Bild: Helmut Fohringer/APA/dpa

Gefährlicher Goldrausch

Preise für Sicherheitslücken explodieren

1,5 Millionen für einen Bug in Apples iOS? Oder dürfen es 3 Millionen US-Dollar sein? Unternehmen wie Zerodium oder Crowdfense überbieten sich mit Preisen für den Ankauf von sogenannten 0day-Exploits. Und die zugrundeliegenden Sicherheitslücken sind unbeherrschbare Cyber-Waffen, die jederzeit losgehen können.

Von Uli Ries und Jürgen Schmidt

Der Ankauf von Zero Day Exploits (kurz: 0days, gesprochen „oh days“) erreicht schwindelerregende Preisregionen. Das in Dubai angesiedelte Crowdfense bietet nach eigener Auskunft bis zu 3 Millionen US-Dollar für einen Bug in Apple iOS oder Google Android, der sich für „Zero Interaction Remote Code Execution“ missbrauchen lässt. Also zum Ausführen von beliebigem Code auf dem Smartphone oder Tablet des Opfers aus der Ferne, ganz ohne dass der Anwender auf einen Link oder einen E-Mail-Anhang klicken muss (Zero Interaction). Ist ein Klick nötig, sinken die Preise auf 2,5 Millionen (iOS) beziehungsweise 2 Millionen US-Dollar.

Dagegen wirken Summen wie 1,5 Millionen US-Dollar (Apple iOS), 1 Million US-Dollar (Tor Browser), 500.000 US-Dollar (Messenger wie iMessage, WeChat oder WhatsApp) oder 200.000 US-Dollar (Microsoft Outlook) fast schon bescheiden. Die bietet das von Chaouki Bekrar gegründete Unternehmen Zerodium seinen Bug-Lieferanten im Rahmen von befristeten Programmen. Für 0days in Unix-basierten Betriebssystemen wie OpenBSD, FreeBSD oder NetBSD sowie in Linux-Distributionen wie Ubuntu, Debian oder Tails sind derzeit bis zu 500.000 US-Dollar drin.

Prall gefüllte Töpfe

Nach eigener Auskunft hat Crowdfense in den ersten zwei Monaten nach Start seines Ankaufprogramms im April 2018 bereits 4,5 Millionen US-Dollar an Einsender von Exploit-Code ausgezahlt. Insgesamt sollen sich 10 Millionen US-Dollar im Topf befinden. Zwar stammen diese Zahlen aus einer – ungewöhnlich genug in der Branche der Exploit-Händler – veröffentlichten Pressemitteilung. Damit ist dann aber auch schon Schluss mit der Transparenz. Denn nachprüfen lassen sich diese Summen ebenso wenig wie die von Crowdfense und Zerodium versprochenen Höchstbeträge. Unseren Quellen zufolge zahlen Zerodiums Kunden sechsstellige Beträge pro Jahr für den Zugang zu deren 0day-Exploit-Arsenal. Für die Exklusivrechte an einem Exploit kommen nochmal Kosten hinzu, die um ein Mehrfaches höher liegen.

Anders als offener auftretende Bug-Bounty-Plattformen wie Bugcrowd oder HackerOne geben Zerodium und Crowdfense weder die Namen ihrer Zulieferer und Kunden noch die pro Exploit ausgezahlten Beträge preis. IT-Sicherheitsforscher äußerten in Interviews an den von Crowdfense und Zerodium versprochenen Millionenbeträgen bereits Zweifel. Ein Insider sortierte die Summen gegenüber c’t unter „Marketing-Lärm“ ein, der nur dazu dienen solle, Bug-Jäger auf die Unternehmen aufmerksam zu machen. Und von denen gibt es laut Alex Rice, CTO und Mitgründer von HackerOne, nicht genügend: „Der Markt ist offenbar eingeschränkt, da es nicht genug Individuen gibt, deren Wertesystem hinreichend beschädigt ist.“ Rice spielt darauf an, dass der Verkauf an Händler wie Zerodium moralisch bedenklich ist, da diese die betroffenen Hersteller nicht über die Schwachstelle informieren.

Ihre Kunden verorten Bekrar und sein Kollege Andrea Zapparoli Manzoni, Director bei Crowdfense, im Bereich Strafverfolgungsbehörden und Nachrichtendienste – und zwar angeblich nur in moralisch einwandfreien Ländern mit demokratischen Regierungen. Zumindest Bekrar wurde allerdings bereits nachgewiesen, dass er es mit der Moral nicht so genau nimmt. Wie geleakte Dokumente belegen, verkaufte seine frühere Firma

Vupen Zero-Day-Exploits an das Privatunternehmen HackingTeam. Und das belieferte mit seiner Spionage-Software auch repressive Regimes wie das Königreich Bahrain, die damit Dissidenten in der eigenen Bevölkerung bespitzelten.

Nur knapp am GAU vorbei

Und selbst wenn man Zero-Day-Exploits nur an demokratisch legitimierte Regierungsorganisationen liefert, bleibt es ein Handel mir Cyber-Waffen, die jederzeit losgehen können. Das hat zuletzt WannaCry eindrücklich demonstriert. Der Verschlüsselungs-Trojaner verbreitete sich über eine schwerwiegende Sicherheitslücke in Windows und infizierte damit über 300.000 Rechner. Den dabei entstandenen Schaden schätzt etwa die Sicherheitsfirma Trend Micro auf etwa 4 Milliarden US-Dollar. Noch viel größeres Unheil verhinderte nur die zufällige Entdeckung eines sogenannten Kill-Schalters im WannaCry-Code, der die weitere Ausbreitung stoppte. „Wir sind damals nur nur haarscharf einem echten Cyber-GAU entgangen“, warnt Informatik-Professor Rüdiger Weis bei jeder sich bietenden Gelegenheit.

Dabei kannte die NSA die von WannaCry ausgenutzte kritische Sicherheitslücke seit vielen Jahren. Sie hätte die jederzeit dem Windows-Hersteller melden können, um für die Entschärfung des damit verbundenen Sicherheitsproblems zu sorgen. Doch der US-Nachrichtendienst hielt die Lücke lieber geheim und nutzte sie stattdessen in seinem Exploit EternalBlue, um jahrelang selbst in fremde System einzubrechen.

Das ging solange gut, bis der NSA dieser und andere 0day-Exploits gestohlen wurden. Eine dubiose Gruppierung namens Shadow Brokers veröffentlichte sie am 14. April 2017 im Internet. Weniger als einen Monat später, am 12. Mai 2017, startete der Amoklauf von WannaCry auf Basis von EternalBlue. Hätte die NSA die Lücke also schließen müssen, sobald sie davon Kenntnis erlangte?

Ein ähnliches Dilemma haben wir auch in Deutschland. Zwar verpflichtet sich das Bundesamt für Sicherheit in der Informationstechnik (BSI) immer wieder lautstark, Sicherheitslücken unverzüglich zu beseitigen. Allerdings gibt es da auch noch die Zentrale Stelle für Informationstechnik im Sicherheitsbereich (Zitis), die etwa BKA und Verfassungsschutz mit Spionage-Trojanern versorgen soll und dafür ebenfalls auf die begehrten 0days angewiesen ist. Den Einkauf solcher Sicherheitslücken wollte der Behördenchef Wilfried Karl kürzlich in einem Interview der Tagesschau nicht ausschließen.

Natürlich wird dieser immer weiter steigende Bedarf nach einer sehr knappen Ressource die Preise auf den grauen und schwarzen Märkten weiter in die Höhe treiben. Es stellt sich aber auch die Frage: Kann Zitis seine 0days wirklich besser schützen als die NSA? Oder müssen wir vielmehr damit rechnen, dass demnächst ein globaler Cyber-GAU mit deutschen Steuermitteln finanziert wurde?

Überfällige Regulierung

Wann immer Exploits in einem solchen Zusammenhang auftauchen, wird der Ruf nach Regulierung laut. Schließlich sind die Exploits Bestandteil von Cyber-Waffen. Anders als bei ihren Pendants in der wirklichen Welt, gibt es beim Handel mit Cyber-Waffen jedoch nur wenig staatliche Vorgaben.

China hat dazu kürzlich eine Verordnung erlassen, laut der Bug-Finder Schwachstellen nur noch an das betroffene Softwareunternehmen direkt melden, aber nicht mehr an Bug-Händler oder -Plattformen verkaufen dürfen. Wahlweise, und darauf dürfte die Regelung abzielen, können sie die Bugs auch im eigenen Land behalten, sodass ihre jeweiligen Arbeitgeber sie verwenden können.

In den Vereinigten Staaten gibt es den seit dem Jahr 2010 gültigen Vulnerabilities Equities Process (VEP). Er schreibt Regierungsbehörden vor, Exploits nach bestimmten Kriterien zu bewerten und auf dieser Basis zu entscheiden, ob die Informationen an den betroffenen Hersteller weiterzugeben sind – oder geheim gehalten werden dürfen. Kaufen die Behörden ihre Exploits aber auf dem Graumarkt, gilt der VEP nicht mehr: Unternehmen wie Zerodium verlangen Geheimhaltungsvereinbarungen von ihren Käufern, und eine solche vertragliche Verpflichtung sticht den VEP aus.

In Deutschland beziehungsweise Europa gibt es bisher keine relevanten gesetzlichen Regelungen für den Umgang mit 0day-Exploits. Das kann auch eine Chance sein. Wie wäre es mit einem klaren europäischen Bekenntnis zu „Security First“, das alle Behörden verpflichtet, Sicherheitslücken beim jeweiligen Hersteller des betroffenen Produkts zu melden? Und zwar anders als in den USA und China „ohne Wenn und Aber“. Der IT-Standort Europa würde davon sicher profitieren. *(ju@ct.de)* c't

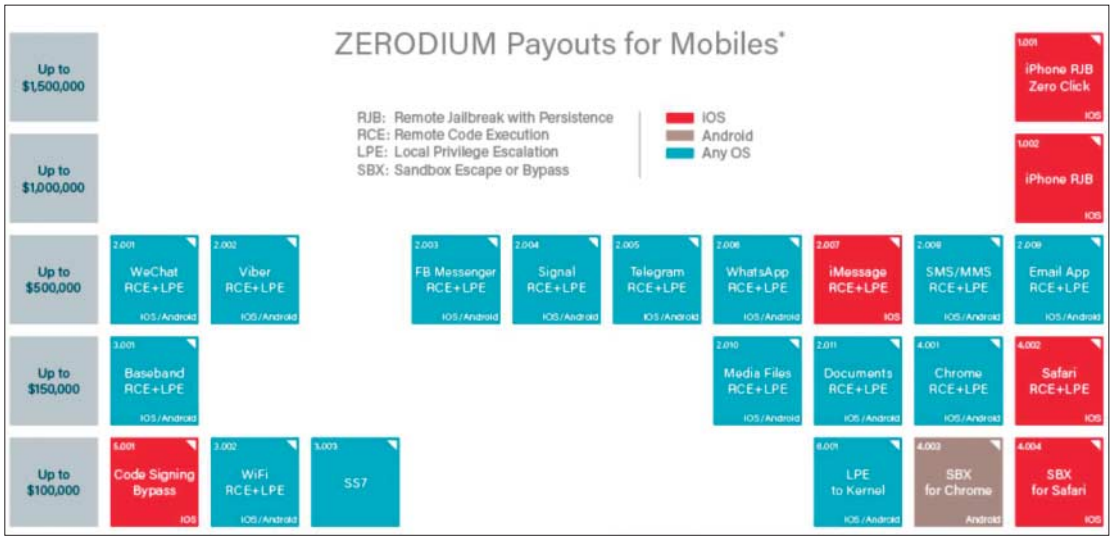

Bild: Zerodium

Cyberwaffen-Dealer wie Zerodium locken Sicherheitsforscher mit Millionensummen für Schwachstellen, die bisher niemand kennt.