Finn Eckstein, Ria Rosenauer, Pascal Huppert, Melanie Volkamer, Dominik Herrmann

RFC 9116 („security.txt“) an deutschen Hochschulservern

RFC 9116 ist ein einfach umsetzbarer, aber bisher wenig verbreiteter Standard, der ein maschinenlesbares Format für die Bereitstellung der Kontaktdaten des Webseitenbetreibers festlegt, an die Sicherheitslücken gemeldet werden sollen. Um die Verbreitung dieses Standard-Formats zu steigern, wurden alle deutschen Hochschulen mit unterschiedlich formulierten E-Mails über den Standard informiert. Die Anzahl der „security.txt“-Dateien hat sich im Beobachtungszeitraum immerhin verdreifacht, allerdings auf niedrigem Niveau. Interessant für zukünftige Sensibilisierungskampagnen ist, dass die Form der Ansprache dabei keine große Rolle spielte.

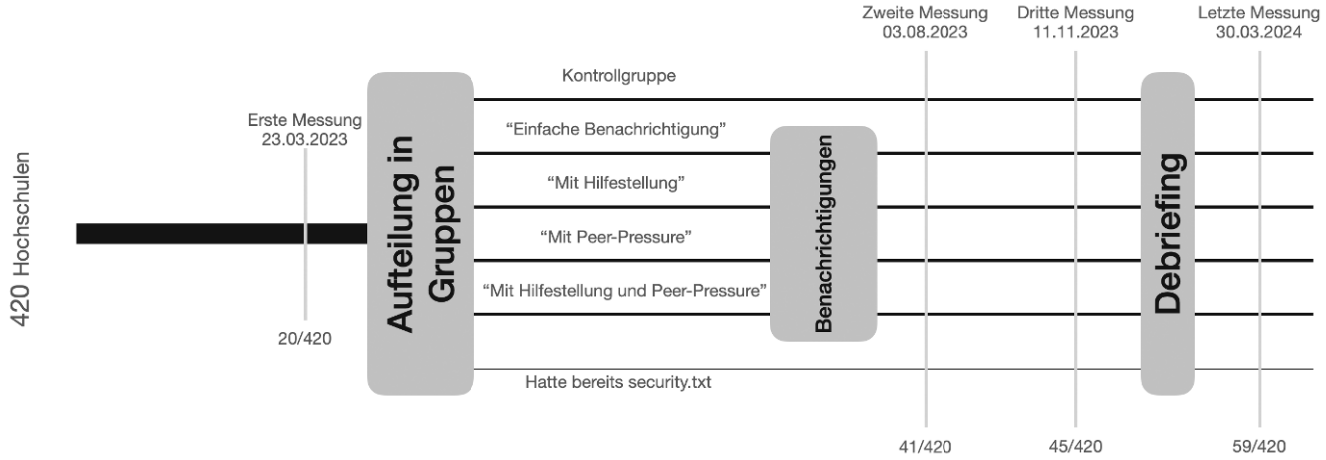
1 Einleitung

Im Jahr 2023 kam es an mindestens neun Hochschulen zu schwerwiegenden IT-Sicherheitsvorfällen [1], die teilweise zu tage- und wochenlangen Beeinträchtigungen führten. Neben Reputationsschäden drohen Datenschutzverletzungen, etwa durch die Offenlegung personenbezogener Daten von Studierenden (z. B. Prüfungsergebnissen) und Beschäftigten (z. B. Personalakten). Die Umsetzung effektiver Schutzmechanismen ist angesichts der beschränkten IT-Ressourcen für viele Hochschulen eine Herausforderung.

Eine einfach umsetzbare Maßnahme ist die Implementierung von RFC 9116. Dieser Standard sieht vor, die Kontaktdaten der Ansprechpersonen für Informationssicherheit in einer maschinenlesbaren Datei mit dem Namen „security.txt“ an einem bestimmten Ort auf dem Webserver zu hinterlegen. Diese Maßnahme soll Außenstehenden die Kontaktaufnahme bei der Meldung von Sicherheitslücken erleichtern, sodass diese schneller geschlossen werden können.

Allerdings wurde der im April 2022 veröffentliche Standard bisher nur von wenigen Webseitenbetreibern umgesetzt. Unser Ziel war es, die Verbreitung der „security.txt“ bei Hochschulen zu erhöhen und herauszufinden, welche Faktoren bei der Sensi-

Abb. 1| Ablauf der Studie mit den zugehörigen gemessenen Ergebnissen und den Datumsangaben



bilisierung eine Rolle spielen. Im Rahmen einer Studie haben wir dazu alle deutschen Hochschulen, die den Standard noch nicht implementiert haben, per E-Mail angeschrieben.

Um Einflussfaktoren bei der Sensibilisierung zu überprüfen, haben wir die 400 betroffenen Hochschulen zufällig in Versuchsgruppen eingeteilt und den Inhalt der E-Mails variiert. Eine Versuchsgruppe erhielten in den E-Mails nur einen Hinweis auf den Standard, eine zweite erhielt darüber hinaus eine konkrete Hilfestellung zur technischen Umsetzung, eine dritte wurde darauf hingewiesen, welche benachbarten Hochschulen den Standard bereits implementiert hatten („Peer Pressure"), und bei der vierten Gruppe kamen sowohl „Hilfestellung" als auch „Peer Pressure" zum Einsatz. Darüber hinaus gab es eine Kontrollgruppe, deren Mitglieder wir zunächst nicht anschrieben, sondern die wir nur beobachteten.

Vor dem Versand unserer E-Mails im März 2023 hatten nur 20 von 420 Hochschulen (4,8%) eine security.txt-Datei hinterlegt. 100 Tage nach dem Versand unserer E-Mails stieg der Anteil auf 9,8%, ein Zuwachs um 21 Hochschulen. Im November 2023 informierten wir alle Hochschulen in einer Debriefing-Nachricht über unsere Studie. Am Ende des Betrachtungszeitraums (März 2024) hatten insgesamt 59 Hochschulen (14,0%) die Datei hinterlegt. Dabei konnten wir keinen wesentlichen Unterschied zwischen den Versuchsgruppen feststellen.

Die insgesamt geringe Wirksamkeit unserer Nachrichten ist vor dem Hintergrund der einfachen Umsetzbarkeit überraschend. Zu den Beweggründen, die „security.txt"-Datei nicht zu hinterlegen, äußerten sich die angeschriebenen Hochschulen nicht. In den meisten Fällen blieben unsere Nachrichten unbeantwortet, die wir an die im Impressum der Hochschulen genannte E-Mail-Adresse sandten. Möglicherweise haben einige unserer E-Mails gar nicht die für Informationssicherheit zuständigen Personen erreicht.

In den folgenden Abschnitten erklären wir den Aufbau der Datei „security.txt" und erläutern unser Studiendesign. Anschließend präsentieren und diskutieren wir die erhaltenen Ergebnisse.

2 Inhalt der „security.txt"

Sicherheitsforscherinnen und -forscher, die Sicherheitslücken identifizieren und melden, spielen eine wichtige Rolle für die IT-Sicherheit. Der Meldeprozess stößt jedoch oft schon bei der Identifikation der zuständigen Ansprechpartner auf Schwierigkeiten. Häufig werden Meldungen irrtümlich an nicht mit der IT-Sicherheit vertraute Inhaltsverantwortliche weitergeleitet oder es fehlen klare Kontaktinformationen. Solche Hindernisse verzögern die Behebung von Sicherheitsproblemen und erhöhen das Risiko, dass Meldungen verloren gehen.

Um die Kontaktaufnahme mit den zuständigen Personen zu vereinfachen, schlägt RFC 9116 vor, auf Webseiten die Datei „security.txt" zu hinterlegen [2]. Der Nutzen dieser Maßnahme wird auch durch eine Empfehlung des Bundesamts für Sicherheit in der Informationstechnik unterstrichen [3]. Der Standard sieht zwei Ablageorte für die Datei security.txt vor: entweder im Root-Verzeichnis, also unter „/security.txt", oder unter „/.well-known/security.txt". Hinterlegt werden dort Kontaktdaten und optional weitere relevante Informationen. Der Mindestumfang besteht aus den Angaben „Contact" und „Expires", wobei letzteres ein Ablaufdatum der Gültigkeit angibt. Die Angabe weiterer Felder, etwa „Encryption", „Acknowledgements", „Preferred-Languages", „Canonical", „Policy" und „Hiring", ist nicht verpflichtend. Abb. 2 zeigt beispielhaft den Inhalt einer „security.txt"-Datei.

Abb. 2 | Beispielinhalt der Datei „security.txt"

```
Contact: mailto:security@example.com
Encryption: https://example.com/pgp-key.txt
Policy: https://example.com/disclosure-policy.html
Expires: 2021-12-31T18:37:07z
```

3 Studiendesign

3.1 Vorgehensweise

Als Datenbasis diente uns die täglich aktualisierte Liste aller deutschen Hochschulen, die auf der Webseite „Hochschulkompass" (https://hs-kompass.de/kompass/xml/download_hochschule.htm) unter der URL https://hs-kompass.de/kompass/xml/download/hs_liste.txt abrufbar ist. Diese Liste enthält unter anderem die URLs der Homepages aller Hochschulen.

Mittels eines Skripts haben wir am 23.03.2023 für jede der 420 in dieser Liste enthaltenen Webseiten geprüft, ob die Datei „security.txt“ an einem der beiden standardisierten Orte abrufbar und ob das „Contact“-Feld enthalten ist. Acht Webseiten mussten auf Grund von technischen Problemen von Hand geprüft werden.

Da die Liste des Hochschulkompass‘ keine E-Mail-Adressen enthält, haben wir die für die Benachrichtigung zu verwendenden E-Mail-Adressen aus dem Impressum der jeweiligen Webseiten ermittelt. Dazu wurde mittels eines Skripts auf der Homepage nach den Begriffen „Impressum“, „imprint“, „contact“ und „Kontakt“ gesucht. Wurde eine entsprechende URL gefunden, wurde dort nach einer geeigneten Kontakt-E-Mail-Adresse gesucht. Diese wurde für die Benachrichtigung genutzt. Der Versand der E-Mails erfolgte am 23.03.2023.

Bei einigen E-Mails erhielten wir automatisierte Antworten, die darauf hindeuteten, dass unsere Nachricht nicht zugestellt werden konnte. Bei den betroffenen Hochschulen haben wir die Zustellung am 24.03.2023 erneut versucht. Bei acht Hochschulen scheiterte die Zustellung weiterhin. Diese waren gleichmäßig auf unsere Versuchsgruppen verteilt, sodass keine systematische Verzerrung der Ergebnisse zu erwarten war.

Nach dem Versand unserer Benachrichtigungen haben wir mehrmals überprüft, ob die Hochschulen zwischenzeitlich die Datei „security.txt“ auf ihren Webseiten angelegt hatten. In diesem Beitrag stellen wir die Ergebnisse für die Messungen dar, die 100 Tage nach dem Aussenden der Benachrichtigungen, sowie für die Messungen, die unmittelbar vor dem Aussenden unserer Debriefing-Nachricht und nach dem Aussenden der Debriefing-Nachricht erfolgten.

3.2 Inhalt unserer E-Mails

Um zu untersuchen, welche Faktoren die Bereitschaft zur Einführung der „security.txt“-Datei beeinflussen, haben wir die Hochschulen in vier Versuchsgruppen und eine Kontrollgruppe aufgeteilt und den Inhalt unserer E-Mails variiert. Die Basis für unsere E-Mails war folgender Text, der in allen E-Mails verwendet wurde:

Guten Tag,
wir schreiben Ihnen, weil Ihre E-Mail-Adresse als Kontaktadresse für die Webseite […] aufgeführt ist. Wir sind eine Gruppe von Studierenden verschiedener Hochschulen und befassen uns mit dem 2017 eingeführten Sicherheitsstandard security.txt. Dieser Standard wurde vom IETF als RFC 9116 veröffentlicht und wird allen Webseitenbetreibern empfohlen. Es handelt sich dabei um eine .txt-Datei auf einem Webserver. In dieser Datei werden Kontaktinformationen hinterlegt, an die gefun-

dene Sicherheitsprobleme gemeldet werden können. Wir möchten die Verbreitung dieses Standards fördern.
Bei unserer Recherche ist uns aufgefallen, dass auf Ihrem Webserver noch keine security.txt- Datei vorhanden ist. Die Implementation ist nicht aufwändig und kann in wenigen Minuten umgesetzt werden.
Bei Fragen stehen wir Ihnen gerne zur Verfügung.
Mit freundlichen Grüßen
[…]
Diese Mail wurde im Rahmen eines studentischen wissenschaftlichen Projekts verschickt. Beteiligt sind Studierende der Universität zu Köln, Universität Münster, RWTH Aachen und Universität Groningen. Datenschutzhinweise zur Studie finden Sie auf security-txt-research.de

Die Erkenntnisse früherer Studien zur möglichst effektiven Ansprache bei Benachrichtigungen zu Sicherheits- und Datenschutzaspekten [4, 5, 6] deuten darauf hin, dass die Effektivität einer Benachrichtigung gesteigert werden kann, indem sie um eine kurze zusätzliche Hilfestellung ergänzt wird. Dazu wurde der Inhalt ausgewählter E-Mails wie folgt ergänzt:

Hilfestellung:
1. Erstellen Sie ein Textdokument „security.txt" in dem Verzeichnis /.well-known/ Ihrer Webseite. Falls das aus technischen Gründen nicht möglich ist, kann die Datei auch in das root-Verzeichnis aufgenommen werden.
2. Das Textdokument sollte mindestens Kontakt- daten in der Form „Contact: mailto:security@example.com" enthalten. Genauere Informationen zum Aufbau finden Sie im Internet, zum Beispiel unter: securitytxt.org

Der zweite Aspekt, den wir variierten, leitete sich aus Gesprächen mit Mitarbeitenden eines Hochschulrechenzentrums ab. Diese äußerten, dass man sich bei Sicherheitsmaßnahmen zumeist daran orientiere, welche Maßnahmen die benachbarten Hochschulen ergriffen. Um diesen „Peer Pressure"-Effekt in den Benachrichtigungen zu erzeugen, nahmen wir in einen Teil unserer E-Mails den Hinweis auf, welche der benachbarten Hochschulen bereits eine „security.txt"-Datei veröffentlicht hat:

{Andere Hochschule} hat dies bereits umgesetzt (siehe Adresse {URL zur security.txt an der anderen Hochschule})

Jede Versuchs- und die Vergleichsgruppe umfasste jeweils 80 bzw. 81 Hochschulen. Bei der Erzeugung der Gruppen haben wir darauf geachtet, die Hochschulen hinsichtlich ihrer Eigenschaften „Bundesland", „Hochschultyp" und „Größe" gemäß der Hochschulliste gleichmäßig auf die Gruppen zu verteilen. Die vollständigen Texte der E-Mails und den Datensatz haben wir veröffentlicht [7].

3.3 Ethik und Datenschutz

Vor der Durchführung der Studie haben wir abgeklärt, dass unser Vorgehen sowohl forschungsethisch als auch rechtlich unbedenklich ist.

Wie bei anderen Benachrichtigungsstudien haben wir die untersuchten Hochschulen angeschrieben ohne sie vorher zu fragen, ob sie an der Studie teilnehmen möchten. Auch haben wir in unserer ersten Nachricht unser Studiendesign nicht offengelegt. Die Empfänger wussten also nicht, dass wir überprüfen würden, ob eine Hochschule nach unserer E-Mail die „security.txt"-Datei anlegt und dass wir die Hochschulen mit verschiedenen E-Mail-Varianten angeschrieben haben. Dieser Eingriff in die Autonomie der Empfänger bedarf einer ethischen Rechtfertigung. In unserem Fall war er erforderlich, um aussagekräftige Daten zu gewinnen und beispielsweise eine Verzerrung des Verhaltens durch Beobachtungseffekte zu vermeiden. Wie bei solchen Studien üblich erfolgte die Aufklärung der untersuchten Hochschulen über die Studie zu einem späteren Zeitpunkt in einer gesonderten E-Mail („Debriefing").

Weiterhin ist eine Abwägung möglicher Schäden und Nutzen angezeigt. Die Bearbeitung unserer E-Mails könnte kurzfristig erheblichen Mehraufwand erzeugen, etwa wenn sich IT-Personal und Hochschulgremien intensiv damit auseinandersetzen. Angesichts der einfachen Umsetzung ist dies jedoch im Regelfall nicht zu erwarten. Auf Dauer verursacht die Veröffentlichung und Pflege einer „security.txt"-Datei keinen nennenswerten Aufwand. Diesen Kosten steht der Nutzen gegenüber, dass eine „security.txt"-Datei im Falle der Entdeckung einer Schwachstelle eine schnellere und effizientere Benachrichtigung erlaubt und möglicherweise verhindert, dass es zu deren Ausnutzung und einem schweren IT-Sicherheitsvorfall kommt. In der Gesamtschau erscheinen uns die Kosten im Vergleich zum Nutzen daher vertretbar.

Aus rechtlicher Sicht sind insbesondere Anforderungen der DSGVO zu beachten. Der Versand der E-Mails erfolgte von einem deutschen E-Mail-Anbieter, mit dem wir einen Vertrag zur Auftragsverarbeitung geschlossen haben. Unter der in unserer Absender-E-Mail-Adresse verwendeten Domain war eine Webseite mit den nach Art. 13 und 14 DSGVO erforderlichen Informationen hinterlegt. Auf diese wiesen wir die Empfänger in unserer Debriefing-Mail auch noch einmal explizit hin.

4 Ergebnisse

Von den 420 Hochschulen in unserem Datenbasis hatten zu Beginn der Studie 17 Hochschulen eine „security.txt" veröffentlicht. Weitere drei Hochschulen, deren Webseiten Subdomains der Webseiten der betreffenden Bundesländer sind, mussten sich nicht selbst um die Bereitstellung kümmern, da die Webseiten des Bundeslands eine „security.txt"-Datei bereitstellten. Auch wenn gemäß dem Sicherheitsstandard RFC 9116 jede Subdomain ihre eigene Security.txt besitzen sollte, haben wir dies als im weiteren Sinne existierende Security.txt gewertet und nicht weiter betrachtet.

Von unseren ursprünglich versandten 322 E-Mails konnten acht nicht zugestellt werden. Bei 27 Hochschulen kam eine automatische Eingangsbestätigung; bei drei dieser Hochschulen antwortete in den darauffolgenden Wochen ein Mensch, in zwei dieser Fälle wurde die „security.txt"-Datei angelegt. Auf 279 (87%) unserer E-Mails erhielten wir keine Antwort.

100 Tage nach dem Versand unserer Benachrichtigungen hatte keine Hochschule aus der Kontrollgruppe die „security.txt"-Datei eingeführt. In allen anderen Versuchsgruppen haben hingegen einige Hochschulen die Datei angelegt. Über den gesamten Zeitraum waren dies in der Gruppe „einfache Benachrichtigung" fünf (6%), in der Gruppe „mit Hilfestellung" acht (10%), in der Gruppe „mit Peer Pressure" vier (5%) und in der Gruppe „mit Hilfestellung und Peer Pressure" ebenfalls vier (5%). Insgesamt

hatten somit nach 100 Tagen 21 weitere Hochschulen die „security.txt“-Datei eingeführt.

Zwischen der Messung am 03.08.2023 und dem Debriefing am 11.11.2023 führten drei weitere Hochschulen die Datei ein; eine Woche nach der Übermittlung des Debriefings per E-Mail (auch an die Hochschulen in der Kontrollgruppe) existierte die „security.txt“ bei weiteren 16 Hochschulen (nicht nur aus der Kontrollgruppe).

Bei einer letzten Überprüfung am 30.03.2024 war die „security.txt“ auf den Seiten von 59 Hochschulen vorhanden. Zwei Hochschulen, die die „security.txt“ nach unserer Benachrichtigung angelegt hatten, hatten sie am 30.03.2024 wieder entfernt.

5 Diskussion

Der Einfluss des Inhalts der Benachrichtigungen war geringer als erwartet – aus den Ergebnissen ist kein starker Einfluss der Varianten „mit Hilfestellung“ und „mit Peer Pressure“ auf die Einführung der „security.txt“ erkennbar.

Die geringe Verbreitung der „security.txt“-Datei auf den Webseiten deutscher Hochschulen und die geringe Bereitschaft zur Einführung lässt sich allerdings nicht auf alle Webseiten verallgemeinern. Auch lassen sich die Beobachtungen nicht auf andere empfohlene Sicherheitsmaßnahmen übertragen, da dort möglicherweise andere Entscheidungskriterien eine Rolle spielen und andere Anreizsysteme existieren.

Für den hohen Anteil an benachrichtigten Hochschulen ohne Reaktion können mehrere Gründe ursächlich sein. Zum einen haben wir unsere Nachrichten nach Möglichkeit an die E-Mail-Adressen verschickt, die im Impressum der Hochschulwebseiten angegeben waren. Es ist daher vorstellbar, dass die angeschriebenen Personen sich nicht für technische Fragen zuständig fühlten oder unsere Nachricht nicht an die richtige Stelle weitergeleitet haben. Wir können allerdings keine Schlüsse darauf ziehen, wie effektiv die Kontaktaufnahme über das Impressum bei der Meldung einer schwerwiegenderen Schwachstelle wäre.

Möglicherweise wurde unseren Nachrichten auch keine große Bedeutung beigemessen, weil sie – wie in den E-Mails kommuniziert – im Rahmen eines studentischen Projekts versandt wurden. Es erscheint lohnend, in zukünftigen Studien zu untersuchen, ob bei einer Benachrichtigung durch Einrichtungen, die den Hochschulen bekannt sind, etwa das BSI oder das DFN-CERT, die Bereitschaft zum Handeln größer ist.

6 Fazit

Unsere Studie hat dazu beigetragen, den Anteil der Hochschulen, die eine „security.txt“-Datei auf ihren Webseiten veröffentlichen, zu steigern. Ausgehend von 20 Seiten im März 2023 hat sich die Zahl auf 59 Seiten im März 2024 etwa verdreifacht. Angesichts der geringen Umsetzungsrate sind die beobachteten Unterschiede zwischen den Versuchsgruppen „mit Hilfestellung“ und „mit Peer Pressure“ allerdings zu gering, um Aussagen über die Effektivität dieser Formulierungsvarianten abzuleiten.

Der geringe Umsetzungsgrad und der insgesamt sehr geringe Rücklauf auf unsere Benachrichtigungen ist angesichts der einfachen Umsetzbarkeit und trotz aktueller Sicherheitsvorfälle im Hochschulsektor überraschend.

Sofern die Hinweise ignoriert wurden, weil sie von Studierenden stammten, könnte das dazu führen, dass auch Studierende, die Schwachstellen verantwortungsbewusst melden, sich nicht ernst genommen fühlen und dies zukünftig unterlassen. Es bleibt zu hoffen, dass die Hochschulen besser reagieren, wenn ihnen akute Schwachstellen gemeldet werden oder wenn sie Hinweise von Organisationen erhalten, die ihnen bekannt sind, etwa dem Bundesamt für Sicherheit in der Informationstechnik oder dem CERT des Deutschen Forschungsnetzes.

References

[1] Eva Wolfangel. *Er hat die Server von Unis gehackt. Zum Glück ist er einer von den Guten*. ZEIT Nr. 04/2023 https://www.zeit.de/2023/04/it-sicherheit-hochschule-sicherheitsluecken-hacker.

[2] Edwin Foudil and Yakov Shafranovich. *A File Format to Aid in Security Vulnerability Disclosure*. RFC 9116, April 2022. https://www.rfc-editor.org/info/rfc9116.

[3] Bundesamt für Sicherheit in der Informationstechnik, *Sicherheitskontakte mit Hilfe einer security.txt nach RFC 9116 angeben*, BSI-CS149,09.04.2024 https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/TechnischeRichtlinien/TR02102/BSI-TR-02102-2.pdf?__blob=publicationFile&v=7

[4] Ben Stock, Giancarlo Pellegrino, Frank Li, Michael Backes, and Christian Rossow. *Didn't you hear me? – towards more successful web vulnerability notifications*. In: Network and Distributed System Security (NDSS). February 2018. https://publications.cispa.de/articles/conference_contribution/Didn_t_You_Hear_Me_---_Towards_More_Successful_Web_Vulnerability_Notifications/24612648.

[5] Max Maass, Alina Stöver, Henning Pridöhl, Sebastian Bretthauer, Dominik Herrmann, Matthias Hollick, and Indra Spiecker. *Effective notification campaigns on the web: A matter of trust, framing, and support*. In: 30th USENIX Security Symposium

[6] Qasim Lone, Alisa Frik, Matthew Luckie, Maciej Korczyński, Michel van Eeten, and Carlos Gañán. *Deployment of Source Address Validation by Network Operators: A Randomized Control Trial*. In: 2022 IEEE Symposium on Security and Privacy (SP), San Francisco, CA, USA, 2022.

[7] Eckstein, F., Rosenauer, R. M. A., & Huppert, P. (2024). Schwer erreichbar: security.txt an deutsche Hochschulen bringen – Datensätze und Scripte [Data set]. Zenodo. https://doi.org/10.5281/zenodo.13683979