Zeitschrift: ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift

Herausgeber: Schweizerische Offiziersgesellschaft

Band: 178 (2012)

Heft: 5

Werbung

Grosses Schadenpotenzial

Cyber-Angriffe beinhalten ein sehr grosses Schadenpotenzial. Sie sind bereits heute Bestandteil von kriegerischen Handlungen. Aus Mangel an genauen Angaben ist die Schweiz – wie zurzeit alle andere Länder auch – auf grobe Schätzungen über die Häufigkeit und das Potenzial von Cyber-Angriffen angewiesen. Die Tendenz in den letzten Jahren ist aber eindeutig und unbestritten: Vorfälle, bei denen Staaten, Unternehmen und Individuen via Datennetzwerke angegriffen und geschädigt werden, nehmen sowohl in ihrer Anzahl sowie ihrer Qualität zu. Die Fortschritte und die Professionalität der Täterkreise sowie die eingesetzten Mittel und damit die Gefährlichkeit der Angriffe nehmen ebenfalls zu.

«Cyber-Angriffe beinhalten ein sehr grosses Schadenpotenzial. Sie sind bereits heute Bestandteil von kriegerischen Handlungen.»

Es wäre irreführend, Angriffe auf IKT-Infrastrukturen nur als technisches Problem abzuhandeln. Es sind nicht bloss die Ziffern 0 und 1, die in Codezeilen verändert werden. Es werden Informationen und Werte gestohlen, kompromittiert oder zerstört; die Integrität und die Verfügbarkeit von Systemen wird eingeschränkt oder unterbrochen. Und wenn wichtige Infrastrukturen ausfallen, sind Menschen gefährdet. Ja, Cyber-Angriffe können sogar töten[7].

Cyber-Angreifer unterscheiden sich durch ihre Absichten und Auftraggeber. Es gibt keine a priori zivilen oder militärischen Akteure. Allen Akteuren stehen dieselben vielfältigen Methoden und Werkzeuge zur Verfügung und viele der benötigten «Waffen» sind bereits für wenig Geld im Internet zu haben. Andere «Waffen» hingegen werden von professionell organisierten Tätern (organisierte Kriminalität, Staaten) mit einem viel massiveren Aufwand und für präzise Verwendungen entwickelt. Da ein absoluter Schutz vor solchen Angriffen realistischerweise kaum zu erreichen ist, stehen reaktive Fähigkeiten zur Schadensbegrenzung und Wiederherstellung der Ausgangslage im Vordergrund. Der Phantasie sind keine Grenzen gesetzt, wenn es darum geht, neue Cyber-Angriffsmethoden zu finden!

Fazit

Cyber-Risiken sind real, nehmen stetig zu und gehören keiner besonderen Kategorie an. Um Cyber-Risiken effizient abzuwehren, bedarf es eines einheitlichen und koordinierten Vorgehens, unabhängig davon ob sie kriminell oder sicherheitspolitisch relevant sind, ob sie zivil oder militärisch, national oder international, privat oder öffentlich sind. Weil ein vollständiger Schutz vor Cyber-Angriffen nicht realistisch ist, sind ein effizientes Krisenmanagement und Reaktionsfähigkeiten mit hoher Verfügbarkeit unabdingbar. ■

1 Im Dezember 2010 rief die Hacker-Gruppe «Anonymous» zu einem Angriff auf PostFinance auf. Auslöser war die Schliessung des Postcheck-Kontos von Julian Assange, dem Gründer von WikiLeaks.
2 Seit Jahren wird zum Beispiel der Trojaner ZeuS eingesetzt; das Schadprogramm wird über gefälschte oder manipulierte Webseiten bei Privatpersonen eingeschleust, um Geld aus dem Online-Banking abzuzweigen.
3 Im Oktober 2009 wurde ein Spionagefall gegen das Eidgenössische Departement für auswärtige Angelegenheiten entdeckt; er gelangte via E-Mail in das Netzwerk und blieb lange unentdeckt.
4 Im Juni 2010 ging es um STUXNET; diese Schadsoftware erzeugte einen Softwarefehler in den Steuerungssystemen (SCADA) und beschädigte dadurch eine iranische Urananreicherungsanlage.
5 2008, während des Krieges zwischen Russland und Georgien, wurden die IKT-Infrastrukturen Georgiens massiv gestört. Diese Handlungen können als kriegerische Unterstützungsaktionen qualifiziert werden.
6 Terroristische Organisationen kennen und nutzen das Internet (Propaganda und Radikalisierung, Rekrutierung, Ausbildung, Beschaffung von Geldmitteln); obwohl hauptsächlich konventionelle Mittel verwendet werden, sind zukünftige Cyber-Angriffe durch Terroristen denkbar.
7 Wie der Bericht der Civil Aviation Accident and Incident Investigation Commission zeigte, könnte ein Trojaner im Zentralrechner der Spanair-Fluggesellschaft eine der Ursachen gewesen sein, welche 2008 den Absturz einer MD82 in Madrid verursacht hat.

Colonel EMG
Gérald Vernez
Géologue dipl UNIL,
MAS ETH SPCM
1580 Avenches