



Abrüstungsgespräche zum Cyberwar - futurezone.ORF.at

Kategorie: ANALYSE | 21.12.2009 | Erstellt um 06:00 Uhr

Im Rahmen der Gespräche über nukleare Abrüstung liegt erstmals auch das Thema Cyberwar auf dem Verhandlungstisch zwischen Russland und den USA. Die zunehmende Vernetzung macht auch Russland angreifbar, zudem kontrollieren russisch-amerikanische Gangs weltweit einen Großteil der Botnet-Infrastruktur, die ebenso für Spam wie für DDoS-Angriffe auf große Staaten geeignet ist.

Während sich europäische Politiker aller Couleurs immer vernehmlicher beklagen, dass sich in den transatlantischen Verhältnissen auf Diplomatenebene bis jetzt rein gar nichts zum Besseren gewandelt habe, setzt US-Präsident Barack Obama sehr wohl auf das diplomatische Instrumentarium - allerdings anderswo auf der Welt.

Ende der vergangenen Woche wurde bekannt, dass die USA mit Russland nicht nur über eine nächste Runde zur Beschränkung des Nuklearwaffenarsenals verhandeln, sondern dass erstmals auch das Thema Cyberwarfare auf dem Tisch ist.

Bis zum Schluss hatte sich die Regierung von Ex-Präsident George W. Bush diesbezüglichen Avancen verweigert und Russland im Gegenzug aufgefordert, erst einmal das Cybercrime-Abkommen des Europarats zu unterzeichnen.

Enttäuschte Europäer

Quer durch die Fraktionen des EU-Parlaments zeigt man sich zunehmend enttäuscht, dass US-Präsident Barack Obama den unilateralen Kurs der Bush-Regierung gegenüber Europa vorerst nicht ändert. Bei der gerade fälligen Erneuerung des Abkommens, das den USA einseitig Zugriff auf die Finanzdatenzentrale SWIFT gibt, wurde das offen ersichtlich. Bei der Erneuerung des Abkommens zur Übertragung von Flugpassagierdaten im kommenden Jahr ist Ähnliches zu erwarten.

- Streit über SWIFT festgefahren (<http://futurezone.orf.at/stories/1632193/>)
- "Obama hat den Laden nicht im Griff" (<http://futurezone.orf.at/stories/1631678/>)

Asymmetrisches Paradox

Dieser Ansatz basierte auf der irrigen Annahme, dass die militärtechnologische Überlegenheit der USA auch automatisch die Dominanz im virtuellen Krieg mit sich bringe.

Tatsächlich ist das Gegenteil der Fall. Wie zuletzt das Beispiel der DDoS-Attacken auf Südkorea gezeigt hat, wirkt ein solcher asymmetrischer Angriff umso verheerender, je besser die zivile IT-Infrastruktur des Verteidigers ausgebaut ist.

Mehr Bandbreite bedeutet in diesem Fall schlicht mehr Feuerkraft für den Angreifer. Je mehr gesellschaftliche Prozesse im angegriffenen Staat nun bereits IT-vernetzt funktionieren, desto mehr finanziellen Schaden richten derartige Angriffe an.

Taktische Waffe DDoS

Allerdings handelt es sich etwa bei DDoS-Attacken bis jetzt um ein rein taktisches und kein strategisches Instrument. Sie wirken weder "nachhaltig" - um einen viel strapazierten Begriff einmal anders zu verwenden -, noch wird dadurch die strategische Ausgangslage verändert.

Anders gesagt: Sie taugen (noch) nicht dafür, einen Schlag zu führen, der mitentscheidend für den Ausgang einer

kriegerischen Auseinandersetzung sein könnte.

Dafür sind Cyberwar-Attacken für Drohgebärden (Estland 2007) gut geeignet, oder sie dienen als Auftakt für einen realen Krieg. Bereits der Angriff auf den Irak 2003 hatte mit Spam an alle Militärs, dem "Defacement" aller offiziellen Websites und gezielten DNS-Sperren begonnen, von denen auch der Fernsehsender al-Jazeera tagelang betroffen war.

Mehr zum Thema Cyberwar

Die "Armee muss noch funktionieren, wenn nichts mehr funktioniert. Das wichtigste Mittel ist in dem Fall für uns jedenfalls die völlige Abschottung nach außen", sagte Oberst Walter Unger, Leiter der Abteilung C im Abwehramt des österreichischen Bundesheers, zu ORF.at. Man sehe sich also sehr genau an, wie die Schnittstellen der Heereskommunikation zu den öffentlichen Netzen abgesichert seien.

- Die Cyberabwehr des Bundesheeres (<http://futurezone.orf.at/stories/1629459/>)
- Die Militarisierung des Cyberspace (<http://futurezone.orf.at/stories/1628444/>)
- Twitter weiter unter Beschuss (<http://futurezone.orf.at/stories/1623026/>)
- Clinton soll die Bot-Nets stoppen (<http://futurezone.orf.at/stories/1619826/>)
- Gestaffelter Netzangriff auf Südkorea (<http://futurezone.orf.at/stories/1617025/>)

Auch im Georgien-Krieg waren DDoS-Attacken auf das Internet in Georgien nur der Auftakt für Bomben und Kanonendonner gewesen, danach spielten sie keine weitere Rolle für das Geschehen.

So wie es ist, bleibt es nicht

Allerdings wird die Lage nicht so bleiben, wie sie sich momentan darstellt. Zum einen wächst die Angreifbarkeit gerade eines Schwellenlandes wie Russland mit dem Ausbau der IT-Infrastruktur schneller, als Sicherheitsmaßnahmen eingezogen werden können.

Zum anderen richtet sich die Aufmerksamkeit der Militärs in den USA auf die zunehmende Vernetzung kritischer Infrastrukturen wie Stromnetzen und Leitsystemen für Verkehrsmittel von der U-Bahn bis zum Straßenverkehr mit dem Internet.

"Network-Centric Warfare"

Das Pentagon wiederum kontrolliert jene Armee, die seit gut 15 Jahren auf "Network-Centric Warfare" setzt. Wie schon der Name sagt, basiert diese Strategie auf permanentem Informationsaustausch zwischen allen beteiligten Einheiten und dem Generalstab. Die waffentechnische Überlegenheit der USA basiert zu einem Gutteil auf einem funktionierenden Informationsfluss in diesen ständig wachsenden Militärnetzwerken.

Es gibt noch einen weiteren triftigen Grund, der Russland und die USA dazu gebracht hat, erstmals über mögliche Abrüstung bei IT-Waffen zu verhandeln. Er ist bilateraler Natur, denn in fast allen gerichtsanhängig gewordenen Fällen von organisiertem Datendiebstahl handelt es sich um gemischte Gangs von US-Staatsbürgern und Russen.

130 Millionen Datensätze

In New Jersey und mehreren anderen Orten steht gerade jene Gang vor Gericht, die in die Systeme des Finanzdienstleisters Heartland Payment Systems und anderer Firmen eingedrungen war.

130 Millionen Datensätze von Bankomatkarten- und Kreditkartenbesitzern wurden dabei kopiert. Das ist die größte bis jetzt abgezogene Datenmenge - begehrte Handelsware für einen kriminellen Untergrund aus Phishern, Spammern, Erpressern und Identitätsbetrügern.

Wenn diese nicht ohnehin über eigene Netze aus Zombie-Rechnern verfügen, kurbeln sie das Geschäft der Botnet-Infrastrukturbetreiber an.

"Russische Hacker"

Womit wir wieder bei DDoS-Attacken und dem damit eng verbundenen Geschäftszweig der Malware-Autoren sind, den Herstellern von Schadsoftware, von denen ein Gutteil aus dem ehemaligen Ostblock stammt.

Die Spuren der wirklich großen Botnets, deren Existenz bekannt ist, weisen in den allermeisten Fällen denn auch nach Russland, was aber nicht automatisch bedeutet, dass sie allein von "russischen Hackern" kontrolliert werden.

Organisierte Datenkriminalität

- Datendiebstahl und -verlust nehmen zu (<http://futurezone.orf.at/stories/1633982/>)
- Visa: Datenleck noch immer nicht gefunden (<http://futurezone.orf.at/stories/1632388/>)
- Kreditkarten-Austauschaktion auch in Österreich (<http://futurezone.orf.at/stories/1632293/>)
- US-Datendieb bekennt sich schuldig (<http://futurezone.orf.at/stories/1625627/>)
- Datendiebstahl bei Twitter (<http://futurezone.orf.at/stories/1618926/>)

"Wenn die Amerikaner und Russen das wollten, könnten sie alle größeren Botnets ziemlich schnell aus dem Verkehr ziehen", sagt Joe Pichlmayr vom österreichischen Anti-Virus-Hersteller Ikarus, der auch über eine Niederlassung in Russland verfügt.

"Richtig gute Botnets"

Gerade diesen Staaten mit ihren mächtigen Geheimdienstapparaten stünden mehr als genug Ressourcen dafür zur Verfügung, doch anscheinend habe man sich dafür bis jetzt zu wenig interessiert, so Pichlmayr.

Das Interesse der Militärs richte sich weit eher darauf, "die wirklich guten Botnetze zu finden, die eben nicht durch Spam auffällig geworden sind".

Gemeint sind damit weitaus kleinere, aber gut programmierte, hoch automatisierte Botnetze, die aus dem Nichts auftauchen wie jenes, das den Netzverkehr in ganz Südkorea eine Woche lang teilweise zum Erliegen brachte.

Das israelische Militär

Eine ganze Reihe von Armeen weltweit verfügt über derartige Angriffswaffen, die derzeit noch als "taktisch" eingestuft werden. Am vergangenen Dienstag, wenige Tage nach Bekanntwerden der russisch-amerikanischen Gespräche, hielt Generalmajor Amos Jadlin, oberster Chef der israelischen Militärgeheimdienste in Tel Aviv, einen überraschenderweise öffentlichen Vortrag am Institute for National Security Studies.

"Das Gebiet Cyberwarfare passt sehr gut zur bestehenden Verteidigungsdoktrin Israels", sagte Jadlin der Nachrichtenagentur Reuters. Nicht nur die USA und Großbritannien, auch Israel habe seine eigenen Soldaten und Offiziere, die sich damit beschäftigten.

Jadlin weiter: "Der Cyberspace verleiht auch kleinen Ländern und Individuen eine Macht, die bis jetzt den großen Staaten vorbehalten war."

"Digitales Pearl Harbor"

Smarte Stromzähler in Österreich

Während im Nachbarland Deutschland "intelligente" Stromzähler ab 2010 für Neubauten und totalsanierbare Gebäude verpflichtend werden, lässt man sich mit einer Einführung der neuen Technologie in Österreich noch Zeit. Viele Punkte sind noch ungeklärt, und die Regulierungsbehörde E-Control, der Verband der Elektrizitätsunternehmen Österreichs (VEÖ) und der Fachverband Gas Wärme (FGW) arbeiten derzeit an einer einheitlichen Lösung.

- Spielregeln für smarte Stromzähler (<http://futurezone.orf.at/stories/1628551/>)
- Energie Steiermark testet Smart Metering (<http://futurezone.orf.at/stories/1633035/>)

15 Jahre lang sei er über all jene hergefallen, schreibt Ira Winkler von der Sicherheitsberatungsfirma CSO, die mit Warnungen vor einem neuen, diesmal "digitalen Pearl Harbor" in die Schlagzeilen kommen wollten.

Die geplante Einführung des "Smart Metering" - die auch in Europa geplante Aufrüstung von Haushalten mit vernetzten Stromzählern - habe ihn jedoch gezwungen, seine Meinung zu ändern.

Wenn zig Millionen Haushalte mit diesen Kästchen ausgerüstet werden, dann steige die Wahrscheinlichkeit mit der Zeit enorm, dass irgendjemand eine fatale Schwachstelle in der Hard- oder Software entdecke und die

Stromerzeugung erfolgreich angreife, so Winkler. Das hätte die Qualität eines strategischen Schlags wie jenem, den Japan am 7. Dezember 1941 in Pearl Harbor gegen die US-Flotte geführt hatte.

Russland statt Raunzer

Links zum Thema

- Analyse der Cyberwar-Kapazitäten Chinas (<http://www.securityaffairs.org/issues/2009/16/mazanec.php>)
- Der weltweite Stand im Jahresbericht von McAfee (http://newsroom.mcafee.com/article_display.cfm?article_id=3594)
- Ira Winkler über "Digital Pearl Harbor" (http://www.csoonline.com/article/509213/I_Was_Wrong_There_Probably_Will_Be_an_Electronic_Pea:
)
- Ikarus Security Software (<http://www.ikarus.at/>)

Insgesamt gibt es also Gründe genug dafür, dass die Regierung Obama gegenüber Russland Konzessionen macht und über fehlenden Datenschutz und mangelnde "Reziprozität" raunzende EU-Staaten links liegen lässt.

Während es durch bessere Beziehungen mit Russland also Vorteile zu erreichen gibt, hat die US-Regierung naturgemäß wenig Lust, bei grundlegenden Neuverhandlungen mit den Europäern zu den Themen SWIFT- und Flugpassagierdaten bestehende - strategische - Vorteile aufzugeben: den alleinigen und tagesaktuellen strategischen Überblick über einen großen Teil der globalen Finanz- und Flugbewegungen.

(futurezone/Erich Moechel)