Cyberterrorismus nur Panikmache?!

*Hans-Ulrich Helfer**

Bereits seit Mitte der Neunzigerjahre sprechen die Massenmedien von Cyberterrorismus und verbreiten Schreckensszenarien. Die bekannte Suchmaschine Google listet mit dem Suchwort über 50‘000 Beiträge, ohne dass wirklich verdeutlicht würde um was es überhaupt geht oder in Zukunft gehen könnte.

Der Begriff Cyberterrorismus meint, dass Terroristen für ihre Ziele Computersysteme nutzen. Dabei ist ganz besonders zwischen zwei Anwendungen zu unterscheiden. Erstens Terroristen, welche die Computertechnologie als Logistikmittel für ihre Ziele nutzen. Und zweitens Akteure, die mit einem Computer einen virtuellen terroristischen Angriff auf beispielsweise Kernkraftwerke, Stromversorgungen oder ähnliche Strukturen durchführen. In der ersten Definition handelt es sich lediglich um den gegenwärtig viel genutzten Cyberterrorismus als Logistikmittel. In der zweiten Beschreibung um den viel gefährlicheren 'echten' Cyberterrorismus der Zukunft.

Cyberterrorismus als Logistikmittel

Obschon wir eine gewaltige Zunahme von Computerangriffen in privaten, wirtschaftlichen und staatlichen Bereichen verzeichnen, sind nur wenige Prozente den Terroristen zuzurechnen. Die meisten illegalen Pc-Anwendungen sind Cyberkriminalität und nicht Cyberterrorismus. Natürlich ist die Anzahl der politisch motivierten Angriffe durch Hacker und Cracker ebenfalls gestiegen. Diese Aktionen als Cyberterrorismus zu bezeichnen, zielt eindeutig am Problem vorbei und verschleiert sogar die tatsächliche Bedrohung. Cyberterrorismus als Logistikmittel umfasst beispielsweise folgende Erscheinungsformen:

Interne Kommunikation
Seien es die klassischen nationalen Terrororganisationen oder weltumspannende wie die Al Quida, alle nutzen heute das Internet für ihre Kommunikation. Benutzt wird nicht nur die bekannte eMail, sondern auch Websites, Blogger, Chat, Foren, SMS usw. Die Vielzahl der Möglichkeiten und Systeme sowie Sprachen verunmöglicht eine Kontrolle durch die Behörden.

Propaganda
Mittels eMail-Massenversand und Websites in fast allen Sprachen propagieren die nationalen wie internationalen Terrororganisationen ihre Ziele. Sie stellen auf Download-Server Material kostenlos zur Verfügung.

Rekrutierung
Die Rekrutierung über das Internet erfolgt indirekt, da die Terrororganisationen Einschleusungen von Beamten befürchten. Potentielle Bewerber werden vorerst über Chatrooms angesprochen. Dabei wird alleine schon durch die Sprache eine wichtige Selektion vorgenommen. Ein Blick in die wichtigen Chats wie etwa bei Bluewin oder Yahoo usw. zeigen die unzähligen kaum kontrollierbaren Chat-Rooms.

Online-Ausbildung

Die ideologische und theoretische Grundausbildung geschieht grösstenteils nicht mehr in Trainingslagern irgendwo im Hinterland unter der Satellitenbeobachtung etwelcher westlicher Staaten, sondern über das Netzwerk des so gehassten Feindes. Unzählige Anweisungen und Handbücher in etlichen

Zweiter Halbjahresbericht von MELANI

Gezielte Spionageangriffe aus China, Phishing und Pharming sowie eine ausführliche Einschätzung zum Thema **Cyberterrorismus**: Dies sind Themen des zweiten Halbjahresberichts, den die Melde- und Analysestelle Informationssicherung (MELANI) vorlegt. Der Bericht unter dem Titel «Informationssicherung: Lage in der Schweiz und international» ist abrufbar unter http://www.melani.admin.ch.

MELANI beleuchtet in dem Bericht die aktuelle Lage, Gefahren und Risiken, erläutert die wichtigsten Tendenzen rund um die Informations- und Kommunikationstechnologien (IKT) und gibt eine Übersicht über Ereignisse im In- und Ausland. In Form von Einzelbeispielen werden die wichtigsten Ereignisse der zweiten sechs Monate des Jahres 2005 aufgezeigt. Zum ersten Mal bietet der Bericht auch ein Glossar der wichtigsten Begriffe aus dem Bereich Informationstechnologie.

Zudem beleuchtet der Bericht auch die Thematik des **Cyberterrorismus**. Er zeigt auf, in welchen Bereichen dieser tatsächlich aufzufinden ist und wo es sich bei diesem Begriff vor allem um leere Worthülsen handelt. Weiter richtet MELANI das Augenmerk erneut auf die Professionalisierung der Hackerszene und die gezielten Spionageangriffe aus China gegen Verwaltungen und kritische Infrastrukturen in englischsprachigen Ländern.

MELANI
Melde- und Analysestelle Informationssicherung
Friedheimweg 14
3003 Bern
http://www.melani.admin.ch

Sprachen kursieren auf dem Hinternet. Die Terroristen nutzen für die Online-Ausbildung modernste Technologie wie Internettelefonie sowie Chatrooms usw.

Geldbeschaffung
Online-Geldsammelaktionen für undurchsichtige Wohltätigkeitsorganisationen jeder Art gibt es unzählige. Seit den Kontensperrungen der Behörden sind die Terroristen vorsichtiger geworden und benutzen für ihre Belange auch bekannte Hilfswerke. Die Beschaffung geschieht auch über den Verkauf von Popagandamaterial wie Filme, Musik, Flyer usw.

Psychologischer Krieg
Mit dem Internet haben terroristische Organisationen erstmals die Möglichkeit gefunden, mit den grossen staatlichen oder privaten Massenmedien gleichzuziehen. Sie agieren schnell und gekonnt und schocken nicht selten den Bürger und die verantwortlichen Beamten mit Folter und Enthauptungen auf Videos, die sie übers Internet verbreiten.


Samstag, 29. April 2006
Neues El Kaida-Video
Diesmal ist es Sawahiri
Innerhalb weniger Tage hat sich das Terrornetzwerk El Kaida zum dritten Mal zu Wort gemeldet. Im Internet tauchte am Freitag nach Angaben des US-Nachrichtensenders CNN ein neues Video der Nummer zwei des Terrornetzwerkes El Kaida, Eiman el Sawahiri, auf. Laut CNN preist Sawahiri die Anschläge der Aufständischen im Irak und fordert die Pakistaner zum Sturz von Präsident Pervez Musharraf auf.
El Sawahiri in einem Ausschnitt aus dem aktuellen Video

Der echte Cyberterrorismus ist noch nicht Gegenwart

Terroristen suchen immer nach neuen Anschlagsmöglichkeiten und effizienteren Waffen (siehe Interview mit Prof. Dr. Leonid Fituni Seite 26). Wenn es Terroristen also möglich ist, den Computer als eigentliche Waffe einzusetzen, so werden sie dies auch tun. Aus diesen Überlegungen ergeben sich natürlich tatsächlich Schreckensszenearien, denn die westlichen Gesellschaften nutzen in einem äussersten starken Ausmass die Systeme, die mit einem Pc angreifbar sind.

Dies führt dazu, dass immer wieder angeblich stattgefundene oder geheim gehaltene Angriffe von Cyberterrorismus kolportiert werden. So berichtete etwa die namhafte Zeitung Washington Post ein Hacker sei in das Computersystem des Theodore-Roosevelt-Stausees in Arizona eingedrungen. Hätte er die Schleusentore geöffnet, so wären in den Städten Tempe und Mesa rund eine Million Personen ertrunken. Die Wahrheit ist aber, dass der Hacker nie nur eine Sekunde die Herrschaft über das System oder sogar die Schleusentore hatte.

Cybercrime und Cyberterrorismus siehe auch: http://www.crime-research.org

Cyberterroristische Angriffe auf nationale Logistiknetzwerke wie Kernkraftwerke, Flugleitsysteme, Bankzentren, Wasserwerke, Satellitenkommunikation, Raketenbasen, Städte-Notfallsysteme und Militärstützpunkte sind gegenwärtig noch Phantasien und Visionen der Massenmedien. Bis heute ist kein einziger Fall von 'echtem' Cyberterrorismus bekannt oder öffentlich belegt.

Genauso umstritten wie die Bedrohung durch ABC-Terrorismus ist auch der Cyberterrorismus (noch) nicht greifbar und nur schwer zu beurteilen. Gegenwärtig werden beide Formen hauptsächlich in der Literatur und in der Filmbranche dargestellt. Allerdings ist zu beachten, dass alles was denkbar ist auch eines Tages ausgeführt wird. Osama bin Laden würde wohl keine Sekunde zaudern, könnte er lediglich über seinen Personalcomputer ein Verkehrsflugzeug in das Weisse Haus rasen oder eine amerikanische Stadt in den Fluten versinken lassen. In diesem Sinne ist der in den Massenmedien dargestellt Cyberterrorismus noch reine Panikmache, niemand weiss wann er Tatsache in der Gegenwart sein wird.

Der Autor
*Hans-Ulrich Helfer, 21. April 1951, verheiratet, von 1976 bis 1983 Staatschutzbeamter, 1983 Gründer der Presdok AG, von 1995 bis 2000 FDP-Gemeinderat von Zürich. Heute Geschäftsführer der Presdok AG Zürich, im besonderen Berater von staatlichen Institutionen, Konzernen sowie Privatpersonen zu wirtschaftlichen und sicherheitspolitischen Sonderfragen. (Wirtschaftsdokumentationen, Gefährdungsanalysen, Risikostudien, Länderanalysen). ◆

Rätsel-Krimi

Der Fehler im System

Kommissarin Katja Rulandt zog die schweren Samtvorhänge auf. Tageslicht flutete herein und fiel auf den jungen Mann, der tot neben einem umgestürzten Drehstuhl lag. Der zellenartige Raum stand voll mit Computern. Kriminalassistent Meerbusch stolperte fluchend über eins der Kabel, die sich kreuz und quer über den Teppichboden spannten, während die Kommissarin nach einer Visitenkarte fischte, die dem ermordeten Bernie Baldauf offenbar aus der Tasche gerutscht war. «Lars Weimer, Softwaresysteme», konnte sie auf dem wertvollen Büttenpapier lesen. Weimer schien von Bernies Tod nicht sonderlich überrascht. «Sie würden anhand der Fussspuren sowieso herausfinden, dass ich letzte Nacht um seine Wohnung herumgeschlichen bin», quetschte er hervor. «Ich hatte den Verdacht, dass Bernie Teile unserer Software geklaut hat, um damit seine eigene Firma aufzumachen. Deshalb wollte ich ihn zur Rede stellen. Doch als ich vor seinem Haus ankam, sah ich Baldauf durchs Fenster tot auf dem Teppich liegen. Vor Schreck bin ich sofort abgehauen, ohne die Polizei zu verständigen. Wie hätte ich der auch meine Anwesenheit erklären sollen?» Die Kommissarin meldete Zweifel an: «Wir haben herausgefunden, dass Baldauf eine Sicherheitslücke in dem Programm-System entdeckt hat, das Sie für teures Geld an Ihre Kunden verkaufen.» - «Ach, und jetzt denken Sie, ich hätte kurzerhand für sein ewiges Schweigen gesorgt», schnaubte Weimer, «so ein Unsinn!» Katja Rulandt lächelte: «Und wieso haben Sie uns dann in einem Punkt belogen?» - In welchem?

Die Auflösung zu «Rätsel-Krimi» siehe Seite 29.