Cyber Defense der Schweiz : vor was muss sich die Schweiz schützen? Teil 1.

Autor(en): **Vernez, Gérald**

Objekttyp: **Article**

Zeitschrift: **ASMZ : Sicherheit Schweiz : Allgemeine schweizerische Militärzeitschrift**

Band (Jahr): **178 (2012)**

Heft 5

PDF erstellt am: **05.07.2024**

Persistenter Link: https://doi.org/10.5169/seals-309571

Cyber Defense der Schweiz – Vor was muss sich die Schweiz schützen? (1/4)

Am 10. Dezember 2010 beauftragte der Bundesrat das VBS, eine nationale Strategie für Cyber Defense auszuarbeiten. Die Strategie soll aufzeigen, wie Cyber-Risiken aussehen, wie die Schweiz sich dagegen rüstet, wo die Mängel liegen und wie diese am wirksamsten und effizientesten zu beheben sind.

Gérald Vernez

Einige Stimmen sagten: *«Dies ist kein militärisches Thema; das VBS hat hier nichts zu suchen.» Andere behaupteten: «Es handelt sich um ein rein technisches Problem und somit nur mit Computer-Freaks zu lösen», «Die Bekämpfung von Internetkriminalität hat nichts mit Cyber Defense zu tun», «Wir haben eine Software, die Sie zu 100 Prozent schützt», «Cyber Defense soll voraussichtlich auf internationaler Ebene gelöst werden», «Die Lösung liegt bei der Aufstockung der bestehenden Instrumente», «Kopieren Sie einfach die Strategie Deutschlands».* Diese Aussagen sind nicht alle falsch, aber im Lichte der komplexen Realität unserer Gesellschaft und der Cyber-Risiken kann damit keine vollständige, glaubwürdige und dauerhafte Lösung für unser Land ausgemacht werden.

Was sind Cyber-Risiken?

Wie werden Cyber-Risiken definiert? Welches sind die Schwierigkeiten, um eine nationale Cyber Defense Strategie zu definieren? Welches sind die Grundsätze einer effizienten Lösung? Wie sieht unsere Strategie aus? Antworten auf die erste Frage liefert dieser Artikel. In drei weiteren Kurzartikeln werden wir auf die weiteren Fragen eingehen. Damit sollen die Leserinnen und Leser befähigt werden, sich selbst ein Bild von Cyber Defense zu machen und zu verstehen, wo und wie sie betroffen sind und ihren Teil zur Lösung beitragen können und müssen.

Wie werden Cyber-Risiken definiert? Die Informations- und Kommunikationstechnologien (IKT) sowie die globale digitale Vernetzung haben Staat, Wirtschaft und Gesellschaft in den letzten drei Jahrzehnten grundsätzlich, weltweit und irreversibel verändert. Die erfolgten Fortschritte und die Gewinne dank IKT sind enorm. Die Medaille hat aber auch eine Kehrseite: die Gesellschaft wird von der IKT immer abhängiger und wegen deren Schwächen verletzlicher. Die Unübersichtlichkeit der dahinterliegenden Prozesse nimmt stetig zu; mit der Komplexität der Systeme nehmen auch deren Fehler- und Störanfälligkeit und die potenziellen Angriffsmöglichkeiten zu. Tatsache ist, dass moderne IKT-Systeme zahlreiche «Sicherheitslöcher» aufweisen und gleichzeitig das Wissen um deren eigene (Aus-)Nutzung sehr weit verbreitet ist. Störungen, Manipulationen und sogar Angriffe auf diese Infrastrukturen gehören zum Alltag und nehmen kontinuierlich zu. Die Möglichkeiten, die IKT zu missbrauchen oder zu beeinträchtigen, sind wie deren positive Nutzung praktisch unbegrenzt. Davon zeugt auch die tägliche Medienberichterstattung.

Bei einem Ereignis ist es oft sehr schwierig, die Ursache zu lokalisieren. Grundsätzlich können zwei Fälle unterschieden werden: *absichtlich verursachte Schäden* sowie *zufällige Vorfälle*. Im sicherheitspolitischen Bericht 2010 werden Risiken generisch als Sammelbegriff von B*edrohungen* und *Gefahren* verstanden.

Bedrohungen	Konflikt
	Terrorismus
	Sabotage
	Spionage
	Kriminalität
	Aktivismus
	Vandalismus
Gefahren	Vorfälle

Unter Gefahren im Cyberspace versteht man unvorhersehbare Ereignisse oder Unfälle wie Systemausfälle durch vorschnelle Abnützung, Überbeanspruchung, Fehlkonstruktion oder mangelhafte Wartung. Die Ursache kann ein Unfall sein, aber weit öfter ist es die Folge eines unprofessionellen oder fahrlässigen Verhaltens, wofür jemand die Verantwortung zu tragen hat, bis hin zu einer Strafverfolgung.

Bei den Bedrohungen stehen persönliche, kriminelle, terroristische, politische oder staatliche Motive im Vordergrund (vgl. Abbildung). In allen Fällen ist es natürlich die Umsetzung einer Absicht, die je nach ihrer Bedeutung, ihrer Intensität und ihrer Konsequenzen, Strafverfolgungs- und/oder sicherheitspolitische Relevanz haben kann.

Hinter Cyber-Angriffen verbergen sich verschiedenste Täterkreise und Motive: Es sind Einzeltäter mit beschränkten Mitteln und ohne Bereicherungsabsicht, Aktivisten[1] mit politischen Zielsetzungen, Kriminelle mit Betrugs-[2] oder Erpressungsabsichten, Wirtschaftsakteure, die Marktvorteile erzielen wollen, staatliche Spionage-[3] oder Sabotagedienste[4] oder Armeen[5], aber auch Terroristen[6], die den Staat und/oder die Gesellschaft stören und destabilisieren wollen. Die IKT ist für Angriffe nicht nur deshalb attraktiv, weil sie viele Möglichkeiten für Missbrauch, Manipulation und Schädigung bietet, sondern auch weil sie sich dafür billig, aus der Ferne, anonym und mit wenig Aufwand nutzen lässt. Dies ermöglicht es den meisten Tätern unerkannt und somit unbestraft zu bleiben, was sehr vorteilhaft ist.

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