Worum es geht:

Der hessische Landtag berät heute über das „Gesetz zur Neuausrichtung des **Verfassungsschutzes** in Hessen“. Nach dem Entwurf der **Koalition** soll der Verfassungsschutz einen sog. **Staatstrojaner** zum **heimlichen Einbruch** in Computersysteme bekommen.

Was wichtig ist:

- Der Gesetzesentwurf zum „Gesetz zur Neuausrichtung des Verfassungsschutzes in Hessen“ wurde Anfang Oktober auf einer gemeinsamen Pressekonferenz der Fraktionen von CDU und Grünen durch den hessichen Innenminister Peter Beuth (CDU) vorgestellt.
- Die Einführung eines Staatstrojaners steht in **direktem Widerspruch zum Wahlprogramm** der Grünen. Auf ihrer Landesmitgliederversammlung am Samstag hat die **grüne Basis** daher ihre Fraktion aufgefordert, dem Gesetz in dieser Form **nicht zuzustimmen**. Netzpolitiker der hessischen Grünen **kritisierten** im Vorfeld des Parteitages, über die Trojaner-Pläne **nicht informiert** worden zu sein.
- Neben Einschränkungen von Bürgerrechten, die mit Einführung des Trojaners verbunden wären, gibt es ein weiteres wichtiges Gegenargument, das oft übersehen wird: **Staatstrojaner gefährden** die **IT-Sicherheit** insgesamt: Um in PCs, Laptops oder Smartphones eindringen zu können, braucht der Staatstrojaner eine **Sicherheitslücke** in der Software des Gerätes, also z.B. in Windows, Android, Internet Explorer oder einer anderen Software.
- Erlangen **Kriminelle** oder **Terroristen** Kenntnis von solchen Sicherheitslücken, können sie diese ebenfalls ausnutzen, um z.B. Geld zu **erpressen** oder **kritische Infrastruktur** und Industrie **lahmzulegen**. Dies kann auch indirekt geschehen, wenn **geknackte Geräte als Waffe** gegen andere Ziele missbraucht werden.
- Ein Verfassungsschutz, der Staatstrojaner einsetzt, hat **kein Interesse** daran, dass Schwachstellen geschlossen werden. Er wird die vom Staatstrojaner genutzten Lücken nicht an die Softwarehersteller melden, und so **schützende Updates verhindern**. Das prominesteste Beispiel hierfür ist die Schadsoftware „WannaCry“, die Sicherheitslücken in Windows aus dem Repertoire der NSA ausnutzen konnte, da diese vor dem betroffenen Softwarehersteller Microsoft jahrelang geheimgehalten wurden. „WannaCry“ brachte unter anderem den Betrieb in vielen britischen **Krankenhäusern** zum Erliegen[1].
- Offene Sicherheitslücken sind also eine **tickende Zeitbombe**. Sie gefährden uns alle, auch wenn wir keine Terrorverdächtigen oder Kriminelle sind. Der im Gesetzesentwurf vorgesehene **Richtervorbehalt** stellt daher **keinen wirksamen Schutz** der Zivilgesellschaft dar.
- Der Einkauf von Sicherheitslücken ist teuer. Der Verfassungsschutz müsste für seinen Staatstrojaner **Steuergelder** auf dem **Schwarzmarkt** ausgeben und diesen so unterstützen.

Wir fordern:

- Sicherheit wahren - Kein Staatstrojaner für Hessen!
- Meldepflicht für entdeckte Sicherheitslücken!
- Sicherheitslücken gefährden alle - Schwachstellen-Suche unterstützen!

1 Weitere Infos unter: hessentrojaner.de/#wannacry

Warum Staatstrojaner eine schlechte Idee sind:

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

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

Schwarzmarkt
Sicherheitslücken werden typischerweise auf einem Schwarzmarkt erworben. Auch der Verfassungsschutz 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 beispiels-weise 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. Geheimdienstwaffen 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 „digitale Beweise“ ohne weiteres verfälscht, vernichtet oder untergeschoben werden.

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

PRESSE-READER

zur geplanten Einführung eines hessischen Staatstrojaners

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.