Determining the Efficiency of Mitigations Based on Covered Threats

Matthias Winterstetter [1]

Abstract: Prioritization of threats is an important skill for experts working in the cybersecurity field. With daily new discovered threats and a variety of tools providing information, warnings, and alerts, it is essential for experts working in cybersecurity to identify the most important warnings and threats and handle them efficiently to stay ahead of the growing competence, organization, and size of threat groups. To assist cybersecurity experts with these tasks, this paper provides an approach covering six steps that can be used to determine the efficiency of mitigations for a system under consideration. To this end, this paper describes a straightforward approach and provides an example in which it has already been used.

Keywords: Cybersecurity, IT-Security, Mitigations, Threat Actors, Threat Groups, Mitigation Efficiency.

1 Introduction

The resources a company is willing to invest in security tends to be limited financially and in terms of human resources. This stems from the fact that security does not add any inherent value to an organization but instead serves to ensure that the existing value of the organization is not decreased by accidents or malicious actors. This tends to lead to a very strict cost benefit analysis by the management. Additionally, experts in cybersecurity are, like all experts in the tech industry, very sought-after, further limiting the resources an organizations cybersecurity team has available. Furthermore, in the event of a cybersecurity incident occurs or a relevant new vulnerability is made public, a fast and efficient response is necessary.

This limit on resources necessitates a prioritization of vulnerabilities to determine which vulnerability to handle first. This necessity is covered by a large number of risk management tools that also highlight critical vulnerabilities. With the ability to determine which vulnerability has to be handled first comes the ability to choose which mitigations to implement first. However, mitigation techniques can be vastly different from each other and can require large amounts of resources. For instance, changing a registry key or uninstalling software can be done much faster and is much cheaper than buying and configuring a firewall. At the same time, a properly configured firewall can mitigate more vulnerabilities than a change in the registry or uninstalled software.

[1] University of Stuttgart, Insitut für Arbeitswissenschaft und Technologiemanagement, Nobelstraße 12, Stuttgart, 70569, Matthias.Winterstetter@iat.uni-stuttgart.de https://orcid.org/0000-0001-9093-4381

doi:10.18420/OID2024_17

While the management of risks and vulnerabilities has been given a lot of attention by the research community, the same cannot be said for managing and prioritizing mitigations. Simply knowing which mitigations can handle the given vulnerability does not enable one to know which mitigation is best for a given scenario. To make an informed decision in such a situation, knowledge about the time a mitigation takes to implement, the required cost for implementing the mitigation, how many relevant vulnerabilities a mitigation can cover and what mitigations are already in use is required. To assist security experts with this decision-making, this paper presents an approach that can be used to determine the most efficient mitigations with respect to the number of threats covered.

The next chapters of this paper will cover the related work in chapter 2, the used methodology in chapter 3, a discussion about the results and the methodology in chapter 4 and an outlook in chapter 5.

2 Related Work

There are many articles, scientific papers, frameworks, and methodologies that concern themselves with risk management and the handling of vulnerabilities. For instance, [Le21], [Ek23], [Za23] and [Ku20] are all relatively recent contributions to the scientific community and introduce new methods for risk management. There are also articles going over the top choices for risk management frameworks [Wi00]. On the vulnerability side, there are a number of globally accessible knowledge bases, among them is MITRE ATT&CK [Mi19] which, among other things, provides a taxonomy of tactics, techniques, and procedures (TTP).

While there are many methodologies for managing risks and prioritizing vulnerabilities, the prioritization of mitigations has not been given as much attention. For instance, [GMP20] states that most vulnerability assessment tools, while performing exceptional at identifying vulnerabilities, do not have the capability to perform prioritized mitigation of said vulnerabilities. It goes on to introduce the cybersecurity vulnerability mitigation framework (CyFEr) to fill this gap. An alternative method was presented by [Be20] which also focuses on prioritizing mitigations on the basis of potential damage.

When it comes to prioritizing mitigations regarding available resources, the landscape becomes scarcer still. However, there are some proposed solutions, like [Sa13] which presents a method that can determine the most resource efficient set of mitigations given a set of mitigations and threats based on the effectiveness at blocking threats, implementation costs and probability of attacks. Another alternative is presented in [OTK08] by introducing a method through which a pareto optimal selection of mitigations can be calculated. To this end, this method uses a graded security model, representing the degree of protection, security groups, representing a set of security measures and a fitness function that represents the confidence of achieving the given security goals for a set of countermeasures. Given the scarcity of resources that

cybersecurity professionals have to deal with, the topic of optimizing mitigation usage still requires more attention in the opinion of the author.

3 Approach

The approach presented in this chapter can be used to determine the efficiency of mitigations for a system under consideration. The approach can be split into the following six Steps:

Step 1: Determine the relevant threat groups based on the threat groups motivation and their capability to target the system under consideration.

Step 2: Finalize the threat list and weight the threats: Prune the list of threats to remove threats that are not relevant to the system under consideration. Determine the weight of the threats regarding their relevancy to the system under consideration.

Step 3: Sort the threats according to their weight.

Step 4: Determine mitigations for the threats.

Step 5: Determine how many threats each mitigation can cover.

Step 6: Aggregate the weight of the covered threats with the efficiency of the covered mitigations.

To determine the relevant threat groups in step 1 the motivation behind the known threat groups and their used techniques are analysed. Based on this, we can determine how well the victim would fit into the profile of known victims of those threat groups. As a result of this analysis, we get a list of threat groups that would be motivated to attack the system under consideration as well as have the ability and know-how to implement an attack. With the list of relevant threat groups comes a list of their used threats. These lists can be aggregated into a list of threats and weighted for step 2. In step 2 we prune the list of threats that could not be used to attack the system under consideration due to physical limitations. A lack of cloud infrastructure, for instance, would make cloud-based threats irrelevant. To weight the threats for step 2 their relevancy for the system under consideration is used. This can, for instance, be the number of threat groups that make use of that threat. After each threat has been weighted, they are sorted in step 3.

For step 4 and 5 we first determine the possible mitigation methods for the threats in the list from step 3 and aggregate them into one list of relevant mitigations. Following this, we can determine the efficiency of mitigations. This can be done by determining the number of threats covered by each mitigation. Step 6 completes the process by aggregating the efficiency of mitigations with the relevancy of the threats. This can be done by summing up the weights of the threats covered by a mitigation. For a more fine-

tuned output, an attack-defence tree as presented in [AN15] can be used. Alternatively, the method presented by [Sa13] could also be used for step 5 and 6. The resulting value shows the efficiency of a mitigation regarding relevant threats and threat groups.

3.1 Example

This methodology was used in the ONCE project to determine the efficiency of mitigations. ONCE is a wallet solution for digital identities. To determine the relevant threats and threat groups we used the Risk Analysis Platform RALF. RALF was configured with the technical components involved in ONCE and the results of a questionnaire concerning the motivation of different attack groups regarding ONCE that were answered by partners from different types of stakeholders in the ONCE consortium.

Threat Name	Threat ID (MITRE)	Threat Group Usage
Malicious File	T1204.002	17
Spearphishing Attachment	T1566.001	15
Windows Command Shell	T1059.003	11
Drive-by Compromise	T1189	11
Scheduled Task/Job	T1053	9

Tab. 1: Weight of Threats

As a result of this first step, we obtained a list of 22 attack groups that would be both motivated to attack and have been recorded exploiting threats that are relevant for ONCE. Based on the relevant threat groups, the relevant threats and the number of their uses by the threat groups could be determined, thus completing step 2. For step 3 the threats were sorted according to their number of uses. The top 5 threats can be seen in Tab. 1. For step 4 we determined the possible mitigation methods using MITRE ATT&CK and sorted them based on how many threats they would cover for step 5. Lastly, for step 6 we summed up the weights for the threats covered by each mitigation, to determine the efficiency value of each mitigation resulting in the list shown in Tab. 2.

Threat Name	Mitigation ID (MITRE)	Efficiency
Restrict Web-Based Content	M1021	54
Execution Prevention	M1038	49
User Training	M1017	46
Privilleged Account Management	M1026	31
User Account Management	M1018	30

Tab. 2: Efficiency of Mitigations

The methodology presented in this chapter uses the Risk Analysis Platform RALF which is based on the patent [Ku20] to determine the relevant threats and threat groups. The

patent covers an automated system for the evaluation of information security risks. Although RALF was used in ONCE and as the basis for step 1, the presented methodology is not dependent on RALF and can use other sources to determine the relevant threats.

4 Discussion

The approach presented in the previous chapters can prioritize mitigations for a system under consideration regarding the relevancy of the threats. This knowledge gives cybersecurity experts a better understanding over the mitigation landscape of the system they are supporting. Beyond that, this knowledge can be used to optimize the employed mitigations for a system. For instance, redundant mitigations that cover a threat that can also be covered by other mitigations that are already in place can be removed if they don't add any additional protection. This can reduce the available attack surface that an attacker can exploit. A prerequisite for this methodology to work properly is an automated and precise method for discovering threats and relevant threat groups.

While this methodology can be used as is and provide more insight into the mitigation landscape of a system under consideration, there is room for improvement with the methodology as it stands now. For instance, the weighing of the threats in step 2 can be done with the number of threat groups that make use of the threat alone. To provide more context to the relevancy of the threat, the likelihood of a threat occurring can be considered as well. Furthermore, techniques for evaluating the efficiency of mitigations in step 6 should be tested and optimised to determine the most optimal implementation.

5 Conclusion

This paper presents an approach for assessing the efficiency of mitigations for a system under consideration regarding the number of threats that a given mitigation can cover. The presented methodology is detailed and shown at the hand of an example, and it's advantages and room for growth are described. The next steps would be to optimize step 2 and step 6, test the approach with different systems under consideration and have the results be evaluated by experts in the cybersecurity field.

6 Bibliography

[AN15] ASLANYAN, ZARUHI ; NIELSON, FLEMMING: Pareto Efficient Solutions of Attack-Defence Trees. In: FOCARDI, R. ; MYERS, A. (Hrsg.): *Principles of Security and Trust, Lecture Notes in Computer Science*. <Springer><Berlin Heidelberg>95-114, 2015.

[Be20] BENTLEY, MARK ; STEPHENSON, ALEC ; TOSCAS, PETER ; ZHU, ZILI: A Multivariate Model to Quantify and Mitigate Cybersecurity. Risk 8/2020, 61, 2020

[Ek23] EKSTEDT, MATHIAS ; AFZAL, ZEESHAN ; MUKHERJEE, PREETAM ; HACKS, SIMON ; LAGERSTRÖM, ROBERT: Yet another cybersecurity risk assessment framework. *International Journal of Information Security* 22/2023, 1713-1729, 2023

[GMP20] GOURISETTI, SRI NIKHIL GUPTA ; MYLREA, MICHAEL ; PATANGIA, HIRAK: Cybersecurity vulnerability mitigation framework through empirical paradigm Enhanced prioritized gap analysis. *Future Generation Computer Systems* 105/2020, 410-431, 2020

[Ku20] KUROWSKI, SEBASTIAN: Automatisches Abschätzen von Informationssicherheitsrisiken. DE: 10 2018 216 887.3, 2018/2020

[Le21] LEE, IN: Cybersecurity: Risk management framework and investment cost analysis.: *Business Horizons*, 64/2021, 659-671, 2021

[Mi19] MITRE: *MITRE ATT&CK*. https://attack.mitre.org/. 2019-10-14

[OTK08] OJAMAA, ANDRES ; TYUGU, ENN ; KIVIMAA, JYRI: Pareto-optimal situaton analysis for selection of security measures. In: *MILCOM 2008 <IEEE,>*< San Diego, CA, USA> 1–7, 2008

[Sa13] SAWIK, TADEUSZ: Selection of optimal countermeasure portfolio in IT security planning. *Decision Support Systems*, 55/2013, 156–164, 2013

[Wi00] *Today's Top Risk Management Frameworks*. https://www.splunk.com/en_us/blog/learn/risk-management-frameworks.html. 2024-02-13

[Za23] ZADEH, AMIR ; LAVINE, BRANDON ; ZOLBANIN, HAMED ; HOPKINS, DONALD: A cybersecurity risk quantification and classification framework for informed risk mitigation decisions. *Decision Analytics Journal*, 9/2023, 100328, 2023