Vivy GmbH, Schützenstraße 18, 10117 Berlin, Deutschland - Email: security@vivy.com

Stellungnahme zum Bericht der modzero GmbH

27. Oktober 2018

Inhaltsverzeichnis

Zeitlicher Ablauf

Datum	**Beschreibung**
22. Sep 2018 09:45	Erhalt des ersten Berichts von modzero
22. Sep 2018 11:00	Telefonkonferenz zwischen CTO der Vivy GmbH und modzero
22. Sep 2018 12:00	Abschluss Analyse des Incidents und Auswertung der Auswirkungen
22. Sep 2018 23:00	Abschluss der Verbesserung aller gefundenen sicherheitsrelevanten Angriffsvektoren
24. Sep 2018 21:00	Treffen mit modzero zwecks Erläuterung
3. Okt 2018 22:30	Erhalt des finalen Berichts von modzero
3. Okt. 2018 23:30	Abschluss Analyse des Incidents und Auswertung der Auswirkungen
4. Okt. 2018 11:00	Abschluss der Verbesserung aller gefunden sicherheitsrelevanten Angriffsvektoren
5. Okt. 2018	Abschließender Bericht zur Auswertung der gefundenen Angriffsvektoren
10. Okt. 2018	Start der Penetrationstests durch ERNW und OptimaBit zur erneuten kompletten Systemüberprüfung von Vivy
25. Okt 2018	Information von modzero an Vivy, dass die Analyse der Presse übergeben wurde

Dokumentenhistorie

Version	Autor	Datum	Kommentar
0.1	Rowanto Rowanto	22. Sep. 2018	Erstellung der Grundanalyse
0.2	Rowanto Rowanto	23. Sep 2018	Ergänzungen
0.3	Rowanto Rowanto	3. Okt. 2018	Erhalt des finalen Berichts und Ergänzung
0.4	Rowanto Rowanto	4. Okt. 2018	Ergänzungen
0.5	Christian Rebernik	24. Okt. 2018	Formatierung und Ergänzungen
0.6	Rowanto Rowanto	25. Okt. 2018	Ergänzungen
0.7	Oliver Wehn	25. Okt. 2018	Formatierung
0.8	Rowanto Rowanto	26.Okt. 2018	Ergänzungen und Finalisierung

Zusammenfassung

Sicherheit auf höchstem Niveau ist im Umgang mit den hochsensiblen Daten unserer Nutzer ein Grundpfeiler des Selbstverständnisses der Vivy GmbH. Darum arbeitet unser Unternehmen fortlaufend an der Verbesserung der Sicherheitsarchitektur und lässt die Vivy-App, die Vivy-Browser-Applikation und die Backend-Systeme regelmäßig durch externe IT-Sicherheitsexperten überprüfen. Im Rahmen sogenannter *Bug Bounty*-Programme lädt die Vivy GmbH zudem unabhängig agierende IT-Fachleute dazu ein, die Sicherheit ihrer Systeme auf Schwachstellen zu testen.

Fünf Tage nach dem offiziellen Launch von Vivy, hat ein Beratungsunternehmen für IT-Sicherheit, die *modzero GmbH,* eine Reihe hypothetischer Angriffsmöglichkeiten auf die Vivy-App und die von Ärzten verwendete Browser-Applikation aufgezeigt. Gemäß standardisierter *Incident*- und *Change*-Prozesse wurden jeweils alle identifizierten potentiellen Angriffsvektoren ausnahmslos binnen 24 Stunden nach Erhalt des Berichts behoben.

Der Großteil der beseitigten Angriffsmöglichkeiten hat gezeigt, dass sie entweder einen kompromittierten Computer des Arztes, oder ein kompromittiertes Smartphone des Nutzers (umgangssprachlich auch *jailbroken* oder *rooted* genannt) voraussetzen. Selbst im Falle erfolgreicher Angriffe wären maximal fragmentierte Datensätze einzelner Nutzer, nie jedoch größere Datenbestände einsehbar gewesen. Einige Kombinationen von Angriffen waren auch im Analysezeitraum in der von der modzero GmbH dargestellten Form in der Realität nicht umsetzbar.

Alle im Nachgang durchgeführten Analysen zeigen, dass zu keinem Zeitpunkt Patientendaten in Vivy kompromittiert wurden, weder durch die modzero GmbH noch durch andere Angreifer.

Vivy basiert auf einer vielschichtigen Sicherheitsarchitektur, die auf dem neuesten Stand der Technik beruht und fortlaufend erweitert wird, um den Nutzern bestmögliche Sicherheit Ihrer persönlichen Daten zu gewährleisten (https://www.vivy.com/sicherheit/).

In den folgenden Abschnitten werden die von modzero GmbH identifizierten potenziellen Angriffsvektoren analysiert und die umgesetzten Maßnahmen beschrieben, mit denen Vivy auch diese unwahrscheinlichen Angriffe adressiert hat.

1. Sicherheitskonzept Vivy

Sicherheit und Datenschutz der zum Teil hochsensiblen Daten der Nutzer genießen bei der Vivy GmbH höchste Priorität. Auf der Website https://www.vivy.com/sicherheit/ können sich Nutzer über die umfangreichen Sicherheitskonzepte, Sicherheitsprozesse und Zertifizierungen des Unternehmens informieren. Für Experten hat die Vivy GmbH ein detailliertes Whitepaper zum Thema Sicherheit veröffentlicht.

Sicherheitsrelevante Anfragen und Meldungen können über security@vivy.com PGP-verschlüsselt eingereicht werden. Hierzu steht ein öffentlicher Schlüssel zur Verfügung.

Des Weiteren hat Vivy zum 1. Oktober 2018 das von Beginn an geplante und öffentliche „Bug Bounty und Vulnerability Disclosure"-Programm gestartet. Darin werden Security-Experten und Hacker weltweit aufgefordert, auf potentielle Angriffsvektoren der Vivy-Systeme hinzuweisen, sodass die Vivy GmbH diese frühzeitig adressieren kann.

2. Bericht der modzero GmbH

Am 22. September wurde die Vivy GmbH durch die modzero GmbH auf verschiedene potenzielle Angriffsvektoren in der Browser-Anwendung sowie der App für iOS und Android hingewiesen. Am 3. Oktober hat das IT-Sicherheitsunternehmen einen finalen Bericht an die Vivy GmbH übergeben.

Der Bericht wurde ohne Abstimmung mit der Vivy GmbH erstellt, sodass etliche von der Vivy GmbH umgesetzte Sicherheitsmaßnahmen, beispielsweise im Browser-Umfeld, im Bericht nicht berücksichtigt werden konnten. Alle von der modzero GmbH aufgezeigten potenziellen Angriffsvektoren wurden nach dem Vivy Incident- und Change-Prozess analysiert und binnen 24 Stunden adressiert. Eine weitere detaillierte Analyse hat zudem ergeben, dass zu keinem Zeitpunkt Nutzerdaten durch die von modzero benannten, potentiellen Angriffsvektoren kompromittiert wurden.

Die folgende Analyse auf Basis des Berichts der modzero GmbH ist in vier Abschnitte unterteilt. Diese Abschnitte behandeln jeweils einen der vier thematisierten Bereiche für potenzielle Angriffe auf die Vivy-Anwendungsarchitektur. Diese sind: konzeptionelle Sicherheitsrisiken, die Vivy-Plattform, die Browser-App und die Smartphone-Apps. Als Referenz sind die Nummern der relevanten Abschnitte des modzero-Berichts in den jeweiligen Überschriften angegeben.

3.1. Allgemein

Der Bericht der modzero GmbH beginnt mit zwei konzeptionellen Angriffsszenarien, die erfordern, dass entweder die Vivy-Plattform selbst oder der einzelne Benutzer auf seinem Endgerät kompromittiert wird. Diese hypothetischen Angriffe berücksichtigen nicht, dass die Vivy-Plattform zahlreiche Sicherheits-Schichten hat und Maßnahmen einsetzt, um eine Kompromittierung der Vivy-Server zuverlässig zu verhindern. Desweiteren blendet der modzero-Bericht in seiner Bewertung zahlreiche grundsätzliche Sicherheitsmaßnahmen aus, wie die durchgängige *TLS 1.2*-Verschlüsselung aller Verbindungen, das *Certificate Pinning* innerhalb der Apps oder den Brute-Force-Schutz durch entsprechende Alarme und IP-Blocking seitens der Vivy-Server.

3.1.1. Fehlende Authentifizierung beim Schlüsselaustausch (4.1.1.)

Im Bericht der modzero GmbH wird die fehlende Authentifizierung beim Austausch der zur sicheren Übertragung notwendigen Schlüssel kritisiert. Um diesen sehr hypothetischen Angriffsvektor zu nutzen, um an Nutzerdaten zu kommen, müsste ein Angreifer zunächst unbemerkt die Vivy-Server kompromittieren, um überhaupt die Möglichkeit zur Sabotage des öffentlichen Schlüssels des jeweiligen Nutzers zu haben. Im Anschluss könnten dann nur die zeitlich nach der Kompromittierung übermittelten Dokumente entschlüsselt werden. Eine Entschlüsselung bereits existierender Dokumente wäre in keinem Falle möglich und ein Zugriff auf die bestehende Gesundheitsakte weiterhin ausgeschlossen.

Wie bei anderen Private-Public-Key-Anwendungen wie z.B. PGP oder Threema, stellt der Schutz und die Integrität der Schlüssel die Basis für die Gesamtsicherheit der Anwendung dar. Um solche Angriffe verhindern und manipulierte Anfragen erkennen zu können, ermöglicht Vivy den Kommunikationspartnern, den öffentlichen Schlüssel des Benutzers vor einem Dokumentenupload selbst zu überprüfen.

Bereits heute bietet Vivy die Möglichkeit einer Registrierung für Ärzte, so dass diese in Zukunft für die Kommunikation mit dem Nutzer persönliche Konten mit individuellen Schlüsseln nutzen können.

3.1.2. Fehlende Authentifizierung in der Verschlüsselung (4.1.2.)

Im Weiteren weist modzero darauf hin, dass es aufgrund des als Teil der hybrid realisierten Ende-zu-Ende-Verschlüsselung eingesetzten symmetrischen Verschlüsselungsverfahrens, möglich wäre, verschlüsselte Dateien anhand von Mustern zu identifizieren und gezielt zu manipulieren. So garantiere das Verschlüsselungsverfahren alleine nur Vertraulichkeit aber nicht Integrität der Daten.

Diese theoretische Lücke wird außerhalb des konkreten Einsatzes bei Vivy beschrieben und würde ein Wissen über die Struktur der unverschlüsselten Daten auf Seiten des Angreifers voraussetzen, um die für eine Identifikation nötigen Muster herleiten zu können. Aufgrund der Art und Weise, wie die verschlüsselten Daten bei Vivy ausgetauscht werden, würde dieses Angriffsszenario eine unbemerkte Kompromittierung der Vivy-Server selbst voraussetzen.

Aktuell nutzt die Vivy GmbH bereits ein anderes, noch sichereres Verschlüsselungsverfahren als das im Bericht genannte. Dabei handelt es sich um RSA 4096 bit mit OEAP, und AES 256 bit mit GCM, wobei die Authentizität der Daten über eine Prüfsumme zusätzlich sichergestellt wird.

3.2. Vivy-Plattform

Die beschriebenen Angriffsszenarien auf die Vivy-Plattform basieren durchgängig auf generischen Brute-Force-Angriffen, wie sie gegen jedes aus dem Internet erreichbare System angewendet werden können. Bei der Einschätzung der Kritikalität, wurde von der modzero GmbH nicht berücksichtigt, welche Schutzmaßnahmen die Vivy GmbH gegen Brute-Force-Angriffe seitens der Vivy-Server und -APIs umgesetzt hat.

3.2.1. Preisgabe von mit dem Arzt geteilten Dokumenten und Metadaten (4.2.1.)

Vivy-Server-Versionen vor 488b17 (22. September 2018) hätten erlaubt, dass durch einen Brute-Force-Angriff auf das von Ärzten verwendete Web-Interface für den Datenabruf die in der URL hinterlegte Session-ID (eine fünfstellige alphanumerische Zeichenfolge) einer gültigen Sitzung hätte

ermittelt werden können. Kurzzeitig wären so Versichertendaten (Versicherungsname, Versichertenbild, Versichertennummer) und öffentlich zugängliche Metadaten des behandelnden Arztes (Name der Praxis, Adresse, Ort) einsehbar gewesen. Im gleichen Zuge hätte gegebenenfalls die PIN, die der Arzt vor Einsicht in das geteilte Dokument eingeben muss, ermittelt werden können. Voraussetzung hierfür wäre jedoch gewesen, dass ein Angreifer den Brute-Force-Angriff vollständig innerhalb der Gültigkeitsdauer einer Session hätte durchführen können und dieser Angriff von der automatischen Sicherheitskontrolle der Vivy-Server nicht entdeckt worden wäre, die bei einer hohen Anzahl von Anfragen zu einem Alarm führt. Auch der erweckte Eindruck, das erfolgreiche Ermitteln der korrekten PIN genüge für einen Zugriff auf das in der Sitzung freigegebene Dokument, ist nicht korrekt, worauf unter 3.2.3 nochmals spezifischer eingegangen wird.

Die Session-ID wurde mittlerweile auf eine Gesamtlänge von 8 Zeichen erweitert und die Anzahl der erlaubten ungültigen Anfragen innerhalb definierter Zeiträume an die betroffenen API-Endpunkte so reduziert, dass nun 722.204.136.308.736 mögliche IDs bestehen, von denen die richtige in wenige Versuchen geraten werden muss. Umgesetzt wurde diese Verbesserungen noch am selben Tag.

3.2.2. Weitergabe der Session-ID an externe Dienstleister (4.2.1.1. – 4.2.1.4.)

Wenn ein Browser eine HTTPS-Anforderung an einen anderen Dienst (oder eine andere Domain) sendet, wird die aktuelle Seiten-URL automatisch als Teil dieser Anfrage angehängt. Dienstbetreiber könnten so Zugang zu den Metadaten der Session (siehe oben) und der Session-ID erhalten. Dennoch bleibt der Angriff hypothetisch: Um an die Metadaten zu kommen, müssten die Dienstbetreiber auch nach Erhalt der Session-ID noch einen Brute-Force-Angriff in 24 Stunden auf die einzelne Session-URLs durchführen.

Die genannten externen Dienste in der Browser-App wurden vollständig innerhalb von 24 Stunden entfernt, sodass die Session-ID seither nicht mehr gegenüber Diensten Dritter offengelegt wird.

3.2.3. Dokument wurde bereits vom Arzt abgerufen/Teilen noch nicht beendet (4.2.1.5., 4.2.1.6.)

In dem unwahrscheinlichen Szenario, dass ein potentieller Angreifer bereits eine gültige Session-ID ermittelt hätte, wäre es in der von modzero GmbH betrachten Version des Vivy-Servers möglich gewesen, mit Hilfe einer Brute-Force-Attacke die PIN einer aktiven Sitzung zu ermitteln und die Metadaten der Freigabe (d.h. z.B. sendender Patient und empfangender Arzt) auszulesen (siehe 4.2.1.).

In der Folge wurde eine unbegrenzte Wiederholung der PIN-Eingabe unterbunden. Auch sind nun keinerlei Metadaten mehr einsehbar, bevor nicht die korrekte PIN, wie in der Android- oder iOS-App angezeigt, verwendet und die Übertragung der geteilten Daten vom Nutzer an den Empfänger abgeschlossen wurde. Alle Änderungen wurden von den Experten der Vivy GmbH direkt am selben Tag vorgenommen.

Die in 4.2.1.6. durch modzero formulierte Annahme, eine Dokumentenübertragung an den Angreifer könnte über eine simple Ermittlung der PIN über den zuvor beschriebenen Brute-Force-Ansatz ermöglicht werden, war für keine Version des Vivy-Document-Sharing-Prozesses zu keinem Zeitpunkt zutreffend. Teilt ein Nutzer sein Dokument über die Vivy-App und gibt die Session-URL und die PIN an den Arzt weiter, muss er bis zur erfolgreichen Datenübertragung den Teilen-Bildschirm der App geöffnet halten, um den Vorgang erfolgreich abzuschließen. Die App prüft dabei nur einmal pro Sekunde, ob auf die Session mit der korrekten PIN zugegriffen wird und damit ein autorisierter Datentransfer stattfinden kann.

Da die zuständige API aber keinerlei Rückschluss auf die Korrektheit der übermittelten PIN zulässt und in Anbetracht der angenommenen Abfragerate zur Ermittlung der gültigen PIN, ist die Wahrscheinlichkeit sehr gering, dass der korrekte PIN genau im Augenblick der Prüfung durch die App übermittelt wird.

3.2.4. Überschreibung öffentlicher Schlüssel (4.2.2.)

Das von modzero GmbH beschriebene Szenario einer Überschreibung des von Vivy verwendeten öffentlichen Schlüssels durch einen Angreifer ist unter realen Bedingungen höchst unwahrscheinlich. Der Zugriff auf den entsprechenden API-Endpunkt ist nur mit Hilfe eines gültigen *Access Token* möglich, der bei erfolgreicher Authentifizierung durch den Nutzer individuell ausgestellt wird. *Certificate Pinning* verhindert zusätzlich, dass ein Access Token in der Kommunikation durch einen *Man in the Middle*-Angreifer abgefangen werden kann. Folglich müssen entweder das Endgerät des Nutzers oder die Vivy-Server, die die öffentlichen Schlüssel bereitstellen, selbst unbemerkt kompromittiert worden sein, um einen solchen Angriff in der Realität durchführen zu können.

3.2.5. Brute-Force-Angriff auf Zwei-Faktor-Authentifizierung (4.2.3.)

In der von der modzero GmbH betrachteten Version der Vivy-App konnte, wenn einem Angreifer E-Mail-Adresse und Passwort eines Nutzerkontos bekannt waren, ein Login-Versuch beliebig oft auch mit einem ungültigen als zweiten Sicherheitsfaktor zur Authentifizierung notwendigen TOTP-Token wiederholt werden. Zwar ist jeder TOTP-Token lediglich 30 Sekunden gültig, doch wäre es mit einem auf diesem Wege via Brute-Force-Angriff gefundenen gültigen TOTP-Token möglich gewesen, sich als Nutzer zu authentifizieren und in dessen Namen Funktionen der Vivy-Plattform zu nutzen.

Noch am Tag des Bekanntwerdens dieses Angriffsvektors wurde eine Verbesserung umgesetzt, die die Anzahl von Anfragen mit ungültigem TOTP-Token massiv limitiert. Diese Maßnahme sichert den Authentifizierungsprozess der Patienten zusätzlich und erschwert die von der modzero GmbH beschriebenen Brute-Force-Angriffe.

3.2.6. Fehlermeldungen beim Login beschleunigen Brute-Force-Angriffe (4.2.4.)

Wenn ein Anmeldeversuch bei der Vivy-App fehlschlägt, antwortet das Vivy-System mit entsprechenden Fehlermeldungen, beispielsweise wenn Anmeldedaten nicht korrekt sind oder der TOTP-Token fehlt. Die modzero GmbH nutzte diese Fehlermeldungen, um beispielsweise zu prüfen, ob eine E-Mail-Adresse im System existiert. Außerdem behauptete die modzero GmbH, dass es möglich wäre, anhand der unterschiedlichen Fehlermeldungen, Stück für Stück die einzelnen Informationen, die für eine erfolgreiche Anmeldung im Vivy-System notwendig wären, über gezielte Brute-Force-Angriffe zu ermitteln.

An dieser Stelle berücksichtigt modzero nicht, dass die Anzahl der möglichen Anfragen mit falschem Passwort an den entsprechenden API-Endpunkt bereits im Analysezeitraum limitiert war, so dass der postulierte Angriff in dieser Form nicht umsetzbar gewesen wäre. In der aktuellen Version von Vivy wird darüber hinaus auch die Anzahl ungültiger TOTP-Anfragen und E-Mail-Validierungen deutlich begrenzt.

3.3. Browser-App (4.3.)

Einige der von der modzero GmbH aufgezeigten Angriffsvektoren bezogen sich auf Vivys Browser-App, die zum Dokumentenaustausch zwischen Ärzten und Patienten dient.

Für die Risikoeinschätzung relevant ist an dieser Stelle, dass zunächst nur temporäre Accounts an Ärzte vergeben wurden, die Vivy in ihren Browsern testen konnten. Für den produktiven Standardprozess wird aktuell die *Web Crypto*-API mit nicht extrahierbaren privaten Schlüsseln eingesetzt. Zudem können Ärzte ab Q4/2018 eine eigens entwickelte Browser-App mit permanenten Accounts nutzen. Ein permanenter Account erhöht die Sicherheit erheblich durch die Kombination individueller Anmeldedaten, Zwei-Faktor-Authentifizierung und Speicherung des Schlüssels außerhalb des Browsers.

3.3.1. Unsichere Speicherung von Schlüsselmaterial im Browser (4.3.1.)

In Verbindung mit der Ausnutzung einer der von der modzero gefundenen Cross-Site-Scripting-Schwachstelle, auch *XSS* genannt, war es in der Browser-App möglich, den privaten Schlüssel des temporären Arzt-Accounts zu extrahieren. Dieser hätte zwar theoretisch das Entschlüsseln von Dokumenten erlaubt, die mit dem öffentlichen Schlüssel des Arztes verschlüsselt wurden, wie es z.B. bei mit dem Arzt geteilten Dokumenten der Fall ist. Doch ist der im modzero-Bericht unter 4.3.1.1. entstehende Eindruck, dass so ein beliebiges Herunterladen freigegebener Dokumente per se möglich würde, aufgrund zeitlich begrenzter Sessions und des angewendeten Peer-to-Peer-Prinzips, nicht zutreffend.

Um derartigen Angriffen dennoch vorzubeugen, wurde die Verschlüsselung auf Basis der *Crypto Web*-API neu implementiert und ausgerollt, was erlaubt, die kryptografischen Schlüssel in der öffentlichen Version der Browser-App für XSS-Angriffe unzugänglich zu speichern.

3.3.2. Persistentes Cross-Site-Scripting in geteilten Dokumenten/Profilbildern (4.3.2., 4.3.3.)

Im Dokumenten-Upload via App und Web-Interface war es in den früheren Versionen von Vivy möglich, beliebige Dateitypen hochzuladen. Auch für Profilbilder traf das zu. Nutzer sollten so die Möglichkeit erhalten, verschiedenartige Dokumente aus unterschiedlichen Quellen zu teilen, als Profilbild zu nutzen und in einer Dokumentenvorschau anzusehen.

In ihrem Report weist die modzero GmbH nun darauf hin, dass es beim Anzeigen der Dokumentenvorschau im Web-Interface für die Ansicht geteilter Dokumente möglich gewesen wäre, Skripte innerhalb der isolierten Umgebung der Vivy-Webanwendung im Browser auszuführen und z.B. Metadaten zur Transaktion oder verwendete Passwörter aufzeichnen. Auch das Anzeigen von Profilbildern im betroffenen Webinterface hätte einen Ansatzpunkt für XSS dargestellt.

Mit den zum 23.09.2018 veröffentlichten Änderungen können über das Web-Interface geteilte Dokumenten nur noch angesehen werden, nachdem sie heruntergeladen worden sind. Die Preview-Funktion wurde aus Sicherheitsgründen vollständig entfernt und die zulässigen Dateitypen für Profilbilder wurden auf JPG und PNG limitiert.

3.3.3. Persistentes Cross-Site-Scripting in Benutzernamen (4.3.4.)

Beim Dokumentenaustausch mit dem Patienten erhält der Arzt vom Patienten einen Link zu einem Web-Interface, das es erlaubt, Dokumente (z.B. Röntgenbilder) verschlüsselt zu übertragen.

Bevor ein Vivy-Nutzer Zugriff auf diese Funktionalität erhält, wird dessen Identität durch dafür geschulte Vivy-Mitarbeiter bestätigt („Know Your Customer“ oder *KYC*, siehe auch https://www.vivy.com/sicherheit/). Ein dem Szenario entsprechend missbräuchlich angelegtes Nutzerkonto, das schädlichen JavaScript-Code über den Vornamen einzubringen versucht, hätte bereits zum Prüfzeitpunkt keinen Zugriff auf die Dokument-Anfrage via Vivy erhalten. Eine andere Variante des Dokumentenaustauschs stellt die direkte Dokumenten Anfrage (*Direct Document Request*) dar. Diese Variante verwendet der Benutzer direkt in der Praxis. In diesem Fall kann er dem Arzt einen persönlichen Link zur Verfügung stellen, auch ohne durch die Vivy GmbH im Rahmen des KYC-Prozesses verifiziert worden zu sein. Der Arzt prüft hier die Identität des Patienten im persönlichen Kontakt selbst.

Im beschriebenen Fall könnte sich ein Angreifer nur Zugang zu Daten verschaffen, die der Arzt ihm explizit übermittelt und die er ohnehin durch die vor Ort erfüllte Dokument-Anfrage erhalten hätte.

3.3.4. Fehlende HTTP-Transport-Security-Policy (4.3.5.)

Zum Zeitpunkt des Angriffs durch die modzero GmbH wurden alle Anfragen an die Browser-App für Ärzte standardmäßig via HTTPS verschlüsselt übertragen. Falls ein Arzt die Browser-URL ohne HTTPS eingibt, wird er sofort und automatisch an die HTTPS-Version der Website weitergeleitet. Die erwähnten *HSTS* (*HTTP-Strict-Transport-Security-Header*) ermöglichen nur, dass der Browser die Webseite direkt in HTTPS lädt, obwohl der Arzt die HTTP- statt der HTTPS-Adresse eingegeben hat.

Modzero GmbH behauptet, sollte der Angreifer mit dem WLAN des Arztes verbunden sein, dieser die Weiterleitung auf eine Verbindung via HTTPS (falls der Arzt die URL des Web-Interfaces ohne HTTPS eingegeben hätte) abfangen und sie mit einer Weiterleitung auf eine eigene Webseite ersetzen könnte.

Um mit einem solchen Angriff erfolgreich zu sein und eine Weiterleitung vor der Aktivierung von HTTPS zu ermöglichen, wäre eine Kompromittierung der Internet-Infrastruktur (WLAN, Router) in der Praxis des zugreifenden Arztes notwendig, um als *Man in the Middle* Gesundheitsdaten mitlesen oder abfangen zu können. Würde in einer Arztpraxis die Infrastruktur erfolgreich angegriffen, wären allerdings nicht nur über Vivy transportierte Daten unsicher, sondern sämtliche über dieses Netzwerk erfolgende Kommunikation.

3.4. Mobile App (iOS/Android)

Vorab: Die Vivy GmbH rät auf der Webseite ausdrücklich von der Nutzung der Vivy-App auf Geräten mit Root-Zugriff (Android) oder Jailbreak (iOS) ab, da entsprechend modifizierte Geräte bekannterweise nicht mehr über die durch die entsprechenden Betriebssysteme bereitgestellten Sicherheitsmechanismen verfügen.

3.4.1. Export des privaten Schlüssels im Klartext (4.4.1.)

In der mobilen App für iOS und Android ist es aktuell möglich, den privaten Schlüssel zu exportieren, um den Schlüssel im Falle einer Wiederherstellung auf einem neuen Gerät weiter verwenden zu können.

Würde man sich als Nutzer einen neuen privaten Schlüssel erstellen, wären alle bisher gespeicherten Gesundheitsdaten unwiederbringlich verloren, weil zur Entschlüsselung der passende private Schlüssel des Nutzers fehlt. Die Verantwortung über den privaten Schlüssel liegt einzig und allein beim Nutzer als dessen Eigentümer, der diesen optional mit eigenen Ressourcen verschlüsseln kann.

Um jedoch Nutzern in diesem Punkt weiter entgegenzukommen, arbeitet die Vivy GmbH aktuell an einer Lösung, die es erlaubt, den privaten Schlüssel passwortgeschützt aus der App zu exportieren.

3.4.2. Einbetten von nicht vertrauenswürdigen HTML-Code (4.4.2.)

In den ersten Versionen der Vivy-App bestand die Möglichkeit, HTML-Code in Form bestimmter Dokumente in die Vivy-App für Android einzuschleusen. Diese Möglichkeit hätte potenziell für Phishing missbraucht werden können. Da die Übertragung von Dokumenten Ende-zu-Ende-verschlüsselt ist und in der Regel nur zwischen Arzt und Patient erfolgt, ist dieser Fall ausgesprochen unwahrscheinlich: der behandelnde Arzt selbst hätte ein derartig manipuliertes, interaktives Dokument an seinen Patienten senden müssen.

Die Möglichkeit einer solchen Täuschung bestanden bei *Office-Open-XML*-Dokumenten wie z.B. das DOCX-Format, da diese Dokumente zur Ansicht in der Android-App in HTML-Dokumente konvertiert wurden. Ein Fehler im eingesetzten Software-Modul (*XHTMLConverter*) erlaubte, im Rahmen der Konvertierung beliebigen HTML-Code in das dann angezeigte HTML-Dokument einzuschleusen, was einen potenziellen Ansatzpunkt für Phishing hätte bieten können.

Aus diesem Grund werden in den aktuellen App-Versionen DOCX-Dokumente nicht mehr in HTML konvertiert, um in der Android-App angezeigt zu werden, sondern stattdessen in statische PDF-Dokumente.

3.4.3. Zuordnung von pseudonymisiert gespeicherten Gesundheitsdaten (4.4.3.)

In der Android-Version der App wurden die TOTP-Token vom Nutzer bei der Anmeldung von pseudonymisierten Nutzern mitgesendet. Modzero wies darauf hin, dass es anhand dieses TOTP-Token bei der Anmeldung von pseudonymisierten Nutzern möglich sein würde, pseudonymisierte Nutzer einem Nutzer zuzuordnen. Diese wurden zum Prüfzeitpunkt zwar fälschlicherweise an die Vivy-System übertragen, jedoch zu keinem Zeitpunkt in Zusammenhang mit den pseudonymisierten Daten gespeichert.

Außerdem werden seit dem 04.10.2018 keine Zwei-Faktor-Authentifizierungscodes mehr bei der Anmeldung von pseudonymisierten Nutzern mitgesendet.

3.4.4. Preisgabe vertraulicher Daten aus Gesundheitsakte im System-Log (4.4.4.)

In der Vivy-App für Android konnte die modzero GmbH einen Angriffsvektor auftun, der bei erfolgtem *Rooting* des Geräts (Umgehen des gesamten Betriebssystems und Zugriff auf das Stammverzeichnis von Android, von welchem die Vivy GmbH grundsätzlich abrät) oder über aktivierten Entwickler-Zugang in den System-Logs dokumentierte Abstürze der App und Informationen zu geteilten Daten einsehbar machte.

Seitdem die Anwendung im Zuge des Berichtes der modzero GmbH verbessert wurde, werden im Android-System-Log, soweit möglich, durch die Vivy-App übertragene Dateien nicht mehr aufgeführt.

Wie oben erwähnt, erfordert die Verwendung dieses Angriffsvektors ein *Rooting* des Geräts, was vom Nutzer selbst ausgeführt werden muss. Dies bedeutet, dass dieser Angriffsvektor nur vom Nutzer des Endgerätes selbst eingesetzt werden kann, um seine eigenen Vivy-Logs zu sehen.

3.4.5. Preisgabe vertraulicher Daten aus Gesundheitsakte im Cache (4.4.5.)

Um Daten aus dem Cache auslesen zu können, muss ein Angreifer zuvor in den Besitz des Endgerätes des Patienten gelangen und sich Root-Zugang zu dessen System verschaffen. Wird das Endgerät mit einer Sicherheitsmaßnahme geschützt (Gesichtsentsperrung, PIN, Passwort), wird dieses Szenario noch aufwändiger. Deshalb empfiehlt die Vivy GmbH den Nutzern der App, ihre Endgeräte mit einem sicheren Passwort und anderen Maßnahmen zu schützen. So bleiben die zur Funktion der App notwendigen Daten sicher. Vivy hat seither die Menge der gecachten Daten reduziert.

Da auch dieser Angriffsvektor nur bei erfolgtem Rooting des Geräts möglich ist, kann dieser Angriffsvektor nur vom Nutzer des Endgerätes selbst eingesetzt werden, um Daten aus dem Cache auszulesen.

3.5. Analyse der Kritikalität

Es ist wichtig hervorzuheben, dass zu keinem Zeitpunkt ein Zugriff auf die Gesundheitsakte von einem oder mehreren Nutzern stattgefunden hat. Alle beschriebenen Angriffe zeigen starke Abhängigkeit von Vorinformationen (z.B. gültige temporäre Session-ID) oder sehr spezifischen Vorbedingungen (z.B. kompromittierte Geräte auf Seiten des Nutzers oder Arztes), um überhaupt durchgeführt werden zu können. Auch zielen alle bis auf den unter 3.2.1. behandelten Vektor auf die Kompromittierung einzelner Benutzerkonten ab. In der Praxis lassen sich die meisten aufgeführten Angriffsvektoren nicht kombinieren.

Unabhängig davon, wie kritisch oder wahrscheinlich ein potenzieller Angriffsvektor tatsächlich ist, nimmt die Vivy GmbH jedes potenzielle Sicherheitsrisiko sehr ernst und adressiert dieses umgehend. Routinemäßig wird zudem detailliert geprüft, ob potenzielle Angriffsvektoren vor dem Zeitpunkt der Verbesserungsmaßnahmen ausgenutzt wurden. Alle Punkte im Bericht der modzero GmbH waren Gegenstand einer solchen Analyse. In deren Rahmen wurden auch die Zugriffsprotokolle der Metadaten aller geteilten Dokumente ausführlich untersucht. Dabei zeigte sich, dass es keine verdächtigen Transaktionen von Nutzerdaten gab. Somit konnte sichergestellt werden, dass keine Nutzer oder Nutzerdaten von den Angriffsvektoren betroffen waren.

4. Wie wird Sicherheit bei Vivy kontinuierlich weiterentwickelt?

Bei der Entwicklung der Systeme für ein Produkt wie Vivy spielen die Themen Sicherheit und Qualitätssicherung bereits in der Konzeption eine zentrale Rolle. Dazu gehören umfassende Testkonzepte, eine Sicherheitsarchitektur auf dem Stand der Technik, die fortlaufende Aktualisierung der Datenschutzfolgenabschätzung und vieles mehr.

Doch die höchste Qualität bei technischen Produkten ist nur durch die kontinuierliche Verbesserung in standardisierten Prozessen erreichbar. Elementar hierfür ist die rasche Verbesserung der Software. Vivy stellt dies durch definierte *Incident*- und *Change*-Prozesse sicher. Für den Incident-Prozess stehen Experten 24 Stunden in Bereitschaft.

Diese sind in der Lage, kritische Incidents rasch zu analysieren, zu priorisieren und ein Change-Ticket zu erstellen. Der darauf angestoßene Change-Prozess folgt einer definierten Vorgehensweise für die rasche und einwandfreie Verbesserung der Software.

Incidents können hierbei von Mitarbeitern, Nutzern, Ärzten und anderen Personen gemeldet werden. Für die Bewertung der Priorität stellt die Datensicherheit einen wesentlichen Eckpfeiler dar. Stellt sich heraus, dass es bei dem Incident eine Softwareänderung notwendig ist, wird ein Ticket im Change-Prozess erstellt und die Verbesserung umgesetzt.

Vivy's Entwickler setzen Verbesserungen abhängig von ihrer Kritikalität innerhalb von wenigen Stunden um. Jede Änderung bei Vivy unterliegt dabei einem Qualitätssicherungsprozess, der Sicherheitsüberprüfungen beinhaltet und dem Vier-Augen-Prinzip folgt. Zusätzlich werden Vivy-App und Vivy-Server von externen Experten routinemäßig getestet.

Als Entwickler einer der ersten digitalen Gesundheitsakten unterstützt von gesetzlichen und privaten Krankenversicherungen in Deutschland, weiß die Vivy GmbH um ihre Verantwortung und ist überzeugt, dass Vertrauen und Sicherheit die unverhandelbare Grundlage für die Digitalisierung im deutschen Gesundheitssystem bilden. Darum wertschätzt das Unternehmen ausdrücklich die Bemühungen der modzero GmbH und die daraus resultierenden Hinweise, da sie helfen, die Daten der Nutzer noch besser vor dem Zugriff unberechtigter Dritter zu schützen.