IT Defense: Kritik an laschen Reaktionen auf Snowden-Enthüllungen

Kolonialismus

Jörg Riether

Mitte Februar öffnete die bereits zum zwölften Mal stattfindende Sicherheitskonferenz IT-Defense in Köln ihre Pforten. Unter anderem standen bei der Veranstaltung die USA als „moderne Kolonialherren" des Internets in der Kritik.

Marcus Ranum, Veteran im IT-Sicherheitsumfeld und heute CSO von Tenable Network Security (Nessus), nahm sich in seinem hochpolitischen und scharfzüngigen Vortrag „Internet Under Colonialism" die US-Regierung vor. Seines Erachtens betrachtet sich eben diese als grundsätzlich höhere Instanz, die das Internet als ihren eigenen Besitz versteht und sich international entsprechend verhält. So nehme sich die USA ständig mannigfaltige Rechte heraus, würde diese gleichzeitig aber anderen Ländern nicht zugestehen.

Chinesische Schnüffelmethoden

Ranum führte in diesem Zusammenhang die Kritik der USA an China im Jahr 2010 an, damals ging es um Einbrüche in E-Mail-Konten. Retrospektiv betrachtet und vor dem Hintergrund der durch Snowden offenbarten Details demonstriere dieses und anderes Verhalten, dass die Einstellung der USA vergleichbar mit der einer Kolonialmacht sei.

USA üben massiv Druck aus

Der Security-Experte erläuterte weiterhin, dass die US-Regierung ständigen massiven Druck sowohl nach innen als auch nach außen aufbaue. So habe etwa auf der einen Seite ein Mitarbeiter der US-Air-Force unangenehme Fragen zu erwarten, wenn er etwa Inhalte auf Webseiten von Wikileaks lese. Was den externen Druck auf andere Länder anginge, so werde dieser in erster Linie mit wirtschaftlichen Argumenten aufgebaut. Es sorge ihn sehr, so Ranum, dass man seitens der EU, Chinas, Indiens oder Japans bislang lediglich „lauwarme" Reaktionen bezüglich der Snowden-Enthüllungen vernommen habe.

Kritik aus den eigenen Reihen: Der US-Amerikaner Marcus Ranum (rechts) verurteilte den Internetherrschaftsanspruch seiner Regierung.

Ranum hofft, dass in Zukunft weitere Menschen den Weg von Snowden beschreiten werden. Immerhin sei es um die innere IT-Sicherheit bei der NSA ja offensichtlich nicht zum Besten bestellt. Wie könne es wohl sonst möglich sein, dass ein Mitarbeiter eines beauftragten Unternehmens einen simplen Webspider benutzen konnte, um tonnenweise Daten abzuschöpfen, und es niemandem auch nur ansatzweise aufgefallen sei. Erstaunliche Worte, insbesondere, da sie von einem Vorstandsmitglied eines US-Unternehmens kommen.

Mehr Programme selbst entwickeln

Im Anschluss unternahm Ranum den Versuch, einen Schutz vor etwaiger Überwachung durch die NSA zu skizzieren. Da es nahezu unmöglich sei, sich ein eigenes neues Internet zu kreieren, müssten andere Strategien her. Zum einen sollten etwa die EU, China oder Indien ihre eigenen Betriebssysteme und Software-Stacks entwickeln. Außerdem dachte Ranum laut darüber nach, ob „die große Firewall von China" tatsächlich eine so schlechte Idee sei wie gemeinhin angenommen. Immerhin könne man damit ja etwaige NSA-Aktivitäten bereits an der Landesgrenze unterbinden. Vielleicht sei ja genau dies auch der Grund, dass die US-Regierung sich so sehr darüber aufrege. Ob dieser Vorschlag tatsächlich ernst gemeint war, blieb unbeantwortet.

Sein Fazit fiel düster aus. Man solle niemandem trauen und wenn man heute absolut sicher sein möchte, so solle man entweder komplett aus dem System aussteigen oder aber alles selbst entwickeln.

Dass die Zusammenarbeit von Entwicklern auch Risiken birgt, entdeckte Joshua Tiago (links) beim Untersuchen von Microsofts Team Foundation Server (TFS).

Es gab dieses Jahr erstmals einen exklusiven Paukenschlag in Form einer bislang unveröffentlichten Schwachstelle: Cirosec-Berater Joshua Tiago informierte die Öffentlichkeit über deren Entdeckung in Microsofts Team Foundation Server (TFS). Dieses Produkt kommt etwa dann zum Einsatz, wenn zahlreiche interne wie externe Entwickler gemeinsam an Softwareprojekten arbeiten möchten. Tiago fand nach eigenen Angaben einen Weg, durch manipulierte Unit-Tests die interne Rechteverwaltung des Systems zu umgehen. Dadurch sei es ihm möglich, in sämtliche Entwicklungsprojekte Einsicht zu nehmen. Die Idee hinter dem Angriff sei schlicht, dass etwaige Unit-Tests im Kontext des Build-Prozesses ausgeführt würden. Voraussetzung sei lediglich ein Account als TFS-Entwickler auf dem anzugreifenden System.

Gefährliche Gruppenarbeit

Während seines Vortrags demonstrierte Tiago den Angriff. Am Ende hatte er eine interaktive Kommandozeile auf das eigentliche Entwicklungssystem mit dem TFS als indirektem Vermittler dazwischen. Tiago habe dies sogar am Microsoft-eigenen Cloud-Dienst ausprobiert und auf Video aufgezeichnet. Jenes Video zeigte er im Anschluss der Audienz. Auch hier hatte er am Ende eine interaktive Kommandozeile auf ein Microsoft-Cloud-System. Die einzige ihm bekannte Möglichkeit, sich gegen diese Art von Angriff abzusichern, sei, für jedes separate Projekt einen eigenen TFS zu betreiben.

Bereits im August 2013 habe Tiago dies Microsoft mitgeteilt. Daraufhin sei erst drei Monate später ein schlichter Hinweis vom Software-Giganten eingegangen, dass es sich mitnichten um eine Schwachstelle, sondern um normales Verhalten des Systems handele.

Die kommende IT-Defense wird vom 4. bis 6. Februar 2015 im Westin Hotel Leipzig stattfinden. (ur)