2011/46 Inland

https://jungle.world/artikel/2011/46/tupperparty-mit-trojaner

Was verschweigt das BKA über die Staatstrojaner?

Tupperparty mit Trojaner

Von **matthias monroy**

Das Bundeskriminalamt verrät über die Nutzung von Staatstrojanern der Firma Digitask nur die halbe Wahrheit. Denn die Behörde empfiehlt die Software seit Jahren auch an Nachbarländer.

Im Oktober hat der Chaos Computer Club (CCC) deutsche Kriminalämter öffentlich blamiert: Die Hacker konnten nachweisen, dass die Landes- und Bundesinnenbehörden private Rechnersysteme mit Schadsoftware der hessischen Firma Digitask infiltrieren. Die dabei eingesetzten Programme verfügen dem CCC zufolge über weit mehr Funktionen, als durch das Bundesverfassungsgericht erlaubt ist. Richterlich genehmigt wurde in den meisten Fällen lediglich die Überwachung von Internet-Telefonie mit der »Quellentelekommunikationsüberwachung«. Der vom CCC analysierte Staatstrojaner lässt sich jedoch anscheinend bequem für die »Online-Durchsuchung« aufrüsten, mit der das ganze Computersystem durchforstet werden kann.
Im Innenausschuss des Bundestags wollte Jörg Ziercke, der Präsident des Bundeskriminalamts (BKA), die Vorwürfe im Oktober entkräften. Dabei ging es vor allem um die Frage, ob die Polizeibehörden sich an die engen Vorgaben der richterlichen Anordnungen halten. Die Aufregung über den Trojaner findet man beim BKA offenbar übertrieben. »Glauben Sie mir, meine Mitarbeiter verstehen das nicht«, sagte Ziercke nach dem Ablesen seines zwölfseitigen Redemanuskripts.

Doch Deutschlands oberster Bundeskriminalist hatte den Abgeordneten nicht die ganze Wahrheit gesagt. Denn das BKA beteiligt sich, ebenso wie zwei Landeskriminalämter, seit mindestens drei Jahren an einer internationalen Arbeitsgruppe, die die Nutzung staatlicher Trojaner auch grenzüberschreitend erleichtern soll. Dies ging Anfang November aus der knappen Antwort des Bundesinnenministeriums auf eine parlamentarische Anfrage des bundestagsabgeordneten Andrej Hunko (Die Linke) hervor. Demnach wird seit 2008 ein »Informationsaustausch« gepflegt, für den eigens eine »User Group« für »Remote Forensic Software«, also für eine Software für ferngesteuerte Kriminaltechnik, ins Leben gerufen wurde. Die Gruppe war bis dahin weder über Suchmaschinen noch in Protokollen von EU-Arbeitsgruppen zu finden.
An dem Trojaner-Stammtisch nehmen neben dem BKA weitere »Vertreter von

Sicherheitsbehörden« teil, so aus Baden-Württemberg, Bayern, der Schweiz, Belgien und den Niederlanden. Die »User Group« tagt mindestens zweimal im Jahr. Ihr Arbeitsschwerpunkt liegt dem Bundesinnenministerium zufolge auf »Aspekten der Online-Durchsuchung«. Nur »in geringerem Maße« stehe die »Quellenkommunikationsüberwachung« auf der Tagesordnung. Die informelle Gruppe orientiert sich also nicht an den Vorgaben des deutschen Verfassungsgerichts, das die Durchsuchung privater Rechner an strenge rechtliche Bestimmungen knüpft. Laut Bundesregierung gibt es neben der regelmäßig tagenden Arbeitsgruppe auch »anlassbezogen Kontakt zu ausländischen Sicherheitsbehörden«. Diese Treffen fänden »bei Bedarf« statt. Gemeint sind vermutlich Ermittlungsverfahren, an denen mehrere Länder beteiligt sind.
Vergangene Woche ließ sich das Bundesinnenministerium ein weiteres, wesentliches Detail entlocken: Erst auf eine weitere Nachfrage Hunkos wurde mitgeteilt, dass die Einrichtung der »User Group« »auf Anregung des Bundeskriminalamtes« erfolgte. Die Behörde wollte offenbar deutscher Überwachungstechnologie zur internationalen Marktfähigkeit verhelfen. Tatsächlich firmierte der Zusammenschluss anfangs als »Digitask User Group«. Nach der Umbenennung der Gruppe standen auch Testverfahren anderer Hersteller von »kommerzieller Remote Forensic Software« auf der Tagesordnung. Neben dem »Sachstands- und Erfahrungsaustausch« wurden auch »operativ-taktische Aspekte« behandelt, also die Frage, auf welche Art und Weise ein Rechner mit dem Schadprogramm infiziert werden kann.

Die Gründung der »User Group« erfolgte in einer Zeit, in der mehrere deutsche CDU-Innenpolitiker die Nutzung staatlicher Schadprogramme ins Gespräch gebracht hatten. Auch auf EU-Ebene sind mehrere Initiativen aus dieser Zeit bekannt, die auf die Etablierung von »Maßnahmen zur Erleichterung von Ferndurchsuchungen« in EU-In-stitutionen abzielten. Ob aber Behörden wie Europol Trojaner einsetzen, ist weiter unklar. Zumindest jedoch bietet die europäische Polizeiagentur den Polizeibehörden der EU-Mitgliedstaaten ihre Dienste im Bereich digitaler Forensik an und rühmt sich als »weltweit herausragendes Zentrum der Weltklasse« vor allem im IT-Bereich.
Dabei benötigen die Polizeibehörden mancher Länder durchaus schon einmal Nachhilfe im Einsatz digitaler Spähwerkzeuge. So zitierte das österreichische Nachrichtenmagazin Profil kürzlich einen Datenschutzexperten, der den IT-Angestellten der österreichischen Innenbehörden lediglich »zweitklassiges Kurswissen« attestierte. Fahnder einer Sondereinheit waren zuvor daran gescheitert, einem Verdächtigen einen Trojaner über das Internet unterzuschieben. Profil zufolge wurde die Installation dann im Rahmen eines heimlichen Wohnungseinbruchs vorgenommen. Zum Einsatz kam Software von Digitask. Dabei sollte die Software vermutlich zur Überwachung von Internet-Telefonie per Skype genutzt werden. Die polizeiliche Sondereinheit hatte die Nutzung von Trojanern auch gegen linke Tierrechtsaktivisten beantragt.

Dass deutsche Polizeibehörden zum Abhören von Internet-Telefonie nicht nur innerhalb der »User Group« zusammenarbeiten, hatte Staatssekretär Ole Schröder versehentlich in der Fragestunde des Bundestags ausgeplaudert. In einem Nebensatz sprach er von einem »internationalen Austausch«, unter anderem mit »italienischen Kollegen«. Offenbar sorgt sich das Bundeskriminalamt, dass Skype enger mit Italien kooperiert, als es bei den

deutschen Polizeibehörden bislang der Fall ist. Schröder zufolge werden italienische Po-lizisten allerdings nicht bevorzugt, sondern wie alle Ermittlungsbehörden behandelt. Wenn richterliche Anordnungen vorlägen, händige die Firma gespeicherte Nutzerdaten bereitwillig aus. Skype selbst gibt in einem Informationsblatt weitere Hinweise, wie auf die größtmögliche Menge an Informationen zugegriffen werden kann. So sollen Polizeibehörden im Antrag auf Überwachsungsmaßnahmen ankreuzen, dass sie auf »alle zugehörigen Konten« zugreifen wollen. Die Behörden werden überdies aufgefordert zu beantragen, die Konteninhaber nicht über die Ausspähung zu benachrichtigen.

Doch was wäre der Kapitalismus, wenn der Markt nicht auch auf den zunehmenden Bedarf an Antiüberwachungstechnik reagieren würde. So vertreibt die in Berlin ansässige »Gesellschaft für sichere Mobile Kommunikation« (GSMK) ein sogenanntes Crypto-Phone, das eine verschlüsselte Verbindung zwischen zwei entsprechend modifizierten Geräten verspricht. Im Impressum der Firmenwebsite überrascht die Adresse der Firma, die bislang nur als Geschäftsstelle des CCC Berlin bekannt war. Ein Blick in Branchenverzeichnisse verrät die Namen der Inhaber: Zu den Gesellschaftern der GSMK gehört der CCC-Mitbegründer Andy Müller-Maguhn, als »technischer Geschäftsführer« fungiert der Sprecher des CCC, Frank Rieger. Die Firma vertreibt ihr angeblich abhörsicheres Telefon auf einschlägigen Verkaufsmessen. Darunter befindet sich auch die jüngst zu Ende gegangene »Milipol« in Paris, die Militärs, Geheimdienste und Polizeibehörden weltweit für neue Überwachungstechniken begeistern will.