

Krieg in der Ukraine



Ein bewaffneter Verteidiger der Ukraine trägt in Kiew eine Guy-Fawkes-Maske, Erkennungszeichen des Hackerkollektivs Anonymous. Foto: AFP

Hacker eilen den Ukrainern zu Hilfe

Krieg im Cyberspace Russische Netzkämpfer greifen die ukrainische Verwaltung, das Parlament und Banken an. Nun schlagen Hacker zurück – und legen die Kreml-Website und Propagandaportale lahm.

Mathias Born

Im Schweizer Cyberspace ist es ruhig. Aussergewöhnlich ruhig. Derzeit gibt es kaum Probleme mit Ransomware. Derweil toben in der Ukraine heftige Kämpfe.

Zwischen der entspannten Situation im Schweizer Netz und dem Krieg gibt es einen direkten Zusammenhang: Die meisten virtuellen Angriffe der vergangenen Jahre hatten ihren Ursprung in Russland und der Ukraine. Viele Leute, die sich bislang als Erpresser verdingten, wurden in den Cyberkrieg eingezogen oder werden für die Verteidigung gebraucht.

Der Krieg findet längst auch im Cyberspace statt. Wenige Tage bevor die ersten Panzer die Grenze querten, nahm die Kadenz der virtuellen Angriffe auf die Ukraine zu. Mit sogenannten «Distributed Denial of Service»-Angriffen, bei denen Zentralrechner mit Anfragen bombardiert werden, versuchten russische Angreifer, die Infrastruktur der Verwaltung, des Parlaments und von Banken lahmzulegen, die Kommunikation zu stören und Bankgeschäfte zu unterdrücken.

Damit sollten die Menschen in der Ukraine verunsichert und die Kommunikation erschwert werden. Entdeckt wurde zudem eine Schadsoftware namens «Hermetic Wiper», mit der Daten auf infizierten Rechnern gelöscht werden sollten.

Inwieweit die Kommunikationsinfrastruktur des Landes durch gezielte physische oder digitale Angriffe in Mitleidenschaft gezogen wurde, ist schwer abzu-

«Wir müssen mit Kollateralschäden rechnen.»

Mathias Fuchs, Infoguard

schätzen. Im Moment scheinen die Strom- und Telekommunikationsnetze zuverlässiger zu funktionieren als befürchtet.

Derweil formiert sich im Internet der Widerstand. Die Ukraine bittet in Hackerforen um Unterstützung in der Cyberabwehr und für Cyberangriffe auf russische Einrichtungen. Das internationale Hackerkollektiv Anonymous führte erste Angriffe durch, etwa auf das Propagandamedium «Russia Today».

Auch die Websites des Kreml, des Verteidigungsministeriums und des Parlaments sollen zeitweise lahmgelegt worden sein. Interne Dokumente eines Waffenherstellers wurden veröffentlicht. Am Sonntag meldeten die Hacker, dass ein russisches Telekommunikationsunternehmen erfolgreich attackiert worden sei.

Damit hatte man in Russland offenbar gerechnet. Deshalb wird umgesetzt, was bereits vor Jahren geprobt wurde: Russland koppelt die wichtigste Infrastruktur vom Internet ab und lässt lediglich lokale Anfragen durch. Im Propagandakrieg blockiert Russland zudem soziale Netzwerke wie Facebook und Twitter zumindest teilweise.

«Kriege werden heute hybrid geführt», sagt Nicolas Mayencourt, Geschäftsführer des Sicherheitsunternehmens Dreamlab Technologies und Mitorganisator des Fachkongresses Swiss Cyber Security Days. Noch vor dem physischen Angriff werde versucht, den Gegner zu destabilisieren: mit Zensur und Desinformationskampagnen in den sozialen Medien, mit Störmanövern im Cyberspace, vereinzelt aber auch mit weitaus aufwendigeren gezielten Angriffen auf kritische Infrastrukturen.

Viel Geld – und Straffreiheit

Russland sei eine Cyber-Supermacht – wie die USA und China auch, sagt Mayencourt. «All diese Länder machen von ihren Möglichkeiten rege Gebrauch – in Friedens- wie in Kriegszeiten.» Im Kriegsfall kann Russland auf ein Heer von sehr fähigen, praxiserprobten Fachkräften zurückgreifen. Während sich etwa die Cyberkrieger aus den USA weitgehend mit Trockenübungen begnügen müssen, sind jene aus Russland zivil häufig im kommerziellen Spionage- und Erpressungsgeschäft tätig. Bis der Geheimdienst und die Armee sie kurzfristig einziehen.

«Das organisierte Verbrechen rekrutiert seine Leute beim Militär sowie beim Geheimdienst – und umgekehrt», sagt Mathias Fuchs, Leiter der Abteilung Investigation & Intelligence beim Schweizer Unternehmen Infoguard. Auch er weist darauf hin, dass es in Russland sehr viele Fachkräfte in diesem Bereich gibt.

Das Geschäft mit den Cybererpressungen floriert, weil es sehr viel Geld zu verdienen gibt. Und weil man in Russland kaum Gefahr läuft, für solche Attacken zur Rechenschaft gezogen zu werden. Verfolgt werden einzig Angriffe auf die heimische Infrastruktur. Alle anderen Angriffe werden zumindest toleriert.

Wie gefährlich ist es für ein Land wie die Schweiz, sich mit einer Cyber-Supermacht wie Russland anzulegen? «Wer sich stark exponiert, muss mit Attacken rechnen», sagt Nicolas Mayencourt. Als beispielsweise bekannt wurde, dass das Labor Spiez untersucht, wie der Doppelagent Sergei Skripal in Grossbritannien vergiftet worden war, begannen heftige Angriffe auf die Forschungseinrichtung.

In der Schweiz ist die Lage bis auf einige interne Scharmützel, etwa als die Website der «Weltwoche» wegen einer Polemik über die SRF-Korrespondentin Luzia Tschirky lahmgelegt wurde, bislang ruhig. Das bestätigt Florian Schütz, der Delegierte des Bundes für Cybersicherheit. «Die Situation kann sich jedoch je nach Verlauf der Geschehnisse ändern.» Im Fall von Sanktionen in der Region haben, sollten spezielle Vorsicht walten lassen.»

ren könnte. «Speziell exponiert wären wahrscheinlich Behörden und Finanzinstitute.» Schütz warnt vor Trittbrettfahrern: «Es besteht die Gefahr, dass kriminelle Akteure weltweit den Fokus auf die Vorgänge in der Ukraine nutzen, um vermehrt aktiv zu werden.»

Problem ungezielte Angriffe

Auch Mathias Fuchs von Infoguard erwartet keine unmittelbaren Angriffe auf die Schweizer Informatikinfrastruktur. Weitaus stärker gefährdet seien die USA und Grossbritannien. «Sogar die Russen haben keine unerschöpflichen personellen Ressourcen», sagt er. «Die Fachleute werden im direkten Krieg eingesetzt.»

Es ist aber durchaus möglich, dass die Schweiz die Folgen des Cyberkriegs indirekt zu spüren bekommt. Etwa, falls sich Schadsoftware, die gegen die unmittelbaren Feinde gerichtet ist, unkontrolliert vermehrt – wie es 2017 beim Verschlüsselungstrojaner NotPetya passiert ist. Es sei auch denkbar, dass eine Kriegspartei Systeme zur Energieversorgung lahmlege, etwa Teile der europäischen Gasinfrastruktur, sagt Fuchs. «Wir müssen mit Kollateralschäden rechnen.»

Ähnlich tönt es beim Bund: «Das Nationale Zentrum für Cybersicherheit schätzt aktuell vor allem ungezielte Angriffe als möglich ein, die sich als Nebeneffekt von den Cyberoperationen ereignen», sagt Schütz. «Firmen, die Abhängigkeiten zu Lieferanten oder Nearshoring-Partnern in der Region haben, sollten spezielle Vorsicht walten lassen.»

Telecomfirmen und ÖV bieten Gratisverbindung

Unterstützung Alle drei Mobilfunkanbieter der Schweiz ermöglichen aus ihren Netzen kostenlose Anrufe in die Ukraine. Auch Roaming-Gebühren werden erlassen, wie sie auf sozialen Medien kundtaten.

«Sunrise UPC ist in Gedanken bei der ukrainischen Bevölkerung und all jenen, die von dieser Situation betroffen sind», schreibt das Unternehmen. Bis auf weiteres erlässt es für Privatkunden die Kosten für internationale Mobile-Abo- und Festnetz-Anrufe von der Schweiz in die Ukraine und von der Ukraine in die Schweiz. Ebenso werden die Kosten für Roaming-Anrufe innerhalb der Ukraine und von der Ukraine in die Schweiz nicht verrechnet.

Salt zieht bis vorerst 15. März nach. Quickline erlässt ab sofort bis Ende März die Kosten für alle ausgehenden Festnetz- und Mobile-Anrufe aus der Schweiz in die Ukraine und in deren Nachbarländer Polen, Slowakei, Ungarn, Rumänien und Moldau sowie die ausgehenden Mobile-Anrufe aus der Ukraine.

Auch Swisscom erlässt bis 15. März die Kosten für Telefonate in die Ukraine und die Roaming-Gebühren dort. «Es ist uns wichtig, unsere Kunden in dieser schwierigen Zeit zu unterstützen und ihnen die Kommunikation mit ihren Angehörigen zu ermöglichen. Es ist eine kleine Geste in einer ausserordentlichen Situation», sagt Sprecherin Sabrina Hubacher. Auf die Frage, ob die Mobilfunkinfrastruktur in der Ukraine derzeit noch funktioniert, sagt sie: «Gemäss unseren Kenntnissen funktioniert die Telefon- und Datenverbindung noch, aber wir können nicht versichern, dass dies in allen Regionen der Fall ist.»

Gratisreise für Flüchtende

Die Alliance Swiss Pass, der Zusammenschluss von 250 Transportunternehmen in der Schweiz, ermöglicht aus der Ukraine geflüchteten Personen die Reise von der Grenze zu ihrem Bestimmungsort in der Schweiz oder die Durchreise bis auf weiteres kostenfrei. Ihr Pass gelte als Ticket. Europäische Bahnunternehmen hatten am Sonntag ähnliche Massnahmen beschlossen.

Simone Luchetta und Mathias Born

Börse

SMI
11987 Punkte

0.0%



Die Besten

Givaudan N	+2.7%
Nestlé N	+1.1%
Lonza N	+1.0%

Die Schlechtesten

UBS Group N	-2.8%
Holcim N	-1.2%
CS Group N	-1.1%

Dow Jones Ind.
33'893 Punkte

-0.5%

Nasdaq Comp.
13'751 Punkte

+0.4%

Euro in Franken	1.033	-1.04%
Dollar in Franken	0.918	-0.94%
Euro in Dollar	1.124	-0.10%
GB-Pfund in Franken	1.232	-0.89%
Öl (Nordsee Brent) in Dollar	100.82	3.8%
Gold (Unze) in Dollar	1910.30	1.1%
Silber (Unze) in Dollar	24.47	1.7%