KIM: Kaos In der Medizin

Christoph Saatjohann [1], Fabian Ising [1] und Sebastian Schinzel [2]

Abstract: Die sichere E-Mail-Infrastruktur für Ärzt*innen, Apotheker*innen, Krankenversicherungen und Kliniken in Deutschland, KIM - Kommunikation im Gesundheitswesen - ist mit über 200 Millionen E-Mails in den vergangenen zwei Jahren eine der am meisten genutzten Anwendungen in der Telematikinfrastruktur. Mit dem Ausgeben von S/MIME-Zertifikaten für alle medizinische Beteiligten in Deutschland verspricht KIM sichere Ende-zu-Ende-Verschlüsselung von E-Mails zwischen Heilberufler*innen in ganz Deutschland.

In diesem Paper analysieren wir die KIM-Spezifikation sowie eine beispielhafte KIM-Installation in einer deutschen Zahnarztpraxis. Wir zeigen, dass KIM kryptografisch ein sehr hohes Sicherheitslevel erfüllt, doch in der Verarbeitung der E-Mails bei den Clients eine schwerwiegende Sicherheitslücke besteht. Weiterhin zeigen wir zwei Sicherheitslücken in dem KIM-Verarbeitungsmodul eines großen deutschen Unternehmens für medizinische Software. Diese Defizite zeigen außerdem Mängel in dem verpflichtenden Zulassungsprozess der KIM-Komponenten auf.

Keywords: KIM, Telematikinfrastruktur, gematik, eHealth

1 Einleitung

Nachdem weltweit mehr als 50 Menschen an Wechselwirkungen in Bezug auf das Arzneimittel *Lipobay* verstorben waren, planten Spitzenverbände des deutschen Gesundheitswesens die Einführung einer elektronischen Gesundheitskarte zur Dokumentation von Medikationen. Hieraus startete 2004 mit dem *GKV-Modernisierungsgesetz* das Vorhaben einer staatlich geförderten Digitalisierung des deutschen Gesundheitssystems. Nach einer Phase mit wenig öffentlich sichtbaren Fortschritten wurden im Jahr 2016 mit dem *E-Health-Gesetz* die deutschen Arztpraxen, unter Androhung von Honorarabzügen, verpflichtet, sich bis zum Sommer 2018 an die neu spezifizierte Telematikinfrastruktur (TI) anzuschließen.

Ein Vorteil der TI soll eine leicht zu bedienende, und dabei sichere, Kommunikationslösung zwischen Ärztinnen und Ärzte sein. Dazu wurde 2021 der sichere E-Mail-Dienst Kommunikation im Medizinwesen (KIM) eingeführt. Die Nutzung von KIM ist, auch weil es inzwischen die Basis für weitere Anwendungen in der TI ist, in den vergangenen zwei Jahren stark gestiegen. Zwischen der Einführung Mitte 2021 und dem Herbst 2023 wurden insgesamt über 215 Millionen KIM-Nachrichten in der TI verschickt [ge23b].

1 Fraunhofer SIT | ATHENE – National Research Center for Applied Cybersecurity, Steinfurt, Germany, christoph.saatjohann@sit.fraunhofer.de, https://orcid.org/0000-0002-0511-3616; fabian.ising@sit.fraunhofer, https://orcid.org/0000-0001-9852-1231

2 FH Münster | Fraunhofer SIT | ATHENE – National Research Center for Applied Cybersecurity, Steinfurt, Germany, schinzel@fh-muenster.de, https://orcid.org/0000-0002-7944-5488

Der Kern von KIM ist die Ende-zu-Ende-Verschlüsselung von Nachrichten. Im Gegensatz zu der elektronischen Patientenakte (ePA), welche auch medizinische Informationen verarbeitet und in einer externen Sicherheitsanalyse geprüft wurde [Sl20], gibt es für KIM keine öffentliche Sicherheitsanalyse der Spezifikation oder des Einsatzes im realen Praxisumfeld.

In diesem Beitrag analysieren wir die KIM-Spezifikation sowie den Einsatz in einer typischen Praxisumgebung, mit Fokus auf die lokale Verarbeitung von Nachrichten in der Praxis. Die gefundenen Schwachstellen wurden im Rahmen der Responsible Disclosure gemeldet und behoben. Unseres Wissens ist dies die erste akademische Analyse des KIM-Dienstes.

Verwandte Arbeiten Die TI und ihre Anwendungen werden regelmäßig auf Akzeptanz und Nutzungsverhalten wissenschaftlich evaluiert. Die letzte Evaluation wurde im Februar 2023 veröffentlicht [adHBO23]. Die Daten- und IT-Sicherheit der TI, insbesondere der ePA, steht im besonderen Fokus der Öffentlichkeit. Daher wurde 2020 die von der gematik beauftragte Sicherheitsanalyse einiger Kernelemente der ePA veröffentlicht [Sl20].

Im akademischen Umfeld gibt es aufgrund der engen Anwendungsbegrenzung der TI, eingesetzt ausschließlich in Deutschland, wenig vorherige Arbeiten. Die mentalen Modelle, die sich die Nutzer*innen in Deutschland zu der komplexen ePA bilden, werden in [Pa23] herausgearbeitet und mit der spezifizierten Architektur abgeglichen.

Zu E-Mail-Verschlüsselung und -Signaturen wurden in den vergangenen Jahren immer wieder Publikationen veröffentlicht. So zeigten bereits Müller et al. 2019 [Mü19], dass S/MIME-Signaturen auch in aktuellen E-Mail-Clients gebrochen werden können. 2022 analysierten Mayer et al. [Ma22], wie Experten-Nutzer*innen mit signierten E-Mails umgehen, und wie sie diese auf Manipulationen prüfen.

Danksagungen Christoph Saatjohann und Fabian Ising wurden teilweise vom Forschungsprojekt „North-Rhine Westphalian Experts in Research on Digitalization - NERD II (005-2201-0014)“ vom MKW NRW gefördert. Wir danken der beteiligten Zahnarztpraxis für die Unterstützung.

2 Grundlagen

2.1 S/MIME

Die Secure/Multipurpose Internet Mail Extensions (S/MIME) sind eine Erweiterung der, historisch-bedingt, unverschlüsselten E-Mail-Codierung-Formate Internet Message Format (IMF) und Multipurpose Internet Mail Extensions (MIME), die es erlauben, E-Mails zu verschlüsseln und zu signieren. Im Wesentlichen ergänzen sie die MIME um die neuen `Content-Types` `application/pkcs7-mime` und `application/pkcs7-signature`, die den Versand von S/MIME-kodierten Nachrichten in E-Mails erlauben. S/MIME-Nachrichten werden dabei durch Cryptographic Message Syntax (CMS)-Objekte abgebildet und Base64-kodiert als Body der E-Mail verschickt [RT10, SRT19].

2.2 Telematikinfrastruktur

Die Digitalisierung des Gesundheitswesens in Deutschland soll durch eine zentrale Infrastruktur mit verschiedenen medizinischen Anwendungen und Diensten beschleunigt werden. Dazu wird die sogenannten Telematikinfrastruktur (TI) seit 2005 von der gematik geplant und spezifiziert. Die Spezifikationen sind im Fachportal der gematik [ge23a] abrufbar. Die normativen Anforderungen werden mit einem eindeutigen Anforderungs-Identifikator (AFO-ID) nummeriert. Zu Themen der IT-Sicherheit ist die gematik verpflichtet eng mit dem Bundesamt für Sicherheit in der Informationstechnik (BSI) zusammenzuarbeiten.

Die eigentliche Vernetzung der medizinischen Institutionen wie Praxen und Apotheken startete Ende 2017 mit der Zulassung des ersten TI-Konnektors. Zum einen verbinden diese Konnektoren die Praxen mit der zentralen Infrastruktur und damit den Fachdiensten der einzelnen Anwendungen. Zum anderen führt der Konnektor mittels integriertem Hardware Security Module (HSM) kryptografische Funktionen wie Verschlüsselung oder Signaturüberprüfungen durch. Dazu bietet der Konnektor eine Simple Object Access Protocol (SOAP)-Schnittstelle an, welche von den Praxis-Clients angesprochen wird. Für die Installation der Konnektoren in den Institutionen wurden von der gematik Dienstleister vor Ort (DVOs) geschult, welche die Konnektoren und weiteren TI-spezifischen IT-Dienstleistungen mit einem einheitlichen Sicherheits-Standard in das Feld bringen und für eine regelmäßige Wartung Sorge tragen können. Hier hat sich in der Vergangenheit allerdings gezeigt, dass nicht alle durch DVOs durchgeführten Installationen dem Stand der Technik entsprechen [BKK19, Kl20]. Um die IT-Sicherheit der Praxen zu erhöhen, ist die Kassenärztliche Bundesvereinigung (KBV) seit 2020 gesetzlich verpflichtet eine Zertifizierung von IT-Dienstleistern anzubieten [So19].

Seit der Konnektor-Einführung wurden und werden graduell verschiedene Anwendungen dem medizinischen Personal sowie den Patienten zur Verfügung gestellt. Neben der ePA oder dem eRezept ist eine zentrale Anwendung der KIM-Dienst.

2.3 Kommunikation im Medizinwesen - KIM

Zur sicheren Kommunikation zwischen medizinischen Institutionen wie Praxen, Krankenhäusern und Versicherungen, wurde 2021, zuerst noch unter dem Namen *Kommunikation der Leistungserbringer (KOM-LE)*, KIM eingeführt. Mit KIM können Institutionen im deutschen Gesundheitswesen sicher, und damit datenschutzkonform, medizinische und personenbezogene Daten austauschen. Die Daten werden dabei Ende-zu-Ende verschlüsselt und signiert über die TI transportiert. KIM ist die Basis für weitere medizinische Anwendungen wie die elektronischen Arbeitsunfähigkeitsbescheinigung (eAU) oder den eArztbrief.

Aufbau KIM KIM kapselt die Funktionalität einer E-Mail-Infrastruktur inklusive Public Key Infrastructure (PKI) für die Nutzenden. Dazu definiert die gematik neben der

zentralen PKI-Infrastruktur, die jeder Nutzer*in ein Zertifikat zur Verfügung stellt, drei Akteure: den KIM-Fachdienst [ge21d], den Verzeichnisdienst (VZD) [ge21e] und das Clientmodul [ge21c].

KIM-Nachrichten sind dabei S/MIME-signierte und -verschlüsselte E-Mails. Hierbei wird auf eine Variante von sign-then-encrypt gesetzt, bei der die von der Absender*in verfasste E-Mail – die sogenannte „innere Nachricht“ – inklusive Headern kodiert wird und als Anhang an eine neue Nachricht angehängt wird. Diese wird signiert und dann verschlüsselt und um relevante Header ergänzt. Das Ergebnis ist die sogenannte „äußere Nachricht“.

Erwähnenswert ist, dass obwohl S/MIME in Version 3.2 [RT10] eingesetzt wird, der CMS-Typ `AuthEnvelopedData` genutzt wird, der die Verwendung von Authenticated Encryption (AE)-Algorithmen ermöglicht.

Der Fachdienst ist zum einen für die Vergabe von Zugangsdaten und Adressen zuständig und stellt zum anderen die Simple Mail Transfer Protocol (SMTP)-Infrastruktur für die Zustellung von KIM-Nachrichten zur Verfügung. Der VZD ist ein Lightweight Directory Access Protocol (LDAP)-Server, der für jede KIM-Teilnehmer*in einen Eintrag mit Daten wie E-Mail-Adresse und S/MIME-Zertifikat enthält und allen TI-Nutzer*innen zugänglich ist. Beide Dienste werden zentral angeboten – wobei es mehrere Fachdienst-Anbieter gibt.

KIM-Clientmodul Das KIM-Clientmodul ist eine üblicherweise lokal laufende Softwarekomponente, die die Funktionalität des KIM-Nachrichtenversands anwenderfreundlich kapseln soll. Es kann ggf. in das Praxisverwaltungssystem (PVS) integriert sein und erledigt die komplette Kommunikation mit dem Fachdienst (Versand und Empfang von E-Mails) und die Verschlüsselung und Signatur von KIM-Nachrichten. Es bietet lokal einen SMTP- und Post Office Protocol version 3 (POP3)-Proxy an, der den Abruf und Versand von KIM-E-Mails nutzerfreundlich über einen handelsüblichen E-Mail-Client ermöglichen soll [ge21c]. Diese Funktionalität kann auch durch das PVS zur Verfügung gestellt werden.

3 Analyse und Test-Umgebung

Für die theoretische Spezifikationsanalyse haben wir die entsprechenden Dokumente aus dem gematik-Fachportal geladen und manuell analysiert.

Für die technische Analyse der KIM-Einsatzumgebung hatten wir Zugriff auf eine Zahnarztpraxis mit ca. 20 Mitarbeiter*innen. Die Praxis ist seit 2019 über einen Secunet-Konnektor an die TI angeschlossen. Sowohl die initiale TI-Einrichtung als auch die weiteren TI-relevanten Änderungen, bspw. ein notwendiger Konnektoraustausch oder Lizenz-pflichtige Konnektorupdates werden durch einen von der KBV zertifizierten DVO durchgeführt.

Das KIM-Clientmodul ist auf dem zentralen Windows 2016 Server installiert, auf den die Clients über das lokale Praxisnetzwerk zugreifen. Getestet haben wir das T-Systems-Clientmodul in den Versionen `2.0.7-2-SNAPSHOT-19085` und `2.0.7-2-SNAPSHOT-19820`. Das KIM-Postfach wird von T-Systems gehostet, welches von dem Clientmodul per POP3 für den Mailabruf, und per SMTP für den Mailversand angesprochen wird.

Für die Analyse haben wir den zum Testzeitpunkt aktuellen Thunderbird 91 genutzt und in einem neuen Konto die Verbindung zu dem Clientmodul auf dem Server konfiguriert.

4 Analyse-Ergebnisse KIM-Spezifikation

KIM-Fachdienst – Versand von E-Mails Der KIM-Fachdienst ist für die Übermittlung und Speicherung von KIM-Nachrichten zuständig [ge21d]. Wir beschränken die Analyse der Spezifikation in diesem Beitrag auf die relevanten Aspekte der Verarbeitung und Übermittlung von Nachrichten.

Beim Versand einer Nachricht muss der Fachdienst im Wesentlichen sicherstellen, dass es sich um eine KIM-Nachricht von einer berechtigten Nutzer*in (üblicherweise durch Prüfung von Zugangsdaten) handelt. Ob es sich um eine gültige KIM-Nachricht handelt, wird unter anderem an folgenden Kriterien geprüft: Einhaltung des S/MIME-Profils, Prüfung der Absenderadresse, und Zustellung aus der TI. Insbesondere die Prüfung der Absenderadresse ist in der Spezifikation nicht genau beschrieben – es wird nur darauf hingewiesen, dass Nachrichten mit ungültiger Adresse abzulehnen sind [ge21d, KOM-LE-A_2134]. In unseren Praxistests wurden alle Absenderadressen, die nicht der authentifizierten Nutzer*in zugeordnet sind, vom Fachdienst abgelehnt.

KIM-Clientmodul – Signaturprüfung Das empfangende Clientmodul ist dafür verantwortlich, empfangene KIM-Nachrichten zuerst zu entschlüsseln und dann die Signatur zu prüfen [ge21c, 3.4.4]. Für den eigentlichen E-Mail-Client ist dieser Vorgang nicht mehr nachvollziehbar, es werden nur unverschlüsselte und unsignierte E-Mails per POP3 zur Verfügung gestellt. Die Signalisierung von Fehlern und erfolgreicher Verarbeitung an den Nutzer wird dabei durch das Anfügen eines Footers unter der ursprünglichen Nachricht realisiert.

Die Spezifikation der Signaturprüfung im Clientmodul ist dabei sehr liberal. So sollen E-Mails mit ungültiger Signatur dem Empfänger trotzdem zugestellt werden [ge21c, 3.4.4.2.2]. Das Clientmodul ergänzt E-Mails mit ungültiger Signatur entsprechend durch einen Klartext-Footer im E-Mail-Body, der die Manipulation anzeigt. Problematisch ist hierbei, dass sich dieser Footer im gleichen Kontext befindet wie der von der Versender*in erstellte Inhalt der Nachricht. Jeder E-Mail wird außerdem ein Signaturbericht als PDF-Dokument angehängt, in dem Details zur Signatur stehen.

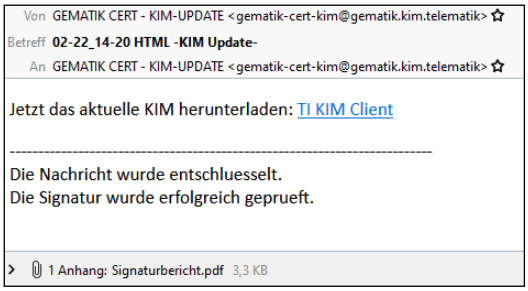

Abb. 1: KIM-Mail mit einer nicht validen Signatur im Thunderbird des Opfers nach der Verarbeitung durch das KIM-Clientmodul.

```
----------------------------------------
Die Nachricht wurde entschluesselt.
Die Signatur wurde erfolgreich geprueft.

<style>
    footer {
      display: none;
    }
    hr {
      display: none;
    }
</style>
```

List. 1: HTML, das den Footer versteckt und diesen durch einen eigenen ersetzt.

In der Spezifikation wird dabei explizit festgelegt, dass das Clientmodul, neben der Signatur selbst, auch das Zertifikat, und die Integrität der Header der äußeren Nachricht prüfen muss. Hierzu sollen einige Header der inneren Nachricht, unter anderem der `from`-Header, mit den Werten in der äußeren Nachricht verglichen werden [ge21c, KOM-LE-A_2048].

Weiterhin erlaubt die Spezifikation des Clientmoduls explizit den Einsatz von HTML-E-Mails im KIM-Kontext [ge21c, AFO: KOM-LE-A_2050-01]. Insbesondere erlaubt dies auch die Verwendung von Cascading Style Sheets (CSS).

5 Ergebnisse KIM-Clientmodul

5.1 Fälschen von Signaturen

Unsere Analyse des KIM-Clientmoduls von T-Systems (Version `2.0.7-2-SNAPSHOT-19085`) zeigt, dass die Kapselung der S/MIME-Funktionalität zu Problemen mit der Sicherheit von Signaturen führt. Spezifikationsgemäß werden E-Mails mit ungültiger Signatur zugestellt – die Sender*in kann hierbei ein Zertifikat mit beliebigen Inhalten verwenden und nur der Footer weist auf die Manipulation hin. Laut Spezifikation müsste allerdings zumindest die E-Mail-Adresse in der inneren Nachricht der äußeren (durch den Fachdienst beim Versand geprüften) entsprechen – das getestete Clientmodul führte diesen Test allerdings nicht durch.

Bereits 2019 zeigten Müller et al. [Mü19], wie es durch geschickte Verwendung von HTML und CSS möglich ist, Signaturen in S/MIME-Nachrichten zu fälschen. Eine Angreifer*in kann hier ausnutzen, dass der Footer und die innere Nachricht im selben Kontext angezeigt werden. Durch ein kurzes Stylesheet (List. 1) ist es möglich existierende Inhalte auszublenden. Somit kann die Angreifer*in das Ergebnis der Signaturüberprüfung im Footer der E-Mail

Die Pruefung der Signatur hat ergeben, dass die Nachricht manipuliert wurde.	
A. Signaturdetails	
Signaturzeitpunkt laut Unterzeichner:	28.02.2022 14:19:51
Datum der Signaturprüfung:	02.03.2022 21:41:14
Dokumentgröße in Bytes:	1677
Hashalgorithmus:	SHA256WithRSA
Signaturalgorithmus:	http://www.w3.org/2007/05/xmldsig-more#sha256-rsa-MGF1
Schlüssellänge in Bits:	2048
	Der vom Unterzeichner signierte Hashwert passt NICHT zu den signierten Daten.

Abb. 2: Ausschnitt des Signaturberichts im Anhang der gefälschten KIM-Nachricht. Ausschließlich hier ist ersichtlich, dass die Signaturüberprüfung nicht erfolgreich war.

verstecken. Um den Angriff zu verschleiern, hängt sie einen eigenen Footer an, der dem für eine korrekt signierte Nachricht entspricht (Abb. 1).

Für nicht technisches Personal ist eine so manipulierte E-Mail nun nicht mehr ohne Weiteres von einer korrekt signierten E-Mail zu unterscheiden. Einzig durch die Kontrolle des angehängten Signaturberichts als PDF (Abb. 2) ist es möglich die Manipulation zu erkennen. In der Praxis wird sich das Personal aber nahezu immer ausschließlich auf den menschenlesbaren Footer verlassen.[3] Auch war es in unseren Tests möglich weitere beliebige Anhänge mit dem Dateinamen `Signaturbericht.pdf` an die Nachricht anzuhängen – somit wird es für Nutzende fast unmöglich den korrekten Bericht zu identifizieren.

Da der VZD innerhalb der TI lesbar ist, konnte über diesen Angriff jeder KIM-Teilnehmende scheinbar korrekt signierte Nachrichten an beliebige weitere Teilnehmende versenden.

Responsible Disclosure Wir haben die gefundenen Schwachstellen am 03.02.2022 an T-Systems und die gematik gemeldet, welche uns am selben Tag die Probleme bestätigten. Die gematik hat am 20.09.2022 einen Spezifikations-Hotfix [ge22a] veröffentlicht, die vorschreibt, E-Mails mit ungültigen und fehlenden Signaturen zu verwerfen und nur eine Fehlernachricht zuzustellen. Am 13.01.2023 wurde auch die Ungenauigkeit bezüglich der Prüfung von Absenderadressen in der Fachdienst-Spezifikation behoben. Nun müssen die unverschlüsselten Absenderadressen (SMTP-Envelope-Adresse und Absenderadresse der äußern Nachricht) explizit einer KIM-Adresse des authentifizierten Nutzers entsprechen.

5.2 Protokollierung von medizinischen personenbezogenen Daten

Das T-Systems KIM-Clientmodul loggte in unserer getesteten Version standardmäßig die komplette SOAP-Kommunikation zwischen dem Clientmodul und dem TI-Konnektor in Logdateien auf dem lokalen Serverlaufwerk mit. Dies umfasst sowohl Kommunikation bei Fehlern als auch Kommunikation bei erfolgreichen Konnektor-Operationen. Im Falle

3 Diese Einschätzung wurde uns in anekdotischen Gesprächen mit medizinischem Fachpersonal bestätigt.

```
Payload: <SOAP-ENV:Envelope
[...]
<ns3:Document><ns5:Base64Data>TUlNRS1WZXJzaW9
zctbwItzIsgc21pbwUtdHIwzT1zawduzwetzGFOYTsgbm
[...]
```

List. 2: Ausschnitt der Base64 enkodierten, entschlüsselten E-Mail.

der Entschlüsselung einer empfangenen KIM-Nachricht wird die Antwort des Konnektors, mitsamt den Base64-enkodierten Daten, protokolliert (siehe List. 2). Diese Daten enthalten die unverschlüsselte E-Mail. Auf Senderseite wird die unverschlüsselte Nachricht ebenfalls in der Konnektor-Anfrage protokolliert. Dementsprechend werden alle KIM-Nachrichten, mitsamt der personenbezogenen Daten, standardmäßig in der Clientmodul-Umgebung gespeichert. Dies kann auf dem lokalen Praxisserver sein, kann aber auch bei einem externen Dienstleister sein. Die Logdateien werden beim Erreichen einer konfigurationsabhängigen Größe automatisch überschrieben. Allerdings werden diese Dateien in den üblichen durchgeführten Backups gesichert und dadurch für eine längere Zeit persistiert.

Das Protokollieren von medizinischen und personenbezogenen Daten ist laut der Spezifikation [ge21c, AFO: KOM-LE-A_2080] nicht erlaubt. Diese Anforderung ist explizit in der Prüfvorschrift [ge21b] als Testfall gelistet, welcher von der gematik durch Bestätigungstests im Rahmen der Zulassung geprüft werden muss. Dieser Bestätigungstest wurde offensichtlich nicht, oder nicht gründlich genug, durchgeführt.

Responsible Disclosure Wir haben die gematik T-System am 03.03.2022 über dieses Problem informiert. Am 14.03.2022 bestätigte T-Systems die Schwachstelle und nannte geplante Maßnahmen zum Deaktivieren der Protokollierung. Anfang April wurden alle T-Systems KIM-Nutzende per KIM-Mail informiert. Hierbei wurde in einer Kurzanleitung gezeigt, wie das Logging der SOAP-Kommunikation deaktiviert werden kann und welche Protokolldaten gelöscht werden sollten. Zeitgleich veröffentlichte die gematik eine entsprechende Meldung im Fachportal [ge22c]. Anfang Mai 2022 wurde ein neues KIM-Clientmodul mit standardmäßig deaktiviertem SOAP-Logging veröffentlicht.

5.3 Log4Shell-Schwachstelle

Unsere Analyse des im Testsetup installierten KIM-Clientmodul, `2.0.7-2-SNAPSHOT-19085`, zeigt, dass eine von der Log4Shell-Schwachstelle [Bu21] betroffene Log4j-Bibliothek, (Version `2.14.1`) eingebunden ist. In der Logdatei-Analyse fanden wir mehrere Ausgaben, die ungeprüft aus Nutzereingaben stammen. Eine der Ausgaben ist der Common Name (CN) im Absender-Zertifikat einer KIM-Nachricht. Der CN wird dabei nach der Entschlüsselung der Nachricht dem Absender-Zertifikat entnommen und vor der Signaturüberprüfung

in die lokale Logdatei geschrieben. Eine Angreifer*in mit einem KIM-Zugang kann aus dem TI-VZD Verschlüsselungs-Zertifikate für jede KIM-Teilnehmer*in abrufen und dementsprechend KIM-Nachrichten verschicken, welche durch die empfangende Person erfolgreich entschlüsselt werden können. Eine Signaturprüfung der KIM-Nachricht kann durch das sign-then-encrypt-Verfahren erst lokal nach dem Entschlüsseln stattfinden. Da das T-Systems Clientmodul den CN vor der Signaturüberprüfung protokolliert, wird keine gültige Signatur benötigt. Dadurch kann die Angreifer*in beliebigen ASCII-Text in das CN-Feld schreiben, welches beim Empfänger durch die Log4j-Bibliothek verarbeitet wird.

In unserem Testsetup setzen wir das CN-Feld des Absenderzertifikates auf den Wert `${jndi:ldap://<AngreiferServer>:<Port>/}`. Als Server und Port nutzen wir die IP-Adresse unserer Testservers, um zu überprüfen, ob das KIM-Clientmodul weiteren Code nachzuladen versucht. Wie in Abb. 3 zu sehen, wurde die KIM-Mail erfolgreich beim Empfänger entschlüsselt, und das KIM-Clientmodul versuchte Code vom Server nachzuladen.

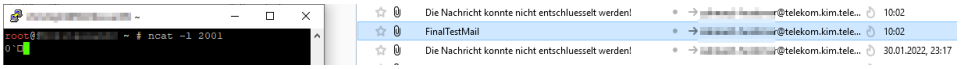

Abb. 3: Erfolgreicher Log4Shell-Proof-of-Concept. Links: Server von dem das Clientmodul versucht Code nachzuladen. Rechts: Thunderbird mit der empfangenen E-Mail, Betreff: ‘FinalTestMail’.

Hervorzuheben ist, dass die E-Mail zum Nachladen von Schadcode nicht geöffnet werden muss. Es reicht, wenn das Clientmodul neue E-Mails aus dem Postfach abholt, da diese automatisch ohne Anwender-Interaktion verarbeitet werden. Da das Clientmodul oftmals mit Administratorrechten auf dem Praxisserver installiert ist, ist es möglich mit einer einzigen maliziösen KIM-Nachricht Administratorzugriff auf den Server, der in vielen Praxen gleichzeitig der Domaincontroller ist, zu bekommen. Weiterhin liegen üblicherweise auf diesem Server die Datenbanken des PVSs mit den medizinischen Daten der Patient*innen. Eine Angreifer*in mit KIM-Zugang hätte gezielt Telekom-KIM-Adressen vom VZD abrufen und diese automatisiert angreifen können.

Updates und Responsible Disclosure T-Systems patchte das betroffene KIM-Clientmodul und stellte die Version `2.0.7-2-SNAPSHOT-19782` am 13.12.2021 zum Download bereit. Eine nochmals gepatchte Version (`2.0.7-2-SNAPSHOT-19820`) stellte T-Systems am 12.01.2022 zum Download bereit. Diese Downloads sind erst nach dem Login mit den persönlichen Praxiszugangsdaten sichtbar. Es gibt weder eine Benachrichtigungsfunktion bei neuen Updates, noch automatische Updates des Clientmoduls. Das händische Einloggen und das Abgleichen der Versionsnummer des aktuellen Downloadpakets mit der installierten Version ist die einzige Möglichkeit von neuen Versionen des Clientmoduls zu erfahren.

Es gab zu diesen kritischen Updates keine weitere Information für die Anwendenden. Während es für andere TI-Komponenten Ankündigungen zum aktuellen Patch gab ([ge21a]), wurden weder die DVOs noch die Kund*innen informiert. Auch das T-Systems-KIM-Portal enthielt weder eine Changelog noch einen Grund für die neuen Versionen. Dadurch wurde unsere Testpraxis nicht vom DVO auf das Update hingewiesen. Auch konnte dieser uns auf

Nachfrage nicht beantworten, welche Änderungen in den letzten Updates von T-Systems vorgenommen wurden und ob es sich um sicherheitskritische Updates handelt.

Wir haben das gematik- sowie das T-Systems-CERT am 02.02.2022 über die Zero-Click-Schwachstelle sowie das Fehlen der Update-Ankündigungen und Empfehlungen informiert. T-System bestätigte die Schwachstelle in der getesteten Version am 10.02.2022 und übermittelte uns die Patch-Historie bezüglich der ausgelieferten Log4j-Bibliothek. Als Begründung, dass keine Informationen zu den Updates verteilt wurden, berief sich T-Systems auf ihre AGB: „In unseren AGBs wird darauf hingewiesen, dass dem Kunden unregelmäßig Softwareupdates zur Verfügung gestellt werden. Zu den Mitwirkungspflichten eines Kunden gehört es, dass dieser das zur Verfügung gestellte Update installiert."

Nach unserem Hinweis hat T-Systems Maßnahmen ergriffen, um das Update zu verbreiten:

- Einen Hinweis auf die kritische Sicherheitslücke und Updates auf der KIM-T-Systems-Informationsseite, welche ohne Login zu erreichen ist.
- Eine KIM-Mail die alle Kund*innen auffordert, die neuste Version zu installieren.
- Eine Update-Aufforderung und Auflistung sicherer Versionsständen im gematik-Fachportal [ge22b].

T-Systems ist nach eigenen Angaben nicht in der Lage herauszufinden, welche Versionen im Feld installiert sind. Nach Aussage des DVOs unserer Testpraxis hatten im Juni 2022, sechs Monate nach den Updates, nur geschätzt 40 % seiner Kund*innen das Update installiert. Ein Grund könnte sein, dass die KIM-Grundinstallation durch einen DVO den Praxen erstattet wird, sie aber Wartung und Updates durch einen DVO selbst finanzieren müssen.

6 Fazit

Eine sichere und leicht zu bedienende Kommunikation ist einer der wichtigsten Faktoren für eine erfolgreiche Digitalisierung der Medizin in Deutschland. Eine medienbruchfreie, sichere und gesetzeskonforme Übertragung von medizinischen Daten ist der Grundbaustein für digitale Arztbriefe, die elektronische Arbeitsunfähigkeitsbescheinigung und weitere digitale Medizindienste. Wir haben gezeigt, wie die von KIM spezifizierte Lösung der Abkapselung der Signaturüberprüfung zum einen die Komplexität der S/MIME-Funktionen vom Anwender Richtung KIM-Clientmodul verschiebt, dabei zum anderen aber kritische Schwachstellen und Angriffe auf die KIM-Infrastruktur ermöglicht.

Neben der Spezifikation ist die eigentliche Implementierung der Sicherheitsfunktionalitäten in der Praxis entscheidend für die Gesamtsicherheit des Systems. Gerade bei Anwendungen, welche höchst sensible Daten verarbeiten, bedarf es verlässlicher Prozesse und Strukturen, um kritische Schwachstellen schnell und flächendeckend im Feld zu beheben. Weiterhin muss die gematik als Zulassungsorganisation für TI-Anwendungen die spezifizierten Testfälle während der Zulassung gewissenhaft prüfen und die Zulassung von diesem Ergebnis abhängig machen.

Literaturverzeichnis

[adHBO23] an der Heiden, Iris; Bernhard, Jannis; Otten, Marcus: Wissenschaftliche Evaluation des Produktivbetriebs der Anwendungen der Telematikinfrastruktur 2022. Bericht, IGES Institut, Februar 2023. https://www.gematik.de/media/gematik/Medien/Telematikinfrastruktur/TI-Atlas/IGES-Studie_Wissenschaftliche_Evaluation_des_Produktivbetriebs_der_Anwendungen_der_TI_2022.pdf, abgerufen am 31.10.2023.

[BKK19] Berndt, Christina; Kampling, Katrin; Klofta, Jasmin: Patientendaten sind meist schlecht geschützt. Süddeutsche Zeitung, November 2019. https://www.sueddeutsche.de/politik/patientendaten-hacker-sicherheit-1.4678689, abgerufen am 31.10.2023.

[Bu21] Bundesamt für Sicherheit in der Informationstechnik: , Kritische Schwachstelle in log4j veröffentlicht (CVE-2021-44228), Dezember 2021. https://www.bsi.bund.de/SharedDocs/Cybersicherheitswarnungen/DE/2021/2021-549032-10F2.pdf?__blob=publicationFile&v=10, abgerufen am 31.10.2023.

[ge21a] gematik: Aktuelles | BSI warnt vor Sicherheitslücke: Auswirkungen auf Dienste der Telematikinfrastruktur. Januar 2021. https://www.gematik.de/newsroom/news-detail/bsi-warnt-vor-sicherheitsluecke-auswirkungen-auf-dienste-der-telematikinfrastruktur, abgerufen am 31.10.2023.

[ge21b] gematik: Produkttypsteckbrief - Prüfvorschrift - KOM-LE-Clientmodul. Februar 2021. version 1.0.0, https://fachportal.gematik.de/fachportal-import/steckbriefe/gemProdT_CM_KOMLE_PTV_1.5.1-0_V1.0.0_Aend.pdf, abgerufen am 31.10.2023.

[ge21c] gematik: Spezifikation KOM-LE-Clientmodul. Februar 2021. version 1.10.0, https://fachportal.gematik.de/fachportal-import/files/gemSpec_CM_KOMLE_V1.10.0.pdf, abgerufen am 31.10.2023.

[ge21d] gematik: Spezifikation KOM-LE-Fachdienst. Januar 2021. version 1.11.2, https://fachportal.gematik.de/fachportal-import/files/gemSpec_FD_KOMLE_V1.11.2.pdf, abgerufen am 31.10.2023.

[ge21e] gematik: Spezifikation Verzeichnisdienst. April 2021. version 1.13.1, https://fachportal.gematik.de/fachportal-import/files/gemSpec_VZD_V1.13.1.pdf, abgerufen am 31.10.2023.

[ge22a] gematik: Aktuelles | BSI warnt vor Sicherheitslücke: Auswirkungen auf Dienste der Telematikinfrastruktur. September 2022. https://fachportal.gematik.de/schnelleinstieg/downloadcenter/releases#c6557, Abgerufen am 31.10.2023.

[ge22b] gematik: Behebung der log4j-Sicherheitslücke: Update des KIM-Clientmoduls nötig. 2022. https://web.archive.org/web/20220514032104/https://fachportal.gematik.de/ti-status#c4790, Archiviert mit Stand 04.05.2022.

[ge22c] gematik: Sicherheitsinformation KIM-Clientmodul T-Systems. 2022. https://web.archive.org/web/20220407171108/https://fachportal.gematik.de/ti-status#c5580, Archiviert mit Stand 07.04.2022.

[ge23a] gematik: Das Fachportal der gematik - der Zugang zur TI. 2023. https://fachportal.gematik.de/, Abgerufen am 31.10.2023.

[ge23b] gematik: TI-Dashboard - Digitalisierung in der Übersicht. 2023. https://www.gematik.de/telematikinfrastruktur/ti-dashboard, Abgerufen am 31.10.2023.

[Kl20] Klofta, Jasmin: IT-Sicherheitslücken in Praxen. Dezember 2020. https://www.tagesschau.de/investigativ/br-recherche/sicherheit-telematik-101.html, abgerufen am 31.10.2023.

[Ma22] Mayer, Peter; Poddebniak, Damian; Brinkmann, Marcus; Sasse, Angela: "I Don't Know Why I Check This . . . " – Investigating Expert Users' Strategies to Detect Email Signature Spoofing Attacks. In: Proceedings of the Eighteenth Symposium on Usable Privacy and Security (SOUPS 2022). USENIX Association, August 2022.

[Mü19] Müller, Jens; Brinkmann, Marcus; Poddebniak, Damian; Böck, Hanno; Schinzel, Sebastian; Somorovsky, Juraj; Schwenk, Jörg: "Johnny, you are fired!" – Spoofing OpenPGP and S/MIME Signatures in Emails. In: 28th USENIX Security Symposium (USENIX Security 19). USENIX Association, Santa Clara, CA, S. 1011–1028, August 2019.

[Pa23] Panskus, Rebecca; Ninow, Max; Fahl, Sascha; Marky, Karola: Privacy Mental Models of Electronic Health Records: A German Case Study. In: Nineteenth Symposium on Usable Privacy and Security (SOUPS 2023). USENIX Association, Anaheim, CA, S. 525–542, August 2023.

[RT10] Ramsdell, B.; Turner, S.: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 3.2 Message Specification. RFC 5751, IETF, Januar 2010.

[Sl20] Slany, Wolfgang: Sicherheitsanalyse zur Sicherheit der kritischen Komponenten derelektronischen Patientenakte nach §291aSGB V. Bericht, TU Graz, März 2020. https://www.gematik.de/media/gematik/Medien/Newsroom/Presse/Dokumente/Sicherheitsanalyse_TU_Graz_zur_ePA_mit_Vorwort_der_gematik.pdf, abgerufen am 31.10.2023.

[So19] Sozialgesetzbuch (SGB) Fünftes Buch (V): § 75b - Richtlinie zur IT-Sicherheit in der vertragsärztlichen und vertragszahnärztlichen Versorgung. Bericht, 12 2019.

[SRT19] Schaad, J.; Ramsdell, B.; Turner, S.: Secure/Multipurpose Internet Mail Extensions (S/MIME) Version 4.0 Message Specification. RFC 8551, IETF, April 2019.