Markus Eisenmann

18.07.2017

Markus Eisenmann nimmt zu dem Entwurf wie folgt Stellung:

Stellungnahme im Begutachtungsverfahren zum Ministerialentwurf des Justizministeriums, Strafprozessrechtsänderungsgesetz 2017 (325/ME)

Bundestrojaner

Ich bin gegen die Legalisierung einer staatlichen Spionagesoftware, einem sogenannten Bundestrojaner, in § 135a StPO-E zur Überwachung verschlüsselter Nachrichtenübertragung.

Die in den Begleitdokumenten enthaltenen Erklärungen beziehen sich ausschließlich ein juristische Spitzfindigkeiten, vernachlässigen jedoch eindeutige techn. Spezifikationen hinsichtlich sicherheitstechnischer Auswirkungen auf IT-Systeme. Eine Remote- oder (direkte) Vorort-Installation ist - insofern der administrative Zugang nicht bekannt ist - lediglich durch Ausnutzung von Sicherheitslücken möglich. Dies, aber auch die grundsätzliche Funktionsweise jedweder Überwachungs-Software, ist ohne tiefgreifende Änderungen (aka einnisten ...) in den OS-Kernel (systembedingt) nicht möglich. Insofern ist nicht auszuschließen, dass somit die Systemsicherheit sowie -stabilität darunter leidet.

Die Überprüfung einer solchen Software durch die Datenschutzkommission (gegenüber DSG 2000) erfolgt meines Erachtens lediglich "um dem Gesetz genüge zu tun". Ohne Prüfung/Review durch OS-Experten kann weder die revisionssichere Eignung und mögliche Fehler (false-positive, Missbrauch durch neue Lücken) festgestellt werden.

Darüber hinaus mangelt es dem Entwurf an grundsätzlichen Abgrenzungen aufgrund Netzwerktechn. Gegebenheiten; beispielsweise fehlt die Abgrenzung zu lokalen Subnetzen. Wenn die Überwachung von USB-Sticks ausgeschlossen ist, müsste für den SMB-Zugriff im gleichen lokalen Subnetz selbiges gelten.

Wie in weiteren Komentaren bereits zu lesen war, ist technisch versierten Benutzer zuzutrauen, ein derart komprimittiertes System zu erkennen oder Gegenmaßnahmen zu ergreifen. Hierzu stelle ich mir die Frage, ob neben der Installation einer Überwachnungssoftware auf Computer auch das Aushebeln von gängigen Sicherheitsmaßnahmen (Router-Firewalls, IDS und IPS) beabsichtigt wird. Sind also Begleitmaßnahmen zu befürchten, um überhaupt die funktionsweise einer derartigen Software zu gewährleisten? Diese Frage ist insofern von Interesse, als insbesondere IT-affine Personen (beispielsweise aus dem Bereich Cyber-Kriminalität) über den Einsatz von Gegen- oder Umgehungsmaßnahmen Bescheid wissen. Insofern befürchte ich ein "Wettrüsten"; besonders da durch Mängel in der technischen Qualität dieses Entwurfs kaum künftige Begehrlichkeiten eingeschränkt werden.

Zu den laufenden Diskussionen fällt mir immer wieder ein Zitat von Benjamin Franklin ein: "Wer wesentliche Freiheit aufgeben kann um eine geringfügige bloß jeweilige Sicherheit zu bewirken, verdient weder Freiheit, noch Sicherheit." Dies finde ich sehr passend, da seitens Politik versucht wird, eine abstrakte Sicherheit mit Einschränkungen und hohem Ressourceneinsatz zu erschaffen. Hinsichtlich Terrorismus aber gegenüber einem "Gegner", der sich aber (eben) nicht systematische Methoden erfassen lässt.