Marcus Ranum auf der Cirosec-Konferenz IT-Defense in Köln

Internetkolonie Deutschland

geschrieben von LANline/Dr. Wilhelm Greiner am 17.02.2014

Bei seiner Keynote auf der IT-Defense in Köln warnte der bekannte Security-Vordenker Marcus Ranum vor den negativen Folgen der einseitigen Vormachtstellung der USA im Internet. Andere Länder, so der CSO von Tenable Network Security, müssten sich entweder mit der US-Hegemonie abfinden oder aber Gegenmaßnahmen ergreifen. LANline befragte Ranum anschließend zu seinen Thesen.

„Es ist zur Zeit recht peinlich, Amerikaner zu sein“, begrüßte Marcus Ranum das Publikum der gewohnt hochkarätigen, von Cirosec veranstalteten Sicherheitskonferenz IT-Defense Mitte Februar in Köln. Was folgte, war eine mal sarkastisch, mal zornig vorgetragene Abrechnung mit den Aktivitäten der US-Führung von NSA-Spionage bis Cyberkrieg - und dies von einem Vordenker der US-IT-Industrie, der an den ersten Firewalls und Intrusion-Detection-Systemen mitgewirkt und auch E-Mail-Server für whitehouse.gov installiert hatte.

Marcus Ranum spannte den Bogen von Stuxnet und Flame zu dem von Edward Snowden aufgedeckten Ausmaß weitreichender und demokratisch weitgehend unkontrollierter Abhöraktivitäten und Wirtschaftsspionage der NSA (sowie verbündeter Geheimdienste). Seine Kernthese: Die USA haben in der IT und im Internet eine hegemoniale Vormachtstellung erzielt und benehmen sich deshalb wie eine Kolonialmacht. Seine düstere Prognose: Es ist wohl bereits zu spät, daran noch etwas zu ändern.

Das Kolonialmachtverhalten, das Ranum den USA vorwirft, zeige sich zum Beispiel am Prinzip der Exterritorialität: Gesetze des eigenen Landes werden auf andere Länder „projiziert“, etwa beim Thema Internet. „Fragen Sie nur Kim Dotkom“, so Ranum.

Das Problem: Exterritorialität entwickle sich schnell weiter zum Unilateralismus, zum Ausnutzen einer Machtdifferenz. Deutlichstes Indiz dieses Unilateralismus ist laut Ranum Malware wie Stuxnet oder Flame, die offenbar vom US-Geheimdienst ausgehe. Stuxnet und Co. seien „unzweifelhaft eine Verletzung des Strafrechts vieler Länder“ ebenso wie der Genfer Konvention, die Angriffe auf Kernkraftwerke ausschließt. Zudem habe Stuxnet Millionenschäden an ziviler Infrastruktur angerichtet (den Schaden in Natanz nicht mitgerechnet).

Edward Snowden habe mit seinen Enthüllungen den Schleier von diesem, so Ranum, „stinkenden Chaos“ gelüftet und deutlich gemacht: „Die USA haben im Grunde in alles eine Backdoor eingebaut, von dem sie glauben, dass man eine Backdoor einbauen kann.“ Ranum hält es sogar für möglich, dass das FBI letztes Jahr nicht Angriffe Chinas auf US-Unternehmen aufdeckte, sondern Manipulationen der NSA, die diese als chinesische Geheimdienstarbeit ausgab.

Wie also sollten die Regierungen von Drittländern (jenseits der verbündeten „Five Eyes“-Nationen USA, UK, Kanada, Australien und Neuseeland) reagieren? Den Ansatz, ein „eigenes“ Internet zu bauen, hält Ranum für nicht praktikabel: Man bräuchte dazu seine eigenen Versionen von DNS (Domain Name Service), Verisign, Cisco, Oracle, Microsoft, Apple, Google, Intel etc. - sprich: Man müsste den kompletten Hardware- und Software-Stack nachbauen - kein umsetzbares Unterfangen.

Für praktikabler (wenn auch nicht unumstritten) hält der Security-Experte Chinas Ansatz einer „Great Firewall of China“: Kontrollmechanismen am Rande des nationalen Netzwerks, die sich bei Bedarf verschärfen lassen. Fraglich sei aber, ob solche Mechanismen NSA-Malware fernhalten könnten.

Seine Folgerung: Die EU, Indien wie auch China „sollten ihre Betriebssysteme und wesentlichen Software-Stacks selbst entwickeln“. Zudem sollten sie Mechanismen für ein DNS-Overlay-Netzwerk erarbeiten, um selbst ein Unmapping lokaler DNS-Einträge oder ein bösartiges Remapping überstehen zu können.

Denn Software sei in zunehmendem Maße ein strategisches Gut, und es gelte: „Wenn eine Nation ihre kritische Infrastruktur auf Komponenten einer Supermacht aufbaut, ist sie de facto eine Kolonie dieser Supermacht.“

Zu den „plausiblen Antworten“ auf die Internet-Hegemonie der USA zählt Ranum zudem „Mutual Assured Destruction“, also die Fähigkeit, durch Backdoors in US-Hard- und Software ebenfalls Schaden anrichten zu können („Upps, war das Ihre Cloud?“, so eine der Fußnoten seiner Slideshow), sowie „Mutual Assured Economic Wastage“, also die Fähigkeit, ein Fehlverhalten der USA mit ökonomischen Konsequenzen beantworten zu können.

Trotz dieser „plausiblen“ Optionen seien die Erfolgsaussichten aber gering, denn: „Die US-Strategie, eine weltweite Cyber-Dominanz zu erreichen, scheint aufgegangen zu sein.“ Nun müssten die Nationen dennoch reagieren - oder aber sich mit der US-Hegemonie abfinden.

„Cyberinsurgency“ - IT-gestützte Protestaktionen wie etwa der „Hacktivism“ von Anonymous - sei damit unvermeidbar, so Ranum. Jungen Programmierern rät der verärgerte Experte: „Nehmen Sie einen Job in Ihrem Polizeistaat an, erhalten Sie Zugang zu den Hebeln der Kontrolle und ... warten Sie.“ Denn, so Ranums Plädoyer: „Wir brauchen Menschen in Positionen, in denen sie diejenigen Entscheidungen treffen können, die Snowden getroffen hat.“

Nach seiner sichtlich mit Wut im Bauch vorgetragener Keynote sprach LANline mit Marcus Ranum zu seinen provokanten Positionen:

LANline: Die deutsche Regierung traut sich nicht einmal, Edward Snowden Asyl anzubieten. Sehen Sie da im politischen Alltag tatsächlich die Möglichkeit, dass Staaten wie Deutschland einen Software-Stack entwickeln, der mit dem US-amerikanischen konkurriert? Ist das Problem auf Nationalstaaten-Ebene überhaupt zu lösen?

Ranum: Wie ich im Vortrag schon sagte: Es ist wahrscheinlich schon zu spät. Auf jeden Fall handelt es sich um ein politisches Problem. Die „Five Eyes“ profitieren vom aktuellen Zustand, Länder wie Deutschland und Frankreich ebenfalls, wenn auch in geringerem Maße. Was mich als US-Bürger wütend macht, ist, dass hier der demokratische Prozess umgangen wird. Der US-Kongress und dessen Intelligence Oversight Committee sollten eigentlich unsere Interessen vertreten, nicht die der Geheimdienste. Wir wurden aber nicht gefragt.

LANline: Wie sollte die Reaktion einer Person aussehen, die sich nicht so gut mit IT auskennt wie Edward Snowden, die Teilnehmer der IT-Defense oder Sie?

Ranum: Diese Person muss zunächst einmal verstehen, wie sehr sie von der NSA verarscht worden ist. Und dass die Geheimdienste ohne legislative oder juristische Kontrolle operieren. Angela Merkel sollte weniger verärgert darüber sein, dass ihr Telefon abgehört wurde, als dass die Telefone von Millionen Deutschen abgehört wurden. Das müssen die Leute begreifen.

LANline: Wie sollten IT-Verantwortliche in Unternehmen reagieren?

Ranum: Auch für Unternehmen gilt: Es ist letztlich ein politisches Problem. Ein CEO, etwa der von Siemens, sollte Druck auf Angela Merkel ausüben. Es gibt schließlich ein Potenzial für wirtschaftliche Sanktionen. Diese Diskussion muss in Deutschland stattfinden.

LANline: In den USA haben Teile der IT-Industrie begonnen, gegen die US-Regierung aufzubegehren. Werden diese Unternehmen in der Lage sein, nennenswerten Druck auszuüben?

Ranum: Nun, all diese IT-Unternehmen sind auch Lieferanten der US-Regierung. Man sollte sich zum Beispiel fragen, warum Amazon in dieser Frage so still geblieben ist. Google wiederum hat den Zuschlag für das E-Mail-Geschäft der Regierung nicht erhalten. Deshalb tun sie sich jetzt leichter zu protestieren.

LANline: Herr Ranum, vielen Dank für das Gespräch.