H. Roßnagel, C.H. Schunck, S. Mödersheim (Hrsg.): Open Identity Summit 2022,
Lecture Notes in Informatics (LNI), Gesellschaft für Informatik, Bonn 2022 113

A user-centric approach to IT-security risk analysis for an identity management solution

Nicolas Fähnrich[1] Matthias Winterstetter[2] Michael Kubach[1]

Abstract: In order to build identity management (IdM) solutions that are secure in the practical application context, a holistic approach their IT-security risk analysis is required. This complements the indispensable technical, and crypto-focused analysis of risks and vulnerabilities with an approach that puts another important vector for security in the center: the users and their usage of the technology over the whole lifecycle. In our short paper we focus exclusively on the user-centric approach and present an IT-security risk analysis that is structured around the IdM lifecycle.

Keywords: identity lifecycle; user-centric; risk analysis; IT-security; cybersecurity; social engineering; identity management; IdM

1 Introduction

For identity management (IdM), the call to put the user into the center of the development efforts for new solutions is not new. Actually, it has already been one key aspect of Cameron's 7-laws of identity [Ca05]. Lately, the widely popular term Self-sovereign identity (SSI), going back to 10 postulated principles by Allen [Al17], puts user control into the center as well. Many see the future for digital identity in this concept and it is in mentioned in many high-profile initiatives, e.g. by the EU or the German government [Bu21d], [Bu21c]. Now it is not the topic of this paper to discuss the whether the implicit or explicit assumption by proponents of these claims that it is the failure to put the user into the center which is the reason why privacy friendly IdM solutions have failed on the market so far. However, if we pursue the path towards self-sovereign identity further to build systems that allow users to fully own and manage their identity without having to rely on a third party [Mü18] this user also should be put into the center of the IT-security risk analysis of such systems. Traditionally, IT-security risk analysis focuses on vulnerabilities of software, hardware, or network systems. The exploitation of humans as attack vectors via so called social engineering attacks is often neglected [BP16]. Generally, the research on social engineering is still in an early stage, when it comes formal definitions, attack frameworks and attack templates [MLV16]. If we look at common procedures in IT-security risk analyses, that follow standards like "ISO/IEC 27001", the NIST Cybersecurity framework [Na18] or the German IT-Grundschutz [Bu21b], we find a similar approach that starts off with a detailed

[1] Fraunhofer IAO, Nobelstraße 12, 70569 Stuttgart, firstname.lastname@iao.fraunhofer.de
[2] Universität Stuttgart, Institut für Arbeitswissenschaft und Technologiemanagement (IAT), Allmandring 35, 70569 Stuttgart, matthias.winterstetter@iat.uni-stuttgart.de

doi:18.18420/OID2022-09

documentation of the IT-infrastructure of a given application. In addition, all data processing operations are documented, including all data categories. Based on these data categories, person-related data is further investigated to derive the individual protection needs. In a following step, possible IT-security threats are identified by a catalogue comparison and potential threats are rated and documented. A risk is then derived based on the probability of occurrence of the identified threats and the protections needs of the processed person-related data. The underdeveloped field of social engineering in IT-security risk analysis might be one reason why IdM-projects tend to rely on the traditional approach to security risk analysis and make do with considering technical aspects, considering the human factor at most in an unstructured and superficial manner. Still, while a thorough analysis of vulnerabilities of software, hardware and network systems is certainly indispensable, is nevertheless incomplete. For an approach that puts users at the center of the control of such valuable data as identity information, we also need to put them at the center of our security risk analysis. In a research project to build an ecosystem of secure and trustworthy digital identities [ON22] we are currently putting our call to action. With this short paper we hope to enrich the discussion on user-centricity in IT-security research, in particular with focus on (self-sovereign) IdM, as a currently underdeveloped field. Through an early publication of the first results of our work we aim to collect valuable feedback than can guide further development efforts. Hence, the remainder of this short paper after this brief introduction presents the user centric approach to IT-security risk analysis we developed for the IdM research project. Then we conclude the paper with a discussion of the preliminary results, limitations, and next steps.

2 Proposed user centric approach

The technical side of IT-security risk analysis, such as the infrastructure design, the choice of security mechanisms, crypto protocols, and authentication methods is without a question of great importance for the overall security of applications. However, the relative disregard of the end user side can lead to significant security problems in practice use, especially in the case of IdM solutions where highly sensitive personal data are being handled, for example, to conclude contracts. Even more so, if the user is the only point of control without reliance on a third party as if in SSI-approaches. In fact, studies analysing the current state of IT-security and attacks show that users are heavily involved in the majority of cyberattacks, with multiple social engineering techniques being used [Bu21a], [G 21]. In the absence of an existing structured procedure for IdM solutions that focuses on the end user side in addition to the technical security aspects, we developed a new approach that builds on the identity lifecycle of Meints and Royer [MR08] (Figure 1).

This enables us to thoroughly analyse every process step within every IdM-lifecycle phase e.g., the interaction between identity providers and end users within the “Revision/Auditing” phase that can potentially be exploited by attackers to commit an attack on the IdM system. To identify relevant attack vectors we made use of Mitre’s Attack Pattern Enumeration and

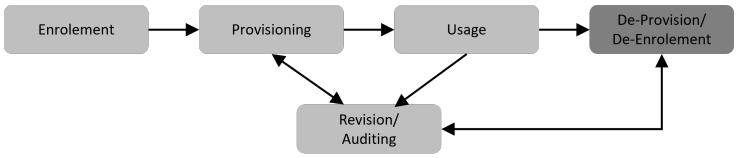

Fig. 1: Identity Lifecycle based on Meints and Royer [MR08]

Classification (CAPEC) [MI22] as it is actively managed, regularly updated and commonly regarded as a global knowledge base for IT-security threats.

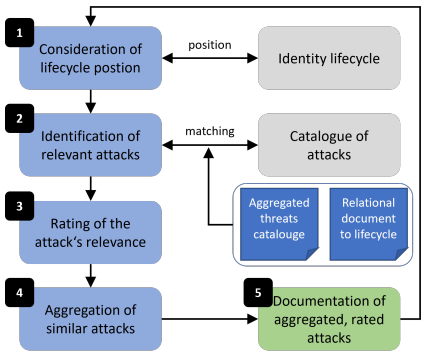

Fig. 2: Procedure for user-centric identification, rating, and documentation of relevant attacks

The developed procedure consists of the following steps and is illustrated in Figure 2:

1. Iterative consideration of one identity lifecycle phase at a time.
2. Identification of relevant attack vectors given in Mitre's Attack Pattern Enumeration and Classification (CAPEC). To assist with this process we created a catalogue of non-technical attacks and a relational document to link the threats to the identity lifecycle.
3. Rating of the attack's relevance within the respective phase of the identity lifecycle considering the statistical frequency of occurrence and ease of carrying out the attack.
4. Aggregation of similar attacks and their respective rating in relevance.
5. Documentation of aggregated and rated attacks for the respective identity lifecycle phase.

In step 1, we set the phase in the identity lifecycle, e.g., "Enrolement", that is to be considered in the following steps of the analysis. A research in the CAPEC catalogue follows in step 2. This is the central phase of the process and consists of matching relevant cyberattacks with the respective identity lifecycle phase. More detail on how this step is performed and supported will be given below. As a result, we obtain a list of relevant cyberattacks which

are then rated in step 3. In this rating we consider different factors such as the statistical frequency of the attack type and the ease for an attacker to carry out the attack. Since this procedure leads to a potentially high number of possible attacks, we aggregate these into corresponding categories in step 4. In step 5 we document the aggregated and rated attacks for the respective identity lifecycle phase. Then the next iteration of the procedure starts again with step 1 and the subsequent phase of the identity lifecycle. This is repeated until all phases of the identity lifecycle have been completed. As our end result, we receive a completed table of categorized and rated cyberattacks that are assigned to the respective phases of the identity lifecycle that should be considered in the architecture and the development of the underlying application. This procedure ensures a high degree of thoroughness since possible attacks are not only matched against the technological aspects of the IdM solution but the end user as potential attack vector is considered as well and this is done along the complete identity lifecycle in a structured form.

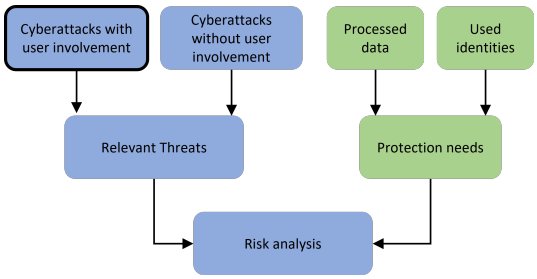

Fig. 3: Attack-based approach for the identification of cyberattacks with user involvement in the context of a risk analysis

This attack-based approach forms the basis for the identification of cyberattacks that require user interaction. It should be noted that this is only a subset of the total quantity of possible cyberattacks, since also technical attacks without user interaction have to be considered. When combining the identified attacks and complementing technical attacks with the protection requirements of the respective application, a comprehensive risk analysis is to be performed (Figure 3). To assist with the identification process of relevant attacks in step 2 of the described procedure, we require a concise overview of possible threats that could affect the system in consideration. To cover this aspect, we aggregated the most relevant non-technical threats, listed under the CAPEC Domains of Attack [MI22]. We focused on non-technical threats since these are usually relevant for user-centric attacks on a system. The threats were documented in an excel-table for easy review. In addition to aggregating the non-technical threats presented by CAPEC, we extended the provided information with a threat evaluation, a generic example of an attack and potential counter measures. The threat evaluations consist of the “kill chain” (description of the phases of an attack) phases in which the threats are most likely to occur, the required technical and social skills for execution, a rough evaluation of the required effort and the likelihood of occurrence. The generic example of the threat provided in the document is separated into flow one through three, describing the three stages of the threat in detail. The actual execution of an attack

regarding the threat may consist of more or less steps than the provided three, as they are only meant to give the reader a general idea of how an attack could occur. Regarding the potential counter measures we provide a list of viable options. We assigned the generic counter measures “user training” and “guidelines” to all threats, as these measures are among the most effective means for dealing with non-technical threats. In total, the document contains 16 non-technical threats (excluding the aggregated threats) for IdM systems. As user identities move through the different phases of the identity lifecycle they become more susceptible to some of the listed threats and less susceptible to others. While all threats are at least partially applicable during the “Usage” phase of the lifecycle, threats like identity theft become more relevant during the “Provisioning”, “Usage” and “Revision/Auditing” phases. Opposed to that, threats like spoofing and phishing can already be relevant during the “Enrolment” phase. To enable an easier identification of relevant threats in each phase of the lifecycle we additionally created a second, relational document to link threats to the lifecycle phases to show if they are applicable in the respective phase. A generic example for each applicable threat is provided for additional explanation thus allowing for an easier identification of threats. This secondary document is meant to serve as a bridge between the overview of the aggregated threats we provided and the lifecycle to ease the identification of relevant attacks in the second step shown in Figure 3.

3 Conclusion

IT-security is key to achieve trustable IdM solutions. Current development approaches focus primarily on technical security aspects although it has shown that end users are an important attack vector on IT-systems through social engineering attacks. Now that developments such as the trend towards SSI put the user in an even more responsible position, a failure to methodologically integrate the human factor into security considerations for the development of novel IdM systems creates an even bigger problem for their overall security. In this paper we therefore present a user-centric approach that leverages the identity lifecycle by on Meints and Royer. Using an iterative approach, each phase of the identity lifecycle is considered to match relevant attacks exploiting the human vector using Mitre’s CAPEC. As a result, we get a documentation of relevant and rated cyberattacks including adequate mitigation measures that can be used in the further development of the IdM solution. This short paper elaborates on our approach covering the non-technical attacks. The analysis of this subset of attacks certainly has complemented as shown in Fig. 3. Furthermore, other standards and guidelines cover non-technical aspects as well, however we think that our approach provides a structured procedure to evaluate the user’s role in attacks over the whole IdM-lifecycle into the risk analysis. This can potentially lead to a higher security level especially for end users. This short paper presents work in progress. We will test our approach as part of the risk analysis of the IdM solution developed in the ONCE research project [ON22] and optimize it further based on the lessons learned.

References

[Al17] Allen, C.: The Path to Self-Sovereign Identity, https://github.com/ChristopherA/self-sovereign-identity, 2017, visited on: 02/05/2022.

[BP16] Beckers, K.; Pape, S.: A serious game for eliciting social engineering security requirements. In: 2016 IEEE 24th International Requirements Engineering Conference (RE). IEEE, pp. 16–25, 2016.

[Bu21a] Bundesamt für Sicherheit in der Informationstechnik: Die Lage der IT-Sicherheit in Deutschland 2021, Bonn, 2021.

[Bu21b] Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz: Informationssicherheit mit System, https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html, Mar. 2021, visited on: 02/15/2022.

[Bu21c] Bundesministerium für Wirtschaft und Energie: Digitale Identität, https://api.bundesregierung.de/resource/blob/992814/1898280/d9819a40553a9543b9e8f3acb620b0c2/digitale-identitaet-neu-download-bundeskanzleramt-data.pdf?download=1, 2021, visited on: 02/15/2022.

[Bu21d] Bundesministerium für Wirtschaft und Energie: High-level scope (ESSIF) - EBSI Documentation - CEF Digital, https://ec.europa.eu/digital-building-blocks/wikis/pages/viewpage.action?pageId=379913698, 2021, visited on: 02/15/2022.

[Ca05] Cameron, K.: The Laws of Identity, https://www.identityblog.com/stories/2005/05/13/TheLawsOfIdentity.pdf, 2005.

[G 21] G DATA CyberDefense AG: Cybersicherheit in Zahlen, Hamburg, 2021.

[MI22] MITRE: Common Attack Pattern Enumeration and Classification (CAPEC): A Community Resource for Identifying and Understanding Attacks, https://capec.mitre.org/, 2022, visited on: 02/10/2022.

[MLV16] Mouton, F.; Leenen, L.; Venter, H. S.: Social engineering attack examples, templates and scenarios. Computers & Security 59/, pp. 186–209, 2016.

[MR08] Meints, M.; Royer, D.: Der Lebenszyklus von Identitäten. Datenschutz und Datensicherheit 32/3, p. 201, 2008.

[Mü18] Mühle, A.; Grüner, A.; Gayvoronskaya, T.; Meinel, C.: A survey on essential components of a self-sovereign identity. Computer Science Review 30/, pp. 80–86, 2018.

[Na18] National Institute of Standards and Technology: Cybersecurity Framework Version 1.1. https://www.nist.gov/cyberframework/framework, 2018, visited on: 02/15/2022.

[ON22] ONCE: Online einfach anmelden, https://once-identity.de/, 2022.