EPICENTER .WORKS for digital rights

Epizentrum – Plattform für grundrechtsbasierte Zukunftspolitik
(vormals AKVorrat; ZVR: 140062668)
Annagasse 8/1/8, 1010 Wien; team@epicenter.works; www.epicenter.works

Kurzzusammenfassung: Auswirkungen einer Bundestrojaner Software

Die Überwachung internetbasierter Kommunikation stellt Strafverfolgungsbehörden vor neue Herausforderungen. Moderne Anwendungen wie WhatsApp oder Skype verschlüsseln die Kommunikationsinhalte vor der Übertragung und sind deshalb einer klassischen Telekommunikationsüberwachung (TKÜ) nicht zugänglich.

Als Lösung für dieses Problem wird derzeit die Überwachung auf dem Endgerät (Smartphone, Laptop) des Nutzers diskutiert. Der einzige Weg dies zu bewerkstelligen, wäre mittels einer staatlichen Spionagesoftware (Bundestrojaner), welche sich ohne das Wissen des Nutzers auf dessen Endgerät einnistet und dort noch vor der Verschlüsselung die Kommunikation überwacht und an Strafverfolgungsbehörden ausleitet (Quellen-TKÜ).

Die Installation eines solchen Bundestrojaners passiert technisch auf demselben Weg, wie die Infektion mit einem Computervirus, nämlich unter Ausnutzung von offenen Sicherheitslücken auf dem Endgerät. Sicherheitslücken werden in aller Regel vom Hersteller nach Bekanntwerden geschlossen und können dann nicht mehr zur Infektion genutzt werden. Sicherheitslücken werden von IT-Sicherheitsforschern (Hackern) entdeckt und entweder verantwortungsvoll dem Hersteller gemeldet oder um viel Geld auf dem Schwarzmarkt angeboten.

Die Republik Österreich müsste auf solchen Märkten mittel- oder unmittelbar als Käufer auftreten und darauf hoffen, dass die gekauften Sicherheitslücken den Softwareherstellern nie auffallen, damit sie weiter nutzbar bleiben. Auch Kriminelle profitieren aber von offenen Sicherheitslücken.

Durch eine Teilnahme an diesem Schwarzmarkt wird mit Steuergeldern aktiv in die Unsicherheit von Computersystemen der in Österreich lebenden Menschen investiert. Es steigt die Gefahr von Angriffen auf kritische Infrastruktur und Cyberkriminelle haben ein leichteres Spiel, da bestehende Sicherheitslücken nicht geschlossen werden. **Unter dem Gesichtspunkt der Sicherheit ist die Legalisierung und Finanzierung staatlicher Spionagesoftware (Bundestrojaner) klar abzulehnen, da dadurch ein enormer Schaden für die öffentliche Sicherheit unabwendbar wäre.**

Zudem ist eine öffentliche Debatte zum Verhältnis des geplanten Cybersicherheitsgesetzes und der dazu widersprüchlichen Ausnutzung von Sicherheitslücken durch staatliche Spionagesoftware dringend notwendig. Durch die Umsetzung der NIS-Richtlinie fällt die Zuständigkeit für die innere IT-Sicherheit in Österreich an das BVT. Gleichzeitig soll das BVT auch für den Bundestrojaner zuständig sein. Eine Behörde wäre dann gleichzeitig für Schutz und Angriffe auf IT-Systeme zuständig, wodurch das Vertrauen an sie schwindet.

Weitere Probleme:

- Gewonnene Beweise sind durch die Infektion und Manipulation des Endgeräts, auf dem sie erhoben wurden, unzuverlässig, daher nur sehr eingeschränkt verwertbar und in weiterer Folge auch nicht gerichtsfest.
- Die Überwachung von Kommunikation lässt sich technisch nicht von der Durchsuchung des gesamten Computersystems (Endgeräts) trennen. Letztere wäre eine unverhältnismäßige Grundrechtsverletzung[1].
- Um vor Sicherheitsupdates der Softwarehersteller[2] geschützt zu sein, muss sich die Spionagesoftware updaten können. Dadurch kann beliebiger Funktionsumfang nachgeladen werden und ungewollte Funktionalität nie ausgeschlossen werden.

Weitere Materialien und Argumente:

- Themenseite: https://epicenter.works/thema/bundestrojaner
- Stellungnahme: https://epicenter.works/document/230
- parlamentarisches Begutachtungsverfahren zum Gesetzesvorschlag aus 2016: https://www.parlament.gv.at/PAKT/VHG/XXV/ME/ME_00192/index.shtml

---

[1] BMJ/BMI Interministerielle Arbeitsgruppe „Online-Durchsuchung“ Bericht Endfassung, 13.03.2008, S 26.

[2] z.B.: Betriebssystemhersteller.