Are these specifications enforced by the system?
  Yes / No / There are no specifications / I do not know / I do not wish to make a statement / Partially: [Free text]
- $Q8^{\diamond}$ In case there is a password expiry in use: Why?
  [Free text]
- Q9 Optional: What reasons spoke against the introduction of a password policy?
  [Free text]

< Page break >

- $Q10^{\triangledown}$ Do you feel it is best practice to require employees to change their passwords on a regular basis (e.g., once a year)?
  Yes / No / Other: [Free Text]

< Page break >

In previous studies, we have seen that employees in many companies in Germany have to change their passwords on a regular basis. In the following, we would like to learn more about the possible reasons that speak in your eyes for or against using such a time-controlled change of passwords.

- $Q11^{\triangledown}$ Are employees technically forced to change their password?
  Yes, after a fixed time interval (days/months/years): [Free Text] / Yes, if there is a suspicion that the password has become known / No, never / Other: [Free Text]
- $Q12^{\triangledown}$ If employees need to change their password regularly (after a fixed time interval): Why?
  [Free Text]
- $Q13^{\triangledown}$ In case employees had to change their password regularly (after a fixed time interval) in the past, but this rule has now been abolished: Why was this changed?
  [Free Text]

< Page break >

- $Q14^{\triangledown}$ Since 2020, the BSI has recommended relying on password compromise detection instead of recurring password change prompts (after a fixed time interval). If you do this: How do you check if passwords are compromised?
  If not: are there reasons that prevent you from doing so? (e.g., technical, structural, or timing reasons).
  [Free Text]

< Page break >

- Q15 Are users prevented from picking passwords that belong to the most common passwords?
  No / Other: [Free text] / I do not know / I do not wish to make a statement / Yes[†] / Yes, examination through$^{\star\diamond}$: [Free text])
- $Q16^{\star\diamond\triangledown}$ Do you make use of a Blocklist/Denylist of elements that are not allowed to be used in a password? (e.g. words from the dictionary or sequences of numbers) *Yes, the following elements cannot be used in passwords: [Free text] / No / There are no specifications / I do not know / I do not wish to make a statement*
- $Q17^{\star\diamond}$ Which Unicode characters can be used in passwords?
  All / a-z / A-Z / 0-9 / All special characters / Special characters, except: [Free text] / Chinese characters / Arabic characters / Emojis / Other: [Free text] / I don't know / I do not want to make a statement
- $Q18^{\star\diamond\triangledown}$ Are there additional password policies for different users? (e.g. System administrators) *Yes / No / I do not know / I do not wish to make a statement*
- $Q19^{\star\diamond\triangledown}$ Optional: How do the different password policies differ? *[Free text]*

< Page break >

The following questions still regard the passwords which are used in your company.

- Q20 Who created the specifications (password policies) for the passwords?
  Myself / My predecessor / Somebody else: [Free text]/ I do not know / I do not wish to make a statement / There are no specifications
- Q21 What are the specifications based on? (Multiple answers possible.)
  Targeted Training$^{\star\diamond\triangledown}$ / Own Know – how$^{\star\diamond\triangledown}$ / Standards defined by own company$^{\star\diamond\triangledown}$ / Industrial Standards$^{\star\diamond\triangledown}$ / Expert panels / Exchange with other companies / NIST (National Institute of Standards and Technology) / BSI (Bundesamt für Sicherheit in der Informationstechnik) / OWASP (Open Web Application Security Project) / Other: [Free text] / I do not know / I do not wish to make a statement
- $Q22^{\star\diamond\triangledown}$ When were the password policies changed last? *[Free text]*
- $Q23^{\star\diamond}$ What changes were made during the last modification?
  [Free text]
- $Q24^{\triangledown}$ Which changes were made?
  [Free Text]
- $Q25^{\star\diamond\triangledown}$ What caused the change? *[Free text]*
- Q26 How do the password policies impact the user-friendliness of the authentication system?
  1: Very negative – 5: Very positive
- Q27 How do the password policies impact the security of the authentication system?
  1: Very negative – 5: Very positive
- Q28 How often do passwords cause problems in your company (e.g., forgotten passwords, etc.)?
  1: Very rarely – 5: Very often

< Page break >

- $Q29^{\star\diamond}$ This year, the BSI published new recommendations for password policies. Have you already dealt with them? *Yes / No / I do not know / I do not wish to make a statement*
- $Q30^{\star\diamond}$ Was your password policy adapted due to the new recommendations or are you planning a change? *Yes / No / I do not know / I do not wish to make a statement*

< Page break >

- Q31 Is there a policy that specifies how the passwords are stored in the system (hash function, length of the salt, etc)?
  Yes / No / I do not know / I do not wish to make a statement
- Q32 Is there a process that initiates an update of the policy on how to store passwords?
  Yes / No / I do not know / I do not wish to make a statement

- Q33 Optional: How are stored passwords protected? We are particularly interested in the hash and salt functions that are used.

  We want to remind you that the data is gathered anonymously and we are not able to link it to your company.
  [Free text]

< Page break >

Biometric Authentication

You stated, that your employees use biometrics to log in. The following questions regard this method.

- Q34 What kind of biometrics are in use?
  Fingerprint / Iris / Face recognition / Other: [Free text]/ I do not wish to make a statement
- Q35 How does the biometric authentication impact the user-friendliness of the authentication system?
  1: Very negative – 5: Very positive
- Q36 How does the biometric authentication impact the security of the authentication system?
  1: Very negative – 5: Very positive
- Q37 How often does the use of biometric authentication cause problems?
  1: Very rarely – 5: Very often
- Q38 Optional: Do you wish to provide us with additional information about this topic?
  [Free text]

< Page break >

Hardware Token

You stated, that your employees use a hardware token to authenticate. The following questions regard this token.

- Q39 Does the token support FIDO2?
  Yes / No / I am not sure / I do not wish to make a statement
- Q40 How does the token impact the user-friendliness of the authentication system?
  1: Very negative – 5: Very positive
- Q41 How does the token impact the security of the authentication system?
  1: Very negative – 5: Very positive
- Q42 How often does the usage of the token cause problems?
  1: Very rarely – 5: Very often
- Q43 Optional: Do you wish to provide us with additional information about this topic?
  [Free text]

< Page break >

Passwordless

- $Q44^{\triangledown}$ There are efforts (e.g., by the Fido Alliance) to completely abolish passwords. What is your opinion of these efforts (also with regard to their feasibility in the company where you work)?
  [Free Text]

< Page break >

Demographics

- $Q45^{\dagger\star\diamond}$ Please check the conditions which apply to your company. (Multiple answers possible.)
  There are employees who can access their emails outside the company network /
  There are employees who can access their emails using a web login /
  There are employees who do not need to know the password for accessing their emails, e.g., as the email-client is pre-configured
- Q46 Is there any additional security for emails? (e.g., encryption in combination with a smart card)
  Yes, obligatory / Yes, voluntary / No / I do not wish to make a statement
- $Q47^{\star\diamond\triangledown}$ What is your companies' field of work? *Automobile Industry / Banks and financial services / Education and research / Services / Retail / Energy industry / Logistics / Telecommunication / Pharmaceutical industry / Tourism / Insurance / Healthcare Marketplace / Other: [Free text] / I do not wish to make a statement*
- $Q48^{\star\diamond\triangledown}$ Is your company an operator of critical infrastructure or is it affected by regulations for operators of critical infrastructure? *Yes / No / I do not know / I do not wish to make a statement*
- $Q49^{\triangledown}$ Is your company certified with a certification relevant to IT security (e.g., PCI-DSS, ISO 27001,..)?
  Yes, the following: [Free Text] / No, but we intend to / No / Other: [Free Text] / I don't know / I do not wish to make a statement
- $Q50^{\triangledown}$ Are there any legal regulations that require you to have any of the previous certifications?
  Yes the following: [Free Text] / No / Other: [Free Text] / I do not wish to make a statement
- $Q51^{\star\diamond\triangledown}$ Where is your companies' headquarter? (Country)
  [Free text]
- Q52 How many employees work in your company?
  1-9 / 10-49 / 50-249 / 250-499 / 500-999 / 1000 or more / Not sure / I do not wish to make a statement
- Q53 How many desktop clients do you manage?
  1-9 / 10-49 / 50-249 / 250-499 / 500-999 / 1000 or more / Not sure / I do not wish to make a statement
- Q54 How many employees in your company work full-time on IT security topics?
  0 / 1 / 2-5 / 6-10 / 11-20 / 21 or more / Not sure / I do not wish to make a statement

- $Q55^{\star\diamond\triangledown}$ What is your position? *Administrator / ISO / CISO / CTO / CSO / Support / Other: [Free text] / I do not wish to make a statement*
- $Q56^{\star\diamond\triangledown}$ How many years of experience do you have in this or related positions? *Under 1 year / 1-3 Years / 4-9 Years / 10 or more years / I do not wish to make a statement*
- $Q57^{\star\diamond\triangledown}$ Is one (or more) of the following situations true for your company when looking at the last 5 years? (MC) *A password of an employee was guessed and used to attack the company (Ransomware, theft,..) / Several passwords have been stolen from the database / None of the above / I do not know / I do not wish to make a statement / Further / Other: [Free text]*

`< Page break >`

- $Q58^{\star\diamond\triangledown}$ Have you already participated in this survey last year? *Yes / No / I do not know /I do not wish to make a statement*
- Q59 How satisfied are you with your authentication system? *1: ☹ – 5: ☺*
- Q60 Has this questionnaire motivated you to update parts of your authentication system in the near future? If yes, which parts?
  Password Policies / Security measures for stored passwords / Adding biometrics / Adding hardware token / No / Other: [Free text]

B Additional Tables

	PCP19	**PCP20**	**PCP22**	**PCP23**
Pw	100.0	100.0	100.0	97.5
Pw + Bio	14.8	17.3	25.4	25.0
Pw + Token	38.9	50.0	57.1	53.8
Pw + Bio + Token	11.1	13.5	19.0	17.5
Token (no Pw + Bio)	0	0	0	1.2

Table 2: Percentage of participants who mentioned that their companies use the different possibilities to login. Pw = Passwords are in use; bio = Biometrics are in use; Token = Hardware token are in use

	PCP19	**PCP20**	**PCP22**	**PCP23**
All Data	172	72	96	122
Only BSI	91	72	96	122
Only complete	71	57	66	83
Individual filter	69	56	66	83
Only accounts	**54**	**52**	**63**	**80**

Table 3: Elimination process of data sets. **Only BSI** = Only answers that were gathered over the BSI newsletter. Only in PCP19 were participants recruited over other channels as well. **Complete** = The participant filled out the whole survey. **Individual filter** = Participants were filtered manually if the answers indicated they did not understand the questions and if the role did not include being able to work on the company's authentication protocols. **Only accounts** = Participants indicated whether the company makes use of a centrally managed account. We only kept those who did.

		PCP19	PCP20	PCP22	PCP23
		$n = 54$	$n = 52$	$n = 63$	$n = 80$
Size of Company (Q52)	1-9	7.4	7.7	7.9	5.0
	10-49	13.0	3.8	11.1	13.8
	50-249	16.7	23.1	15.9	20.0
	250-499	7.4	7.7	9.5	12.5
	500-999	9.3	9.6	11.1	16.2
	≥ 1000	46.3	48.1	44.4	28.7
	Unclear	0.0	0.0	0.0	3.8
Employees working full-time on IT security topics (Q53)	0	14.8	5.8	17.5	17.5
	1	22.2	36.5	27.0	23.8
	2-5	25.9	34.6	31.7	31.2
	6-10	5.6	11.5	7.9	8.8
	11-20	11.1	5.8	0	7.5
	≥ 21	13.0	5.8	11.1	7.5
	Unclear	7.4	0.0	4.8	3.8

Table 4: Demographics of companies that were asked in all three years. All numbers are percentages of that year. "Unclear": Participants did not disclose the information, or we could not infer it from their answers.

		PCP20 $n = 52$	PCP22 $n = 63$	PCP23 $n = 80$
Sector (Q47)	Services	40.4	39.7	41.2
	Industry	17.3	15.9	15.0
	Medical	7.7	7.9	5.0
	Infrastructure	9.6	4.8	7.5
	Public service	9.6	9.5	6.2
	Education and research	5.8	9.5	6.2
	Sales	3.8	1.6	3.8
	Other	0.0	7.9	5.1
	n.d.	5.8	3.2	10.0
Critical Infrastructure (Q48)	Yes	19.2	15.9	13.8
	No	80.8	74.6	81.2
	n.d.	0	9.5	5.0
Incidents at company within last 5 years (Q57, MC)	Easy PW used for attack	11.5	9.5	11.2
	Several PWs were stolen from database	1.9	1.6	0.0
	None of the above	63.5	84.1	65.0
	Other	11.5	0.0	8.8
	n.d./Don't know	15.4	4.8	15.0
Own role (Q55)	IT			
	C-level & management	50.0	39.7	50.0
	ISO	17.3	28.6	20.0
	Admin/DevOps	13.5	12.7	11.2
	Support	0	1.6	0
	Management	1.9	9.5	7.5
	DPO	1.9	0.0	2.5
	Consultant	0.0	0.0	1.2
	n.d.	17.3	7.9	7.5
Own experience (Q56)	$<$ 1 year	1.9	1.6	2.5
	1-3 years	17.3	17.5	12.5
	4-9 years	30.8	30.2	28.7
	$\geq$10 years	44.2	50.8	52.5
	n.d.	5.8	0	3.8

Table 5: Demographics of companies and participants from PCP20, PCP22, and PCP23. All numbers are percentages of that year. "n.d": Participants did not disclose their answers. The participants indicated their current job position. Since some of them indicated holding different roles in the company (e.g., CEO and admin), the numbers exceed 100%.

	Code	**PCP20** $n = 52$	**PCP22** $n = 63$	**PCP23** $n = 80$	**ICR**
Character classes	1	2	1	1	-
	2	2	3	1	0.79
	3	23	25	33	1
	4	16	19	15	1
	Imprecise	3	5	9	0.47
	Special	0	1	2	-
	Total	46 (88%)	54 (86%)	61 (76%)	
	Not mentioned	4	6	10	0.79
	Explicitly not	0	0	1	-
Minimum length	5	1	0	0	-
	6	4	1	1	-
	7	0	0	1	-
	8	18	20	19	1
	9	1	1	2	1
	10	16	14	12	1
	11	0	2	1	1
	12	8	16	24	1
	14	0	2	5	1
	15	0	1	4	-
	16	1	0	2	-
	64	1	0	0	-
	Imprecise	0	2	1	-
	Total	50 (96%)	59 (94%)	72 (90%)	
	Not mentioned	0	1	0	-
Password expiry (days)	14	0	1	0	-
	30	1	0	2	-
	42	1	1	0	1
	60	0	0	1	-
	64	0	0	1	-
	90	12	8	5	1
	120	0	0	1	-
	168	0	1	0	-
	180	6	2	9	1
	230	0	1	0	-
	360	0	0	1	-
	365	5	6	6	1
	540	1	0	0	-
	720	0	0	1	-
	Imprecise	1	2	1	-
	Total	27 (52%)	22 (35%)	28 (35%)	
	Not mentioned	18	25	26	1
	Explicitly not	5	13	18	1
	No policy given	2	3	8	-

Table 6: Codebook of participants' elements of password composition policies (Q6) and how often they occurred. For calculating the ICR, answers from both years were merged. Some codes were not covered in the documents that were used to calculate the inter-coder reliability and indicated as "-" in the table.

Code	Example	Occurrence in PCP23
Demanded by ...		
... Institutions	"PCI DSS (Credit card security) requirement"	5
... Customer (contracts)	"was embedded in customer contracts in the past"	3
... Own company	"In-house or internal definition"	4
Is best practice	"Recommendation by BSI"	2
To increase security	"Improve password security", "Ensure that there are no passwords that are too old and no insecure hash algorithms are used."	17
Currently changing	"We still have the setting but are in discussion rather to increase the complexity, but not to force a change (except in case of loss). Still need to convince the auditor. "	1
Alternative not implemented	"Because there is currently no other technical solution."	4
Inertia	"Still exists from history"	5

Table 7: Codebook of the reason for using password expiry (Q12)

Code	Example	Occurrence in PCP23
Employee check	"Our detection of compromise has so far been the sole responsibility of the employee."	6
Check: Dark web monitoring	"Dark Web Monitoring"	4
Check: Compare to leak database	"On the relevant websites we check whether passwords have been compromised"	8
Check: Anomaly detection	"Detection of compromise by technical means (e.g., logon location)."	16
No check: Lack of..		
..technical measures	"Technically not yet possible, corresponding recognition systems are still missing"	9
...and unclear how	"We do not know any practicable method"	3
...organizational measures	"organizational feasibility"	5
...resources (time, money)	"There would also be a lack of time and staff resources to look into this"	7

Table 8: Codebook of the reason for using password expiry (Q14)

		Has PW Expiry	No PW Expiry	p	OR
H3: Critical Infrastructure	Yes No	5 28	3 14	1.0	0.83
H4: Company Size	<500 >=500	14 16	9 8	1.0	1.29
H5: Last policy change	Before BSI changes After BSI changes	9 19	1 15	0.3	0.14
H6: Technical compromise check	Yes No	13 20	12 5	0.4	0.27

Table 9: Contingency table for H3-6: *Company characteristics or the use of certain policy elements influence whether the companies use a password expiry in 2023.* The results are corrected using a Bonferroni-Holm correction.