Krieg ohne Cyber

Diskrepanz zwischen erwarteten und tatsächlichen Cyberattacken im Ukraine-Krieg

Ende Februar marschierte Russland in die Ukraine ein. Die Vorhersagen, dass massive Cyberangriffe den Beginn der Invasion einleiten, haben sich nicht bestätigt. Wird die Bedrohung durch Cyberattacken überschätzt?

Von Keywan Tonekaboni

Russland hat seinen Krieg gegen die Ukraine weitestgehend konventionell begonnen, mit Raketenbeschüssen und einem Truppeneinmarsch. Die prognostizierten großflächigen Cyberattacken, die den vorrückenden Truppen einen strategischen Vorteil verschaffen sollten, blieben großteils aus und die kritische Infrastruktur in der Ukraine funktionierte in den ersten Tagen der Invasion offenbar. Vorhersagen, Russland könnte mit Cyberattacken die Kommunikation zwischen ukrainischer Regierung und Bevölkerung abschneiden, sind nicht eingetreten. Präsident Selenskyj und sein Stab inszenierten sich erfolgreich medial via Videoclips.

Zwar gab es Berichte über die Malware HermeticWiper, welche am Vorabend der Invasion auf ukrainischen Computern anfing, Daten zu löschen. Nach allem, was man bisher weiß, war die Auswirkung allerdings nicht sonderlich groß. Daneben fanden nur primitive DDoS-Attacken und Webseiten-Defacements statt, auch gegen russische Einrichtungen, die manche Medien mit ausgeklügelten Cyberattacken in einen Topf warfen.

Trotzdem bleibt die Sorge, der Krieg in der Ukraine könnte zu Cyberattacken auf IT-Systeme in der EU oder weltweit führen. So warnte das Bundesamt für Sicherheit in der Informationstechnik (BSI) vor einer erhöhten Gefährdungslage. Zeitgleich mit der Invasion gab es beim Satellitennetzwerk KA-SAT einen Ausfall, wovon auch die Fernüberwachung von Tausenden Windenergieanlagen betroffen war. Laut Reuters vermutet Betreiber Viasat einen Cyberangriff. Es gibt zudem Befürchtungen, Russland könnte auf die verabschiedeten Sanktionen mit Cyberattacken als Gegenmaßnahme reagieren.

Hacktivismus

Russland wurde aber auch selbst Ziel von Cyberangriffen. Die ukrainische Regierung rief eine IT-Armee aus Freiwilligen aus. Auf einem Telegram-Kanal mit mehr als 250.000 Abonnenten wurden Ziele genannt, die wohl vorwiegend auch nur per DDoS angegriffen wurden. Auch das lose Hacking-Kollektiv Anonymous erklärte Russland den „Cyberkrieg“. Beides wird von diversen Experten kritisch gesehen und ist für Beteiligte nicht ungefährlich (siehe Interview). Außerdem lässt Russland diese Angriffe teilweise ins Leere laufen, indem es Aufrufe aus dem Ausland nicht oder nur verlangsamt bedient.

Die Cybergang Conti stellte sich dagegen auf die russische Seite, woraufhin ein offenbar darüber erzürntes Mitglied interne Chats und Daten der vergangenen Jahre veröffentlichte. Das dürfte für die zivile Cybersicherheit vermutlich bedeutender sein als für den Fortlauf des Konfliktes.

NBC News berichtete, in Washington überlege man, auf die russische Invasion mit Cyberattacken zu reagieren. Das wäre bemerkenswert, da US-Präsident Biden selbst davor gewarnt hatte, Cyberangriffe könnten zu einem Krieg eskalieren. Die Sprecherin des Weißen Hauses widersprach denn auch dem Bericht.

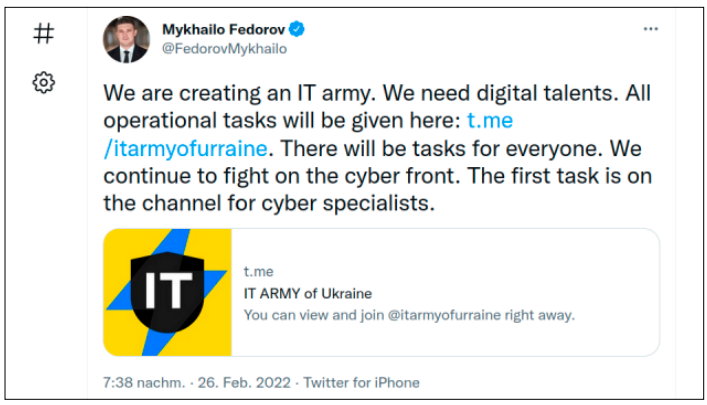
Überschätzte Cyberoperationen

Es gibt aber auch Zweifel, ob gezielte Attacken ohne Weiteres ausführbar sind oder die gewünschten Effekte hätten. „Es gibt eigentlich keine Cyberwaffen“, meint der Politikwissenschaftler Lennart Maschmeyer, der zu Cybersicherheit an der ETH Zürich forscht. „Die Idee ist zwar da, hat aber nichts damit zu tun, wie Cyberangriffe funktionieren.“

Im Unterschied zu klassischen Waffen seien Cyberwaffen auf Schwachstellen ihrer Ziele angewiesen und könnten nur den Schaden anrichten, den das angegriffene System selbst ermöglicht. „Die Mittel existieren nicht unabhängig von den Zielen“, betont Maschmeyer. Zudem beschränkt die Gefahr, den Zugang durch Updates oder Enttarnung zu verlieren, die Wahl des Einsatzzeitpunktes. Dadurch beeinflussen sich bei Cyberoperationen Geschwindigkeit, Intensität und Kontrolle gegenseitig negativ.

Auch der Begriff Cyberkrieg sei fehl am Platz, so Maschmeyer: „Cyberoperationen sind nicht-kriegerische Geheimdienstoperationen und folgen einer eigenen Logik, die mehr der Arbeitsweise von Spionen ähnelt.“ Der Wissenschaftler hat Cyberangriffe der letzten Jahre auf die Ukraine untersucht. Seiner Analyse nach sind deren Effekte geringer als angenommen. Eine Ausnahme bilde die Schadsoftware NotPetya, welche in der Ukraine und international erheblichen Schaden verursachte, aber auch Russland selbst traf.

Seine strategischen Ziele sah Russland mit Cyberoperationen wohl nicht erreichbar, wie nicht zuletzt der reale Krieg in der Ukraine zeigt. *(ktn@ct.de)* c't



Der ukrainische Minister für digitale Transformation, Mykhailo Fedorov, ruft auf Twitter zur Teilnahme an der IT-Armee auf.

„Eine zentralistische Cyberabwehr kann nicht alles schützen.“

Nach dem russischen Angriff auf die Ukraine fordern Sicherheitspolitiker verstärkt den Aufbau offensiver Cyberfähigkeiten in Deutschland. Dr. Sven Herpig, Themenfeldleiter für internationale Cybersicherheitspolitik bei der Stiftung Neue Verantwortung (SNV), plädiert dagegen im c’t-Interview eher für eine breite, zivile Cybersicherheit.

Bild: Sebastian Heise

Dr. Sven Herpig ist Experte für internationale Cybersicherheitspolitik.

c’t: Ukrainische Behörden haben Freiwillige in aller Welt aufgerufen, sich an Cyberattacken gegen Russland zu beteiligen. Halten Sie es für sinnvoll, dabei mitzumachen?

Dr. Sven Herpig: Nein. Natürlich könnten Freiwillige irgendwelche Ziele in Russland ärgern, aber das wird weit weg sein von kriegsentscheidend. Gleichzeitig ist es aus drei Gründen ziemlich gefährlich. Zum einen, weil sich die Personen, die sich daran beteiligen, selbst in das Fadenkreuz der Russen bringen. Zum anderen könnten einzelne dieser Operationen überhaupt nicht im Sinne der Ukraine sein oder auch die Bevölkerung in Russland treffen, die größtenteils nichts für diesen Konflikt kann.

Drittens: Solche freien Hacker dringen wahrscheinlich in Systeme ein, die wenig geschützt sind. Bei denen muss man davon ausgehen, dass zum Beispiel ukrainische oder westliche Nachrichtendienste bereits drin sind. So könnte die russische Seite erfahren, dass sie diese Systeme nicht ausreichend geschützt hat. Damit kann man indirekt die Zugänge von Nachrichtendiensten verbrennen, auf deren Seite man ja eigentlich steht.

c’t: Wie ist Deutschland in Bezug auf seine Cyberabwehr aufgestellt? In der Vergangenheit zeigten Cyberattacken von Kriminellen die Verwundbarkeit.

Herpig: Aktuell lautet die Frage, inwiefern die cyberkriminellen Gruppen, die vielleicht noch erbeutete, aber nicht abgearbeitete Zugänge in bestimmte Organisationen haben, diese priorisieren. Bei mehreren parallel auftretenden Vorfällen, zum Beispiel in Krankenhäusern, sind die staatlichen Ressourcen zur Unterstützung relativ schnell erschöpft.

c’t: Was müsste getan werden, um den Schutz zu verbessern?

Herpig: Ich denke, wir müssen subsidiär besser werden. Eine zentralistische Cyberabwehr kann nicht alles schützen. Man kann viel über Gesetzesänderungen sprechen oder über mehr Ressourcen für das BSI. Aber im Endeffekt müssen wir in der Breite besser werden. Wir brauchen mehr Mobile Incident Response Teams (MIRT), auch in den Bundesländern, die bei gleichzeitigen Vorfällen direkt vor Ort unterstützen. Auch im Bereich Kommunen müssen wir weitaus mehr tun.

c’t: Es gibt Stimmen, die fordern, die Bundeswehr zur bundesweiten Cyberabwehr einzusetzen.

Herpig: Ich bin der Meinung, dass eine zivile Cybersicherheit ausreichend ist. Die Bundeswehr soll ihre eigenen Systeme schützen, damit sind sie schon beschäftigt genug.

c’t: Warum sind Sie für eine zivile Cyberabwehr?

Herpig: Weil der zivile Bereich historisch gewachsen relativ stark aufgebaut ist. Er genießt mehr Vertrauen in der Breite der Organisationen, Firmen und der Bevölkerung. Aber auch, weil ein Großteil von Cyberoperationen nicht während eines Verteidigungsfalls stattfindet. Spionage, Sabotage, Überwachung und vor allem Cyberkriminalität sind alltägliches Geschäft. Ich halte es für völlig ungeeignet, das Militär daranzusetzen, wie es die USA teilweise machen. Das Militär ist nicht dazu da, um sich mit Cyberkriminellen herumzuschlagen oder Wirtschaftsspionage abzuwehren.

c’t: Wie bewerten Sie Forderungen danach, offensive Kapazitäten aufzubauen, also Cyberattacken oder Hackbacks?

Herpig: Für Cyberoperationen flankierend zu Auslandsmandaten gibt es schon eine Rechtsgrundlage. Der Bereich Hackback, also zum Beispiel das Degradieren von Fähigkeiten in ausländischen Netzen, ist ein komplexes Thema. Es kann Grenzfälle geben, wo eine offensive Cyberoperation vereinzelt zu einem temporären taktischen Erfolg führt. In fast allen Anwendungsfällen sind wir aber weitaus besser aufgestellt, wenn wir die wenigen vorhandenen Ressourcen, wie Fachkräfte, dafür einsetzen, um unsere Systeme abzusichern.

c’t: Brauchen wir offensive Cyberfähigkeiten nicht zumindest als Abschreckungspotenzial?

Herpig: Ich habe wenige bis keine Szenarien gesehen, wo Cyberoperationen abschreckende Wirkung haben. Gerade, wenn wir hier über eine Zeitenwende sprechen und Deutschland sich mit neustem Militär-Equipment ausstatten will. Das hat wahrscheinlich mehr abschreckende Wirkung, wenn man denn an Abschreckungstheorien glaubt. Die beste Abschreckung im Cyberraum bleibt weiterhin, dass die Gegner ihre taktischen Ziele nicht erreichen können. Und deswegen sollten wir auch daran arbeiten.