Uli Ries

Digitaler Waffenhandel

Das geheime Geschäft mit Zero-Day-Exploits

Exploits für frische Sicherheitslücken, von denen der Hersteller nichts weiß, werden hinter verschlossenen Türen hoch gehandelt. Unter anderem nutzen Regierungen die Cyber-Waffen zur Verbreitung von Ausspäh-Software. Ein Datenleck gewährt erstmals tiefe Einblicke in diesen Markt.

Ungepatchte Lücken werden nur äußerst selten über Exploit-Kits (siehe Seite 78) ausgenutzt: Dafür sind sie schlicht zu wertvoll. Wenn statt Cyber-Gangs jedoch staatliche Organisationen ausgewählte Ziele attackieren, sieht das anders aus. Bislang diktierte Hörensagen die Diskussion um An- und Verkauf von Zero-Day-Exploits und Bugs – insbesondere dann, wenn es um das Geschäft mit Regierungsorganisationen geht. Ein Vorfall im Juli änderte die Situation schlagartig: Unbekannte stellten unzählige Mails der Firma „Hacking Team“ (HT) ins Netz, einem italienischen Hersteller von Überwachungs-Software [1]. Das Unternehmen kaufte Zero-Day-Exploits ein, um sie als Teil seiner Ausspähwerkzeuge an Regierungsorganisationen weiterzureichen.

Die Italiener waren offenbar laufend auf der Suche nach Lieferanten: Intern verfügten sie entweder kaum oder gar nicht über die zum Programmieren von verlässlich funktionierenden Exploits nötigen Fähigkeiten. Das legt eine ausführliche Analyse der E-Mail-Wechsel nahe, die der IT-Sicherheitsexperte Vlad Tsyrklevich ins Netz gestellt hat.

Die digitalen Einbruchswerkzeuge benötigen Hacking Team und seine Kunden, um ihre Spionagesoftware Remote Control System unbemerkt auf die Rechner und Smartphones der zu Überwachenden zu schleusen. Den E-Mails zufolge wollte HT immer wieder auch auf Wunsch von Bestandskunden, die für den Support des RCS pro Jahr weit über 30 000 Euro zahlten, neue Exploits kaufen.

Exploits mit Garantieanspruch

Von Vitaliy Toropov, einem russischen Programmierer, erwarb Hacking Team beispielsweise drei Zero-Day-Exploits für Adobe Flash. Die Italiener bezahlten 45 000, 40 000 und 39 000 US-Dollar dafür – ohne jedoch die Exklusivrechte zu bekommen. Hätte Hacking Team die Exploits exklusiv beansprucht, wäre der Preis auf das Dreifache gestiegen, wie der Verkäufer seinen Geschäftspartnern per E-Mail mitteilte.

Bemerkenswert ist auch, dass die Schwachstellen anderthalb Jahre nutzbar blieben: Einen von HT im Oktober 2013 angekauften Exploit machte Adobe erst im April 2015 per Update zunichte. Auf einen anderen von Toropov im Januar 2014 verkauften Flash-Bug wurde Adobe erst durch die Veröffentlichung der HT-Daten aufmerksam. Hat ein Hersteller eine Schwachstelle binnen zwei Monaten nach Ankauf des Exploit-Codes geschlossen, leistet der russische Exploit-Entwickler übrigens gratis Ersatz. So geschehen im Mai 2015, als Adobe den erst im April für 39 000 US-Dollar erworbenen Exploit unschädlich machte. Üblich waren auch Ratenzahlungen: 50 Prozent der Summe nach Lieferung, die übrigen Teile dann Monat für Monat, solange der Exploit noch funktionierte.

Auch beim amerikanischen Exploit-Händler Netragard kaufte Hacking Team Angriffscode für Flash – in einem Fall für stolze 215 000 US-Dollar. Der Exploit betraf alle unterstützten Browser unter Windows 7 oder 8.1 und konnte sogar aus der Browser-Sandbox ausbrechen. Der Sandbox-Escape alleine wurde für 120 000 US-Dollar angeboten. Ein anderer Anbieter, Vulnerabilities Brokerage International, hatte Windows-Exploits im Angebot: Einer davon, der eine lokale Rechteerhöhung und die Umgehung von Anwendungs-Sandboxen ermöglichte, sollte 95 000 US-Dollar kosten. Für ein Bug-Paket – Adobe Reader und Windows – verlangte der Anbieter sogar 200 000 US-Dollar. In beiden Fällen scheint Hacking Team nicht zum Zuge gekommen zu sein.

Vorgeschobene ethische Maßstäbe

Netragard hat sein „Exploit Acquisition Program“ zum Ankauf nach dem Leak der Hacking-Team-Interna eingestellt. Man wolle sich jetzt nur noch auf den Teilbereich Penetration-Testing konzentrieren. Grund für den Rückzug sei angeblich der erst jetzt erbrachte Beweis, dass die Käufer mit Geheimdiensten in fragwürdigen Staaten Geschäfte machten. Andere Unternehmer wie Chaouki Bekrar, Gründer des französischen Exploit-Händlers Vupen, ficht das nicht an: Er verkündete Ende Juli den Start von Zerodium, einem Start-up, das sich auf den Ankauf von qualitativ hochwertigen Exploits spezialisieren will. Per Tweet ließ Zerodium verlauten, dass man beispielsweise 100 000 US-Dollar für Bugs wie die gerade aufgetauchte Android-Schwachstelle „Stagefright“ (siehe S. 38) bezahlen würde.

In Bezug auf iOS-Exploits schrieb Netragard-Gründer Adriel Dessautels den Hacking-Team-Vertretern seinerzeit, dass diese zu den am höchsten gehandelten Exploits zählen: Über eine Million US-Dollar wären für eine exklusive Übertragung der Nutzungsrechte fällig. Die Preise seien so hoch, weil sich zahlreiche – wahrscheinlich mit hohen Budgets ausgestattete – Regierungsorganisationen für solche Einbruchswerkzeuge interessierten.

Dreiste Lügen

Die Geschäftsbeziehung zwischen Vupen und Hacking Team wurde vom Vupen-Chef Chaouki Bekrar zuletzt im Februar 2014 nachdrücklich bestritten. Da schrieb er an die Webseite Mashable: „Wir haben keine geschäftliche Beziehung mit Hacking Team, da wir nur mit Regierungsorganisationen zusammenarbeiten“. Diese Aussage kann angesichts der E-Mails getrost als Lüge bezeichnet werden.

Pikant ist, dass sich unter den Anbietern, mit denen Hacking Team in Kontakt stand, auch ReVuln findet. Das von Luigi Auriemma gegründete Unternehmen erlangte unter anderem Bekanntheit durch Hacks von Samsung-Smart-TVs. ReVuln bot Hacking Team Exploits für Angriffe auf Server an, die aber nicht ins Konzept von HT passten. Zu denken gibt die Tatsache, dass sich ReVuln auch auf die Suche von Schwachstellen in SCADA-Industriesteuerungen spezialisiert hat.

Selbst für Insider wie Hacking Team war es schwer, sich im Dickicht der Exploit-Verkäufer zurechtzufinden: Die Italiener haben sich offenbar von einem dubiosen indischen Programmierer namens Manish Kumar einen Exploit für Office 2010 andrehen lassen, der sich dann aber als nutzlos entpuppte. (rei@ct.de)

Literatur

[1] Detlef Borchers, Hacked Team, Die Spionagesoftware-Firma Hacking Team wurde gehackt, c't 17/15, S. 28