12. Sep. 2012

von pano

in Cyber Security, Sicherheitskultur

Kommentare (0)

Security Times

von Andrea Jonjic und Philipp Offermann

"Cyber-Krieg – der Begriff dringt langsam ins öffentliche Bewusstsein" schreibt Eugene Kaspersky heute in der SZ (offline). Eine recht vorsichtige Umschreibung für eine *buzzword*-Karriere, die bald Globalisierungs-artige Züge annehmen könnte. Dass der Begriff mehr verschleiert als erhellt, haben wir hier im Blog schon oft thematisiert. Doch mit der Lektüre des Kaspersky-Beitrags wird nicht nur die Bedrohung eines internationalen Cyber-Kriegs vor Augen geführt – nein, es ist ein "Angriff auf den Alltag". Zumal Kasperskys Aussenansicht im Zusammenhang steht mit einer etwas klandestinen Zusammenkunft in Bonn, dem Cyber Security Summit.

Diese Konferenz ist als *spin-off* der Münchner Sicherheitskonferenz (auch dies ein Klassiker unserer Arbeit) angekündigt, wird aber offensichtlich maßgeblich von der Deutschen Telekom betrieben. Auch dort ist man zu der Erkenntnis gelangt, dass Krieg längst auch in der virtuellen Welt stattfindet: "Die Gefahr, die von Angriffen auf Computersysteme ausgeht, ist enorm". Eine nicht näher benannte Runde von "Top-Managern" und "hochrangigen Führungspersönlichkeiten" möchte daher heute "einen entscheidenden Anstoß geben und das Bewusstsein für Cybersicherheit stärken". Ein kurzer twitter-Check ergibt immerhin eine Art Live-Berichterstattung des offiziellen Konferenz-Accounts (twitter), und Jimmy Schulz ist auch schon da (twitter).

Man kann den versammelten Managern nur wünschen, dass sie etwas differenzierter und sachkundiger an die Problematik herangeführt werden, als es Eugene Kaspersky tut. Da geht es los mit hoch entwickelten Schadprogrammen wie Stuxnet, Flame und Gauss, die "lebenswichtige Infrastrukturen sabotieren" können. Dabei führe die "Anonymität der Cyber-Waffen" dazu, dass nie sicher festgestellt werden kann, wer die Entwickler solcher Programme sind und es sogar dazu kommen kann, dass die Angreifer selbst zum Opfer der eigenen Waffen werden – Gefühle von Sicherheit: not available.

Erkennen die Regierungen die steigende Militarisierung des Internets nicht und einigen sie sich nicht darauf, "Cyber-Waffen" zu kontrollieren, werden diese "wahrscheinlich eines Tages in die Hände von Terroristen gelangen". Die können die "Cyber-Waffe" dann stehlen, kopieren und anpassen und "plötzlich [hält] irgendjemand eine neue Cyber-Waffe in der Hand". Dieses Szenario der unkontrollierbaren Weiterverbreitung ist doch weit hergeholt. Um die komplette Schadsoftware stehlen, kopieren und anpassen zu können,

bedarf es eines Crackers, eher aber eines Teams von Crackern, sowie auf der anderen Seite einer Sicherheitslücke in der Infrastruktur der Entwickler, die so groß ist, dass der Zugriff auf den Quellcode ermöglicht wird. “Details einer Cyber-Waffe”, wie Kaspersky es schreibt, ermöglichen Terroristen dies nicht. Ob die ganze Analogie überhaupt sinnvoll angewendet werden kann, ist zudem mehr als zweifelhaft:

> *Talking about cyber weapons does not change the fact that hacker tools are nothing like weapons. They are opportunistic and they are about outsmarting defenses, not about brute force. As a result, their effect is highly questionable and not controllable in a military sense. [Myriam Dunn Cavelty/Oliver Rolofs]*

Sein Vorschlag und die einzige “Möglichkeit, Cyber-Kriege abzuwehren”, ist eine internationale Kooperation. Da er vorher die weltweit identische Infrastruktur als einen der Hauptfaktoren für die Anfälligkeit von Cyber-Angriffen genannt hat, mutet es seltsam an, wenn er wenig später gemeinsame Spielregeln, Kontrollen und Maßnahmen zur Cyber-Sicherheit verlangt. Aber auch das kann weder Staaten noch privaten Haushalten und Firmen ausreichenden Schutz gewähren. Denn Schadprogramme können nicht nur von Terroristen gestohlen werden, sondern auch ganz von selbst außer Kontrolle geraten. Dann gelangen sie “über das Internet zu praktisch jedem Punkt der Welt”. Man kann sich laut Kaspersky auch am Samstagabend beim Grillen nicht sicher sein, ob auf dem USB-Stick mit den Fotos der Dienstreise im Libanon nicht auch ein Virus liegt, der sich dann vom heimischen Grill “exponentiell um den Globus ausbreiten und jeden treffen” kann. Somit wären wir dann beim titelgebenden “Angriff auf den Alltag” angelangt: Cyber-Waffen und USB-Sticks, Geheimdienstarbeit und Grillabende verschmelzen zu einer Bedrohung, der nichts und niemand entrinnen kann. Außer vielleicht mit Kasperskys Sicherheitssoftware.

Tags: Cyber Spionage, Cyberangriff, Cyberwar, msc, Sicherheitskonferenz

« Die Causa Hindenburg: Ein Lehrstück über Geschichtspolitik und umstrittene Identitäten
Pazifik anstatt Atlantik? Zur asiatisch-pazifischen Ergänzung der US Sicherheitspolitik »

Bislang keine Kommentare

Einen Kommentar hinterlassen

BELIEBT KOMMENTARE NEU

Hell yeah, it's Political Science! Wissenschaftliche Podcasts

Das Internet darf ein cyberfreier Raum sein

Deutschlands Irak-Politik – Verantwortung nach außen, Intransparenz nach innen.

Wir haben Geburtstag!

„Mit Sicherheit nicht!“ Sexuelle Gewalt als politisches Mittel

KATEGORIEN

Außenpolitik (59)
Bürgerkriege (16)
Cyber Security (40)
Demokratisierung (9)
Drohnen (15)
Humanitäre Interventionen (15)
Innere Sicherheit (24)
Interviews (10)
Katastrophen (4)
Konferenz (20)
Militär (27)
Pandemien (2)
Podcast (7)
Popkultur (20)
Sanktionen (8)
Security Culture (13)

Name

Email

Webseite

Kommentar

Geben Sie den Text ein.

reCAPTCHA

Bestätigen

Datenschutz - Nutzungsbedingungen

Kommentar senden

☑ Benachrichtige mich über nachfolgende Kommentare per E-Mail.

BLOGROLL

netzpolitik.org
shabka.org
Terrorismus in Deutschland
theorieblog.de
Verfassungsblog
Vom Bohren harter Bretter
whistleblower-net.de

ARCHIV

Wähle den Monat

Impressum |