Hacking Team: Eine Spionagesoftware ausser Kontrolle

17. Juli 2015

Golem.de

Die geleakten Unterlagen des Hacking Teams offenbaren zwei erschreckende Fakten: Der lukrative Handel mit Spionagesoftware fördert eine Schattenwirtschaft, in der offenbar rechtliche Übertritte zum Alltag gehören - und diese werden wegen der Verflechtung mit staatlichen Auftraggebern auch stillschweigend geduldet.

Sieben Zero-Days und mindestens ein Rootkit: Der Datenfundus des Hacking Teams deckt ein erschreckendes Software-Arsenal auf. Verwerflich ist dabei nicht nur, dass das Hacking Team Sicherheitslücken bei dubiosen Quellen einkauft. Noch beunruhigender ist, dass die Hersteller von Spionagesoftware eine eigene Entwicklungsabteilung besonders für Flash-Exploits und Rootkits betreiben - und das unter dem Schutz der italienischen Behörden.

Einige der jetzt bekanntgewordenen Zero-Day-Lücken hat der Hersteller von Spionagesoftware aber eingekauft. Das bedeutet: Sie waren in einschlägigen Kreisen längst bekannt und haben Millionen Nutzer gefährdet. Geradezu zynisch klingt vor diesem Hintergrund nicht nur das Motto des Unternehmens, es betreibe ethisches Hacking. Auch seine Mitteilungen nach dem Leak lassen ein erschreckendes Weltbild erkennen: Jetzt könnten Terroristen und Pädophile ungehindert ihre Software und die Zero-Days nutzen. Wild West im Internet. Dabei stehen die selbsternannten "ethischen Hacker" den Bösen, die sie bekämpfen wollen, offenbar in nichts nach.

Der dubiose Handel mit gefährlichen Waffen

Nach dem 2013 beschlossenen internationalen Wassenaar-Abkommen gilt für Spionagesoftware die EU-Verordnung (EG) Nr. 428/2009 (Dual Use). Sie lässt sich demnach sowohl für zivile als auch für militärische Zwecke nutzen und fällt somit unter Exportkontrollen.

Aus den E-Mails des Hacking Team geht hervor, dass das Unternehmen die Öffentlichkeit schlichtweg belogen hat, als es versicherte, dass seine Spionagesoftware nicht in Länder verkauft werde, in die es nicht exportiert werden darf. Quittungen belegen, dass die Republik Sudan noch Ende 2014 Geld für das RCS von Hacking Team bezahlte, als längst Exportverbote gegen das Land beschlossen waren.

Keinerlei staatliche Kontrollen

Im Herbst 2014 stoppte die italienische Regierung plötzlich alle Exporte des Hacking Teams in Länder, die im Verdacht standen, Menschenrechte zu verletzen. Nachdem das Hacking Team intensives Lobbying bei seinen italienischen Kunden betrieben hatte - unter anderem mit Briefen an die Carabinieri und hochrangige italienische Militärs - hob das Ministerium für wirtschaftliche Entwicklung das Verbot im Dezember 2014 aber nicht nur auf, sondern erteilte eine umfassende Exportgenehmigung für die Länder, die das Wassenaar-Abkommen akzeptieren.

Auf einzelne Prüfung verzichtete die italienische Regierung fortan. Stattdessen wird gegen diejenigen ermittelt, die möglicherweise die internen Dokumente des Hacking Teams in die Öffentlichkeit gebracht haben.

Spionagesoftware verbreitet sich wie ein Virus

Seine Software verkaufte das Hacking Team nicht nur über Mittelsmänner, sondern auch über private Firmen, darunter eine in Deutschland. Intech Solutions aus Neufahrn bei München will die Spionagesoftware des Hacking Teams unter anderem Behörden geliefert haben und besteht darauf, sämtliche Exportverbote eingehalten zu haben. Aber auch dieses Unternehmen liefert offenbar an Kunden mit zweifelhaften Absichten, wie ein Bericht des Rechercheverbunds aus NDR, WDR und Süddeutscher Zeitung belegt.

Intech Solutions gab die Spionagesoftware demnach an die kurdische Regionalregierung im Nordirak. Das war 2011, lange bevor der islamische Staat auftrat und die Kurden für ihren Kampf gegen ihn mit Waffen beliefert wurden. Stattdessen wurde die Software benutzt, um innerkurdische Ziele auszuspähen.

Die Guten sind die Bösen

Das Hacking Team muss davon gewusst haben, denn der beauftragte Techniker leitete laut Bericht mehrere Dokumente in das Hacking-Team-Hauptquartier in Mailand. Gegenüber Journalisten rechtfertigte sich der Techniker, der Kunde sei ja eine demokratisch gewählte Regierung. Er arbeite für die Guten, nicht für die Bösen. Er habe auch bei dem französischen Spionagesoftware-Hersteller Vupen angefragt. Der hätte aber abgelehnt.

Dass die Privatwirtschaft sich oft ausserhalb staatlicher Kontrollen Übergriffe leistet, zeigt auch das Beispiel der Privatarmee des US-Sicherheitsunternehmens Blackwater Worldwide. Sie wurde von der US-Regierung beauftragt, die US-Armee im Irak zu unterstützen. Die Söldner begingen jedoch schwere Misshandlungen und auch Morde im Irak. Vier wurden wegen Mordes zu lebenslanger Haft verurteilt.

Schlimmer als ein Virus

Das Hacking Team verbreitet eine womöglich tödliche Software unter zweifelhaften Regimen, die auch Dissidenten ausspähen. Das führt womöglich zu deren Verhaftungen oder sogar zu ihrer Ermordung. Hier versagen staatliche Stellen als Kontrollinstanzen gänzlich, vor allem auch deshalb, weil sie, wie die Carabinieri in Italien, die Software selbst nutzen. Dabei entsteht ein Untergrund, der noch gefährlicher sein könnte als sämtliche zweifelhafte Foren und bisherigen Übertritte der Geheimdienste zusammen.

Was ist ein Rootkit?

Was ist eine Zero-Day-Lücke?