# Richtlinie zum „Software-Sprint“

# ml-ransomware – Ransomware war gestern: Undo von Ransomware mittels Machine Learning

## *Schlussbericht*

Zuwendungsempfänger:

Fratz und Held GbR

Gesellschafter:
Matthias Held, Waldhornstraße 2, 77933 Lahr
Matthias Fratz, Haidelmoosweg 27, 78467 Konstanz

Das diesem Bericht zugrundeliegende Vorhaben wurde mit Mitteln des Bundesministeriums für Bildung und Forschung unter dem Förderkennzeichen 01IS18S62 gefördert. Die Verantwortung für den Inhalt dieser Veröffentlichung liegt beim Autor.

## Kurze Darstellung der Aufgabenstellung und Motivation

### *Welches Problem wolltest Du mit Deinem Projekt lösen?*

Der Verlust von privaten Bildern, Videos oder wichtigen Dokumenten ist für viele Menschen ein Schreckgespenst. Kriminelle haben es deshalb auf genau solche Dateien abgesehen, nehmen sie durch Verschlüsselung in virtuelle Geiselhaft und fordern Lösegeld, mit dem ungewissen Versprechen, die Daten wieder zu entschlüsseln. Was für Privatpersonen den Verlust wertvoller Erinnerungen bedeutet, kann für Unternehmen existenzbedrohend sein: Britische Krankenhäuser waren 2017 mehrere Tage kaum funktionsfähig, der internationale Güterverkehr war wochenlang behindert.

### *Was war Deine Motivation?*

Im Rahmen der Masterarbeit von M. Held hatten wir grundlegende Eigenschaften und Erkennungsmerkmale von Kryptotrojanern (engl. Ransomware) analysiert. Die Haupterkenntnis war,

dass bei Nutzung eines modernen Cloudspeichers, wie der persönlichen Open-Source-Cloudlösung Nextcloud, die betroffenen Dateien leicht aus dem Cloudspeicher wiederhergestellt werden können.

Die Zuverlässigkeit der prototypischen Implementierung als App für Nextcloud war noch nicht optimal. Deshalb sollten im Rahmen des PrototypeFund-Projekts nun Machine-Learning-Techniken zur besseren Klassifikation zum Einsatz kommen. Dabei sollte das gesamte System so angelegt werden, dass auch weitere Cloudspeicher leicht von diesem Schutz profitieren können.

### *Wie war die geplante Vorgehensweise zur Problemlösung?*

Moderne Cloudspeicher wie Nextcloud speichern ältere Versionen aller Dateien. Anhand des Schreibverhaltens und der geschriebenen Daten lässt sich ein Kryptotrojaner-Angriff erkennen, so dass für jede Datei die letzte unbeschädigte Version wiederherstellt werden kann. Die im Rahmen der genannten Masterarbeit entwickelte Nextcloud-App „Ransomware Recovery" verwendet handgeschriebene Regeln zur Erkennung dieser letzten unbeschädigten Version. Erste Tests hatten gezeigt, dass Machine-Learning-Techniken eine erhebliche Verbesserung der Erkennungsrate bringen sollten. Daher sollte ein Machine-Learning-Ansatz wissenschaftlich evaluiert und in die Ransomware Recovery-App integriert werden.

Dazu wollten wir das Zugriffsverhalten und die geschriebenen Daten echter Kryptotrojaner erfassen und frei zur Verfügung stellen. Anhand dieser Daten wollten wir ein geeignetes Klassifizierungsmodell bestimmen, welches zur Erkennung von Kryptotrojaner-Angriffen trainiert werden kann.

Um diese Technik sinnvoll einsetzbar zu machen, sollte direkt nutzbares vortrainiertes Erkennungsmodell zur Verfügung gestellt, sowie eine REST-basierte Komponente für die Einbindung in andere Cloudspeicher-Software entwickelt werden. Diese unabhängige Komponente kann dann aus verschiedenen schlanken Apps und Plugins für Cloudspeicher angesprochen werden und damit Schutz gegen Kryptotrojaner bieten.

*Milestones:*

- **M1 Datensatz:** Erweiterung und Systematisierung unseres Datensatzes der Zugriffsmuster und zerstörten Dateien von Kryptotrojanern, so dass dieser für Machine Learning geeignet ist.
- **M2 Modellauswahl:** Auswahl und Evaluierung eines geeigneten Modells für die Erkennung von Kryptotrojanern.
- **M3 fertiges Modell:** Training des gewählten Machine-Learning-Modells auf Basis dieses Datensatzes, um ein auslieferbares Modell zu erhalten.
- **M4 Schnittstellen:** Entwicklung von Schnittstellen für den Zugriff auf das Machine-Learning-Modell zur Integration in weitere Cloudspeichersysteme.
- **M5 Integration:** Integration in Cloudspeichersysteme, insbesondere Nextcloud.

## Beitrag des Projektes zu den Zielen der Förderinitative „Software-Sprint“

### *Wer ist die Zielgruppe für Deine Lösung und wie profitiert sie von den Ergebnissen Deines Projekts?*

Die Allgemeinheit profitiert von unserer Lösung durch Zugriff auf Cloudspeichersysteme, in die an eine Instanz unseres Klassifizierungs-Dienstes angebunden sind. Im Falle von Nextcloud sind dies grundsätzlich jegliche Nextcloud-Instanzen, unabhängig davon ob diese von Firmen, Organisationen oder Privatpersonen betrieben werden, da sich die App mit wenigen Klicks in der Administrationsoberfläche der Nextcloud-Instanz aktivieren lässt.

Durch das Angebot unseres Klassifizierungswerkzeugs als Open-Source-Software können technisch versierte Personen dies in andere Cloudspeichersysteme integrieren oder darauf aufbauend eigene Systeme entwickeln. Zielgruppe sind hier zunächst vor allem Open-Source-Projekte, aber auch Anbieter proprietärer Systeme können die entwickelte Software nachnutzen. Eine entsprechende Sichtbarkeit wird durch ein öffentliches Projekt auf GitHub unter einer geeigneten Open-Source-Lizenz erreicht.

Forschende profitieren zusätzlich von dem zusammengestellten Ransomware-Datensatz, welcher lauffähige Samples für die meisten bekannten Ransomware-Familien der letzten Jahren enthält und für die Analyse dieser Malwaregruppe eingesetzt werden kann. Ergänzt wird dieser durch die von jedem Ransomware-Sample verschlüsselten Dateien aus unserem Referenz-Datensatz. Forschende können anhand dieser Datensätze neuartige Erkennungsmethoden oder -systeme entwickeln, welche mittelfristig wiederum in den Klassifizierungsdienst einfließen können. Die wissenschaftliche Community soll durch eine Datenpublikation im Sinne des Open Science sowie einer zugehörigen wissenschaftlichen Veröffentlichung erreicht werden.

### *Welche Bezüge gibt es zu den Themenfeldern und Zielen des Software Sprints?*

Sicherheit ist eines der Grundbedürfnisse des Menschen und muss sich im Zeitalter der Digitalisierung auch auf die „Digitale Welt“ erstrecken. Dazu gehört einerseits der Schutz vor Kriminellen, andererseits aber auch vor Überwachung durch Unternehmen oder staatlichen Stellen.

Die Wiederherstellung von durch Ransomware zerstörten Dateien schützt einerseits direkt vor kriminellen Erpressern, und kann damit zur IT-Sicherheit unserer Nutzergruppe beitragen. Die Nextcloud-App liefert zusätzlich ein weiteres kleines Alleinstellungsmerkmal von Nextcloud gegenüber öffentlichen Cloud-Anbietern. Dadurch unterstützt sie das Ziel, den Wechsel von kommerziellen Cloud-Anbietern mit teilweise fragwürdigen Geschäftspraktiken auf offene und vertrauenswürdige Infrastrukturen zu fördern.

Ein offener Datensatz von Ransomware-verschlüsselten Dateien unterstützt direkt den Open-Science-Gedanken. Daraus abgeleitete Erkenntnissen über die Verhaltensmuster von Ransomware sowie die Erkennung derselben mittels Machine Learning können dem allgemeinen wissenschaftlichen Fortschritt dienen.

Durch Offenlegung unserer Vorgehensweise möchten wir außerdem das Bewusstsein der interessierten Allgemeinheit für das Thema Ransomware schärfen. Wir hoffen dadurch sowohl die allgemeine Informationssicherheit zu verbessern, aber auch den Menschen durch Zugriff auf alle

Informationen die Möglichkeit bieten, sich an diesem Thema über das versehentliche Ausführen von Ransomware auf dem heimischen Rechner hinaus zu beteiligen.

## Ausführliche Darstellung der Ergebnisse

### *Welche konkreten Ergebnisse hast Du erzielt?*

- Die Nutzeroberfläche der Nextcloud-App wurde, dank der Unterstützung von SimplySecure im Rahmen des UI-Coachings, bereits erheblich nutzerfreundlicher gestaltet. Aus einer zweiten Runde von Feedback gegen Ende des Projekts ergaben sich weitere Verbesserungsmöglichkeiten, die nun ebenfalls eingepflegt werden sollen.
- Anhand von Statistiken aus einer großen (>1000 aktive Accounts) Nextcloud-Instanz wurde ein 1GB großer Datensatz mit „typischen" Dateien geschaffen, der zur Analyse von Ransomware-Verhalten geeignet ist. Die Verteilung von Dateitypen und -größen in diesem Datensatz der Victim-Dateien entsprechen in etwa den Verteilungen auf der betrachteten Nextcloud-Instanz und sollten einigermaßen realistisch für verschiedene Dateisammlungen sein. Diese Dateien sind teilweise synthetisch aus Wikipedia-Artikeln erstellt, teilweise aus Wikimedia Commons entnommen, und mit den jeweiligen Provenienzmetadaten versehen, so dass diese Victim-Daten unproblematisch weiterverbreitet werden können.
- Eine Liste von 61 konkreten Ransomware-Samples, die in der gewählten Cuckoo-VM funktionieren und Dateien verschlüsseln. Viele Ransomware-Samples sind nicht mehr lauffähig, da sie entweder auf nicht mehr erreichbare Server im Internet angewiesen sind oder die unübliche Konfiguration der VM (Single-Core mit nur 2GB RAM / 32GB Festplatte) erkennen und die Funktion verweigern. Diese Liste kann besonders neuen Forschenden im Ransomware-Feld also erheblich Zeit sparen.
- Die Open-Source-Software Cucoo Sandbox wurde so konfiguriert und agepasst, dass sie für die Analyse von Ransomware auf großen Datenmengen geeignet ist. Damit können die ausgewählten Ransomware-Samples zuverlässig auf den 1GB großen Referenzdatensatz angewendet werden.
- Aus der Ausführung dieser Samples ergibt sich ein weiterer, einzigartiger Datensatz von Dateien, die von Ransomware zerstört wurden. Zusätzlich zu den 45GB der eigentlichen Dateien sind in fast allen Fällen die exakten Timings der Schreib- und Löschvorgänge vorhanden, die Aufschluss über das Verhalten des jeweiligen Ransomware-Samples geben.
- Ein Satz von Machine-Learning-geeigneten Features auf diesen Dateien, die in einer Nextcloud-App leicht aus der Datei zu bestimmen sind. Da PHP dafür nur bedingt geeignet ist, sollten sich diese Features auch in jeder anderen Programmiersprache und -umgebung leicht bestimmen lassen. Für jedes Feature besteht zudem eine initiale Abschätzung, wie indikativ dieses Feature für Ransomware-zerstörte Dateien ist. Daraus lässt sich begründen, einige der initialen Features wegzulassen, insbesondere da sich die am schwersten zu berechnenden Features als nicht besonders nützlich erwiesen haben.
- Zu jeder Ransomware-zerstörten Datei sind die extrahierten Features sowie einige Metadaten als zusammengefasster Datensatz vorhanden. Dieser bildet die Grundlage für

sämtliche Machine-Learning-Anwendungen des Projekts und kann grundsätzlich auch für weitere Forschung in diesem Bereich genutzt werden.

- Es konnte nachgewiesen werden, dass bereits einfachste Modelle (in diesem Fall ein Linearer Classifier) recht gute Ergebnisse (ca. 96%) bringen. Damit sollte die Anwendung von Machine Learning hier eindeutig zielführend sein.
- Eine vorläufige REST-Schnittstelle des Klassifizierungs-Dienstes wurde definiert, um diesen aus beliebigen Programmiersprachen und damit Cloud-Diensten ansprechen zu können. Diese vorläufige Schnittstelle lässt sich leicht um weitere Features erweitern und kann damit bereits als Basis für Entwicklungen dienen.

*Konnten alle Meilensteine erreicht werden?*

- **M1 Datensatz:** abgeschlossen. Die erzeugten Datensätze von lauffähiger Ransomware, repräsentativen Dateien vor deren Zerstörung, sowie Ransomware-zerstörter Dateien sind bei den „konkreten Ergebnissen" beschrieben.
- **M2 Modellauswahl:** begonnen. Die Anwendung einfacher Modelle zeigt, dass bereits diese gut funktionieren. Darauf ausgehend konnte die Menge der erforderlichen Features bereits reduziert werden, und die Nützlichkeit des Datensatzes mit Ransomware-zerstörten Dateien wurde nachgewiesen. Für den Abschluss dieses Milestones wird eine große Menge von Dateien benötigt, die für „ganz normale" Dateien (d.h. vor der Zerstörung) repräsentativ sind. Die für die Victim-Dateien angewandte Methode stößt hier an ihre Grenzen.
- **M3 fertiges Modell:** begonnen. Ein initiales Modell ist vorhanden und sollte ersten Tests zufolge eine Genauigkeit von 96% erreichen. Dieses Modell wir entsprechend der Ergebnisse von M2 Modellauswahl fortlaufend aktualisiert. Hier ist abzusehen, dass bei Abschluss von M2 Modellauswahl dieses Modell nahezu ohne Mehraufwand zur Verfügung steht.
- **M4 Schnittstellen:** größtenteils abgeschlossen. Die vorläufige REST-Schnittstelle des Klassifizierungs-Dienstes muss noch um weitere Machine-Learning-Features erweitert werden, was aber zu keinen strukturellen Änderungen mehr führen wird. Das entsprechende Backend befindet sich in aktiver Entwicklung.
- **M5 Integration:** größtenteils abgeschlossen. Die Oberfläche der Nextcloud-App wurde benutzerfreundlicher gestaltet und auf ein strukturiertes UI-Framework umgestellt. Die Kommunikation mit unserem Klassifizierungdienst ist implementiert und muss noch Integrationstests unterzogen werden.

*Welche zusätzlichen Erkenntnisse hast Du aus der Projektarbeit gewonnen, auch im Hinblick auf die Begleitung durch die Open Knowledge Foundation?*

Während der Projektphase hat sich die Koordination der Entwicklung an verschiedenen Standorten als schwieriger herausgestellt als ursprünglich erwartet. Durch Aufteilung der Arbeit in unterschiedliche, voneinander unabhängige Module konnten wir die Entwicklung aber auf relativ unabhängige Arbeit am jeweiligen Modul fokussieren. Für die verbleibende Koordination der Entwicklung, insbesondere der Schnittstellen und wichtiger technischer Entscheidungen, waren Internet-Telefonkonferenzen mit der Möglichkeit zum Screen-Sharing sehr hilfreich. Dies könnte als

Hilfestellung für andere Projektteams dienen, die ebenfalls nicht am selben Standort arbeiten können.

Das UI-Coaching durch SimplySecure brachte große Verbesserungen an der Oberfläche der Nextcloud-App. Wir würden dieses Coaching deshalb allen Projekten nahelegen, die unentschieden sind, welches der beiden angebotenen Coachings (UI oder Projektmanagement) für sie sinnvoller ist. Eine weitere Empfehlung daraus ist, nach Möglichkeit bereits mit einem Mockup oder einer bestehenden Oberfläche mindestens ins zweite Coaching zu gehen, weil dadurch die Iteration im Rahmen des Coachings erheblich produktiver ist.

## Zielgruppe, Nutzen und mögliche Weiterentwicklungen

### *Welcher Nutzen ergibt sich für die Zielgruppe aus den Ergebnissen Deines Projekts?*

Wie bei den Zielgruppen beschrieben, ergibt sich für diese der folgende Nutzen:

- Die Nextcloud-nutzende Allgemeinheit kann die App nutzen, um nach einem Ransomware-Angriff zerstörte Dateien einfach wiederherzustellen.
- Technisch versierte Personen können unsere Komponenten als Basis für eigene Entwicklungen nutzen.
- Forschende können die erstellten Datensätze im wissenschaftlichen Bereich einsetzen.

### *Welche weitergehenden Effekte ergeben sich aus der Open-Source-Stellung der Ergebnisse?*

Durch die Open-Source-Stellung unseres Vorgehens sowie unserer Ergebnisse bei der Ransomware-Analyse hat jeder Einblick in unsere Arbeit und kann bei Interesse nachvollziehen, wie wir Ransomware analysiert, die Ergebnisse interpretiert und aus diesen interpretierten Daten eine Software entwickelt haben, welche Nutzer vor Ransomwareangriffen schützt. Das dient einerseits dem Open-Science-Gedanken, Einblick in die eigene Forschungsarbeit zu gewähren, und verbessert andererseits die Vertrauenswürdigkeit der entwickelten Software, da die Herkunft der Modelle besser nachvollzogen werden kann. Das Klassifizierungsmodell kommt nicht aus einem undurchsichtigen Forschungsprojekt oder ist Firmengeheimnis einer Antivirus-Firma, sondern ist das Ergebnis eines offenen und dokumentierten Prozesses.

Die Open-Source-Stellung ist in unserem Fall auch ein wichtiges Mittel, um die Nachhaltigkeit der Projektergebnisse sicherzustellen. Die Methode an sich sowie die Nextcloud-App im speziellen lassen sich, auch wegen vieler Softwarepatente in diesem Bereich, nicht soweit kommerzialisieren, dass die Entwicklung und Pflege ohne Unterstützung durch die Open-Cource-Community möglich ist.

### *Gibt es Ideen für die Weiterentwicklung Deiner Lösung und Pläne zu deren Umsetzung?*

- Wir möchten einen größeren (50-100GB) Referenzdatensatz von nicht zerstörten Dateien sammeln. Dieser Referenzdatensatz einerseits und unser Datensatz von Ransomware-zerstörten Dateien andererseits bildet dann die beiden Klassen des Supervised Learning, mit dem wir die Modell- und Feature-Auswahl weiterführen möchten.

- Anhand des daraus gewonnenen Feature-Sets soll eine erste stabile Version der REST-Schnittstelle des Klassifizierungs-Dienstes definiert werden. Parallel soll eine Referenzimplementation des Klassifizierungs-Dienstes erstellt werden, welche dann für die Integration in die Nextcloud-App genutzt werden kann.

- Die Nextcloud-App soll fortlaufend an neuere Nextcloud-Versionen angepasst werden. Soweit möglich, planen wir außerdem neue Ransomware-Familien weiterhin zu analysieren und die Modelle entsprechend anzupassen.

*Hat die Arbeit in dem Projekt Dich in Deiner persönlichen, fachlichen Weiterentwicklung unterstützt?*

Die Arbeit am Projekt ermöglichte uns einerseits die fachliche Weiterbildung im Bereich der Analyse von Malware, der Methoden des Machine Learning sowie dem Entwurf und der Entwicklung grafischer Benutzeroberflächen. Andererseits konnten wir unser Wissen über Open-Source-Software und Projektentwicklung weiter vertiefen und hatten Einblick in die Möglichkeiten und Herausforderungen der selbstständigen Softwareentwicklung, die wir so vor dem Projekt noch nicht in Betracht gezogen hatten.

## Kurze Darstellung der Arbeiten, die zu keiner Lösung geführt haben

*Gab es Arbeiten bzw. Lösungsansätze, die nicht weiter verfolgt wurden? Was waren die Hintergründe, und wie bist Du alternativ vorgegangen?*

- Die ursprünglich vorgesehene Filterung nach dem Vorkommen des Wortes „ransomware“ in den Erkennungen von VirusTotal war zu selektiv, da nur wenige Hersteller erkannte Ransomware auch mit dem Wort „ransomware“ beschreiben. Üblicher sind Erkennungen der Art „Trojan.Ransom.*“ oder „Ransom.*“. Daher wurde stattdessen nur nach „ransom“ gesucht, sowie nach einer Liste von benannten Ransomware-Familien, die manuell aus verschiedenen Quellen zusammengetragen wurde.

- Die Gruppierung von Ransomware in Familien mittels des automatisierten Werkzeugs AVclass war für eine Auswahl der auszuführenden Samples nicht ausreichend. Es wurden mehrere tausend Familien erkannt, ohne dass diese anhand der Anzahl Samples weiter gefiltert werden konnten: Auch Familien mit nur einem erkannten Sample enthielten bekannte Ransomware. Initial wurde daher die (kuratierte) öffentliche „theZoo“ Sammlung genutzt. Danach wurden Samples gewählt, die auf die manuell zusammengetragenen Namen der Ransomware-Familien passten.

- Bei 1GB Daten funktionierte die in Cuckoo eingebaute Funktion zur Sammlung veränderter Dateien nicht mehr zuverlässig. Außerdem waren einige Ransomware-Samples in der Lage, die Analyse durch Cuckoo nahezu vollständig zu umgehen und dadurch unbeobachtet Veränderungen an Dateien innerhalb der VM vornehmen. Daher wurde nach jeder Analyse ein Snapshot der Festplatte der VM erstellt, aus dem die vollständige Liste der veränderten oder zerstörten Dateien in jedem Fall wiederhergestellt werden kann. Hierbei geht allerdings die Information zum Timing der Schreib- und Löschzugriffe größtenteils verloren.

- Cuckoo ist in der Lage, den Netzwerkzugriff für Malware einzuschränken, unterstützte in unserer Umgebung aber nur Vollzugriff oder keinen Netzwerkzugriff. Durch eine kleine Anpassung am Source Code konnten wir zusätzlich den Zugriff nur auf Web-Dienste ermöglichen, ohne vollständigen Internetzugriff zu ermöglichen. Diese Anpassung ist für unsere Anwendung sinnvoll, für Cuckoo sollte aber eventuell eine andere, generellere Methode entwickelt werden.

- Ursprünglich war geplant, mittels tensorflow.js auch einer Erkennung ohne laufenden Klassifizierungsdienst zu ermöglichen. Wegen der erforderlichen Datenweitergabe vom Backend bis ins Frontend im Browser erscheint diese Lösung aber nicht wirklich praktikabel. Wie die Architektur entsprechend angepasst werden muss ist derzeit noch nicht entschieden.

## Kurze Angabe von Präsentationsmöglichkeiten für mögliche Nutzer

***Wo können sich Interessenten detailliert über Deine Projektergebnisse informieren (z.B. Webseite, GitHub, Veröffentlichungen)?***

Die beschriebenen Zielgruppen sollen durch Platzierung der jeweiligen Ergebnisse in jeweils geeigneten Kanälen erreicht werden:

- Die aktualisierte Version der Nextcloud-App „Ransomware Recovery" wird nach angemessenen Tests über die normalen Update-Kanäle verbreitet.
- Alle Daten und Informationen zu den durchgeführten Experimenten, sowie der Source Code der entwickelten Software, werden öffentlich und zentral gesammelt über eine GitHub-Organisation (http://github.com/undo-ransomware) zugänglich gemacht.
- Die Datensätze sollen auf Zenodo bereitgestellt werden. Zusätzlich ist geplant, die Datensätze und das Vorgehen durch eine wissenschaftliche Publikation der Öffentlichkeit zur Verfügung zu stellen.
- Die jeweiligen Resourcen sollen auf der Informationsseite zum Projekt auf protypefund.de (https://prototypefund.de/project/undo-von-ransomware-mittels-machine-learning/) verlinkt werden, so dass sie ausgehend vom Projekt leicht gefunden werden können.

## Kurze Erläuterung zur Einhaltung der Arbeits- und Kostenplanung

***Gab es im Projektverlauf Ereignisse, die eine Anpassung der Planung erforderlich machten – z.B. Mehr- oder Minderaufwand bei der Bearbeitung von Teilaufgaben?***

Beim Meilenstein „M1 Datensatz" stellte sich die Systematisierung unseres Datensatzes als wesentlich umfangreicher als ursprünglich geplant heraus. Jedoch ist und war er zentraler Meilenstein unseres Projekts, da er einerseits die Grundlage für den Machine-Learning-Aufgabenteil darstellt, andererseits aber auch das größte Potential für die Nachnutzung durch die wissenschaftliche Community bietet. Um unbrauchbare Ergebnisse durch schlechte Eingabedaten zu vermeiden, wurde der Schwerpunkt auf diesen Milestone gelegt und die Modell- und Feature-Auswahl entsprechend etwas zurückgestellt. Dies führte dazu, dass der Milestone „M1 Datensatz" parallel zu allen anderen Meilensteinen bis zum Projektende weitergeführt wurde, da wir immer

weiteren Einblick auf das Verhalten von Ransomware bekamen. So war es uns möglich einen einzigartigen Datensatz zu erstellen, der das schlussendlich zu entwickelnde Modell auf wissenschaftlich solide Beine stellt.

## Kurze Darstellung von etwaigen Ergebnissen bei anderen Stellen

***Gab es Entwicklungen anderer Personen oder Institutionen, die Einfluss auf Deine Arbeiten und die Zielsetzung hatten? Wenn ja, worin bestand dieser und wie bist Du damit umgegangen?***

Ein weitere Suche nach wissenschaftlichen Veröffentlichungen in diesem Bereich förderte etliche Publikationen während der Projektlaufzeit zu Tage. Diese unterteilen sich in die folgenden Familien:

- Anwendung von Machine-Learning-Methoden auf den Maschineninstruktionen oder dem (lokalen) Verhalten eines Ransomware-Programms zur Erkennung desselben. Diese Methoden können, wie klassische Antivirus-Programme, die Recovery auf Nextcloud komplementieren, sind aber für das Projekt an sich nicht relevant.
- Anwendung von Machine-Learning-Methoden auf den Netzwerkverkehr eines Rechners, um den Netzwerkverkehr von Ransomware zu erkennen. Dies kann im Rahmen des Netzwerkmanagements bei größeren Institutionen sehr hilfreich sein und die Ausbreitung von Malware effektiv einschränken. Unsere Erfahrung zeigt aber, dass viele Ransomware-Familien auch ohne Netzwerkzugriff sehr effektiv Dateien zerstören. Wir sehen diesen Forschungsbreich deshalb als orthogonal zu unserem Projekt an.
- Anwendung von Machine-Learning-Methoden auf die geschriebenen Daten.

Die Ergebnisse von 2 Veröffentlichungen dieser letzten Familie sind direkt relevant im Rahmen des Projekts, da eine sehr ähnliche Fragestellung erprobt wird. Aufgrund des Publikationsdatums gegen Ende des Projekts konnten diese Ergebnisse im Projekt leider nicht mehr genutzt werden, sondern sind in die Ideen zur Weiterentwicklung unserer Lösungen eingeflossen.

- K. Lee, S. Lee and K. Yim, „Machine Learning Based File Entropy Analysis for Ransomware Detection in Backup Systems," in *IEEE Access*, vol. 7, pp. 110205-110215, 2019. https://doi.org/10.1109/ACCESS.2019.2931136
  Lee et al. verwenden sehr ähnliche Methodiken in einem effektiv identischen Setup (Backups). Die dortigen Ergebnisse zeigen, dass die Erprobung weiterer Features und Machine-Learning-Algorithmen zielführend ist.
- M. J. May and E. Laron, „Combating Ransomware using Content Analysis and Complex File Events," 2019 10th IFIP International Conference on New Technologies, Mobility and Security (NTMS), CANARY ISLANDS, Spain, 2019, pp. 1-5. https://doi.org/10.1109/NTMS.2019.8763851
  May und Laron verwenden eine sehr viel umfangreichere Analyse der Dateiinhalte mittels Apache Tika. Eine direkte Anwendung muss erwogen werden, sofern in PHP und als Nextcloud-App umsetzbar. Die Evaluation anhand einer einzelnen Ransomware-Familie bestärken uns aber auch darin, unseren Datensatz sorgfältig zu beschreiben und zu veröffentlichen.

Im Bereich der Ransomware selbst trat mit Sodinokibi eine neue Familie (bzw. Variante von GandCrab) in Erscheinung. Da unser Basis-Datensatz für Ransomware vom Februar 2019 stammt, war Sodinokibi in diesem Datensatz nicht vorhanden. Daher wurden 7 Samples von Sodinokibi manuell von VirusShare heruntergeladen und in unserer Ransomware-VM analysiert. Davon erwiesen sich 6 als lauffähig und sind in unserem Datensatz zerstörter Dateien vertreten.