SWISS CYBER STORM MEDIENMITTEILUNG

Für Rückfragen: Mark A. Saxer – 079 753 78 27

Bern – Zürich – Luzern, den 20. Juni 2013

It's Cyber Cold War!

Swiss Cyber Storm zeigt wesentliche Schwächen der Cyber-Sicherheit auf

Vor dem Hintergrund des NSA-Skandals in den USA tagte Mitte Juni in Luzern der Kongress „Swiss Cyber Storm". Arrivierte ICT-Experten und Entscheidungsträger diskutierten die Sicherheit im Cyber-Raum – um zum nüchternen Schluss zu kommen: „It's Cyber Cold War". Gleichzeitig massen sich junge Cyber-Talente in Challenges. Die Sieger fahren als Schweizer Delegation an den Cyber Alpen Cup. Ein Finalist erhielt aufgrund der Konferenz, die Entscheidungsträger und Talente in Kontakt bringen wollte, bereits ein Stellenangebot.

Spionagesoftware wird immer komplexer, zahllose Unternehmen sind nach wie vor ungenügend geschützt. Und wer weiss, wie suchen, der findet auch Flusskraftwerksteuerungen offen zugänglich im Netz – Swiss Cyber Storm 4 war dominiert von Schlaglichtern der globalen Unsicherheit.

Sitzen-Know-how und Industrialisierung

Costin Raiu, Direktor des globalen Research & Analysis Team von Kaspersky, eröffnete die Konferenz mit nüchternen, aber gleichzeitig aufrüttelnden Fakten: Sowohl Flame als auch Red October wüteten Jahrelang, bevor man sie auch nur entdeckte, und beispielsweise Flame sei mit seinen 20 MB Grösse „so komplex und raffiniert aufgebaut, sodass eine vollständige Analyse bis zu 10 Jahren in Anspruch nehmen würde."

Dass die Entwicklung und der Einsatz von derlei Schadprogrammen neben Spitzen-Fachwissen auch perfekte Organisation, ja Industrialisierung voraussetzen, bestätigte auch *Timo Steffens*, Vorstand des Nationalen Deutschen IT Lagezentrums und des CERT-Bunds: „Wir sehen Anzeichen dafür, dass gezielte Angriffe in Phasen wie Aufklärung, Infiltration und Datenbeschaffung respektive Datenabzug unterteilt werden, wobei in jeder Phase unterschiedliche hierzu spezialisierte Teams zum Zuge kommen."

…wobei es oft auch einfacher geht

Candid Wüest, Virenjäger bei Symantec, zeigte jedoch auf, dass längst nicht alle gezielten Angriffe ausgeklügelte Malware einsetzten. Trotzdem seien die meisten erfolgreich. Von den mehr als hundert täglich registrierten gezielten Angriffen auf Unternehmen zielten letztes Jahr 31 Prozent auf KMUs mit weniger als 250 Beschäftigten ab, die häufig nicht adäquat geschützt seien. Allerdings mache nicht die Malware den Unterschied zum Massenphänomen, sondern die Person hinter der Malware, die den Angriff mit viel Wissen steuere, so Wüest.

Diese Perspektive vertrat auch *John Matherly*, der 2009 die Geräte-Suchmaschine Shodan gründete. „Wissen Sie wie vielen Leuten Sie via ungeschützte Webcams in die Wohnung schauen können? Wahrscheinlich mehr Personen als Sie denken. Shodan , zeigt es ihnen – und sagt Ihnen auch gleich, über welche Website Sie die Haussteuerung übernehmen können". Die Suchmaschine zeigt aber noch mehr: Ein Krematorium, das sich über eine ungeschützte Webseite ebenso bedienen lässt wie eine Seilbahn, Windkraftwerke und ein Flusskraftwerk. Fazit: „Nicht vorhandenes Bewusstsein für Informationssicherheit" ist geradezu erschreckend verbreitet.

Entscheidungsträger und Talente vernetzen

Swiss Cyber Storm präsentierte sich mit der Nummer „4" erstmals in seinem neuen Gewand. Organisiert und durchgeführt vom hierzu eigens gegründeten Verein „Swiss Cyber Storm" wendete sich die Fachtagung an internationale Sicherheitsspezialisten – wobei sie das Ziel verfolgte, namhafte Entscheidungsträger und junge ICT-Talente zu vereinen und zu vernetzen. Die Konferenz wurde erstmals unter dem Patronat von MELANI (Melde- und Analysestelle Informationssicherung des Bundes) und Swiss Police ICT, einem privaten Verein zur Vernetzung von Strafverfolgung und ICT-Industrie, durchgeführt.

In dem von Compass Security zur Verfügung gestelltem Hacking-Lab konnten sich Schüler und Studenten ab April unentgeltlich an verschiedensten Aufgaben versuchen und sich für das Finale qualifizieren. Die zehn besten Teilnehmer wurden zum Swiss Cyber Storm 4 eingeladen um sich im Final zu messen – es wurde eine knappe Entscheidung. Eine Fünfergruppe wird die Schweiz nun Security Alpen Cup gegen Österreich vertreten. Besonders erfreulich: Ein Teilnehmer bekam infolge des Kongresses bereits ein Stellenangebot.

It's Cyber Cold War!

In der abschliessenden Podiumsdiskussion mit Costin Raiu, *Stefan Lüders*, dem ICT-Security Verantwortliche des CERN und dem chinesischen Blogger *Michael Anti* wurden der jüngst publizierte US-Abhörskandal um PRISM und die Diskussionen um „Cyber War" aufgegriffen. Anti war deutlich: „The Great Firewall of China", aber auch Überwachungssysteme wie PRISM opfern die Internet-Freiheit der Überwachung. Der Westen habe inzwischen jeden moralischen Vorsprung verspielt. Es fand sich auf dem Podium niemand, der widersprach. Die Diskussion verdeutlichte insgesamt, wie schwierig es ist, auf dem schmalen Grat zwischen Sicherheit und Freiheit Balance zu halten.

Dabei kam auch der omnipräsente, aber undefinierte Begriff „Cyber War" ins Spiel. Dass Klärungsbedarf besteht, waren sich alle Podiumsteilnehmer einig. Der gemeinsame Nenner war am ehesten: „It's Cyber Cold War". Unterschiedliche Konstellationen bedrohen unterschiedliche Ziele auf unterschiedliche Art – aber niemand kann sich die volle Eskalation leisten.

Swiss Cyber Storm
Der Verein Swiss Cyber Storm wurde Ende 2012 gegründet. Der Verein bezweckt die regelmässige Durchführung von Cyber-Security Fachveranstaltungen für Fachleute und Führungskräfte mit Fokus auf der Swiss Cyber Storm Konferenz. Er ist nicht Gewinn-orientiert. Präsident ist ZHAW-Dozent Bernhard Tellenbach.

■