LOAD e.V. – Verein für liberale Netzpolitik

Weil Angriff nicht die beste Verteidigung ist

Zur Notwendigkeit einer defensiven Cybersicherheitsstrategie

Policy Brief

LOAD Policy Brief

Weil Angriff nicht die beste Verteidigung ist

Zur Notwendigkeit einer defensiven Cybersicherheitsstrategie

"Die Gefährdungslage ist weiterhin hoch. Im Vergleich zum vorangegangen Berichtszeitraum hat sie sich weiter verschärft und ist zudem vielschichtiger geworden." So beschreibt das Bundesamt für Sicherheit in der Informationstechnik (BSI) die Lage der IT-Sicherheit in Deutschland. Vor diesem Hintergrund ist es begrüßenswert, dass es eine verstärkte mediale Berichterstattung zum Thema gibt. Der positive Nebeneffekt ist ein verbessertes Problembewusstsein in der Wirtschaft und bei den Bürgerinnen und Bürgern. Die Politik – genauer: die Bundesregierung – ist nicht untätig und stimmt laut Recherchen aktuell Details zur Cyberabwehr ab. Deutschland müsse offensive Cyberabwehr betreiben, die im Falle eines Angriffs einen Gegenschlag (sogenannter „Hackback“) ermöglichen soll.

Es ist müßig darüber zu sinnieren, welche Behörden und Ministerien im Falle eines Cyberangriffs bei der Lagebeurteilung einbezogen werden müssten und ob am Ende des Tages das Militär, eine Polizeibehörde oder der Bundesnachrichtendienst (BND) für die Ausführung von Hackbacks zuständig sein sollte. Auch ist es nicht zielführend, juristische Debatten darüber zu führen, ab welchem Punkt die hohen verfassungsrechtlichen Hürden für den Einsatz deutscher Streitkräfte erfüllt wären. Stattdessen muss Deutschland eine strikt defensive Cybersicherheitsstrategie verfolgen und sich auf europäischer und internationaler Ebene für die Ächtung digitaler Waffen und für eine strategische Autonomie im Hardwarebereich einsetzen.

LOAD verurteilt den Einsatz und die Bereitstellung offensiver Wirkmittel im Cyberraum. Wir setzen uns ein für eine strikt defensive Cybersicherheitsstrategie. Dafür gibt es mehrere Gründe:

Kollateralschäden nicht absehbar

Auch die versiertesten Hackerinnen und Hacker schreiben Code, der nicht intendierte Folgen haben kann. Niemand kann ausschließen, dass bei komplexen Cyberoperationen nicht Schäden an den Systemen unschuldiger Personen oder Institutionen verursacht werden. Selbst vermeintlich erfolgreiche Cyberoperationen, wie die Stuxnet-Attacke auf das iranische Atomprogramme, hatten massive Nebenwirkungen. Tausende weitere Steuersysteme wurden weltweit infiziert. Auch aktuelle hochgerüstete Schadprogramme wie bspw. TRITON oder INDUSTROYER funktionieren nicht hundertprozentig genau.

Computerprogramme (im Falle eines Hackbacks: Malware als digitale Waffe) haben keine Hände, Ohren oder Augen. Eine digitale Waffe, die sich auf einem System frisch wiederfindet, hat daher große Schwierigkeiten festzustellen, wo sie sich befindet, was das System für eine Aufgabe hat oder gar in welchem Land das System steht. Daher lässt sich keine zielgenaue Cyberwaffe bauen.

Gefahr für zivile kritische Infrastruktur

Da es nach aktuellem Stand der Technik technisch ausgeschlossen ist, sicher zu bestimmen, von welchen Systemen ein Angriff ausgegangen ist, muss davon ausgegangen werden, dass ein Gegenangriff immer auch kritische zivile Infrastruktur – beispielsweise Energie-, oder Wasserversorgung, Krankenhäuser oder Katastrophenschutz – treffen könnte. Kriegerische Handlungen gegen zivile Infrastruktur sind durch verschiedene internationale Vereinbarungen bereits

geächtet. Sowohl die Zusatzprotokolle der Genfer Konvention als auch die deutlich ältere Haager Landkriegsordnung untersagen Angriffe auf zivile Infrastruktur im weiteren Sinne.

Da die Definition kriegerischer Handlungen aber auch hoffnungslos veraltet ist, sollte Deutschland sich auf internationaler Ebene für eine *Digitale Genfer Konvention* einsetzen. Der erste Schritt zur Verbesserung der Cyberabwehr wäre zu definieren, was tatsächlich einen Cyberangriff einer ausländischen Macht darstellt, im Gegensatz zu einem bloßen Streich eines jugendlichen Hackers oder einer Industriespionage. Daran anknüpfend können politische Sanktionen entwickelt werden.

Digitale Abschreckung funktioniert nicht

Wie beim Gleichgewicht des Schreckens im Kalten Krieg argumentieren Befürworter offensiver Cyberoperationen heute, dass die Möglichkeit digitaler Vergeltungsschläge abschreckend auf potentielle Angreifer wirken würde. Abschreckung und Konfliktfähigkeit – die Möglichkeit glaubhaft zu drohen – im digitalen Raum funktionieren aber nicht analog zum Kalten Krieg, als die Arsenale der beiden Großmächte, zum Beispiel durch Militärparaden, vorgeführt und dadurch bekannt waren. Staaten werden es tunlichst vermeiden, einen für die globale Öffentlichkeit sichtbaren Test digitaler Waffen durchzuführen. Ganz im Gegenteil werden sie sogar darum bemüht sein, beispielsweise die neuesten Zero-Day-Exploits so geheim wie möglich zu halten, da diese Schwachstellen sonst geschlossen werden oder der Gegner diese gegen einen selbst richten könnte. Daher funktioniert Abschreckung im digitalen Raum nicht.

Nach jedem erfolgreichen Einsatz einer Digitalwaffe ist die zugrundeliegende Schwachstelle dem Gegner bekannt und kann sogar von ihm selbst eingesetzt werden. Sowohl Angreifer wie Angegriffener werden nach einem Digitalwaffeneinsatz versuchen, die eigenen Systeme gegen diese Waffe abzusichern.

Die Zivilgesellschaft und Unternehmen haben diese Gelegenheit nicht, da die digitale Waffe von beiden Konfliktstaaten weiterhin geheim gehalten werden würde. Selbst wenn also die Konfliktteilnehmer sich absichern könnten – die Zivilgesellschaft und die nicht-staatlichen Infrastrukturen können weder vor Kollateralschäden, noch vor direkten Angriffen geschützt werden.

Attribution von Angriffen nicht möglich

Hackerinnen und Hacker sind Meister der Verschleierung und verwischen ihre Spuren, indem sie Dinge wie gefälschte IP-Adressen und von anderen Staaten entwickelte Hacking-Tools verwenden. Es ist auch sehr schwierig bis unmöglich, sicher zu sein, dass ein Computer, der hinter einem Angriff zu stecken scheint, nicht selbst gehackt wurde und nur zur Verschleierung der Herkunft des Angriffs genutzt wird. Es kann daher nie vollständig ausgeschlossen werden, dass bei einem Hackback die falschen Systeme ins Visier genommen werden. Ein digitaler Vergeltungsschlag verbietet sich daher.

Vulnerabilites Equities Process schafft Unsicherheit

Länder wie Großbritannien oder die Vereinigten Staaten haben bereits einen sogenannten "Vulnerabilites Equities Process" (VEP) implementiert. Andere Staaten, wie zum Beispiel Deutschland, denken darüber nach, dies zu tun. Ein VEP ist ein Prozess, in dem ein staatliches Gremium entscheidet, ob ihm bekannt gewordene Sicherheitslücken an den Hersteller gemeldet oder zurückgehalten werden. Die Geheimhaltung hat den Zweck, dass diese Sicherheitslücken nicht behoben werden, sondern den Sicherheitsbehörden zur Ausnutzung und Infiltration von betroffenen Systemen erhalten bleiben. Ein solches Vorgehen – vermeintlich im Namen der nationalen Sicherheit – führt weder für den Staat noch für die Wirtschaft oder die Zivilgesellschaft zu einem höheren Sicherheitsniveau. Stattdessen werden die Überwachung und Infiltration von Computersystemen durch Behörden und Kriminelle vereinfacht.

Wir sind der Meinung, dass Sicherheitslücken, sobald diese bekannt werden, unbedingt und ausnahmslos gemeldet und durch den Hersteller sofort behoben werden müssen. Da es teilweise mehrere Jahre dauern kann, bis die entwickelten Softwareaktualisierungen, die die Sicherheitslücke beheben, überall aufgespielt sind, können die Sicherheitsbehörden diese Lücken über entsprechende Zeiträume nutzen, wenn es für diese Maßnahme eine richterliche Anordnung gibt. Ein VEP ist kein Mittelweg zwischen Offensive und Defensive, sondern ein Prozess, bei dem Wirtschaft und Zivilgesellschaft dauerhaft Bedrohungen ausgesetzt werden.

Wer klug ist, beugt vor: Eine defensive Cybersicherheitsstrategie

Eine offensive Cybersicherheitsstrategie wird die in sie gesetzten Hoffnungen nicht erfüllen und im schlimmsten Fall zu umfangreichen Kollateralschäden führen. Stattdessen sollte Deutschland eine strikt defensive Cybersicherheitsstrategie wählen. Dazu bedarf es unter anderem folgender Maßnahmen:

Kluge Investitionen in Bildung

Wir wissen, dass unsere digitalen und kritischen Infrastrukturen bisher nicht ausreichend geschützt werden und fordern daher, deren IT-Umgebungen nach dem Prinzip *„Security by Design“* zu gestalten. Dies schützt proaktiv gegen Angriffe aus dem Cyberraum und stärkt die digitale Resilienz. Alle IT-Fachkräfte müssen konstante Security-Weiterbildungen erhalten, um auf dem aktuellen Stand der Technik zu bleiben. So können wir nachhaltig den Wirtschaftsstandort durch weltbeste IT-Sicherheit stärken. Dies gilt nicht nur im Bereich des Betriebs sondern auch in der Entwicklung und der Gestaltung sicherer IT-Umgebungen. Dazu fordern wir in allen Informatikstudiengängen die IT-Sicherheit zu behandeln und die Einführung weiterer Lehrstühle mit Schwerpunkt auf IT-Sicherheit.

Einsatz für Digitalwaffensperrvertrag

Sollte nationale Gesetzgebung in Kraft treten, die Hackbacks ermöglicht, werden weitere Staaten ermutigt, ihre eigenen Gesetze darauf anzupassen. Einige Staaten sind dadurch versucht, es weitaus einfacher zu machen, auf vermeintliche Cyberattacken offensiv zu reagieren. Das würde die Eintrittswahrscheinlichkeit für eine Cyberkatastrophe erhöhen. Deutschland sollte sich stattdessen für ein internationales Abkommen einsetzen, das jegliche offensive Wirkmittel im digitalen Raum als Digitalwaffen (D-Waffen) einstuft und diese im Rahmen eines Digitalwaffensperrvertrags international verbietet. Weiterhin sind wir der Meinung, dass Deutschland mit gutem Beispiel voran gehen sollte und solche Waffen weder entwickeln noch einsetzen darf. Die geplanten Gesetzesänderungen zum Einsatz offensiver Wirkmittel im Cyberraum, an denen das BMI arbeitet, dürfen nicht durchgeführt werden.

Europäische Anstrengung für digitale Souveränität!

In Zeiten des politischen Systemwettbewerbs und vor dem Hintergrund bestehender Abhängigkeiten unserer Lieferketten ist es umso wichtiger digitale Souveränität herzustellen. Europa ist im Vergleich zu China und den USA im Bereich Software und Hardware nicht konkurrenzfähig. Nur durch gemeinsame europäische Zusammenarbeit, nach dem Vorbild von Erfolgsgeschichten wie CERN oder Airbus, können wir Wettbewerbsfähigkeit herstellen und Souveränität gewinnen. Aufgrund mangelnder Konkurrenzfähigkeit im Bereich von Hard- und Software droht Europa seine digitale Souveränität vollständig zu verlieren. Es bedarf einer gemeinsamen europäischen Zusammenarbeit für die eigenständige Entwicklung von Hard- und Software, insbesondere für sicherheitsrelevante Infrastrukturkomponenten.

Aktiv werden, um die Defensive zu stärken

Wir erkennen an, dass die Grenze zwischen offensiven und defensiven Technologien schwer definierbar und je nach Situation auch fließend sein kann. Wir denken, dass Maßnahmen wie zum Beispiel das Umleiten von Datenverkehr, das temporäre Blockieren einzelner Anschlüsse, von denen Angriffe ausgehen, oder die Analyse des Datenverkehrs um zum Beispiel DDoS-Angriffe zu blockieren, als defensive Maßnahmen zählen. Auch die Separierung von ganzen Netzsegmenten mit dem Zweck der Entstörung der Netze stellt in diesem Kontext eine defensive Maßnahme dar.

Ein wichtiges Kriterium zur Einschätzung, ob eine Maßnahme der Cyberabwehr noch defensiv oder schon offensiv ist, ist in unseren Augen die Frage der Geheimhaltung. Muss ein Wirkmittel geheim gehalten werden, um seine volle Wirkung zu entfalten? Wenn ja, dann ist diese Maßnahme in unseren Augen offensiv und abzulehnen.

Gerade noch defensive Maßnahmen sind beispielsweise der Einsatz von Schwachstellen-Scannern wie zum Beispiel nmap oder nessus, oder der Einsatz von Exploit-Frameworks wie Metasploit oder Kali, da diese Frameworks lediglich öffentlich bekannte Exploits verwenden, gegen die aktuell gehaltene und gepflegte Systeme immun sein sollten.

Wir wissen, dass manche Werkzeuge aus dem Bereich der IT-Sicherheit einen Dual-Use-Charakter haben. Daher wollen wir die Illegalität an die Notwendigkeit der Geheimhaltung des Wirkmittels, aber auch an die Intention der Handlung knüpfen, indem entsprechende Gesetze wie zum Beispiel §§ 202a bis 202d StGB (sogenannte „Hackerparagraphen", „Abfangen und Ausspähen von Daten“ und „Datenhehlerei“) angepasst werden.

Genau wie bei B- und C-Waffen kann es unter Umständen notwendig sein, D-Waffen zu entwickeln, damit man eine Verteidigung dagegen aufbauen kann. Bei B- oder C-Waffen wären dies zum Beispiel Schutzkleidung, Medikamente, Gasmasken etc. Bei D-Waffen bestünde diese Verteidigung beispielsweise aus Patches, Intrusion-Detection und Firewallregeln.

In unseren Augen ist eine klare Grenzüberschreitung das unbefugte Ausführen von Software auf fremden Systemen, mit dem Ziel der Spionage, Datenausleitung oder Schädigung der Funktion des Systems. Diese Maßnahmen sind bereits durch das IT-Grundrechte-Urteil des Bundesverfassungsgerichts untersagt. Grundrechte gelten auch im Internet. Auch BGP-Hacks (Manipulation des Routing von Datenpaketen), mit dem Ziel, nationale Netze zu stören oder zu infiltrieren oder Angriffe auf Certificate Authorities sollten von der internationalen Staatengemeinschaft geächtet werden.

Was darf die Bundeswehr?

Die Leitungsebenen im Bundesministerium des Inneren und im Bundesministerium der Verteidigung möchten die Bundeswehr zu einer Cyber-Truppe weiterentwickeln, die auch im Cyberraum militärisch aktiv wird. Ein Tätigwerden der Bundeswehr setzt allerdings voraus, dass die hohen verfassungsrechtlichen Hürden für den Einsatz deutscher Streitkräfte erfüllt sind. Die Bundeswehr ist durch unser Grundgesetz eine reine Verteidigungsarmee. Zentral ist hier Art. 87a GG, der vorschreibt, dass die Streitkräfte außer zur Verteidigung nur dann eingesetzt werden dürfen, soweit es das Grundgesetz ausdrücklich zulässt. Die in den Ministerien diskutierten Szenarien, bei denen ein Hackback angebracht wäre, entsprechen aber nicht den Kriterien, die im Grundgesetz für den Verteidigungsfall festgeschrieben wurden. Aufgrund dieser hohen verfassungsrechtlichen Vorgaben gibt es auch Überlegungen Computer Network Operations (CNO) – das präemptive Infiltrieren von Systemen, um Informationen zu sammeln oder Backdoors zu installieren – durch den BND vorbereiten zu lassen, beziehungsweise dem BND diese Erlaubnis zu geben.

LOAD lehnt die Schaffung von rechtlichen Möglichkeiten zum Einsatz der Bundeswehr im Cyber- und Informationsraum ab. Auch der BND darf solche Kompetenzen nicht bekommen, denn wenn bereits eine Parlamentsarmee keine offensiven Wirkmittel im Cyber- und Informationsraum einsetzen darf, gibt es keinen Grund diese Kompetenz einem Nachrichtendienst zukommen zu lassen.

LOAD verurteilt den Einsatz und die Bereitstellung jeglicher offensiver Wirkmittel im Cyberraum. Wir setzen uns ein für eine strikt defensive Cybersicherheitsstrategie, denn Angriff ist nicht die beste Verteidigung.

Quellen

Herpig, Sven (2018): Hackback ist nicht gleich Hackback. Stiftung neue Verantwortung, Juli 2018

Schulze, Matthias (2019): Überschätzte Cyber-Abschreckung. Stiftung Wissenschaft und Politik

Schulze, Matthias (2019): Governance von 0-Day-Schwachstellen in der deutschen Cyber-Sicherheitspolitik. Stiftung Wissenschaft und Politik

Zimmermann, John (2019): Cyberabwehr in Deutschland. Wissenschaftliche Dienste des Deutschen Bundestages, WD 2 – 3000 – 090, 19, August 2019

Danksagungen

Unser Dank geht an die Mitglieder von LOAD e.V., die dieses Papier ehrenamtlich und in Ihrer Freizeit nicht nur erarbeitet, sondern auch umfassend mit allen anderen Mitgliedern diskutiert haben.

Vielen Dank auch an die Arbeitsgruppe kritische Infrastruktur für die Impulse und das Feedback. http://ag.kritis.info

Autoren

Ruben Dieckhoff (@rdieckhoff) , Johannes Rundfeldt (@ijonberlin)

Impressum

LOAD e.V. – Verein für liberale Netzpolitik
Reinhardtstraße 5
10117 Berlin

Vorsitzende: Ann Cathrin Riedel

info@load-ev.de
www.load-ev.de

Stand: September 2019