GESELLSCHAFT
FÜR INFORMATIK

Stellungnahme zu den Drucksachen 19/5412 und 19/5782

Gesetzentwurf der Fraktionen der CDU und BÜNDNIS 90/DIE GRÜNEN für ein Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen

Prof. Dr. Hannes Federrath
Universität Hamburg, Fachbereich Informatik
Präsident der Gesellschaft für Informatik e.V. (GI)

6. Februar 2018, mit Ergänzungen vom 8. Februar 2018

Vorbemerkungen

Die Gesellschaft für Informatik beschränkt sich in dieser Stellungnahme erstens auf Artikel 1 des Gesetzesentwurfs und dort insbesondere auf die Erweiterung der Befugnisse des Landesamts zur Quellen-Telekommunikationsüberwachung nach § 6 Abs. 2-4 Hessisches Verfassungsschutzgesetz (HVSG), zweitens zum verdeckten Zugriff auf informationstechnische Systeme (§ 8 HVSG) und drittens auf die Beherrschbarkeit automatisierter Datenanalysen (Big-Data-Analysen) nach § 25a Hessisches Gesetz über die öffentliche Sicherheit und Ordnung (HSOG-E). Diese Befugniserweiterungen berühren nicht nur die Grundrechte der betroffenen Personen, sondern auch die Sicherheit informationstechnischer Systeme und somit die Fundamente der digitalen Gesellschaft.

Beschaffung von Sicherheitslücken

Sowohl die Maßnahmen zur Telekommunikationsüberwachung (§ 6 Abs. 2-4 HVSG) als auch zum verdeckten Zugriff auf IT-Systeme (§ 8 HVSG) erfordern das Ausführen von Software auf dem System einer Zielperson. Damit Software dort ohne physischen Zugang zur Ausführung gebracht werden kann, muss sie entweder von der Zielperson selbst unbewusst gestartet werden (etwa durch das Klicken auf einen E-Mail-Anhang) oder durch die Ausnutzung einer Sicherheitslücke auf dem System der Zielperson eingespielt und gestartet werden. Eine solche Sicherheitslücke kann entweder in der Betriebssoftware (Firmware und/oder Betriebssystem)

oder in einer Anwendungssoftware, die die Zielperson installiert hat, vorliegen. Das Einspielen der Software mittels einer Sicherheitslücke wird gewöhnlich ohne Zutun und Kenntnisnahme der Zielperson erfolgen und setzt somit nicht die Unachtsamkeit oder Fahrlässigkeit der Zielperson voraus, wodurch die Gefahr einer Entdeckung sinkt.

Damit der Eingriff über eine Sicherheitslücke im Betriebssystem oder in einer anderen Software erfolgreich sein kann, ist eine Sicherheitslücke erforderlich, die der Allgemeinheit, insbesondere aber den Herstellern der Betriebssoftware, der Anwendungssoftware und zusätzlich den Herstellern von Malware-Scannern bisher unbekannt ist. Bei bekannten Sicherheitslücken würde ein Einspielversuch auf Systemen mit aktuellen Sicherheitsupdates scheitern. Wird ein aktueller Malware-Scanner genutzt, kann der Versuch sogar entdeckt werden.

Die Kenntnis von bisher unbekannten Sicherheitslücken ist entweder durch eigene (hier: durch oder im Auftrag des Bedarfsträgers) Suche nach ausnutzbaren Softwarefehlern zu erlangen oder durch Ankauf von Informationen zu solchen Sicherheitslücken. Ein wesentlicher Anteil der Nachfrage auf dem gewerblichen Markt für Sicherheitslücken kommt von Cyber-Kriminellen, die unbekannte Sicherheitslücken beispielsweise als Grundlage für Erpressungssoftware (sog. Ransomware) benötigen.

Die auf solchen Märkten angebotenen Sicherheitslücken werden von ihren Entdeckern zunächst geheim gehalten. Der staatliche Ankauf von Sicherheitslücken stärkt solche geheimen Märkte und verringert die Motivation von Hackern, Sicherheitslücken in einer verantwortungsvollen Weise den Software-Herstellern zu melden, diesen genügend Zeit zum Schließen der Lücken einzuräumen, um ggf. anschließend die Lücke zu veröffentlichen.

Die Gesellschaft für Informatik fordert eine Melde- und Veröffentlichungspflicht von Sicherheitslücken, nachdem sie geschlossen sind, um Bürger, öffentliche Verwaltung und Unternehmen in die Lage zu versetzen, die IT-Sicherheitsrisiken realistisch einzuschätzen und frühzeitig geeignete Schutzmaßnahmen zu ergreifen.

Verbreitung von Sicherheitslücken

Damit der Zugriff auf das System einer Zielperson gelingt, werden zumeist Sicherheitslücken ausgenutzt, die in einer Vielzahl von Systemen existie-

ren, weil sie dann mit hoher Wahrscheinlichkeit auch bei einer Zielperson ausgenutzt werden können. Solche der Öffentlichkeit bzw. den Softwareherstellern bisher unbekannte Sicherheitslücken (zumeist von IT-Sicherheitsexperten als Zero-Day-Exploits bezeichnet) stellen nicht nur eine Verwundbarkeit für einzelne, eingrenzbare Systeme von Zielpersonen dar, sondern setzen die Allgemeinheit der Gefahr aus, dass während einer Überwachungsmaßnahme auch Kriminelle diese Sicherheitslücken ausnutzen.

Die Geheimhaltung einer Sicherheitslücke durch Behörden ist kein geeigneter Schutz vor den Gefahren dieser Sicherheitslücke. Erstens werden Sicherheitslücken auf den o.a. geheimen Märkten nicht exklusiv angeboten. Zweitens kann eine existierende Lücke jederzeit erneut entdeckt und anderswo angeboten und ausgenutzt werden. Drittens werden die auf den geheimen Märkten angebotenen Sicherheitslücken üblicherweise auch nicht, nachdem die fragwürdige gewerbliche Nutzung abgeschlossen ist, auf verantwortungsvolle Weise den Software-Herstellern gemeldet, sondern bleiben weiterhin länger geheim, als dies für eine konkrete staatliche Maßnahme eigentlich erforderlich ist. Insbesondere hier leistet die staatliche Überwachung mit solchen Methoden nach Auffassung der Gesellschaft für Informatik der Unsicherheit und Schutzlosigkeit von Bürgern und Unternehmen unverantwortlichen Vorschub.

Schäden, die für die Allgemeinheit durch behördlich bekannte Sicherheitslücken entstehen, sind vermeidbare Schäden. Die Beseitigung der Sicherheitslücken zum Schutz der Allgemeinheit sollte Vorrang vor der Zugriffsmöglichkeit durch Behörden haben, gerade auch, weil das Ausmaß der Folgeschäden für Bürger und Unternehmen (insbesondere im Bereich der kritischen Infrastrukturen) gar nicht abschätzbar ist und somit eine Abwägung nicht vorgenommen werden kann.

Gefahr für kritische Infrastrukturen

Sicherheitslücken in Standardsoftware für Endanwender, wie sie für Eingriffe nach Maßgabe der vorliegenden Gesetzesänderung benötigt werden, stellen eine Gefahr für kritische Infrastrukturen dar. Standardsoftware wie etwa das Betriebssystem Windows wird ebenfalls in Behörden, bei Energieversorgern und in Krankenhäusern eingesetzt. Grundbausteine dieser Standardsoftware finden sich beispielsweise auch in Spezialsoftware für die Anlagensteuerung in Verkehrssystemen und Kernkraftwerken

wieder, wodurch diese Systeme ebenfalls verwundbar werden bzw. bleiben.

Teile der kritischen Infrastruktur sind nach Bekanntwerden einer Sicherheitslücke zudem länger verwundbar als Systeme von Endanwendern, da sie aufgrund notwendiger Stabilitätstests oder komplexerer Update-Prozesse weniger schnell auf das Bekanntwerden einer Sicherheitslücke und die Bereitstellung eines Sicherheitsupdates reagieren können. Umso mehr ist es für die Sicherheit kritischer Infrastrukturen erforderlich, dass Sicherheitslücken schnell, zuverlässig und kontrolliert geschlossen und anschließend mit ausreichender Vorwarnzeit veröffentlicht werden.

Unkontrollierbarkeit eines Eingriffs

Technische Mittel zum Eingriff in informationstechnische Systeme einer Zielperson haben unübersehbare Konsequenzen und gefährden die Integrität und Vertraulichkeit dieser Systeme. Eine Einschränkung der Funktionalität der technischen Mittel auf einen lediglich lesenden Zugriff oder auf ausgewählte Anwendungssoftware (z.B. verschlüsselnde Chat-Programme) unterliegt zwangsläufig immer dem Vorbehalt der Korrektheit dieser Mittel. In der Praxis ist es nicht auszuschließen, dass ein eingesetztes technisches Mittel aufgrund eines Fehlers von vorgesehenen Einschränkungen abweicht oder durch eigene Sicherheitslücken das System in einen durch Dritte verwundbaren Zustand versetzt. Dies kann Folgeschäden nach sich ziehen, für die der Verursacher – hier eine staatliche Stelle – verantwortlich ist.

Fehlende Beherrschbarkeit von Big-Data-Analysen

Der § 25a HSOG-E soll die automatisierte Verknüpfung von Daten aus verschiedenen Quellen zur vorbeugenden Bekämpfung von Straftaten ermöglichen. Solche automatisierten Datenanalysen liefern grundsätzlich nur probabilistische, d.h. ungenaue und mit einer gewissen Wahrscheinlichkeit auch falsche Ergebnisse. Neben falsch-negativen Ergebnissen (keine Erkennung von verdächtigen Ereignissen) führen solche automatisierten Verfahren – technisch unvermeidlich – stets auch zu falsch-positiven Ergebnissen (eine Person wird fälschlicherweise verdächtigt).

Automatisierten Datenanalysen nutzen üblicherweise Verfahren des maschinellen Lernens. Die im laufenden Betrieb solcher Analysen notwendi-

ge und teilweise ohne menschliches Eingreifen stattfindende Anpassung der Algorithmen zur Verringerung der Anzahl von falsch-negativen Ergebnissen führt jedoch zur Vergrößerung der Anzahl von falsch-positiven Verdächtigungen und umgekehrt. Dementsprechend erfordert die Konfiguration, Durchführung und Ergebnisbewertung von automatisierten Datenanalysen besondere Sorgfalt und hohe statistische Fachkenntnis.

Die automatisierte Datenanalyse ist ein in der Informatik derzeit sich sehr schnell entwickelndes Forschungsfeld. Insgesamt scheinen solche technischen Verfahren derzeit noch nicht ausreichend erforscht, um für den vorbeugenden Einsatz zur Bekämpfung von Straftaten oder zur Gefahrenabwehr zuverlässig einsetzbar zu sein.

Fazit und Forderungen

Die Gesellschaft für Informatik lehnt den vorliegenden Gesetzesentwurf für die Neuausrichtung des Verfassungsschutzes Hessen in dieser Form ab und sieht hinsichtlich der informationstechnischen Aspekte des Gesetzesentwurfs folgenden Handlungs- und Änderungsbedarf:

1. Ein Eingriff in informationstechnische Systeme unter Ausnutzung unbekannter Sicherheitslücken ist zu untersagen.

2. Bei Kenntnisnahme von bisher unbekannten Sicherheitslücken sind Behörden dazu zu verpflichten, diese unverzüglich an den Hersteller zu melden und kontrolliert zu veröffentlichen.

3. Ein staatliches Förderprogramm zur Suche nach Sicherheitslücken in Software mit dem Ziel der Behebung der Schwachstellen ist einzurichten.

4. Die automatisierte Datenanalyse ist aufgrund ihrer Komplexität und Fehleranfälligkeit als Ermittlungsinstrument nicht geeignet.

Danksagung

Für die fachliche Zuarbeit bei der Erstellung dieser Stellungnahme danke ich meinen wissenschaftlichen Mitarbeitern Christian Burkert und Matthias Marx.

GESELLSCHAFT
FÜR INFORMATIK

Kontakt

Prof. Dr. Hannes Federrath
Präsident der Gesellschaft für Informatik e.V. (GI)
E-Mail: hannes.federrath@gi.de

Universität Hamburg, Fachbereich Informatik,
Arbeitsbereich Sicherheit in Verteilten Systemen (SVS)
Web: svs.informatik.uni-hamburg.de

Gesellschaft für Informatik e.V. (GI)

Geschäftsstelle Berlin
im Spreepalais am Dom
Anna-Louisa-Karsch-Str.2, 10178 Berlin
Tel.: +49 30 7261 566-15
Mobil: +49 163 8694216
Fax: +49 30 7261 566-19
E-Mail: berlin@gi.de

Geschäftsstelle Bonn
im Wissenschaftszentrum
Ahrstr. 45, 53175 Bonn
Tel.: +49 228 302-145
Fax: +49 228 302-167
E-Mail: bonn@gi.de

Web: www.gi.de