Cyberfahnder-Newsletter 5 vom 27.05.2010

Schwerpunkt: Cyberwar

Die Urlaubspause ist vorbei [1].

Der ▸ Cyberfahnder meldet sich mit einem neuen Arbeitspapier zurück:

▸ Dieter **Kochheim**, Netzkommunikation, Juni 2010

Netzkommunikation und Cyberwar

Die ersten Kapitel des Arbeitspapiers befassen sich mit den verschiedenen Kommunikationstechniken, also den Telefonnetzen, der Adressierung und der Struktur des Internets. Eine besondere Bedeutung kommt dabei dem Routing zu, das die Netzbetreiber in die Lage versetzt, Datenströme gezielt und wirtschaftlich effektiv zu steuern.

Auf der Grundlage dieser technischen Erklärungen befasst sich das Arbeitspapier schließlich mit den bekannten Manipulationsmöglichkeiten und der Cybercrime [2]. Sie liefern die Überleitung zur Auseinandersetzung mit dem Cyberwar.

Cyberwar

Die heutigen Erkenntnisse lassen es erwarten, dass sich die Methoden im Cyberwar nicht besonders von denen der Cybercrime unterscheiden werden, so dass in seiner ersten unterschwelligen, noch „Kalten Phase“ bevorzugt Hacking, DoS-Angriffe, Malware, Botnetze und das Social Engineering zum Einsatz kommen. Sie dürften mit zunehmender Eskalation um geheimdienstliche, terroristische und militärische Methoden erweitert werden.

Ich definiere Cyberwar als eine gezielte und zerstörerische Auseinandersetzung mit den Mitteln und gegen die gegnerischen Infrastrukturen der Netzkommunikation. So verstanden umfasst der Begriff nicht nur militärische Akteure, sondern auch politische Aktivisten, Unternehmen und die organisierte Cybercrime. Er ist gekennzeichnet von dem strategischen Einsatz der Informations- und Kommunikationstechnik mit dem Ziel, Gegner und Opfer existenziell zu schädigen, also nicht nur ihre Datenverarbeitung und Netzkommunikation zu stören oder auszuschalten, sondern ihre Funktionstüchtigkeit insgesamt.

Dabei dürften sich anfangs die Akteure kaum unterscheiden. Ob die Hinterleute kriminelle, terroristische oder militärische Ziele verfolgen, dürfte unerheblich sein, weil sie zunächst auf die kriminellen Fachleute zurückgreifen werden, der sich die Organisierte Cybercrime bereits jetzt bedient.

Deshalb komme ich auch zu dem Schluss, dass der erste Schritt zur Bekämpfung des Cyberwar in der grenzüberschreitenden Bekämpfung der Cybercrime besteht.

Cyberwar als höchste Stufe der Cybercrime

Das Arbeitspapier ist kein Handbuch für destruktive Handlungen im Internet, so dass ich nur wenige praktische Beispiele aufzeige, die die Gefahren erkennen lassen.

Cybercrime und Cyberwar stellen sich nach heutigem Kenntnisstand als Stufen der Eskalation dar.

⇨ Die unterste Stufe stellt die allgemein zu erfahrende Cybercrime dar. Sie äußert sich im Phishing, im Identitätsdiebstahl, dem Verbreiten von Malware und den Betrügereien, die im Zusammenhang mit Warenbestellungen, Paketstationen und falschen Identitäten begangen wird.

Für sie gilt dasselbe wie für alle kriminellen Alltagserscheinungen: Diese Kriminalität führt zu keinen vernichtenden Schäden, wohl aber zu einer allgemeinen Verunsicherung und dadurch zu einem wachsenden Misstrauen gegen den staatlichen Rechtsschutz und an der Effektivität der Strafverfolgung.

---

[1] Während meines Urlaubs sind rund 250 E-Mails eingegangen, die dann unwiederbringlich verloren gegangen sind. Sollten wichtige Nachrichten dabei gewesen sein, die nach einer Reaktion von mir verlangt hätten, so bitte ich mein Schweigen nachsichtig zu entschuldigen.

[2] ▸ Dieter **Kochheim**, Cybercrime, Mai 2010.

⇨ Auf der zweiten Stufe befinden sich die Neugierigen, die Mitläufer, Krämer, Script-Kiddies und Webshopinhaber, die sich in Hacker-Boards tummeln, Kontozugangs- und E-Mail-Daten vertickern und abgeschottet rege miteinander kommunizieren. Für sie gilt das, was vielfach auch von anderen Tätergruppen mit gemeinschaftlicher Sprache, Herkunft oder Neigungen gilt: Sie müssen nicht zu Straftaten überredet werden und sprechen unbekümmert und bedenkenlos über geplante oder durchgeführte Taten und Angriffe sowie über die damit verursachten Schäden.

Die Beteiligten aus der zweiten Stufe sind weitgehend dieselben Personen, die die Massenkriminalität aus der ersten Stufe ausführen. Auch wenn sie bei ihren Absprachen und Tätigkeiten kaum von der Öffentlichkeit wahrgenommen werden, schaffen sie damit ein erhebliches kriminelles Gefahrenpotential, das es ebenfalls zu bekämpfen gilt.

⇨ Auf der dritten Stufe befinden sich die Organisierten Internetverbrecher, wobei ich einen von McAfee eingeführten Begriff verwende. Zu ihnen zähle ich die Operation Groups, zu denen sich professionelle Malwareschreiber, Botnetz- und Forenbetreiber verbunden haben, und die Schurkenprovider, die getarnte Infrastrukturen und Geldwäsche betreiben.

Diese Täter lassen sich kaum mit den heute bekannten Methoden und dem vorhandenen Personal der Strafverfolgung bekämpfen. Hierzu müssen neue Strukturen und Kompetenzen gebildet werden und bedarf es einer reibungslosen internationalen Zusammenarbeit.

⇨ Die vorletzte Stufe bildet der Kalte Cyberwar. Bei ihm kommen zunächst dieselben organisierten Strukturen und Personen zum Einsatz, die auch die Organisierte Cybercrime bilden. Ihre kriminellen oder terroristischen Aktivitäten sind jedoch langfristig ausgerichtet, dienen dem Ausspähen gegnerischer Organisationen, ihrer Unterwanderung und Penetration. Zerstörerische Aktionen kommen nur vereinzelt vor, sind nicht nachhaltig und dienen zur Bedrohung, zum Kräftemessen und zur Beschaffung von Geld.

Die Erscheinungsformen des Kalten Cyberwar können in politisch motivierten DoS-Angriffen, der zunehmenden Industriespionage und Hacking-Angriffen gesehen werden, über die der Cyberfahnder berichtet [3]. Es ist zu erwarten, dass sich vermehrt auch geheimdienstliche, militärische, terroristische und mafiöse Hinterleute am Kalten Cyberwar beteiligen.

⇨ Im Heißen Cyberwar geht es darum, die Gegner existenziell zu bekämpfen. In ihm werden nicht nur die Methoden der Cybercrime, sondern auch „harte“ terroristische und militärische Aktionen zum Einsatz kommen.

Perspektiven

Die Beschäftigung mit der Cybercrime und dem Cyberwar kann leicht dazu führen, die guten Auswirkungen der modernen Technik auszublenden und bis hin zur Verzweiflung in Düsternis zu verfallen. Auch dagegen möchte ich mich wenden.

Die moderne Telekommunikationstechnik und das Internet haben ungeahnte Informations- und Kommunikationsmöglichkeiten geschaffen. Im Allgemeinen gilt das zum Beispiel für die Angebote des ▸ Heise-Verlages, den Suchmaschinen und der ▸ Wikipedia, unter juristischer Sicht die ▸ Gesetze im Internet von Juris und die Veröffentlichungen der obersten Bundesgerichte (▸ BGH, ▸ BverfG).

Die Betrachtung der Gefahren aus dem Netz muss das Ziel haben, Gefahrenpotentiale zu benennen und Auswüchsen zu begegnen. Ich denke, die Chancen dazu sind vorhanden.

Mit besten Grüßen

Ihr Cyberfahnder

---

[3] Siehe zuletzt: ▸ Verfassungsschutzbericht 2009. Tatort Internet, 26.06.2010