German
Business Protection

Risk Consultancy
Business Enablement
Health & Safety
Compliance & Security

Sicherheitslagebild Deutschland

August 2017

Berlin, den 16. August 2017

Hotline	+49 30 63967027-0
Fax	+49 30 63967027-99
E-Mail	info@gbp-security.com
Internet	gbp-security.com

Die deutsche Neudefinition der IT-Überwachung

Das Bundeskriminalamt (BKA) rüstet seine IT auf. Noch in diesem Jahr will das BKA einen sogenannten „Staatstrojaner“ zum Einsatz bringen um Smartphones hacken und verschlüsselte Nachrichten mitlesen zu können. Diese Entwicklung ist auf eine Entscheidung des Bundestags zurückzuführen, die es den Sicherheitsbehörden fortan mit entsprechender richterlicher Erlaubnis ermöglicht, Überwachungssoftware auch auf PCs oder Smartphones mutmaßlicher Straftäter einzuschleusen. Bislang durfte das BKA nur dann Geräte hacken, wenn es um die Prävention von internationalem Terrorismus ging.

Den Trojaner hat das BKA selbst programmiert: Die sogenannte „Remote Communication Interception Software“ (RCIS), die Anfang 2016 erstmalig zum Einsatz kam. Neben den selbstentwickelten Trojanern setzt das BKA aber auch auf kommerzielle Überwachungssoftware. Diese Software wurde von einer externen Firma entwickelt und soll als Ersatz-Trojaner dienen, für den Fall, dass RCIS enttarnt wird. Tatsache ist jedoch, dass dieses „externe“ Tool so einiges mehr kann als RCIS und vom Hersteller zum Beispiel als komplettes Hacker-Portfolio beworben wird.

Die Entscheidung des Bundestags, den Einsatz von Trojanern massiv auszuweiten um den Kampf gegen organisierte Kriminalität und Terrorismus zu stärken, ist zu begrüßen. Allerdings muss man bedenken, dass nicht nur deutsche Behörden sich solche Werkzeuge zunutze machen um an sensible Daten zu gelangen.

Obwohl der externe Partner des BKA den Verkauf seiner Überwachungssoftware an totalitäre Regime offiziell ausschließt, hat das Wall Street Journal bereits im Jahr 2011 ein geheimes Memo des ägyptischen Innenministeriums veröffentlicht, aus dem hervorgeht, dass diese den Behörden in Kairo sehr wohl angeboten wurde. Es ist also davon auszugehen, dass sowohl ausländische Dienste als auch kriminelle Gruppen Zugang zu dieser Technologie erhalten haben und sie somit gezielt Wirtschaftsspionage betreiben können.

Für Firmen hat dies eine ganz klare Konsequenz – kein elektronischer Austausch ist absolut sicher. Man muss damit rechnen, dass alles abgefangen werden kann. Nur kann man eben nicht mehr wissen, was abgefangen wurde und von wem – war es das BKA oder etwa Dritte? Hochsensible Informationen und Geschäftsgeheimnisse sollten daher auf klassische Weise transportiert werden: Durch den Botengang zum Geschäftspartner. Andernfalls droht die Rückkehr der alten mechanischen Schreibmaschine …