IFSH
Institut für Friedensforschung
und Sicherheitspolitik
an der Universität Hamburg

Offensive Cyber-Operationen: digitalen Angriffen proaktiv begegnen

Cyber-Angriffe aus Russland und China nehmen zu. Immer mehr Staaten ergänzen daher ihre defensive Abwehr im virtuellen Raum mit offensiven Komponenten. Operateure dringen dabei in Friedenszeiten in gegnerische IT-Systeme ein, um das Vorgehen von Angreifern zu antizipieren und Schutzmaßnahmen zu ergreifen. Damit es dabei nicht zu unbeabsichtigten Eskalationen kommt, sollten offensive Cyber-Operationen

- nur unter strengen ethischen Gesichtspunkten durchgeführt werden, vorab die Risiken abwägen und nicht automatisiert, sondern kontrolliert ablaufen,
- sich in Friedenszeiten nicht gegen zivile kritische Infrastruktur des Gegners richten,
- von einer Einsatzdoktrin begleitet werden, die zuvor öffentlich gemacht wurde, und
- Informationen zur Härtung eigener und alliierter IT-Systeme generieren.

03|24

MATTHIAS SCHULZE | 2024

Viele Staaten entwickeln als Reaktion auf russische und chinesische Cyber-Spionage und Sabotage gegen ihre kritischen Infrastrukturen offensive Cyber-Fähigkeiten. Dabei dringen IT-Sicherheitsfachleute lange vor einer zu erwartenden Attacke in die Systeme potenzieller Angreifer ein. Dort beobachten sie das gegnerische Verhalten und entwickeln konkrete Schutzmaßnahmen. Die so gewonnenen Erkenntnisse sollten genutzt werden, um die IT-Sicherheit unter westlichen Alliierten zu stärken. Demokratien sollten allerdings Cyber-Operationen in Friedenszeiten begrenzt einsetzen und ihre Einsatzdoktrinen veröffentlichen.

OFFENSIVE CYBER-STRATEGIEN AUF DEM VORMARSCH

Staaten nutzen heute Cyber-Angriffe, um Macht in der internationalen Politik auszuüben. Russland nutzt Cyber-Operationen im Ukrainekrieg zur politischen Aufklärung, zur Begleitung konventioneller Einsätze und um den Westen psychologisch zu beeinflussen. China setzt Cyber-Spionage ein, um systematisch High-Tech-Wissen aus dem Westen zu stehlen. Dies verschafft dem Land Vorteile im internationalen Wettbewerb. Beide Staaten infiltrieren mit gestiegener Intensität kritische Infrastrukturen, um im Falle einer konventionellen Auseinandersetzung mit dem Westen Sabotageakte durchzuführen.

Bisher reagierten die meisten Staaten darauf mit defensiven Maßnahmen, d. h. damit, die eigenen IT-Systeme zu „härten“ und resilient gegenüber solchen Angriffen zu machen. Viele erwägen nun auch offensive Maßnahmen. Hierbei dringen Operatoren in gegnerische IT-Systeme ein, beobachten dort den Gegner über lange Zeit und stören seine Angriffssysteme. Finnland, Schweden, Dänemark, die Niederlande und Polen diskutieren aktuell, erstmals offensive Fähigkeiten in Friedenszeiten zu nutzen, ebenso wie Indien, die Ukraine und Kanada. Die USA, Großbritannien und Frankreich bauen ihre schon vorhandenen offensiven Strategien weiter aus. Auch Japan entwickelt zum ersten Mal eine offensive Cyber-Strategie und stellt ein neues Cyber-Kommando mit 4000 Dienstposten auf. In Deutschland hat trotz einiger politischer Ansätze noch kein solcher Strategiewandel stattgefunden.

„MIT DEM KAMPAGNENANSATZ LÄSST SICH GEGNERISCHES ANGRIFFSVERHALTEN BESSER ANTIZIPIEREN.“

KONSTANTE BEOBACHTUNG

Zudem hat sich der Charakter offensiver Cyber-Strategien gewandelt. Bislang haben viele westliche Staaten eine Form der Cyber-Abwehr betrieben, bei der offensive Techniken nur ad hoc und als Reaktion auf einen Angriff eingesetzt wurden. Gegnerische Angriffssysteme werden dabei gestört, um im Idealfall bereits laufende Attacken aufzuhalten. Bei dieser, auch als „aktive Cyber-Abwehr“ geläufigen Methode kommen offensive Elemente nur bei „besonders schwerwiegenden“ Cyber-Attacken als Strafmaßnahme und als letztes Mittel zum Einsatz. In der Praxis hat sich dies aber als ineffizient erwiesen. Cyber-Operationen benötigen oft mehrere Wochen Vorlauf. Zudem verfügen Angreifer heute in der Regel über redundante, virtualisierte Infrastruktur. D. h. einzelne Angriffssysteme auszuschalten bringt wenig, da Angreifer diese schnell auswechseln können. Schwerwiegende Angriffe sind zudem selten. Häufiger treten viele kleine und niedrigschwellige Angriffe ein und desselben Akteurs auf, die aber einen logischen Bezug zueinander haben.

Inspiriert von den Erfahrungen der USA übernehmen immer mehr Länder den Ansatz des „konstanten Kontakts“. Statt ad hoc auf laufende Angriffe zu reagieren, dringen Operateure dabei proaktiv in gegnerische Angriffssysteme ein, um das Verhalten von Angreifern an der Quelle zu beobachten. Dies erfolgt langfristig, kontinuierlich und systematisch – d. h. die aus vielen, einzelnen und kleineren Cyber-Operationen des Gegners gesammelten Erkenntnisse werden zusammen betrachtet. Man spricht hier auch von einem „Kampagnenansatz“.

WISSEN, WIE DER ANGREIFER VORGEHT

Durch das kampagnenartige Vorgehen lässt sich gegnerisches Angriffsverhalten besser antizipieren. Denn Cyber-Angreifer nutzen oft vorhersehbare Angriffsroutinen, automatisierte Skripte und favorisierte Tools. Durch langfristiges psychologisches und technisches „Profiling and Fingerprinting“ werden ihre Aktionen vorhersehbarer. Auch kann gegnerische Angriffssoftware, die sich noch in der Entwicklung befindet, gegebenenfalls direkt auf den Angriffssystemen gescannt werden. Über Detektionsregeln und sogenannte „Threat Intelligence Feeds“ kann die Signatur an das IT-Sicherheitspersonal in Behörden oder privaten Unternehmen weitergeleitet werden, damit dieses sie dann aufspürt. Offensive und defensive Cyber-Abwehr müssen hier eng zusammenarbeiten. Wenn das Wissen um Angriffsmuster und forensische Spuren des Gegners nicht schnellstmöglich mit der eigenen Verteidigung und mit Alliierten geteilt wird, ist nichts gewonnen.

DAS ZIEL: GEGNERISCHE GEWINNE VEREITELN

Ziel des Kampagnenansatzes ist nicht mehr die Abschreckung. Konsequenzen anzudrohen, um den Gegner davon zu überzeugen, von Angriffen abzulassen, funktioniert im Cyber-Raum kaum. Denn zahlreiche Sicherheitslücken machen Angriffe leicht und kostengünstig. Für den Gegner sind die Gewinne aus Cyber-Operationen, etwa Diebstahl geistigen Eigentums, daher meist größer als die Konsequenzen, die er zu befürchten hat. Statt Cyber-Angriffe also vollends verhindern zu wollen, geht es im Kampagnenansatz darum, dem Gegner die Gewinne zu verwehren. Sind Angreifer etwa auf sensible Daten aus, dann werden ihnen manipulierte Daten untergeschoben, aus denen sich kein nachrichtendienstlicher Gewinn ziehen lässt. Sollen Hintertüren platziert werden, können diese durch Isolation ins Leere geführt werden, was sie weitgehend nutzlos macht.

„OFFENSIVE UND DEFENSIVE CYBER-ABWEHR MÜSSEN ENG ZUSAMMENARBEITEN.“

VERANTWORTUNGSVOLLE CYBER-OFFENSIVE

Das Ziel von Cyber-Sicherheit muss langfristig sein: nämlich die vielen Sicherheitslücken in Hard- und Software zu schließen. Wenn aber immer mehr Demokratien nun ebenfalls offensive Cyber-Operationen einsetzen, sollte dies zumindest kontrolliert erfolgen. Dazu gehört die technische Begrenzung: Um Kollateralschäden und Kaskadeneffekte zu verhindern, sollten Cyber-Operationen zielgerichtet, auf konkrete Zielsysteme maßgeschneidert und vor dem Einsatz in Testumgebungen simuliert werden. Auf automatisierte Verbreitungsmechanismen wie „Würmer” sollte verzichtet werden. Daneben kann das „Targeting“ begrenzt werden: Verantwortungsvolle Cyber-Operationen sollten nur auf gegnerische Angriffssysteme abzielen, nicht aber auf zivile und vor allem kritische Infrastruktur. Im bewaffneten Konflikt gelten die Regeln des humanitären Völkerrechts. Die Operationsführung sollte interdisziplinär sein und neben einer juristischen Einschätzung eine politische Risiko- und

Eskalationsanalyse sowie eine technische Analyse der Folgen umfassen. Wichtig ist zudem, dass aus eigener Cyber-Offensive gesammelte Spuren in die Defensive eingespeist werden. Die Offensive muss im Dienst der Defensive stehen!

Westliche Staaten, die offensive Cyber-Operationen durchführen, sollten sich untereinander austauschen. Multilaterale Foren können helfen, Zielkonflikte zu bearbeiten, so dass sich Alliierte nicht gegenseitig behindern. Offensive Operationen sollten von einer Kommunikationsstrategie begleitet werden, die sich an Alliierte und Partner richtet. Gegenüber dem Gegner können Post-Hoc-Notifikationen als vertrauensbildende Maßnahme eingesetzt werden. Zur Kommunikation und Transparenz gehört schließlich auch, dass Staaten ihre Cyber-Doktrinen, in denen sie definieren, nach welchen Kriterien die eigenen Cyber-Operationen durchgeführt werden, veröffentlichen. Dänemark, Frankreich und Großbritannien können hier als Vorbilder dienen. Schließlich sollten sich europäische Staaten, etwa im Rahmen der EU oder der NATO, auf einheitliche Regeln für Cyber-Operationen verständigen.

OFFENSIVE CYBER-OPERATIONEN: KEIN ERSATZ, ABER SINNVOLLE ERGÄNZUNG

Offensive Strategien ersetzen nicht die solide Investition in defensive Cyber-Sicherheit, können sie aber ergänzen und effektiver machen. Damit sie nicht einer Entgrenzung von Angriff und Gegenangriff Vorschub leisten, müssen sie verantwortungsvoll, transparent und kooperativ gestaltet werden.

ÜBER DEN AUTOR

Dr. Matthias Schulze ist Leiter des Forschungsschwerpunkts „Internationale Cybersicherheit“ am Institut für Friedensforschung und Sicherheitspolitik an der Universität Hamburg (IFSH). Vor seiner Tätigkeit am IFSH war er stellvertretender Leiter der Forschungsgruppe Sicherheitspolitik an der Stiftung Wissenschaft und Politik (SWP). Er ist promovierter Politikwissenschaftler, Cybersicherheitsexperte und Host des Podcast „Perception.de“.

ÜBER DAS PROJEKT

Der Forschungsschwerpunkt Internationale Cybersicherheit erforscht Cyber-Konflikte und ist vom Auswärtigen Amt finanziert.
Die Projektwebsite lautet: https://international-cybersecurity.com/

Gefördert vom:

Auswärtiges Amt

ÜBER DAS INSTITUT

Das Institut für Friedensforschung und Sicherheitspolitik (IFSH) erforscht die Bedingungen von Frieden und Sicherheit in Deutschland, Europa und darüber hinaus. Das IFSH forscht eigenständig und unabhängig. Es wird von der Freien und Hansestadt Hamburg finanziert.

Gefördert von:

Hamburg | Behörde für Wissenschaft, Forschung, Gleichstellung und Bezirke

DOI: https://doi.org/10.25592/ifsh-policy-brief-0324

IFSH – **Institut für Friedensforschung und Sicherheitspolitik** an der Universität Hamburg
Beim Schlump 83 20144 Hamburg Germany Phone +49 40 866077-0 ifsh@ifsh.de www.ifsh.de