Hallo LMV-Besucher*in,

in einem Schreiben vom 24. Mai informierte die Grüne Landtagsfraktion im HLT den Parteirat über Änderungen im „Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen“. Statt wie bisher geplant, sollen Quellen-Telekommunikationsüberwachung und Online-Durchsuchung nicht im Verfassungsschutzgesetz geregelt werden, sondern im Hessischen Sicherheits- und Ordnungsgesetz (HSOG).

Die Probleme, die mit dem Vorhalten einsatzbereiter Staatstrojaner einhergehen, bleiben damit bestehen.

Das Schreiben der Fraktion an den Parteirat haben wir auf https://www.ccc.de/de/updates/2018/hessentrojaner-polizei im Volltext veröffentlicht. Alle im Flyer genannten Primärquellen haben wir unter **hessentrojaner.de** zusammengestellt.

Dieser Flyer ist Teil der Informationskampagne hessentrojaner.de, einem Gemeinschaftsprojekt von hessischen Organisationen aus dem Umfeld des Chaos Computer Club, die sich für die Sicherheit von IT-Systemen und gegen den geplanten Staatstrojaner engagieren. Alle Beteiligten arbeiten ehrenamtlich an dem Projekt.

Warum Staatstrojaner eine schlechte Idee sind

Offene Einfallstore
Der Staatstrojaner benötigt zum Angriff Sicherheitslücken. Damit er erfolgreich ist, dürfen diese Lücken nicht von Software-herstellern geschlossen werden und werden deshalb geheim gehalten.

Diebstahl von Lücken
Niemand kann garantieren, dass die genutzten Sicherheitslücken nicht in falsche Hände geraten. Auch die NSA war hierzu nicht in der Lage, wie bereits am Beispiel *Wannacry* zu sehen war.

Schwarzmarkt
Sicherheitslücken werden typischerweise auf einem Schwarzmarkt erworben. Auch das Land Hessen wird hier keine andere Wahl haben und über Umwege kriminelle Händler unterstützen müssen.

Kritische Infrastruktur
Dem Hersteller nicht bekannte Sicherheitslücken stellen ein enormes Gefährdungspotenzial für sicherheitskritische Infrastruktur wie beispielsweise Krankenhäuser oder Windparks dar.

Kriminelle Gegenspieler
Da der Staatstrojaner auf den Rechner einer überwachten Person aufgespielt wird, kann diese ihn finden und selbst gegen Dritte verwenden. Mächtige Tools zur Kompromittierung fremder IT-Systeme in den Händen von organisierter Kriminalität und Terroristen wären die Folge.

Volle Kontrolle
Staatstrojaner erfordern die Möglichkeit, Daten auf dem überwachten Gerät zu verändern. Das Zielgerät nur zu beobachten ist technisch unmöglich. Dadurch können mittels Trojaner erlangte „Beweise“ ohne weiteres verfälscht, vernichtet oder jemandem untergeschoben werden.

Missbrauchspotenzial
Einsatzbereite Trojaner stellen ein mächtiges Mittel zum Machtmissbrauch dar und haben einen enormen Wert auf dem Schwarzmarkt. Eine Zweckentfremdung des Trojaners kann niemals vollständig ausgeschlossen werden.

Keine gerichtsfesten Beweise
Da zum Zeitpunkt der Kompromittierung des überwachten Gerätes eine offene Sicherheitslücke auf dem Gerät existiert haben muss, könnten auch Dritte Daten auf dem Gerät manipuliert haben.

Kein Staatstrojaner für ~~den Verfassungsschutz!~~ die Polizei

Staatstrojaner stellen eine reale Gefahr für die **IT-Sicherheit** von sicherheitskritischer Infrastruktur dar, bieten ein hohes **Missbrauchspotenzial**, sind rechtsstaatlich schwer bis gar **nicht kontrollierbar** und können vor Gericht **keine rechtskräftigen Beweise** liefern.

Die Gefährdung der Sicherheit von kritischer Infrastruktur wie z.B. Atomkraftwerken, unserer Wasserversorgung oder Krankenhäusern steht in keinem Verhältnis zum Nutzen eines Staatstrojaners.

Was bisher geschah

Ende letzten Jahres stellte die Koalition einen Entwurf für ein neues hessisches Verfassungsschutzgesetz vor. Dieser enthielt Regelungen, die dem Verfassungsschutz den Einsatz von Staatstrojanern erlauben sollte (Onlinedurchsuchung, „Quellen-TKÜ"). Auf der LMV vom 24. November 2017 wurde ein Antrag angenommen, der „Entwicklung, Einsatz und Proliferation digitaler Waffen" generell ablehnt.

Der Gesetzesentwurf wurde mit dem Negativpreis „Big Brother Award" ausgezeichnet und in einer Expertenanhörung des Landtags von allen 25 Sachverständigen aus verschiedensten Gründen scharf kritisiert. Fraktions- und Landesvorstand haben daraufhin mit der CDU nachverhandelt und wollen nun im neuen Polizeigesetz (HSOG) genau die selben Maßnahmen einführen (nur eben für die Polizei).

Die Einführung eines Staatstrojaners im HSOG widerspräche der Argumentation des beschlossenen Antrags der LMV im November letzten Jahres. Auf der heutigen LMV steht deshalb der Antrag „Für ein Hessen ohne Staatstrojaner" zur Abstimmung, der den Trojaner in diesem und allen künftigen hessischen Landesgesetzen ablehnt und so nochmals die Position aus den vergangenen grünen Wahlkämpfen sowie der parlamentarischen Arbeit der grünen Bundestagfraktion bekräftigt.

Herausgeber: Chaos Computer Club Darmstadt e.V., Wilhelminenstraße 17, 64283 Darmstadt

Sicherheitspolitik – verantwortungsvoller ohne Staatstrojaner

Um Staatstrojaner einsetzen zu können, muss dieser über eine offene Sicherheitslücke im Endgerät der zu überwachenden Person Zugriff auf dieses Informationstechnische System erhalten. Der Staat hat somit ein Interesse daran, diese Schwachstelle nicht an den Hersteller der betroffenen Software zu melden und schließen zu lassen. Der in Hessen entwickelte Staatstrojaner aus dem Jahre 2011 war nicht nur rechtswidrig eingesetzt worden, sondern schuf auf den infiltrierten Rechnern sogar weitere Lücken.

Alle bisherigen Versuche deutscher Behörden, Staatstrojaner zu entwickeln und einzusetzen, sind entweder aus technischen Gründen oder vor dem Bundesverfassungsgericht gescheitert. Der Staat sollte seine Bürger und die Wirtschaft vor Schadsoftware schützen sowie das Grund-recht auf Gewährleistung der Integrität und Vertraulichkeit Informationstechnischer Systeme verwirklichen. Das heißt ganz praktisch auch, von der Entwicklung und Finanzierung von Schadsoftware abzusehen.

„In der hessischen Gefahrenabwehr darf Online-Durchsuchung nicht eingesetzt werden. Hessen muss sich dafür einsetzen, dass auf Bundesebene die Durchsuchung privater Rechner ausgeschlossen wird."

— „Digitales Hessen", Positionspapier der hessischen Grünen-Fraktion im Vorfeld der Landtagswahl 2013

„Entwicklung, Einsatz und Proliferation digitaler Waffen wie eine Software zur „Onlinedurchsuchung" können keine Bestandteile einer verantwortungsvollen Sicherheitspolitik sein!"

— Beschluss der LMV vom 24. November 2017

Eine unabhängige richterliche Kontrolle im Vorfeld solcher Spähsoftware-Platzierungen und Onlinedurchsuchungen sei „nicht möglich", erklärt die Grünen-Rechtsexpertin Katja Keul. „Dass Richter sich vollständig auf die Informationen der Exekutive verlassen müssen, widerspricht dem Prinzip der Gewaltenteilung." Derart schwere Grundrechtseingriffe ohne effektiven Richtervorbehalt seien rechtsstaatlich nicht vertretbar und Produkt einer „übereilten und verantwortungslosen Gesetzgebung".

— MdB Katja Keul in „Regierung mauert beim Staatstrojaner", RP Online zum BKA-Gesetz vom 29. Mai 2018