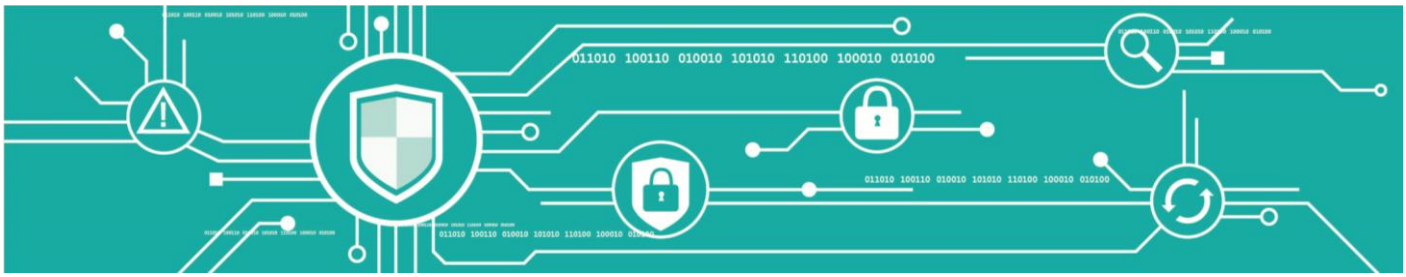

Wenn der kalte Cyber-Krieg heiss wird, ist das Internet am Ende

Stell dir vor, es ist Cyber-Krieg und alle machen mit

Hinter den Kulissen findet seit vielen Jahren ein Wettrüsten der Cyber-Waffen statt – der kalte Krieg des Internet-Zeitalters. Gesehen hat die Öffentlichkeit davon immer nur kleinste Ausschnitte – anhand von extrem ausgefeilten, massgeschneiderten Cyber-Waffen wie Stuxnet, die chirurgisch präzise einzelne Infrastrukturen angegriffen haben. Im Falle von Stuxnet beispielsweise das iranische Atomprogramm.

Bei Stuxnet und ähnlich präzisen Cyber-Waffen hatten die Angreifer kein Interesse an der breitflächigen Verbreitung der Schadsoftware, denn das hätte nur die Chance auf ihre Entdeckung vergrössert. Weniger zielgenaue Cyber-Waffen wie gross angelegte Distributed-Denial-of-Service-Angriffe (DDoS), die breitflächig Internet-Infrastruktur lahmlegen, sind langfristig viel gefährlicher. Statt chirurgisch präziser Angriffe und der Spionage an individuellen Einrichtungen gehen DDoS-Angriffe mit roher Gewalt vor und überfluten die Opfer mit sinnlosen Anfragen, was ganze Server-Netzwerke in die Knie zwingt. Dadurch wird das Internet insgesamt in Mitleidenschaft gezogen.

Alles, was DDoS-Angreifer dafür benötigen, sind riesige Bot-Netzwerke aus mit dem Internet verbundenen Geräten. Es ist nicht schwer, solche Netzwerke zu rekrutieren – Millionen von Geräten, die am Netz hängen, sind schlecht oder gar nicht abgesichert. Bei einigen billigen IP-Kameras made in China ist beispielsweise sogar das allgemein bekannte Standard-Passwort hardwareseitig festgelegt und lässt sich nicht ändern.

DDoS: schon Anfänger" können grosse Schäden anrichten

Leicht lassen sich die Angriffe so konfigurieren, dass die Anfrageflut von verschiedenen gefälschten IP-Adressen zu kommen scheint, was die Abwehr des Angriffes erschwert.

Trotz der häufig relativ geringen technischen Kenntnisse innerhalb dieser Milieus sind die Schäden von DDoS-Angriffen schon heute enorm. Die wenigstens davon sind sichtbar. Wer sich unter Betreibern grösserer Webauftritte umhört, weiss, dass regelmässige DDoS-Angriffe zum Alltag vieler System-Administratoren gehören. Oft ist dabei völlig unklar, warum sie passieren. In den meisten Fällen halten die Server stand – auch wenn jeder DDoS-Angriff Kosten verursacht, allein durch den höheren Datenverbrauch im Rechenzentrum.

Wenn schon technisch oft nicht besonders versierte Kriminelle und Skript-Kiddies in der Lage sind, ein solches Internet-Erdbeben auszulösen, bekommen wir eine Ahnung davon, wozu staatliche Angreifer in der Lage wären, sollte der kalte von Spionage und Sabotage geprägte Cyber-Krieg einmal heiss werden. Ausgeschlossen ist das nicht: Nach dem Hack von E-Mails der Demokratischen Partei in den USA, hinter der die US-Regierung staatliche russische Hacker vermutet, drohte das Weisse Haus ganz offen mit dem Einsatz einer solchen Cyber-Waffe auf Russland als Racheakt.

Ein Cyber-Weltkrieg wäre das Ende des offenen globalen Internets

Die grundlegende Natur des Internets macht ein Eskalations-Szenario leider wahrscheinlich. Damit das Internet als das grosse, innovative und demokratische Medium, das es ist, funktioniert, muss jeder Teilnehmer Daten senden und empfangen können. Als offenes Netz, an dem grundsätzlich jedes Gerät teilnehmen kann, wird das Internet damit immer verwundbar für solche Angriffe bleiben.

Die USA wären vermutlich schon heute in der Lage, weite Teile der Internet-Infrastruktur eines riesigen Landes wie Russland oder China lahmzulegen. Es ist anzunehmen, dass die Antwort auf einen solchen Cyber-Angriff nicht lange auf sich warten lassen würde. Das globale Internet würde als Kollateralschaden zwei sich bekriegender Nationen vermutlich schnell aufgrund der Last der Daten zusammenbrechen. Nur Abschottung und Ausschliessen grosser IP-Adressbereiche böte dann noch Schutz – das Internet würde fragmentiert, in viele kleine Netze zerbröseln.
Ein Cyber-Erstschlag, wie er von den USA kürzlich öffentlich angedroht wurde, könnte daher das Ende des Internets bedeuten, wie wir es kennen.

Ist die Eskalationsspirale staatlicher DDoS-Angriffe erst einmal in Gang gesetzt, gibt es es kaum einen Weg zurück zu einem globalen Internet. Daher wäre es nun wichtig, dass sich die Uno-Staaten endlich zu Regeln und Einschränkungen beim Einsatz von Cyber-Angriffen verpflichten. Kommt ein internationaler DDoS-Krieg erst einmal in Gang, kann es schon zu spät sein.

Rittmeyer AG
6341 Baar, Schweiz
T +41 41 767 10 00, F +41 41 767 10 70
security@rittmeyer.com, www.rittmeyer.com/itsecurity