Graz University of Technology

IAIK – Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie

Inffeldgasse 16a
8010 Graz

Tel. +43 (0)316 873-5514
Fax. +43 (0)316 873-5520

http://www.iaik.tugraz.at

DVR: 008 1833 UID: ATU 574 77 929

Graz, 08 August 2017

Entwurf des Strafprozessrechtsänderungsgesetzes 2017
(Stellungnahme IAIK TU-Graz)

Diese Stellungnahme des Instituts für Angewandte Informationsverarbeitung und Kommunikationstechnologie der Technischen Universität Graz adressiert technische Risiken der im Entwurf des Strafprozessrechtsänderungsgesetzes 2017 vorgesehenen Maßnahme zur Einführung einer neuen Ermittlungsmaßnahme zur „Überwachung verschlüsselter Nachrichten“ (§§ 134 Z 3a, 135a StPO). Die Stellungnahme bezieht sich insbesondere auf Risiken im Zusammenhang mit folgenden Punkten:

- Remote Aufbringung
- Umgehbarkeit und Abgrenzung zur Online-Durchsuchung
- Förderung von Internetkriminalität
- Technische Realisierbarkeit und Kosten

Bevor auf die Punkte jeweils in einzelnen Kapiteln dieser Stellungnahme eingegangen wird, wird das Institut, das die Stellungnahme abgibt, kurz vorgestellt:
Das Institut für Angewandte Informationsverarbeitung und Kommunikationstechnologie (IAIK) ist das längst existierende und größte universitäre Forschungsinstitut, das sich mit allen Aspekten der IT Sicherheit (Hardware, Software und Kryptographie) in Österreich beschäftigt. Eine Gruppe von ca. 70 Forschern arbeitet an neuen Verschlüsselungsmethoden, Hardware- und Systemsicherheit aber auch an verifizierbar sicheren Systemen. Am Institut laufen derzeit mehr als 20 Forschungsprojekte im Themenfeld Informationssicherheit, die sowohl Grundlagenforschungsthemen umfassen als auch viele Projekte mit österreichischen und europäischen Unternehmen. Unter den Projekten sind europaweit hoch kompetitiv vergebene Förderungen der EU, wie beispielsweise ein ERC Consolidator Grant. Die Forschungsergebnisse des Instituts werden regelmäßig auf internationalen Topkonferenzen im Bereich Informationssicherheit veröffentlicht. Gleichzeitig werden praxisnahe Prototypen erstellt. Basierend auf Patenten und Forschungsarbeiten wurden beispielsweise kryptographische Bibliotheken, Zertifikatssysteme, Prototypen der österreichischen

Handy-Signatur etc. erstellt. Das IAIK ist sowohl national als auch international ein zentraler Ansprechpartner zu Themen der IT Sicherheit.

1. Remote Aufbringung

Risiko

Bei einer reinen „Remote Aufbringung“ kann technisch im Allgemeinen nicht mit hinreichender Sicherheit festgestellt werden, dass sich das System auf dem die Software installiert wird im Inland befindet und dass das System auch tatsächlich das System der zu überwachenden Zielperson ist.

Technischer Hintergrund

Es ist davon auszugehen, dass Krimielle Maßnahmen ergreifen um im Internet nicht leicht identifizierbar zu sein. Hierfür gibt es technisch eine Vielzahl von Möglichkeiten. Um die Privatsphäre von Internetnutzern sicher zu stellen gibt es beispielsweise Anonymisierungsnetzwerke wie Tor. Personen mit krimineller Energie können aber auch direkt in Systeme unschuldiger Dritter eindringen und ihren gesamten Internetverkehr über die IP Adresse dieser dritten Person lenken und so das Gerät dieser Person zum Ziel für die Installation von Überwachungssoftware machen. Durch derartige Weiterleitungen bzw. Netzwerke wie Tor ist basierend auf MAC oder IP Adressen nicht nur die Identität nicht mehr festzustellen, sondern auch nicht mehr festzustellen ob sich ein Gerät im Inland oder Ausland befindet. Der Umstand, wo sich ein Gerät befindet könnte aber in Bezug auf die Anwendbarkeit der Strafrechtsordnung relevant sein. Technisch weniger versierte Kriminelle können auch einfach gestohlene Geräte oder Identitäten verwenden und so im Internet auftreten.
Aber selbst wenn nicht vorsätzlich versucht wird die Identität zu verbergen, kann eine Identifikation schwierig sein. Ein und dasselbe Mobiltelefone tritt beispielsweise unter verschiedensten IP Adressen im Internet auf je nachdem ob die Kommunikation über das Mobilfunknetz erfolgt oder ob über eines der zahlreichen frei verfügbaren WLAN Netze (Restaurants, ÖBB, wichtige öffentliche Plätze, …) verwendet wird. Auch durch VPN Netzwerke wird die IP Adresse verändert.
Inwieweit Identifikation, die nicht auf physischen Parametern (z.B. Gerät in der Wohnung von Betroffenen...) basiert, überhaupt möglich ist, kann nur im konkreten Einzelfall technisch geprüft werden. Kritisch ist in jedem Fall, dass bei einer Remote Installation nur sehr limitierte Möglichkeiten bestehen zu prüfen ob das richtige Gerät getroffen wurde. Eine Durchsuchung eines Geräts zur Identitätsfeststellung ist auf Grund der Abgrenzung zur Online-Durchsuchung nicht möglich.

2. Umgehbarkeit und Abgrenzung zur Online-Durchsuchung

Risiko

Durch die Einschränkung der Überwachung auf ganz konkrete Applikationen ergibt sich eine Vielzahl technischer Möglichkeiten eine Überwachung leicht zu umgehen. Bei Erweiterung der Überwachung zur Reduktion der Umgehungsmöglichkeiten besteht das Risiko der Nichtabgrenzbarkeit zu einer Online-Durchsuchung.

Technischer Hintergrund

Der Gesetzesentwurf und die entsprechenden Erläuterungen betonen die Abgrenzung des aktuellen Gesetzesentwurfs zu einer Online-Durchsuchung. Konkret werden deshalb Dokumente, die offline verschlüsselt werden, allgemeine Keylogger und sämtliche Dateien eines Systems, die nicht in direktem Zusammenhang mit einer end-to-end Verchlüsselung sehen, nicht überwacht. Die Überwachung ist somit eingeschränkt auf ganz konkrete Applikationen zur Kommunikation, wie Skype oder WhatsApp. Dies erlaubt eine Vielzahl von Umgehungsmöglichkeiten der Überwachung. Konkrete Beispiele sind:

- Es kann ein Programm für die Offline-Verschlüsselung verwendet werden (diese Art von Programmen wird explizit nicht überwacht) um Nachrichten oder Dokumente zu verschlüsseln um diese dann via Email oder einem beliebigen Kommunikationsprogramm zu versenden. Selbst wenn das Kommunikations-programm überwacht wird, kann die Klartextnachricht nicht mehr ermittelt werden.
- Es können browserbasierte Kommunikationskanäle verwendet werden. Hierbei gibt es keine explizite Kommunikationssoftware auf einem Zielsystem, die überwacht werden könnte. Die Kommunikation erfolgt über Scripts im Browser, die für jede Kommunikation auch beliebig angepasst und verändert werden können.
- Es kann Software für die verschlüsselte Kommunikation selbst entwickelt werden, die mit einer hohen Frequenz verändert und aktualisiert wird. Somit wären die Behörden gezwungen in der Software ständig neue Schwachstellen zu suchen, die Überwachungssoftware anzupassen und neu aufzubringen.

Das Risiko der Umkehrbarkeit kann eingeschränkt werden, wenn nicht konkrete Applikationen überwacht werden, sondern wenn eine Überwachungssoftware in die unteren Ebenen des Betriebssystems integriert wird. In diesem Fall würde aus technischer Sicht gleich wie bei einer Online-Durchsuchung das System vollständig überwacht. Natürlich ist es möglich auch in einem solchen Fall bewusst die Überwachung einzuschränken, aber jede Einschränkung ist gleichzeitig wieder eine Gelegenheit für eine Umgehung. **Will man aus technischer Sicht keine Umgehungsmöglichkeiten bieten, so ist eine Überwachung in einem Ausmaß notwendig, dass eine Unterscheidung von einer Online-Durchsuchung in der Praxis nicht mehr gegeben sein wird.**

3. Förderung von Internetkriminalität

Risiko

Es besteht das Risiko, dass Internetkriminalität insbesondere durch zwei Aspekte des vorliegenden Gesetzesentwurfs gefördert wird:

- **Belassen von Sicherheitslücken:** Je länger eine Sicherheitslücke in einem System vorhanden ist, desto wahrscheinlicher ist die Identifikation der Lücke durch Kriminelle und desto länger kann sie auch durch Kriminelle ausgenutzt werden. Deshalb wird allein durch das bewusste Belassen von Sicherheitslücken in Systemen zum Zweck der Installation von behördlicher Überwachungs-software die Chance für Internetkriminalität erhöht.
- **Kommerzialisierung der von den Behörden erstellten Software für kriminelle Zwecke:** Die Installation von Überwachungssoftware durch die

Behörden könnte durch Kriminelle bewusst provoziert werden um dadurch die Schwachstellen zu lernen mit denen in Systeme eingedrungen werden kann. Dieses Wissen der Schwachstellte könnte dann selbst verwendet bzw. auf illegalen Märkten kommerzialisiert werden.

Technischer Hintergrund

Das Installieren von Überwachungssoftware nutzt Schwachstellen in Systemen aus, wie sie auch von Kriminellen benutzt werden, um Privatpersonen oder Firmen zu schädigen. Auch die Durchführung einer Überwachung eines Zielsystems durch die Behörden ist technisch gleich bzw. sehr ähnlich wie Industriespionage und vielen Arten von Schadsoftware. Dies hat mehrere Folgen. Zunächst ist es so, dass die Software der Behörden mit einer Vielzahl vorhandener kommerzieller Lösungen zur Detektion von Schadsoftware isoliert und identifiziert werden kann. Natürlich lässt sich Software dieser Art zu einem gewissen Grad tarnen, aber insbesondere der durch die Software erzeugte Datenverkehr, der die Nachrichten für die Behörden ausleitet, ist leicht detektierbar. Selbst hochkomplexe Software wie Stuxnet bei der keine Kommunikation im Vordergrund stand wurde am Ende detektiert, isoliert und analysiert.
Kriminelle haben aus zwei Gründen Interesse an einer Detektion und Analyse der Überwachungssoftware der Behörden. Einerseits geht es darum festzustellen ob eine Überwachung vorliegt und damit das Kommunikationsverhalten anzupassen ist. Andererseits stellt die Software selbst einen großen Wert dar. Gelingt einem Kriminellen die Beobachtung durch welche Sicherheitslücke die Software installiert wird, so kann das Wissen über diese Lücke verwendet werden um Software für kriminelle Zwecke zu erstellen.
Konkret ist Folgendes Szenario denkbar: Es wird bewusst ein System als sogenannter „Honeypot“ aufgesetzt anhand dem die Installation der Überwachungssoftware der Behörden beobachtet wird. Hierdurch wird die ausgenutzte Schwachstelle gelernt basierend auf der das Platzieren der Software möglich wird. Es existiert ein Markt für solche Schwachstellen, der von einigen tausend Euro pro Schwachstelle bis hin zu mehr als einer Million Euro für weitreichende Betriebssystemschwachstellen reicht. Somit könnte aus der Installation von Überwachungssoftware durch den Überwachten Profit generiert werden. Im Bewusstsein der Überwachung würde natürlich keine relevante Information über den überwachten Kanal übermittelt.

4. Technische Realisierbarkeit und Kosten

Risiko

Die Überwachung verschlüsselter Nachrichten ist, wie im Entwurf erläutert, sehr resourcenintensiv. Aus technisch-wirtschaftlicher Sicht besteht das Risiko, dass das Ziel, dass Straftäter durch die Wahl des technischen Kommunikationsmittels keinen wie immer gearteten Vor- oder Nachteil erlangen, mit den geplanten finanziellen Mitteln nicht realisierbar ist.

Technischer Hintergrund

Wenn heutige Verschlüsselungsverfahren korrekt angewendet werden (wovon bei Programmen wie Skype oder WhatsApp auszugehen ist), ist durch das Lesen einer verschlüsselten Nachricht keine Information aus der Nachricht extrahierbar. Die Nachricht kann, wie im Entwurf auch beschrieben, nur vor der Verschlüsselung oder nach der Entschlüsselung im Klartext abgefangen werden. Hierfür ist das aktive

Einbringen von Software auf einem zu überwachenden Zielsystem notwendig, da nur dort der Klartext vorhanden ist. Dies erfordert das Überwinden/Umgehen von Sicherheitsmaßnahmen des Zielsystems. Im Vergleich zu einer einfachen passiven Überwachung von Klartextnachrichten ist dieser Vorgang um ein Vielfaches komplexer und in gut gesicherten Systemen überhaupt nur sehr schwer zu realisieren.
Derzeit arbeiten tausende Sicherheitsforscher in Universitäten und in Unternehmen weltweit an Methoden, um Schwachstellen zu verhindern, wie sie für die Umsetzung der „Überwachung von verschlüsselten Nachrichten“ notwendig sind. Die Sicherheit von Betriebssystemen wird immer höher und bereits heute werden bis über eine Million Euro auf Plattformen wie zerodium.com für entsprechende Schwachstellen bezahlt. Es ist absehbar und aus Sicht einer Informationsgesellschaft auch wünschenswert und notwendig, dass immer weniger Schachstellen in Systemen sind. Die Kosten zum Aufspüren und Ausnutzen von Schwachstellen werden also weiter steigen.
Gleichzeitig ist es so, dass die Schwachstellen sehr spezifisch sind. Sprich: für die Überwachung jedes Geräts müssen abhängig von der exakten Version des Betriebssystems und der exakten Version der überwachten Kommunikationssoftware Schwachstellen gefunden werden. Aufgrund der technischen Struktur mobiler Geräte (z.B. Android oder IOS) müssten die Schwachstellen, um der Grundidee des Entwurfes zu folgen, sogar auf der Ebene der Applikation gefunden werden bzw. in Kooperation mit dem System- bzw. Applikationshersteller eingebracht werden. Bei einem Update auf eine neue Version müssen potentiell neue Schwachstellen gefunden werden. Vor diesem Hintergrund ist fraglich inwieweit die technischen Voraussetzungen für eine effiziente Überwachung mit den geplanten finanziellen Mitteln gegeben sind.

Mit freundlichen Grüßen,

SIGNATURINFORMATIONEN

Unterzeichner	Reinhard Posch
Datum/Zeit-UTC	2017-08-08T11:18:55+02:00
Prüfinformation	Informationen zur Prüfung der elektronischen Signatur finden Sie unter: https://www.signaturpruefung.gv.at
Hinweis	Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument hat gemäß Art. 25 Abs. 2 der Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 ("eIDAS-VO") die gleiche Rechtswirkung wie ein handschriftlich unterschriebenes Dokument.

Prof. Reinhard Posch,

Signator: Stefan Mangard
Datum: 08.08.2017 11:36

www.handy-signatur.at

Dieses mit einer qualifizierten elektronischen Signatur versehene Dokument hat gemäß Art. 25 Abs. 2 der Verordnung (EU) Nr. 910/2014 vom 23. Juli 2014 ("eIDas-VO") die gleiche Rechtswirkung wie ein handschriftlich unterschriebenes Dokument.

Dieses Dokument ist digital signiert!

Prüfinformation:
Informationen zur Prüfung der elektronischen Signatur finden Sie unter:
www.handy-signatur.at

A-TRUST einfach sicher

Prof. Stefan Mangard