Zentrum für sichere Informationstechnologie – Austria
Secure Information Technology Center – Austria

A-SIT

Seidlgasse 22 / 9, 1030 Wien
Tel.: (+43 1) 503 19 63–0
Fax: (+43 1) 503 19 63–66

Inffeldgasse 16a, 8010 Graz
Tel.: (+43 316) 873-5514
Fax: (+43 316) 873-5520

http://www.a-sit.at
E-Mail: office@a-sit.at

DVR: 1035461 ZVR: 948166612 UID: ATU60778947

STELLUNGNAHME VON A-SIT ZUM ENTWURF DES STRAFPROZESSRECHTSÄNDERUNGSGESETZES 2017

1. August 2017
Herbert Leitold – Herbert.Leitold@a-sit.at

A-SIT wurde als unabhängige Organisation zur Beratung und Unterstützung der öffentlichen Verwaltung eingerichtet und beschäftigt sich dabei ausschließlich mit IT-Sicherheit. Aufgaben sind dabei unter anderem Bestätigungsstelle zur elektronischen Signatur, Konformitätsbewertungsstelle zu Vertrauensdiensten, technische Aspekte in der Zahlungssystemaufsicht oder als aktuelles Beispiel das Sicherheitskonzept der Registrierkassen. Dies wird angeführt, um darauf hinzuweisen, dass A-SIT als Art österreichisches Pendant zum Deutschen Bundesamt für Sicherheit in der Informationstechnik über die nötige Expertise verfügt.

Der Entwurf zur Änderung der Strafprozessordnung konzentriert sich auf den strafrechtlichen Aspekt. In der Materie hat der technische Aspekt aber einen wesentlichen Einfluss. Dieser scheint noch nicht hinreichend erfasst, worauf auch die Erläuterungen insofern hinweisen, als die genannte Expertengruppe hochrangige Kapazitäten der Rechtswissenschaften ausweist, eine äquivalente Benennung technischer Wissenschaften zur qualitativen Untermauerung des Stands der Technik nicht genannt ist.

Diese Stellungnahme beschränkt sich auf die zur Überwachung verschlüsselter Übermittlung vorgesehenen Maßgaben (v.a. §§ 134 Z 3a und 135a) samt deren Erläuterungen. Es wird hier aus technischer Sicht Nachbesserungsbedarf in folgenden Punkten gesehen:

1. Der Vorschlag umfasst die Ermächtigung der Überwachung, die Identifikation von betroffenen Personen und Objekten ist nicht hinreichend eingegrenzt
2. Das Aufbringen der Software wäre besonders zu evaluieren
3. Die in Remote-Aufbringung von Software immanenten Risiken wären zu betrachten
4. Das Entfernen der Software stellt Herausforderungen dar
5. Begleitmaßnahmen in der Ausbildung und technischen Expertise wären wünschenswert

Ad 1.: Die unzweifelhafte Identifikation der Person als Inhaber eines Computersystems wird ohne physischen Kontakt, d.h. im Fall der Remote-Aufbringung von Software, schwierig und teils unmöglich sein und kann auch zu zusätzlich zu betrachtenden Risiken führen (vgl. Punkt 3.). Es sind in den Erläuterungen zwar technische Parameter angeführt (IP-/MAC-Adresse, IMSI, SIM-Karte), die sind aber auch aktiv änderbar und kriminelle Personen werden das Möglichste tun, um diese Identifikation zu verhindern. Dies ist etwa über aktives Ändern von MAC-Adressen, onion routing (z.B. Tor), Nutzung von WLAN bei Mobilgeräten vs. SIM Karte etc. möglich. Der Vergleich in den Erläuterungen mit der Identifikationsproblematik in der Überwachung unverschlüsselter Kommunikation berücksichtigt nicht das aktive Eingreifen in Komponenten und damit die Zusatzrisiken (Pkt. 3.).

Ad 2.: Im Aufbringen der Software wird die Beschränkung rein auf die zu überwachende Kommunikationssoftware (WhatsApp, Skype etc.) nicht ohne Beeinflussung anderer Komponenten des Computersystems möglich sein. Etwa haben verschiedene Apps mobiler Geräte unterschiedliche Signaturen oder getrennte Benutzer. Nachdem Kooperation der App-Hersteller nicht generell angenommen werden kann, muss ein kompromittierender Eingriff auf Systemebene erfolgen. Zu berücksichtigen wäre auch, dass in der Remote-Aufbringung oft nicht mit Sicherheit festgestellt werden wird können, ob sich das Computersystem zum Zeitpunkt des Eingriffs auch in Österreich befindet, der Eingriff in die Eigentumsrechte (Computersystem aber auch der Hersteller der Kommunikationssoftware) unter gesetzlicher Ermächtigung schwer argumentiert werden kann.

Ad 3.: Das Remote-Aufbringen von Software muss auf Systemschwächen aufbauen, sei es unter Ankauf von Schwachstellen oder in Kooperation mit Herstellern. Einerseits stellt der Erhalt von Systemschwächen ein Risiko dar (vgl. jüngste Vorfälle mit WannaCry oder Petya), andererseits zielt der Entwurf auch auf die Überwachung spezifischerer Komponenten (WhatsApp, Skype, …) womit eine viel breitere und damit technisch herausfordernde und kostenintensivere Basis an Schwachstellen für alle Systeme, Anwendungen und deren Kombinationen vorgehalten werden muss. Nicht berücksichtigt scheint, dass in der Remote-Aufbringung kriminelle Personen die Überwachung auch annehmen und dies aktiv nutzen können: Ein Erkennen des Eingriffs und Ausnutzen bzw. Isolieren der Methode (i.S. eines HoneyPots) wird nicht zu verhindern sein. Damit ist aber eine Analyse der genutzten Systemschwächen und Nutzung für kriminelle Handlungen ein zu betrachtendes Risiko.

Ad 4.: Die an sich sinnvolle Vorgabe des Entfernens des Eingriffs wird nicht garantierbar sein. Beispiele sind die Wiederherstellung eines Systems von einem, während des Eingriffs gezogenen Backups oder nicht mehr Erreichbarkeit des Computersystems während des Eingriffs (vom Netz nehmen, geänderte Konfiguration hinter Proxy oder Firewall betriebener Geräte). Eine Deinstallation über Information des Betroffenen wird wohl kaum möglich sein, da damit diesem die Software bekannt und damit nutzbar wird.

Ad 5.: Sinnvoll wäre die technische Begleitung durch unabhängige Expertengruppen, die am Stand der Technik dahingehend unterstützen können, wann die Identifikation der Personen und Objekte (Pkt. 1) sichergestellt ist und ob aus der Systematik ein gesteigertes Risiko für Dritte oder durch verminderte Internetsicherheit entsteht (Pkt. 3.). Auch scheint die systematische Ausbildung von Exekutive und Staatsanwaltschaft geboten, was das Verstehen der Technik und damit die Möglichkeiten und Unmöglichkeiten betrifft.

SIGNATURINFORMATIONEN	**Unterzeichner**	DI Herbert Leitold
	Datum/Zeit-UTC	2017-08-01T12:55:54+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.	