This document contains the description of our project that we agreed on with the data protection officer.
The document contains the description of a second part of the study that was originally planned, but that we didn’t conduct. The affected part is marked red. We also didn’t collect all the data that we originally intended to. This part is also marked red.

Studie zur Verbesserung der E-Mail-Sicherheit an der LUH

Gemeinsam mit dem LUIS plant das Fachgebiet IT-Sicherheit der Fakultät für Elektrotechnik und Informatik eine Untersuchung der E-Mail Sicherheit an der LUH mit dem Ziel die Sicherheit von E-Mail in Zukunft weiter zu erhöhen. Das LUIS setzt bereits wenn möglich bestmögliche Sicherheitsstandards ein. So werden E-Mails auf dem Transportweg wenn möglich mit TLS verschlüsselt, es werden für die E-Mailkonten sichere Passwortrichtlinien eingesetzt und moderne Spamfilter und Antivirensoftware genutzt. Desweiteren bietet das LUIS seit 2003 eine Zertifizierungsstelle für S/MIME Zertifikate an, mit denen E-Mailnutzer*innen ihre Kommunikation Ende-zu-Ende verschlüsseln können, um maximale Sicherheit zu erreichen. Der Einsatz und das Angebot der oben genannten Sicherheitstechnologien auf Seiten des LUIS als Diensteanbieter ist jedoch nur ein Teilaspekt von E-Mail-Sicherheit. Dem LUIS ist bisher nicht bekannt welche der gebotenen Sicherheitsmaßnahmen von ihren Nutzer*innen tatsächlich zum Einsatz kommen. Im Rahmen der geplanten Studie soll darüber Kenntnis erlangt werden und basierend auf den Ergebnissen weitere Maßnahmen ergriffen die E-Mail-Sicherheit an der LUH weiter zu erhöhen.

Die Studie wird in drei Phasen durchgeführt werden. Im Anschluss daran werden Maßnahmen entwickelt, die zur Erhöhung der E-Mail-Sicherheit geeignet sind. In den ersten beiden Phasen werden vorhandene bzw. noch zu generierende Logfiles, welche am LUIS für einen sicheren und fehlerfreien Betrieb notwendig sind genutzt. Im Rahmen der Sicherheitsanalyse werden personenidentifizierende Merkmale (PII) pseudonymisiert, um Datenschutzrechte der Nutzer von E-Mail an der LUH zu gewährleisten. Das genaue Vorgehen zur Pseudonymisierung wird weiter unten dargelegt.

Zum einen werden zur E-Mail-Sicherheit gehörige Metadaten von versandten und empfangenen E-Mails der letzten 25 Jahre untersucht. Eine Untersuchung über einen solch langen Zeitraum wird nicht nur dabei helfen wie die Situation im Hinblick auf E-Mail-Sicherheit aktuell ist, sondern wird auch dabei helfen zu erkennen wie schnell neue Sicherheitsmechanismen von Nutzer*innen in der Vergangenheit angenommen worden sind. Es ist geplant folgende Sicherheitsaspekte und Metadaten einer Sicherheitsanalyse zu unterziehen:

- Erhebung der Nutzung von Ende-zu-Ende Verschlüsselung: Hierzu wird in E-Mails die Nutzung von PGP und S/MIME überprüft. Dies schließt eine Überprüfung der verwendeten kryptographischen Parameter (Algorithmen, Schlüsselgrößen, Gültigkeitsdauer von Zertifikaten) mit ein. Diese Daten werden aus technischen Gründen als Datei im Anhang einer E-Mail oder im E-Mail-Header gesendet.[1]
- Effektivität der an der LUH eingesetzten Spamfiltermechanismen: Hierzu werden Spamfilterkennzahlen für E-Mails aus E-Mailheadern und der entsprechende Mailboxordner (z.B. Inbox) ausgewertet.

[1] Korrektur des ursprünglichen Dokuments: Im ursprünglichen Dokument hieß es, dass die Daten nur aus dem Header ausgelesen werden. Zu weiteren Details siehe Ergänzungsdokument: “Ergänzung: Studie zur Verbesserung der E-Mail-Sicherheit an der LUH“

- Aktualität der verwendeten E-Mailclients, um die Nutzung unsicherer Clients festzustellen: Überprüfung der verwendeten E-Mailclients und genutzter Erweiterungen durch Analyse des User-Agent E-Mailheaders und der Client-Informationen beim Login.
- Verwendung von DKIM (DomainKeys Identified E-Mail): Überprüfung der Nutzung von DKIM als Anti-Spammechanismus durch Analyse von E-Mailheader Informationen.

Überblick über analysierte Sicherheitsparameter pro Email

Datum	**Enthält PII**	**Pseudonymisierung**
Tag/Uhrzeit	nein	-
Absender	ja, wird pseudonymisiert	random ID
Empfänger	ja, wird pseudonymisiert	random ID
Gruppenzugehörigkeit	ja, wird anonymisiert	Fakultät/Studierend/Nichtwissenschaftliches Personal
Postfach (z.B. Inbox)	evtl, wird pseudonymisiert	inbox, outbox, spam, 30dTrash, junk, other
Nutzung von PGP/S/MIME - Zertifikat - Zertifizierungsstelle - Signatur - Verschlüsselt - Gültigkeit: Start-Ende - Signaturalgorithmus - Schlüsselgröße - Schlüsseltyp	- nein - ja, wird pseudonymisiert - nein - nein - nein - nein - nein - nein - nein - nein	- random ID - - - - - - - -
Verwendeter Client - Typ - Version - Betriebssystem - Plugins	- nein - nein - nein - nein - nein	- - - - -
Verwendung von DKIM	- nein	-
Nachrichtenverlauf (References, Message ID)	- ja, wird pseudonymisiert	randomID
Spam detection Ergebnisse - DFN spam detection - LUIS spam detection	- nein	-

Zum zweiten werden aktuelle Logfiles der E-Mailserver (Eingangs- (IMAP/POP3) und Ausgangsserver (SMTP)) im Hinblick auf verwendete Sicherheitsparameter untersucht. Auch hierbei ist geplant ausschließlich folgende Metadaten zu analysieren:

- Identifikation des verwendeten Anmeldeprotokolls der Nutzer der LUH. Im Mittelpunkt steht hierbei die Fragestellung ob und wenn ja mit welchen kryptografischen Parametern TLS zur Übertragung zwischen Client und E-Mailservern der LUH verwendet werden.
- Analyse der verwendeten E-Mailclients (Clientsoftware, Version/Patchstand, Betriebssystem)
- Für E-Maileingangs- und Ausgangsserver wird des weiteren das verwendete Netzwerkprotokoll analysiert. Hierbei steht eine Sicherheitsanalyse der Transportsicherheit zwischen den E-Mailservern der LUH und den nächsten E-Mailrelays, die zur E-Mailkommunikation der LUH Nutzer genutzt werden, untersucht. Im Mittelpunkt liegt auch hier die Evaluation der verwendeten kryptographischen Parameter für das TLS Protokoll.

Überblick über analysierte Sicherheitsparameter pro Logeintrag

Datum	**Enthält PII**	**Pseudonymisierung**
Tag/Uhrzeit	nein	-
Absender	ja, wird pseudonymisiert	random ID
Empfänger	ja, wird pseudonymisiert	random ID
Gruppenzugehörigkeit	ja, wird anonymisiert	Fakultät/Studierend/Nichtwissenschaftliches Personal
Emailprotokoll	- nein	IMAP, POP3, SMTP
Passwortsicherheit - zxcvbn[2]	- nein	-
Nutzung von TLS/STARTTLS - version - kex - selected cipher suite - list of supported cipher suites	- nein - nein - nein - nein - nein	-
Login-Location	ja, wird pseudonymisiert	random ID
Nutzung von PGP/S/MIME	- nein (s. oben)	-
Verwendeter Client	- nein (s. oben)	-

[2] https://www.usenix.org/conference/usenixsecurity16/technical-sessions/presentation/wheeler

Um den Datenschutz der Nutzer*innen der LUH und ihrer Kommunikationspartner*innen zu gewährleisten, wird auf Seiten des LUIS eine Pseudonymisierung aller PII vorgenommen. Insbesondere werden E-Mailadressen und S/MIME bzw. PGP Zertifikate pseudonymisiert. Im Rahmen der Pseudonymisierung wird auf die Nutzung von Hashfunktionen verzichtet, da diese Rückschlüsse auf einzelne Nutzer*innen zulassen würden. Auf Seiten des LUIS werden PII durch zufällige IDs ersetzt und in einer Datenbank gespeichert, die nur dem LUIS zugänglich ist. Eine Gruppierung von Nutzer*innen geschieht lediglich auf Fakultätsebene bzw. Zugehörigkeit zu den Gruppen “Studierende” und “Nichtwissenschaftliches Personal”. Dies stellt sicher, dass die beteiligten Forscher*innen des Fachgebiets IT-Sicherheit der LUH keinen Zugriff auf PII erlangen und keine Rückschlüsse auf einzelne Nutzer*innen schließen können. Insbesondere werden im Rahmen der Sicherheitsanalyse keine IP Adressen verarbeitet und gespeichert.

Basierend auf den Ergebnissen der oben beschriebenen Sicherheitsanalyse wird das LUIS gemeinsam mit dem Fachgebiet IT-Sicherheit eine Onlineumfrage unter allen E-Mailnutzer*innen an der LUH durchführen, um weitere Hintergrundinformationen zu erfahren. Die Umfrage wird beispielsweise analysieren welche Erfahrungen Nutzer*innen in der Vergangenheit mit dem Einsatz von S/MIME und der Zertifizierungsstelle am LUIS gemacht haben. Weitere Details der Umfrage werden sich im Rahmen der Sicherheitsanalyse ergeben.

Abschließend werden neue Maßnahmen entwickelt, um die E-Mailsicherheit an der LUH weiter zu erhöhen. Mögliche Maßnahmen sind etwa geänderte Passwortrichtlinien, Anleitungen zur Verwendung sicherer E-Mailclients und die Überarbeitung der Nutzerschnittstelle der LUH Zertifizierungsstelle. Auch hier werden sich konkrete Maßnahme im Laufe der Sicherheitsanalysen ergeben.

Datenschutzrechtliche Bewertung

Abwägung nach § 13 Abs. 1 S. 1-2 Niedersächsisches Datenschutzgesetz (NDSG)

Die Datenschutzrechtliche Zulässigkeit dieses Projektes beruht auf § 13 NDSG[3]. Demnach dürfen zu wissenschaftlichen Forschungsvorhaben personenbezogene Daten verarbeitet werden, solange die Verarbeitung keinem schutzwürdigen Interesse der betroffenen Person entgegensteht (a) und das öffentliche Interesse an der Durchführung des Forschungsvorhabens das schutzwürdige Interesse der betroffenen Person überwiegt (b), § 13 Abs. 1 S. 2-3 NDSG.

- (a) Kein entgegenstehendes schutzwürdiges Interesse der betroffenen Personen

Schutzwürdiges Interesse der betroffenen Person ist der Schutz personenbezogener Daten aus Art. 8 Grundrechte-Charta. Dieses Interesse darf das Interesse der Forscher*innen an der Datenverarbeitung im Forschungsprojekt nicht überwiegen. Dies ist dann der Fall, wenn

---

3 http://www.nds-voris.de/jportal/?quelle=jlink&query=DSG+ND+%C2%A7+13&psml=bsvorisprod.psml&max=true

die Datenverarbeitung verhältnismäßig ist. Dazu müsste die Verarbeitung einem legitimen Zweck dienen, geeignet sein, einen der Zwecke zu fördern sowie erforderlich und angemessen sein.

Der legitime Zweck liegt hierin darin, dass die Frage geklärt werden soll, ob und wie Nutzer*innen Verschlüsselung und Signaturen in E-Mails nutzen. Darin ist ein legitimes Ziel zu sehen, das von Art. 5 Abs. 3 GG erfasst ist.

Die Verarbeitung müsste auch geeignet sein, um den Zweck zu fördern. Durch das analysieren der verwendeten Verschlüsselungen und Signaturen in E-Mails, können die Wissenschaftler*innen auf Grundlage dieser Erkenntnisse Empfehlungen zur Verbesserung der E-Mail Sicherheit entwickeln. Die Datenverarbeitung ist also auch geeignet.

Erforderlich ist die Datenverarbeitung, wenn es kein milderes Mittel gibt, um denselben Erfolg zu erzielen. Andere Maßnahmen könnten darin bestehen, Studien mit einzelnen freiwilligen Nutzer*innen durchzuführen, die ihre Mailboxdaten anderweitig zur Verfügung stellen. Jedoch hätte eine solche Methode zur Folge, dass ein unvollständiges Bild über durchschnittliche E-Mail Nutzer*innen entsteht und keine zuverlässigen wissenschaftlichen Erkenntnisse auf solch einem Weg erzielt werden können. Eine Auswertung der pseudonymisierte Metadaten aller Mailboxen ermöglicht den Wissenschaftler*innen jedoch einen Einblick in die historische Entwicklung zur Nutzung von E-Mailverschlüsselung und eine wissenschaftliche Einordnung welche Maßnahmen und Ereignisse zur Verbesserung der E-Mailsicherheit beigetragen haben und zukünftige Maßnahmen mit Hilfe dieser Informationen zu verbessern. Es gibt also kein milderes gleich geeignetes Mittel.

Die Datenerhebung müsste auch angemessen sein. Dies ist dann der Fall, wenn der beabsichtigte Zweck nicht außer Verhältnis zu der Schwere des Eingriffs steht. Dies ist gewährleistet, da nur die nötigsten personenbezogenen Daten mit geringer Schutzstufe erhoben werden. Es handelt sich hierbei um die E-Mail Adresse sowie Zertifikate zum Verschlüsseln. Es handelt sich hierbei um Daten geringer Schutzstufe (max. Schutzstufe B) und es werden keine Inhalte der Mails ausgewertet. Ferner ist der Zweck der Verarbeitung keine Leistungsbewertung der betroffenen Person sondern eine Analyse der Nutzung von Verschlüsselung und Signatur.
Gemäß § 13 NDSG Absatz 2 werden die personenbezogenen Daten pseudonymisiert, wobei die personenbezogenen Daten grundsätzlich am Fachgebiet IT-Sicherheit pseudonymisiert verarbeitet werden und die entsprechende Referenztabelle am LUIS unter Verschluss liegt. Im Rahmen einer Umfrage erfordert der Forschungszweck eine de-pseudonymisierung, um die Erfahrungen der betroffenen Person mit den erhobenen Daten zu vergleichen, dies geschieht nur mit ausdrücklicher Zustimmung der betroffenen Person.
Die Referenztabelle wird nach der Verarbeitung der Daten gelöscht, da sie nicht zur Reproduktion der Ergebnisse benötigt wird. Dies geschieht spätestens zum 31.12.2021.
Der Empfehlung der Deutschen Forschungsgemeinschaft und § 5 der Ordnung der Gottfried Wilhelm Leibniz Universität Hannover zur Sicherung guter wissenschaftlicher Praxis folgend, werden die erhobenen Daten 10 Jahre durch das LUIS verschlüsselt archiviert.

Ein Rückschluss auf einzelne Nutzer*innen ist also nicht möglich, sodass die Interessen der Forscher*innen der der Nutzer*innen überwiegen. Die Verarbeitung ist deshalb angemessen.

Insgesamt ist die Datenverarbeitung also verhältnismäßig, sodass die schutzwürdigen Interessen der betroffenen Personen nicht dem Interesse der Forscher*innen an der Datenverarbeitung überwiegen. Mithin können sich die Wissenschaftler*innen auf das Forschungsprivileg aus § 13 NDSG beziehen.

- (b) Überwiegendes öffentliches Interesse

Das öffentliche Interesse besteht hier darin, dass die Frage geklärt wird, ob und wie Nutzer*innen E-Mailverschlüsselung und Signaturen nutzen. Dies kann in der Zukunft dazu beitragen bessere Maßnahmen zur Verbesserung der E-Mailsicherheit an der LUH zu entwickeln. Das öffentliche Interesse besteht konkret darin, potentielle Probleme zu identifizieren, die Nutzer*innen bei der sicheren Nutzung von E-Mail haben und Maßnahmen zu entwickeln, die diese Probleme angehen um die generelle IT-Sicherheit an der LUH zu verbessern. Genau dabei soll dieses Forschungsvorhaben behilflich sein. Es liegt demzufolge ein legitimer Zweck vor. Die Datenverarbeitung ist auch – wie oben beschrieben – geeignet, erforderlich sowie angemessen und mithin verhältnismäßig. Das öffentliche Interesse überwiegt somit das schutzwürdige Interesse der betroffenen Person, sodass sich auch hiernach die Wissenschaftler*innen auf das Forschungsprivileg aus § 13 NDSG beziehen können.

Im Rahmen der Verarbeitung zu Forschungszwecken erfolgt keine Information der betroffenen Personen (Ausnahmen von den Informationspflichten nach Art. 14 DSGVO). Der Aufwand alle Nutzer*innen zuverlässig zu informieren ist unverhältnismäßig (Art. 14 Abs. 5 lit. b. S. 1 Hs. 1 Alt. 1 DSGVO), da keine einzelnen Nutzer*innen während der Analyse identifiziert werden und nicht alle Mailadressen über eine Mailingliste erreicht werden können.

Beispiel Daten einer Signierten Email

Datum	**Original**	**Anonymisiert / Pseudonymisiert**
Tag/KW	16.05.19 14:42 Uhr	KW 20 2019
Absender	sender@mail.de	2b3325cc902077cd96df2b2111b6a4da
Empfänger	empfänger@stud.uni-hannover.de	ad457af2047b8ff38004b2356c6e83dd
Gruppenzugehörigkeit	Studierender	f5c0a1c9384c2e25e79ba1abf5d9a037
Postfach	Posteingang	inbox
Client	Thunderbird/60.6.1	Thunderbird/60.6.1
Betriebssystem	Windows	Windows
Konversationsverlauf	trinity-6338150f-064c-4243-aa77-d56d0e62a92e-1550225565245@3c-app-gmx-bs42, 1bc23cdc-124-ab31-2612-7331e7a4asd@stud.uni-hannover.de, trinity-7d6a9e0a-edee-45a7-b28c-4ddbe43c8a7f-1551643293434@3c-app-gmx-bs80	00a100c7a0f2f524ae3c5e98dec42108, ca626903860c4f5897ff0099c9f4eaf9, a65f440a0c9e3be84f186ba9e4be59a8
X-Spam-Flag	Nein	Nein
Verschlüsselt	Nein	Nein
Signiert	Ja	Ja
Zertifikatstyp	S/MIME	S/MIME
Zertifikatsgültigkeit	10. Januar 2019 - 10. Januar 2020	Januar 2019 - Januar 2020
Schlüssellänge	RSA 2048 bits	RSA 2048 bits
Zertifizierungsstelle	Sectigo RSA Client Authentication and Secure Email CA	Sectigo RSA Client Authentication and Secure Email CA
Signaturalgorithmus	sha256	sha256