INTERGLOBAL

CYBERKRIEG IM INTERNET

Hacken bis zum Sieg

Enno Park

Im Internet folgt die Kriegsführung anderen Spielregeln als auf dem Schlachtfeld. Eine dieser Regeln lautet: Cyberkrieg ist immer offensiv, auch wenn er der Verteidigung dienen soll. Bei Angriffen kommt es auch zu Kollateralschäden, wie im Februar in Luxemburg.

Am Morgen des 24. Februar 2022 fiel die Steuerung von bis zu 5.800 Windenergieanlagen in Mitteleuropa aus. Die meisten davon standen in Deutschland, aber auch Luxemburg war davon betroffen (siehe unseren Artikel „Windenergie: Nicht erpressbar, aber hackbar“ in woxx 1674). Die Ursache war ein Ausfall des Satellitensystems KA-SAT, das die Anlagen mit dem Internet verband, über welches sie ferngesteuert werden. Der Schaden hielt sich in Grenzen: Die Windräder liefen bis zur Behebung des Fehlers für einige Wochen in einem Automatikmodus und versorgten die Bevölkerung durchgängig mit Strom.

Doch dass sich dieser Zwischenfall gleichzeitig mit der Invasion russischer Truppen in der Ukraine ereignete, war kein Zufall. Vielmehr handelte es sich um einen gezielten Angriff russischer Hacker, der auf das ukrainische Militär abzielte. Denn auch dieses nutzt KA-SAT, nur eben zur Steuerung von Waffensystemen und zur Kommunikation. Dass außer den ukrainischen Truppen noch viele andere KA-SAT-Kunden betroffen waren, war ein Kollateralschaden.

Der Cyberangriff auf KA-SAT war bei weitem nicht der einzige in diesem Krieg. Es gab mehrere sogenannte Wiper-Attacken auf ukrainische Behörden und staatsnahe Unternehmen. Dabei wird Schadsoftware auf Geräte losgelassen, die sämtliche Daten einschließlich Anwendungen und Betriebssystem löschen (englisch: to wipe), um die betreffenden Computer unbrauchbar zu machen. Außerdem gab es eine große Zahl sogenannter DDoS-Attacken. Das Kürzel steht für „distributed denial of service“; dabei wird der Zielrechner – beispielsweise ein Server, der wichtige Websites beherbergt – mit einer so großen Zahl von Anfragen bombardiert, dass er unter der Last zusammenbricht und vorübergehend ausfällt.

Hinzu kamen gezielte Angriffe auf ukrainische Websites, um Falschinformationen zu verbreiten und die Bevölkerung zu verwirren. Die ukrainischen Behörden berichten auch von einigen missglückten oder vereitelten Anschlägen. So versuchte die Hackergruppe „Sandworm“, die den russischen Geheimdiensten zugeordnet wird, vergeblich, Umspannwerke des ukrainischen Stromnetzes abzuschalten.

An solche Angriffe auf Infrastruktur denken viele zuerst, wenn sie den Begriff „Cyberkrieg“ hören, dabei sind sie relativ selten und aus militärischer Sicht auch nicht sehr wirkungsvoll. So nimmt ein per Schadsoftware lahmgelegtes Stromnetz kaum Schaden und lässt sich relativ schnell und einfach wieder in Betrieb nehmen. Wirkungsvoller ist dagegen die „kinetische Einwirkung“ auf die Infrastruktur. Das ist Militärjargon für die Zerstörung mit Bomben, Raketen oder Geschützen.

Cyberattacken schaffen viel Unsicherheit, weil es für sie noch keinen allgemein anerkannten Platz in der Hierarchie der Gegenschläge gibt.

Cyberattacken dienen meistens eher dazu, die Kommunikationssysteme des Gegners zu stören und ihn so in seiner Handlungsfähigkeit einzuschränken. Der Angriff auf KA-SAT hatte deshalb vermutlich aus russischer Sicht hohe strategische Bedeutung, auch wenn sich nachträglich kaum einschätzen lässt, wie stark die ukrainischen Streitkräfte durch ihn beeinträchtigt waren.

Nicht zu unterschätzen ist die psychologische Wirkung von Cyberangriffen. Sie können demoralisierend wirken, weil sie das Gefühl vermitteln, der Gegner sei schon da, auch wenn seine Truppen noch sehr weit entfernt sind. Eine Cyberattacke dient auch als Drohgebärde und Machtdemonstration, wie etwa 2007 in Estland. Dort kam es wegen des Umsetzens eines russischen Denkmals wochenlang zu Cyberattacken auf Behörden, Banken und Medienhäuser. Es gab Hinweise, die auf russische Hacker hindeuteten, allerdings dementierte die russische Regierung, an den Attacken beteiligt gewesen zu sein. Schließlich wurde in Estland ein estnischer Staatsbürger angeklagt. Ein Konflikt zwischen Russland und der Nato konnte so vermieden werden.

Cyberkrieg ist ein relativ neues Phänomen, das den Militärstrategen Kopfzerbrechen bereitet, weil es die etablierten Spielregeln des Krieges ändert. Bei kriegerischen Auseinandersetzung gibt es eine teils informelle, teils in öffentlichen Militärstrategien festgehaltene Hierarchie, eine Abstufung der Reaktionen auf Angriffe unterschiedlicher Art. Sie wurde geschaffen, damit ein begrenzter Angriff nicht sofort zu einem Atomkrieg eskaliert. Auch wenn es Unterschiede bei der Bewertung von gewissen Angriffen geben mag, wird beispielsweise kein Land gleich die gegnerische Hauptstadt bombardieren, nur weil es zu einem kleinen Grenzgefecht gekommen ist.

Hier schaffen Cyberattacken viel Unsicherheit, weil es für sie noch keinen allgemein anerkannten Platz in dieser Hierarchie gibt. Da Cyberatta-

Die Abwehr von Cyberangriffen bedient sich immer derselben Methoden, egal ob militärische oder kriminelle Ziele hinter einer Attacke stehen: Sie sollte daher als Teil des Zivilschutzes allen gesellschaftlichen Bereichen zur Verfügung stehen.

FOTO: EPA/RITCHIE B. TONGO

cken bislang vergleichsweise geringe Schäden verursachen, sollten sie weit unten stehen und für sich genommen keine militärische Antwort rechtfertigen. Doch viele Länder behalten sich einen Militärschlag als Reaktion auf Cyberangriffe vor oder lassen die Frage offen - gemäß dem Kalkül, dass die Unsicherheit Gegner davon abhält, solche Angriffe zu verüben.

Auch die Vorstellung ist verbreitet, man könne Cyberangriffe mit Cyberangriffen vergelten, also sozusagen einfach zurückhacken. Diese Vorstellung ist falsch, weil Cyberangriffe völlig anders funktionieren als herkömmliche Kriegsführung. Truppen können ein Ziel auf einen Befehl hin beschießen, aber sie können es nicht von jetzt auf gleich hacken. Das erfordert langfristige Vorbereitung. Der Zugang zu gegnerischen Computern muss in mühsamer Kleinarbeit erlangt werden, die Wochen oder Monate dauern kann. Dabei dringt man oft nicht gezielt in ausgewählte Systeme ein, sondern einfach in alle, die aufgrund einer Sicherheitslücke verwundbar sind.

Es ist also meist entweder Zufall oder das Ergebnis von Monaten, manchmal Jahren gezielter Vorbereitung, wenn beispielsweise Zugriff auf die Steuerungsrechner von Umspannwerken oder Kraftwerken besteht. Und dieser Zugang kann jederzeit verlorengehen, wenn die Systemadministratoren Updates einspielen, die die Sicherheitslücken schließen. Kommt es zum Angriff, kann es sein, dass zahlreiche Rechner ausfallen, aber ausgerechnet diejenigen nicht, die eigentlich Ziel der Attacke waren. Cyberangriffe sind also eine langwierige Angelegenheit mit unsicherem Ausgang.

Das bedeutet auch, dass Cyberattacken nicht der Verteidigung dienen können. Gegenschläge erfordern, dass die Cyberkrieger lange vor Beginn eines Konflikts in die Rechner ihrer Gegner eindringen, um angreifen zu können, wenn es so weit ist. Ein solches Vorgehen ist aber nicht defensiv. Das ist wahrscheinlich vielen Politikern nicht klar, die eine entsprechende Aufrüstung ihrer Streitkräfte fordern.

Cyberabwehr hingegen ist keine militärische Tätigkeit, sondern eher mit den Aufgaben eines technischen Hilfswerks oder des Katastrophenschutzes vergleichbar. Systeme absichern, Schadsoftware entfernen, Eindringlinge ausschließen und Backups einspielen sind Tätigkeiten aus dem Bereich der IT-Security, die immer gleich aussehen, egal ob ein Computersystem Ziel einer Cyberattacke, nur Kollateralschaden einer solchen oder Opfer krimineller Erpresserbanden war. Meinte man es ernst mit dem rein defensiven Charakter der Cyberabwehr, müsste man also, statt eine Armee um „Cybertruppen" zu erweitern, eine Art Cyberhilfswerk schaffen, das allen gesellschaftlichen Bereichen zur Verfügung steht.

Eine problematische Idee ist es übrigens, selbst in den Cyberkrieg zu ziehen, wie einige Hacker das im Kontext des Kriegs in der Ukraine unter dem Label „Anonymous" taten - so sympathisch diese subversiven Aktionen auch wirken mögen. Die Cyberattacken von „Anonymous" beschränkten sich überwiegend auf ein paar DDoS-Angriffe auf russische Server. Einigen gelang es, die Streams russischer Fernsehsender mit eigenen, gegen den Krieg gerichteten Inhalten zu ersetzen, was allerdings die allermeisten Russen gar nicht bemerkt haben dürften, weil sie noch über Kabel, Antenne oder Satellit fernsehen.

Solche nicht mit den kriegsführenden Parteien koordinierten Aktionen könnten jedoch auch fälschlich als Angriff eines Landes und im Extremfall als dessen Kriegseintritt gewertet werden. Wer an solchen Aktionen teilnimmt, kann außerdem theoretisch den Status eines Zivilisten einbüßen und zumindest aus Sicht russischer Behörden zum Kombattanten werden.

Der Journalist Enno Park beschäftigt sich mit dem digitalen Wandel und dessen Auswirkungen auf die Gesellschaft.

woxx - déi aner wochenzeitung / l'autre hebdomadaire, früher: **GréngeSpoun** - wochenzeitung fir eng ekologesch a sozial alternativ - gegründet 1988 - erscheint jeden Freitag · **Herausgeberin:** woxx soc. coop. · **Redaktion:** Joël Adami *ja* (joel.adami@woxx.lu), Karin Enser *cat* (karin.enser@woxx.lu), Thorsten Fuchshuber *tf* (thorsten.fuchshuber@woxx.lu), Richard Graf *rg* (richard.graf@woxx.lu), Susanne Hangarter *sh* (susanne.hangarter@woxx.lu), Tessie Jakobs *tj* (tessie.jakobs@woxx.lu), Raymond Klein *lm* (raymond.klein@woxx.lu), Isabel Spigarelli *is* (isabel.spigarelli@woxx.lu), Florent Toniello *ft* (florent.toniello@woxx.lu), Fabienne Wilhelmy *fw* (fabienne.wilhelmy@woxx.lu). Unterzeichnete Artikel und Grafiken geben nicht unbedingt die Meinung der Redaktion wieder. Die Redaktion behält sich Kürzungen vor. · **Verwaltung:** Martine Vanderbosse (admin@woxx.lu) · **Bürozeiten:** Mo. - Do 9 - 13 Uhr · **Druck:** c. a. press, Esch · **Einzelpreis:** 2,50 € · **Abonnements:** 52 Nummern kosten 103 € (Ausland zzgl. 32 € Portokostenbeteiligung); Bezug als PDF 97 €; Student*innen und Erwerbslose erhalten eine Ermäßigung von 48 € · **Gratis Testabos** siehe abo.woxx.lu · **Konto:** CCPL IBAN LU18 1111 1026 5428 0000 (Neu-Abos bitte mit dem Vermerk „Neu-Abo"; ansonsten Abo-Nummer angeben, falls zur Hand) · **Anzeigen:** Tel. 29 79 99-10; annonces@woxx.lu · **Recherchefonds:** Spenden für den weiteren Ausbau des Projektes auf das Konto CCPL IBAN LU69 1111 0244 9551 0000 der „Solidaritéit mat der woxx" sind stets erwünscht. Bitte keine Abo-Gelder auf dieses Konto · **Post-Anschrift:** woxx, b.p. 684, L-2016 Luxemburg · **Büros:** 51, av. de la Liberté (2. Stock), Luxemburg · **E-Mail: Redaktion -** woxx@woxx.lu; Veranstaltungshinweise - agenda@woxx.lu · **URL:** www.woxx.lu · **Tel.** (00352) 29 79 99-0 · **Fax:** 29 79 79