safeguarding science
SAFEGUARDING-SCIENCE.EU

Open Source Intelligence (OSINT) application to illustrate the potential compromise of academic knowledge security systems

Application at a German Research Performing Organisation (RPO) and a Higher Education Institution (HEI)

Executive Summary of a study report of the Fraunhofer Learning Laboratory for Cybersecurity at Mittweida University of Applied Sciences commissioned by DLR Projektträger

Executive Summary edited by Niklas Gabriel and Gerold Heinrichs

safeguarding-science@dlr.de

ISBN 978-3-949245-24-4

November 2023, DLR Projektträger Bonn, Germany

safeguarding science
SAFEGUARDING-SCIENCE.EU

Open Source Intelligence (OSINT) application to illustrate the potential compromise of academic knowledge security systems

1 Introduction

Universities and research institutions are exposed to unintentional knowledge leakage in many forms. In addition to the human passing on of information, the access of unauthorised third parties by means of technical measures poses a high risk. This can not only lead to a considerable competitive disadvantage, but also cause massive reputational damage. In this context, existing security gaps are often not recognised at all or are recognised too late. IT security at research institutions primarily prevents intrusion from the outside. Less focus is often placed on monitoring information about the institution

available on the internet and its potential misuse. However, sensitive data can be located on the "clean web", the "deep web" or the "dark net". It can be assumed that in most cases there is a lack of knowledge as to whether and which data of one's own institution is affected.

2 Task

The aim of the study was to identify and analyse possible security gaps that could result from openly available information. The results should be used to take appropriate measures to establish an optimised knowledge security system in the future.

The Fraunhofer Learning Laboratory for Cybersecurity at Mittweida University of Applied Sciences carried out an Open Source Intelligence (OSINT) application at a German Research Performing Organisation (RPO) and a Higher Education Institution (HEI) on behalf of the DLR Projektträger (DLR-PT, project management agency) in consultation with the two entities. The Fraunhofer Learning Laboratory for Cybersecurity uses open source intelligence to determine all publicly available information about the institutions, their employees and technical infrastructure. Particularly relevant here is information which could be used by attackers to damage the institution. The target group of the investigation includes the employees of the management, the Corporate Security and Public Relations who are potentially relevant for the information security of the research institution.

The results were discussed with the two analysed entities. The document presented here is an anonymized executive summary of the full-length report which is only available to the two entities. With the executive summary, DLR Projektträger intends to raise awareness at research institutions and universities within the framework of European Safeguarding Science measures.

3 Method

Within the framework of an OSINT application, the first step is to show which methods can be used to detect security vulnerabilities at universities and research institutions. The following items were analysed:

- E-mail addresses
- Password leaks
- Services, IP addresses and vulnerabilities
  - Incompletely configured systems
  - Outdated Software
  - Insufficiently protected access
  - Information leakage
  - Searching for acute vulnerabilities
  - Online Meeting Platforms

The main questions were

- Can concrete cases of leakages and damages be identified and which relevance do they have? What tools can detect vulnerabilities?
- Can an institution check itself and identify possible data leaks, existing data loss or unauthorised data loss?
- What could an OSINT monitoring system in the science institutions look like?

4 Results

The results can be divided into three different topics: firstly emails, secondly password leaks, and thirdly Services, IP addresses and vulnerabilities of the system.

4.1 E-Mail addresses

Information search

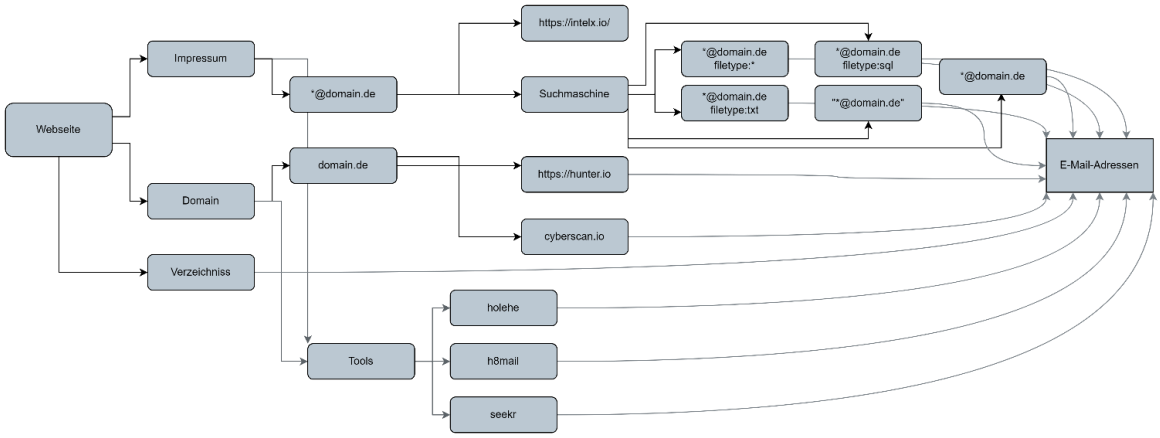

Fig 1: Information search regarding e-mails

Relevance

E-mail addresses play a significant role in OSINT research because they act as digital identifiers and can be linked to a variety of online activities and accounts. The systematic collection and analysis of e-mail addresses enables the extraction of various information such as identification of a person, linking to online accounts or general information retrieval.

Result of analysis

The RPO as well as the HEI provide extensive information about their employees in so-called employee directories on their websites. These directories contain information such as first names, last names, institute, address, room identifier and telephone numbers of the employees. Often, pictures of the employees can also be found in these directories. The study observed that in comparison to private enterprises both institutes made personal information more extensively available to the public. If the number of employees is compared with the number of e-mail addresses found, the ratio for the institutes is about 30/100, while for exemplary selected companies in the private sector the ratio is

6/100. Since each piece of information offers the possibility of carrying out attacks in a more targeted manner, it can be assumed that a social engineering attacker will have a higher chance of success at either institution. Of considerably greater importance than the absolute figures, however, is the existence of detailed employee directories. Such directories are rarely available at companies in the private sector. As a result, the risk of phishing attacks, social engineering and identity theft is increased or even significantly increased for these institutions compared to companies in the private sector.

Risk mitigation measures

It is of great importance that institutions take appropriate security measures to minimize these risks. These measures include the development of data avoidance and data economy concepts to determine which personal data are absolutely necessary for the performance of tasks. A general principle is that the risk of targeted attacks in the area of phishing and social engineering decreases when information in the public domain is kept at a minimal level.

Example of potential misuse

In the study it was possible to create a complete digital actor from the available information in the employee directories. The name and the email address form the basis for generating the digital actor with the help of OSINT. These two pieces of information can be used in conjunction with various search engines to determine further images or video footage of the real person. If sufficient material is available in sufficient quantity and quality, this database can be processed e.g. using the DeepFaceLive software. DeepFaceLive generates the visual appearance for the digital actor. To represent the digital actor in a suitable environment, the address, building or room can be used. This information can be used in search engines to ensure that the digital actor is presented in an environment that is expected by others. Depending on the amount of information available, the

digital actor can use different communication channels and cause severe damage to the institutions including theft of sensitive material.

4.2 Password leaks

Information search

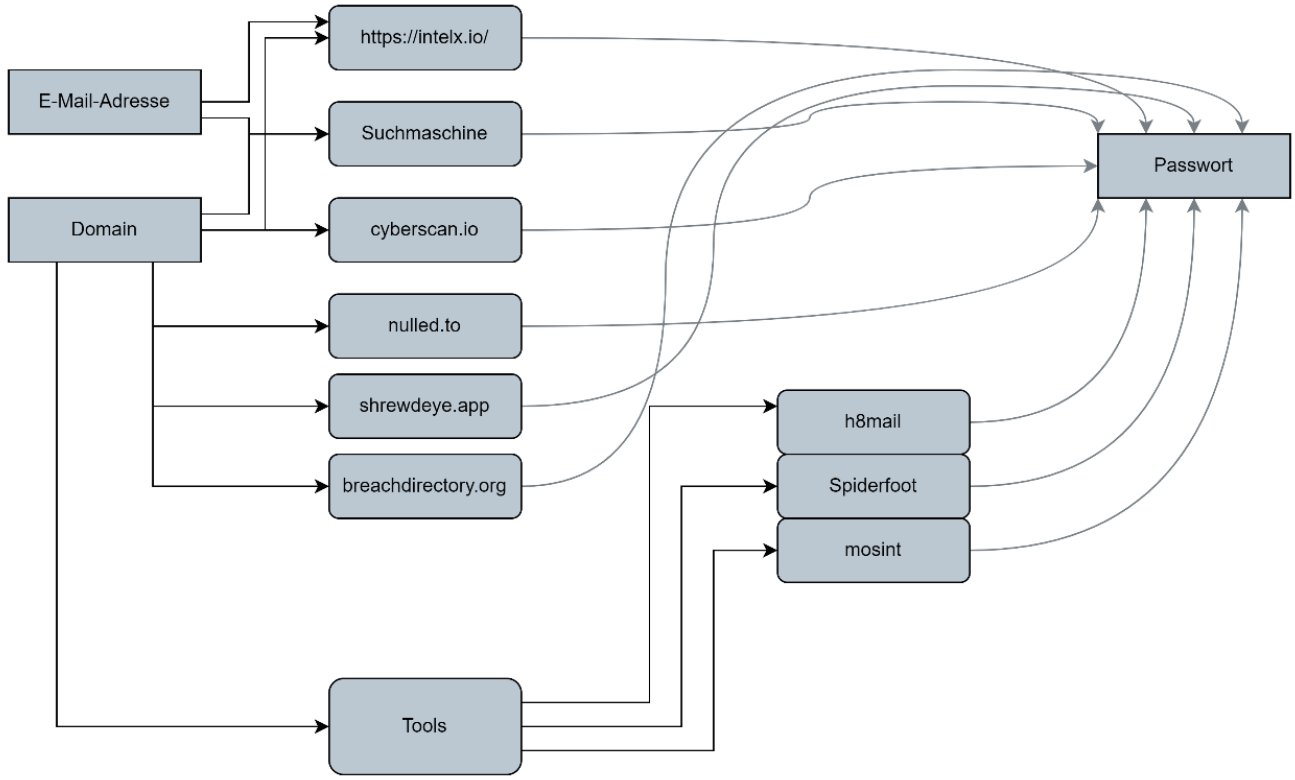

Fig 2. Information search regarding password leak

Relevance

One of the greatest risks which can occur in terms of OSINT research are password leaks. Once a password leak occurs, attackers can access user accounts by using the stolen usernames and passwords. This can lead to identity theft, fraud, access to personal information, or other malicious activities.

Results of Analysis

Through specific services it was possible to find over 3000 password leaks for the RPO and over 10.000 password leaks for the HEI (up to 2021). In comparison, there were around 200 password leaks found for an exemplary selected private company as well as 1500 password leaks for a governmental institution. If the number of password leaks found on the specific service are put in relation to the number of employees in the institutes as well as companies in the private sector / government institutions, an increased incidence of password leaks on the institute level can be observed. Both institutions are at some risk in terms of data compromise and potential security breaches. It should be noted that the numbers provided are only a current state of affairs and cannot capture all potential password leaks. Data leaks are often first used by various groups of perpetrators for their own attacks on systems, until after a certain time they are then offered for sale on various marketplaces. Only then they can be found with OSINT tools.

Risk mitigation measures

Institutes should actively search available password-data and apply counter-measures to reduce misuse. Implementing widespread two-factor authentication can bring significant benefits to the security of the IT infrastructure. By reviewing and adapting existing authentication methods and training employees, the risk of unauthorized access and data theft can be significantly reduced.

Example of potential misuse

Data leaks are often first used by various groups of perpetrators for their own attacks on systems, until after a certain time they are then offered for sale on various marketplaces. By selling these data sets, they are made available to a broader target group. In the course of the research, a data record of an employee from the RPO was found. This record contains both an e-mail address as well as a password in plain text. To select this person, the data set was searched for employees of the RPO. To further enrich

information to this password leak, it is possible at this point to search the employee directories at the RPO addressed in the above section. Consequently, both data found in the leak can be linked to a currently active employee.

4.3 Services, IP addresses and other vulnerabilities

Relevance

In general, every service that can be accessed from the Internet represents an attack surface. Both analysed entities operate a variety of internet-based services. These services are used to provide interfaces for internal and external persons in order to offer working environments and services. They cover various areas such as data management, information provision and cooperative working. They provide platforms for document sharing, communication and information exchange and are used for secure storage and management of data so that it can be accessed from different locations. Some examples of such services are cloud-based storage solutions, collaborative work platforms, virtual research environments and online communication tools. Access to these services is usually only possible / allowed with the appropriate permissions and authorisations via a web interface. These services are based on programmes and software solutions and security problems relate primarily to configuration, patch management and user data separation.

By using active port scanner, the accessible services of a system or network can be revealed. A particularly frequently used port scanner is nmap. A port scanner can determine which network ports are open on a particular system and which services are open.

In Germany, performing a port scan without the consent of the respective system or network operator is illegal. Due to this regulation, an active scan was not performed within the scope of this study. However, it should be noted that this is a purely legal hurdle. An

actor abroad or with general criminal intentions – or the institution itself – has all the technical possibilities to carry out such a scan.

Since it was not allowed to process an active port scan by the study team, this OSINT study used existing port scan applications that continuously scan the internet using port scanners and produce pre-collected data. The collected information is then made available to the public in a searchable form (Figure 3). These search engines and services have the advantage that they already carry out an extensive enrichment of the data stocks independently.

Information search

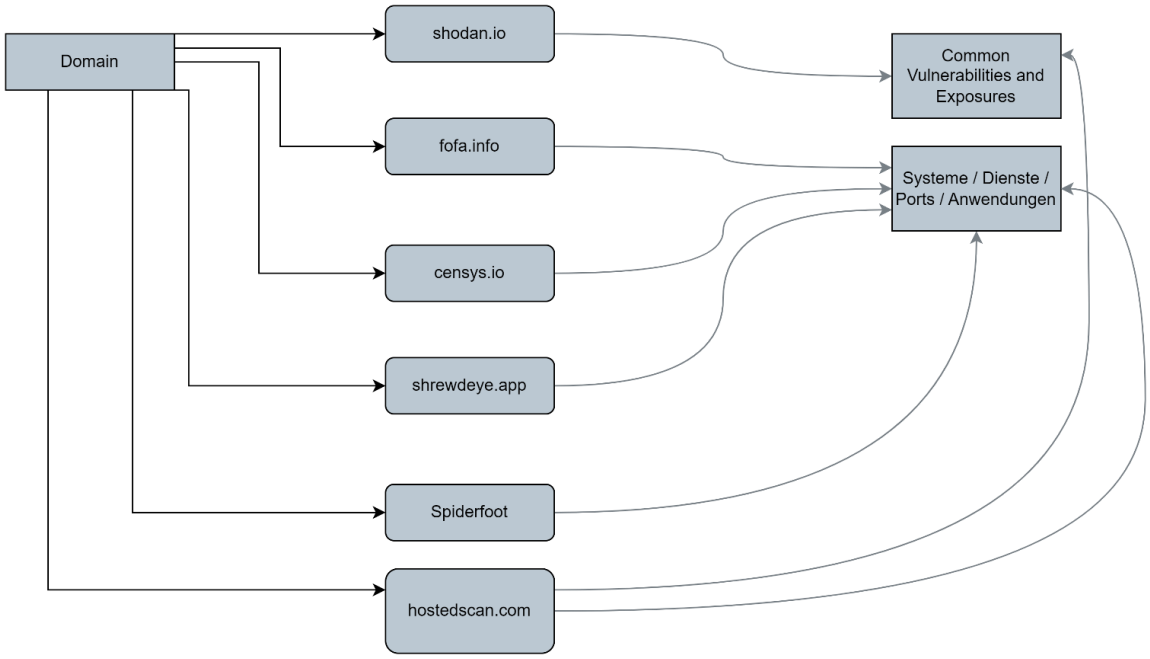

Fig. 3 Gathering information about systems / services / ports and vulnerabilities

Results of the analysis

For the RPO, a total of about 1500 internet accessible services can be detected via these applications, while for the HEI it is about 2600 services. In general, every service that can be accessed from the internet represents an attack surface. In particular, this manifests itself if the service is incorrectly configured or outdated. With the large number of accessible services, the probability increases that there is vulnerable software among them.

Within the scope of an OSINT search, it was not possible to gain access to cameras, printers, door locks, scientific machines, or other Internet of Things devices. Access to these devices typically requires another level of authentication and authorization beyond the scope of the OSINT search. Gaining access to such devices would require additional steps, such as exploiting security vulnerabilities, conducting penetration tests, or obtaining credentials through other means which was not the scope of this study.

Risk mitigation measures

It should be checked which services should be accessible from the Internet. In addition, access via a VPN can also be restricted. For example, services that only communicate internally can be excluded from using a VPN. Access to the corresponding system from outside via a VPN is then also no longer possible.

Example of potential misuse

A potential attacker will observe automatically the systems of the research institution over a longer period of time until a suitable opportunity for an attack arises. If an emerging vulnerability is not fixed immediately, experience shows that it will already be attacked within 24-48 hours.

4.3.1 Incompletely configured systems

Relevance

Incompletely configured systems pose a significant problem and can have potential vulnerabilities that compromise the security of the system. In this context the use of default passwords or weak passwords that have not been changed is of particular concern, as they provide an easy way for attackers to gain unauthorised access to sensitive data or privileged accounts. In addition, open ports and improperly configured services can serve as gateways for potential attacks.

Results of the analysis

From the accessible systems found (RPO 1500 and HEI 2600), approximately 100 incompletely configured web pages were identified using the tool "shrewdeye.app", a web crawler that takes screenshots. The screenshots were then examined for anomalies. For example, not fully configured openly accessible websites were found.

Risk mitigation measures

Visible web pages are not initially a security risk. However, the incomplete configuration gives attackers reason to believe that access to folders or files is not sufficiently restricted and a possibility exists that access to the host system may be extensible. Therefore, to ensure the security of systems, measures are required to identify and correct incompletely configured systems. This includes regular checks of the system configuration to identify potential vulnerabilities and take appropriate countermeasures. Setting up automated configuration monitoring systems and carrying out regular security audits are also important. It is not uncommon in the field of scientific research for systems to be configured for projects, but not to be switched off or managed after the end of the project.

4.3.2 Outdated software

Relevance

The use of outdated software represents a significant security risk in the area of IT security. Old software versions often contain known security gaps and vulnerabilities for which exploits have already been developed. Since these vulnerabilities are no longer fixed by updates or patches, systems using outdated software are more vulnerable to attacks. Attackers can exploit these vulnerabilities to gain unauthorized access, inject malicious code, or steal sensitive data.

Results of the analysis

In both institutions investigated, outdated software was discovered in several cases, which represented potential vulnerabilities.

Risk mitigation measures

In general, it is recommended to be notified about software updates of the software you are running. It is also recommended to automate the software update process and to delete or replace outdated software.

4.3.3 Insufficiently protected access

Relevance

Brute force attacks are a method of systematically trying all possible combinations of passwords or keys to gain access to a system. If a system is not adequately secured against such attacks, attackers can repeatedly and automatically try passwords or keys until they succeed.

Results of the analysis

To detect missing brute force countermeasures, the screenshots of "shrewdeye.app" were searched for login masks. A login with the user name "test" and the password "test" was then attempted 10 times within 3-5 minutes. Attention was paid to whether the system intervened. As a result, 6 unsecured log-in masks could be identified at both institutions, among other things, for an e-learning application and a Siemens remote control system.

Risk mitigation measures

Various measures can be implemented to secure against brute force attempts. First and foremost, this includes setting a timeout for a retry. This can also increase as the number of failed attempts increases. In addition, the account can be blocked after a maximum number of failed attempts. Subsequently, the user can contact an administrator for re-approval. This will inform the administrator that a brute force attack may have been attempted and investigate further. Furthermore, it is possible to link the login to the solving of a capture. Optionally, this can also be switched on after a specified number of failed attempts. This means that a user does not normally have to solve a capture. In principle, however, the measures taken should always be weighed up against the protection value and usability.

4.3.4 Information leakage

Relevance

Information leakage refers to the unauthorised or unintentional outflow of information from a particular system or organisation. It refers to the loss, disclosure or unauthorised dissemination of sensitive or confidential information to unauthorised third parties.

Results of the analysis

Again, the screenshots of the service "shrewdeye.app" were searched for corresponding information. For both institutions, a relevant amount of personal information as well as project data and technical information was discovered.

The evaluation of the information was not possible in the study. Without a precise technical or factual reference to various projects or research activities, it is impossible to filter relevant from non-relevant information from the database.

Risk mitigation measures

A more targeted search can be carried out by those involved in the project or those responsible.

4.3.5 Searching for acute vulnerabilities

Relevance

Through OSINT measures Common Vulnerabilities and Exposures (CVE) can be detected in web-applications, measured by the Common Vulnerability Scoring System (CVSS). This is a framework for assessing the severity of security vulnerabilities in computer systems. The CVSS score consists of a numerical scale of values from 0 to 10. Higher values signal greater severity of the vulnerability. The score is based on various metrics that consider the impact of the vulnerability and its exploitability.

Results of the analysis

A level 10 vulnerability in terms of the CVE (Common Vulnerabilities and Exposures) scale would be extremely severe, as this represents the highest severity level. Such a vulnerability was found in both institutions in a GitLab service. On the date of discovery, 15 days

have already passed in which a security release is available. This period of time is not acceptable for fixing a level 10 vulnerability.

4.3.6 Online meeting platforms

Information search

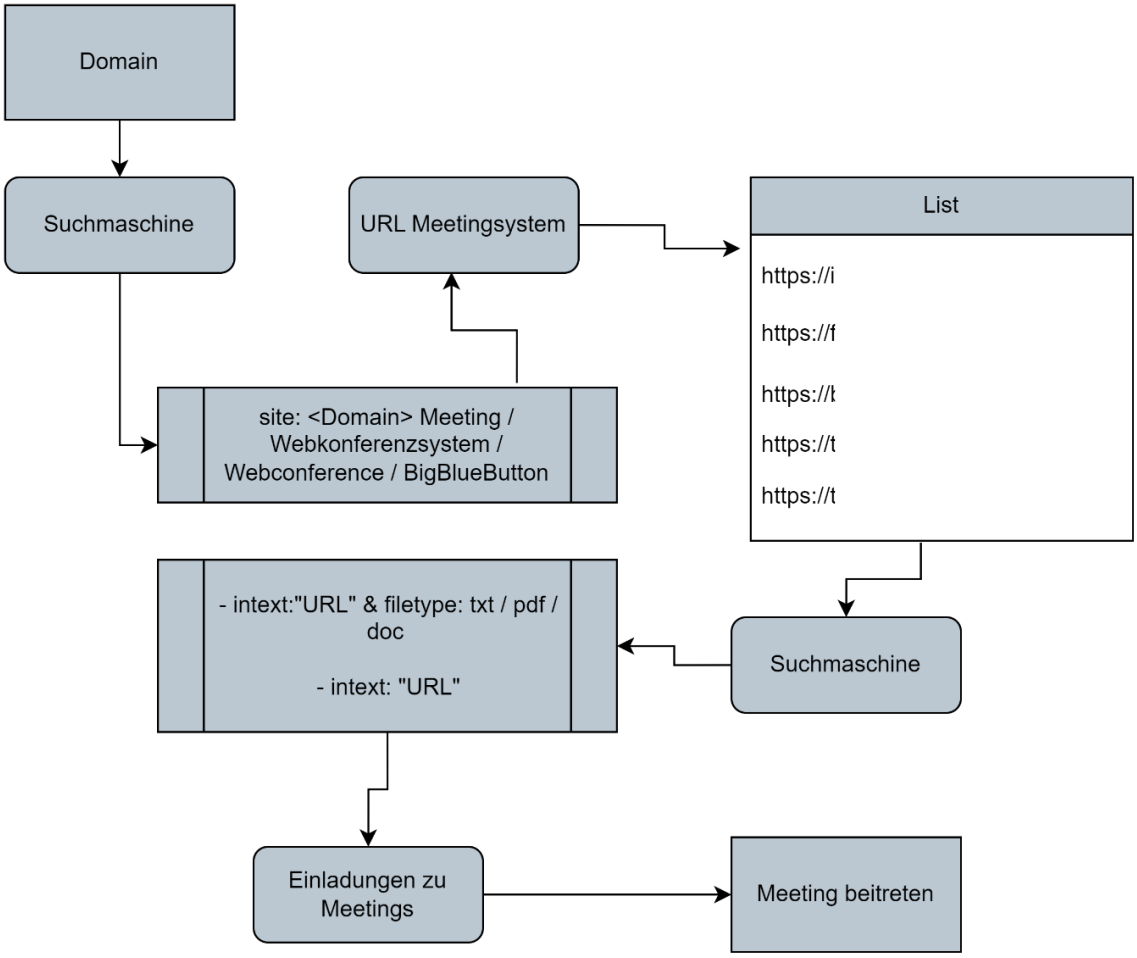

Fig. 4 Information search regarding online meeting platform and using the open rooms

Relevance

Online meeting platforms are tools or software solutions that allow users to hold virtual meetings regardless of their location. These platforms typically offer features such as

video and audio communication, screen sharing, chat, file sharing, and collaboration tools. They are used to connect people over the Internet and enable them to communicate interactively in real time – and - they represent another source of risk. In this study the services of Zoom and BigBlueButton, which were primarily used by the institutes, were researched. Zoom is a widely used video conferencing and online meeting platform. For Zoom, 49 vulnerabilities have been listed in the National Vulnerability Database In the last 12 months. These 49 vulnerabilities have an average weighting of 7.2, placing them in the "High" range. These vulnerabilities impact individual client systems (desktop/mobile) as well as servers and networks.

BigBlueButton is an open-source web conferencing platform designed for online learning and virtual training. In the last 12 months, 14 vulnerabilities have been listed in the National Vulnerability Database. These 14 vulnerabilities have an average weighting of 5.5, placing them in the "Medium" range. These vulnerabilities affect servers and networks.

Results of the analysis

Using the different search engines, it was possible to assign about 430 active online meeting links for the RPO and about 640 active online meeting links for the HEI. In general, it can be assumed that each of these opened rooms is technically to be evaluated according to the same risk. It is not ensured that content is provided exclusively for the specific target group. The meeting rooms can be accessed and misused.

Risk mitigation measures

Access to the online meeting platform should be protected through the use of secure credentials, such as strong passwords. Meeting links and access information should only be shared with authorized participants and should not be publicly available. Considering the vulnerabilities of the last 12 months and the possible spread and thus the possible damage, the use of the online meeting platform BigBlueButton is preferable to the Zoom application. If the findings of the figures are supplemented with other issues, such as

GDPR and data storage on third-party servers, it supports this statement. In general, the operation of different applications that fulfil one and the same purpose in a productive environment is not advisable. An alternative system should only be considered as a backup solution.

Example of potential misuse

When dealing with online meeting platform, there is a possibility to get information from this system on different levels. Meeting rooms, for example, are not closed after the meeting, so it is possible for anyone to enter this online meeting platform and use it for their own purposes. This could be confirmed at both institutes. A variety of criminal acts are conceivable here, e.g., the exchange of image material, the spreading of violence, or agreements to commit criminal acts.

5. Conclusion

Numerous tools on “Open Source Intelligence” are available and they can be used to pose not only a threat to individuals, but also to research institutions and universities. In general, OSINT can be pursued using two different approaches. One approach is the collection of information on individuals in order to confront them with various attack methods. On the other hand, there is the technical reconnaissance of systems and services of a research institution.

In general, it should be noted that the absolute amount of information at both of the institutions examined is contrary to the principle of data economy. This is due, on the one hand, to grown structures and amounts of information, and, on the other hand, to incorrect or incomplete configurations of systems. If an organization discloses vulnerable information or potential vulnerabilities through an external OSINT search, this may indicate that the institution may have inadequate security measures in place. The affected facility should consider this a warning sign and take appropriate action to improve its security practices. Overall, accurately identifying specific breaches requires a more in-

depth investigation that goes beyond an external OSINT search. Identifying, assessing, and remediating specific security breaches requires internal security audits, vulnerability assessments, and penetration testing that provide a more comprehensive view of an institution's security posture. A decentralized approach to stakeholder accountability would provide a better approach. In summary, there is a high density of information on individual employees at an institution, with a great deal of information about their activities, contact information, research projects, and expertise. The density of information should be reviewed and placed in relation to mission fulfilment. In principle, the approach of data economy should be realized here. Many systems and services in the institutes are considered redundant. The existence of such unused resources can lead to unnecessary resource consumption and security risks.

At the analysed HEI, the picture is similar, with two main user groups identified – students and staff. Due to the large number of users here, there is an increased risk of data leaks within this user groups. Many redundant systems and services were observed at the HEI. A total of 2478 resources and services were identified during the research, with approximately 15% of these services being classified as redundant. The OSINT application has demonstrated that the two facilities under consideration have various, relevant and relatively easily detectable vulnerabilities. Both institutions have used the study results immediately to improve their systems. Both institutions were selected to be among the best positioned HEI and RPO institutions in Europe in terms of IT security. We therefore assume that the results are realistically transferable to most European HEIs and RPOs.

It is recommended that the IT security at both, HEI and RPO be expanded to include their own systematic and regular OSINT observations (OSINT Monitoring system as a component of IT-Security and as a part of an integrated Safeguarding Science Management approach) in order to identify threats at an early stage.