Übungsfeld im Cyber-Krieg

In der Ukraine testen und verfeinern russische Hacker ihre Fähigkeiten

Andy Greenberg | **Kurz vor Weihnachten 2016 gingen in Teilen Kiews die Lichter aus – Folge einer Cyber-Attacke auf das ukrainische Stromnetz. Erstmals gelang es kremlnahen Hackern, ein Stück kritische Infrastruktur lahmzulegen. Die gleiche Schadsoftware ist mittlerweile auch in amerikanischen Netzen aufgetaucht. Ist man sich im Westen der Gefahr bewusst?**

Auf einmal gingen die Lichter aus. Oleksi Yasinsky, 40 Jahre alt und Analyst einer Kiewer Cyber-Sicherheitsfirma, hatte mit Frau und Sohn den „Snowden"-Film von Oliver Stone über den Whistleblower der National Security Agency (NSA) geschaut. Nun saßen sie im Dunklen. „Die Hacker wollen nicht, dass wir das Ende des Filmes sehen", scherzte Yasinskys Frau. Er selbst lachte nicht. Yasinsky schaute auf die Digitalanzeige seines Reiseweckers: Genau 00:00 Uhr, Mitternacht. Das war kein normaler Stromausfall.

Nicht nur ihr Wohnblock, das ganze Viertel war stockdunkel. In der Ferne zeichneten sich gespenstisch die Silhouetten alter Sowjetbauten ab. Die Nacht war eiskalt. Wenn der Stromausfall zu lange dauern sollte, würden in Tausenden Wohnungen die Temperaturen sinken und Wasserleitungen einfrieren und platzen. Dann kam Yasinsky der nächste paranoide Gedanke: In den vergangenen Monaten hatte er für ukrainische Firmen und Staatsunternehmen eine ganze Reihe gezielter Cyber-Angriffe analysiert, die offenkundig auf ein- und dieselbe Hacker-Gruppe zurückgingen. Nun hatten diese Phantome, deren digitalen Fingerabdrücken er nachgespürt hatte, ihn selbst erreicht.

Es war ein Angriff mit Ansage: Jahrelang hatten Cyber-Kassandras prophezeit, dass Hacker-Angriffe in naher Zukunft nicht mehr nur digitales Chaos, sondern echte Schäden in der realen Welt anrichten würden. Der Stuxnet-Virus, der 2009 iranische Nuklearzentrifugen so stark beschleunigte, dass sie sich selbst zerstörten, galt als erstes Vorzeichen dieser neuen Ära. Michael Hayden, ehemaliger Chef der NSA und des US-Auslandsgeheimdiensts CIA, verglich dies damals mit den Atombombenabwürfen auf Japan vom August 1945: „Eine neue Waffe kommt zum Einsatz. Und diese Entwicklung lässt sich nicht mehr rückgängig machen."

In der Ukraine gab es einen solchen Cyber-Kriegsakt nun schon zum

zweiten Mal. 2015, zwei Tage vor Weihnachten, war bei fast einer Viertelmillion Ukrainer der Strom ausgefallen; ein Jahr später war der Schaden noch viel größer. Beide Male dauerte der Stromausfall nur wenige Stunden, bis die ukrainischen Ingenieure alle Schalter manuell wieder umgelegt hatten, die die unsichtbaren Saboteure aus der Ferne ausgeschaltet hatten. Doch nach zwei erfolgreichen Tests war die Funktionsfähigkeit des Konzepts bewiesen: In Russlands Schatten war der jahrzehntealte Albtraum, dass Hacker die Infrastruktur einer modernen Gesellschaft direkt angreifen, Wirklichkeit geworden.

Die Blackouts in der Weihnachtszeit sind kein Einzelfall. Sie sind Teil eines digitalen Blitzkriegs, mit dem die Ukraine seit drei Jahren überzogen wird. Systematisch attackiert eine ganze Hacker-Armee verschiedene Bereiche ukrainischer Infrastruktur: Medien, den Finanz-, Transport- und Energiesektor, das Militär, die Politik. Regelmäßig werden Daten vernichtet, Computer zerstört und ganze Firmen lahmgelegt.

6500 Hacker-Angriffe gegen 36 verschiedene ukrainische Ziele habe es allein in den vergangenen beiden Monaten gegeben, klagte der ukrainische Präsident, Petro Poroschenko, im Dezember 2016. Analysten konnten zu diesem Zeitpunkt noch nicht mit abschließender Sicherheit sagen, ob die Angriffe dem Kreml zuzuschreiben waren. Poroschenko dagegen hielt sich nicht zurück. Es gebe eine „direkte oder indirekte Beteiligung russischer Geheimdienste, die einen Cyber-Krieg gegen unser Land führen“. Das russische Außenministerium wollte sich auch auf wiederholte Nachfrage dazu nicht äußern.

Der Konflikt um die Ukraine – im Grunde Moskaus Versuch, die Ukraine als „kleines Bruderland“ in Abhängigkeit von Russland zu halten, mindestens aber eine Hinwendung Kiews zum Westen zu verhindern – wurde von Anfang an auch an der digitalen Front ausgetragen. Schon vor den ukrainischen Wahlen 2014 gelang es der prorussischen Hacker-Gruppe „CyberBerkut“, die Website der ukrainischen Wahlkommission zu hacken und den rechtsextremen Kandidaten Dmytro Jarosch zum Gewinner der Wahlen zu erklären. Die Website-Administratoren entdeckten den digitalen Einbruch erst kurz vor Veröffentlichung der Wahlergebnisse. CyberBerkut steht in Verbindung mit der kremlnahen Hacker-Gruppe, die 2016 für die Attacke auf den Parteivorstand der US-Demokraten verantwortlich war.

Im Ukraine-Konflikt wird auch an der digitalen Front gekämpft

Nicht wenige internationale Cyber-Experten glauben, dass Russland die Ukraine als Labor für die Perfektionierung neuer Methoden eines globalen Cyber-Kriegs nutzt. Die digitalen Bomben, die russische Hacker in der ukrainischen Infrastruktur platzierten, um sie dann gezielt hochgehen zu lassen, wurden auch schon mindestens einmal in der zivilen Infrastruktur der Vereinigten Staaten platziert.

Am Virenscan vorbeigeschlichen

Im Oktober 2015 erhielt Yasinsky von seinem damaligen Arbeitgeber, dem größten ukrainischen Fernsehsender StarLightMedia, einen Notruf. Zwei Server waren ausgefallen. Der zuständige IT-Spezialist konnte sie schnell wieder ans Laufen bringen, doch dass zwei Server gleichzeitig

ausfielen, war höchst ungewöhnlich. Bei der Auswertung der Datenkopien bemerkte Yasinsky, dass der so genannte „Master Boot Record“ der betroffenen Server komplett überschrieben war, also der Teil der Festplatte, der den Rechner das eigene Betriebssystem finden lässt. Und noch delikater: Diese beiden Server waren „Commanding Controllers“, sie hatten Zugriff auf Hunderte anderer Rechner im Netzwerk.

Die Handschrift der Hacker ist deutlich, ihre Motive nicht

Yasinsky druckte den Code aus und legte ihn auf seinem Küchentisch und dem Fußboden aus. Es war die ausgefeilteste Schadsoftware, die er bisher erlebt hatte. Auch war der Schaden noch größer als zunächst angenommen. Die beiden Server hatten auf 13 Laptops von StarLight-Mitarbeitern einen Virus eingeschleust. Diese Infektionen hatten dieselbe Überschreibungstechnik benutzt und zwar gerade in dem Moment, als die Mitarbeiter die Nachrichten zu den aktuellen Lokalwahlen vorbereiteten. Dennoch hatte man Glück. Die „Controllers“ hatten sich selbst frühzeitig abgeschaltet, sonst wären insgesamt 200 Firmencomputer in Mitleidenschaft gezogen worden. StarLights Konkurrent TRK hatte weniger Glück, erfuhr Yasinsky später. Dort wurden mit derselben Methode über 100 Rechner infiziert.

Yasinsky gelang es, eine Kopie des Programms anzufertigen. Die Malware war geschickt getarnt: Sie hatte sich nicht nur an allen Virenscans vorbeigeschlichen, sie hatte sich sogar als Antivirenprogramm ausgeben können. Seit 20 Jahren arbeitete Yasinsky im Bereich Informationssicherheit. Aber noch nie hatte er eine derart raffinierte digitale Waffe zu analysieren.

Als Kern des Virus identifizierte er „KillDisc“, einen zerstörerischen Parasiten, der seit etwa einem Jahrzehnt in bestimmten Hacker-Kreisen im Umlauf war. Er verfolgte die digitalen Fingerabdrücke der Hacker und machte dabei eine Entdeckung, die ihn und seine Kollegen zutiefst schockierten: Der Virus saß schon seit mehr als sechs Monaten im System von StarLightMedia. Ein Trojaner mit dem Namen „BlackEnergy“ hatte den Hackern den ersten Zugriff ermöglicht. Nach und nach hörte Yasinsky von immer mehr Unternehmen und Behörden, die mit derselben Methode angegriffen worden waren, darunter die größte Bahngesellschaft der Ukraine. Einige wollten nicht öffentlich zugeben, dass sie gehackt worden waren.

In fast allen Fällen hatte sich das Programm über den Trojaner BlackEnergy im System eingenistet. Wie eine digitale Sprengbombe entfaltete es dann mit KillDisc seine Zerstörungskraft. Die Handschrift der Hacker war mehr als deutlich, ihre Motive hingegen nicht. Und eines ahnte Yasinsky seinen ausführlichen Analysen zum Trotz nicht einmal ansatzweise: Schon in diesem Dezember 2015 waren BlackEnergy und KillDisc in drei der größten ukrainischen Energieunternehmen platziert und mussten nur noch aktiviert werden.

Post von der Regierung

Kurz vor Heiligabend 2015 – und am Tag vor seiner eigenen Hochzeit – sah Robert Lee zuhause in Cullman, Alabama, die Schlagzeilen von einem Hacker-Angriff auf Teile des Kiewer Stromnetzes. Kurz zuvor hatte Lee als

Bild nur in Printausgabe verfügbar

Eine Cyber-Attacke auf kritische Infrastruktur ist nicht länger nur Theorie: Hochspannungsleitungen in der Ukraine

Cyber-Security-Spezialist bei einem der US-Geheimdienste gekündigt, um ein Start-up für Cyber-Sicherheit zu gründen. Der Meldung aus der Ukraine schenkte er zunächst keine allzu große Beachtung. Cyber-Experten wussten, dass hinter angeblichen Stromnetz-„Hacks“ meist nur ein paar Nagetiere standen, die Kabel angeknabbert hatten. Am nächsten Morgen aber erhielt Lee kurz vor seiner Trauung eine Textnachricht von Mike Assante, Mitarbeiter des SANS Instituts für Cyber-Security-Training und einer der renommiertesten Experten für Hacker-Angriffe auf Stromnetze. Assante war fest davon überzeugt, dass es sich bei dem Stromausfall in Kiew um eine digitale Attacke handelte.

Die Trauzeremonie war gerade vorbei, da meldeten sich ukrainische Cyber-Experten. Sie benötigten Lees Hilfe. Sein ganzes Berufsleben hatte sich Lee mit der Möglichkeit digitaler Attacken auf kritische Infrastruktur beschäftigt. Jetzt war aus der Möglichkeit eine Tatsache geworden. Noch am gleichen Abend begann er, die KillDisk-Software zu analysieren, die die ukrainischen Kollegen ihm zugeschickt hatten. Wenige Tage später erhielt er auch die BlackEnergy-Malware zusammen mit den forensischen Daten der Angriffe.

Das Vorgehen der Hacker war klar nachzuvollziehen. Sie hatten den Virus mittels einer E-Mail mit einer gefälschten Adresse der ukrainischen Regierung als Absender geschickt. Versteckt in einem angefügten Word-Dokument wurde der Virus auf die Rechner geladen. Von dort hatte er sich auf das gesamte System ausgebreitet und dann die Kontrollsoftware kompromittiert, die uneingeschränkten Zugriff auf die Steuerung eröffnete – inklusive der hochspezialisierten Kontrollsoftware für die Sicherungsschalter.

Je länger Lee die Attacke auf die Ukraine studierte, desto deutlicher

wurden die Parallelen mit den Hacker-Angriffen einer Gruppe namens Sandworm. Bereits 2014 hatte die Sicherheitsfirma FireEye vor einer Hacker-Gruppe gewarnt, die BlackEnergy in die Computersysteme mehrerer polnischer und ukrainischer Energie- und Staatsunternehmen eingeschleust hatte. Offensichtlich zielten die Hacker auf spezielle Verbundrechner, die für die ferngeregelte Steuerung von Infrastruktur zuständig sind.

Eine unmittelbare Bedrohung für die Vereinigten Staaten

Auch hier waren die Motive unklar. Aber es wurde immer deutlicher, dass es sich um russische Hacker handelte: Der Firma FireEye war aufgefallen, dass diese Methoden zuerst auf einer russischen Hacker-Konferenz präsentiert worden waren. Danach schafften es die Experten von FireEye, auf die ungesicherten Command-and-Control-Server von Sandworm zuzugreifen. Dort fanden sie russischsprachige Instruktionen für BlackEnergy.

Noch erstaunlicher war allerdings, dass Sandworm bereits Angriffe in den USA ausgeführt hatte. Dieselbe Hacker-Gruppe, die für diesen Angriff verantwortlich zeichnete, hatte Teile der amerikanischen Energie-Infrastruktur mit demselben Virus infiziert. Schon 2014 hatte die US-Regierung berichtet, dass die Hacker-Gruppe einen BlackEnergy-Virus in den Netzwerken von Wasser- und Energiekonzernen platziert hatte.

Lee war sich nun sicher: Die Gruppe war für die Angriffe auf das ukrainische Stromnetz ebenso verantwortlich wie auf das amerikanische: „Ein Gegner, der bereits amerikanische Energieunternehmen attackiert hatte, hatte eine rote Linie überschritten und ein Stromnetz lahmgelegt“, sagt er. „Somit ist diese Gruppe eine unmittelbare Bedrohung für die Vereinigten Staaten.“

Mit KillDisk in die Winteroffensive

An einem klaren, kalten Tag einige Wochen später landete ein Team von US-Sicherheitsexperten in Kiew. Unter ihnen befanden sich Mitarbeiter des FBI, des Heimatschutz- und des Energieministeriums sowie der North American Electric Reliability Corporation, eine für die Koordinierung des Stromnetzes in den USA zuständige Behörde. Zu ihnen gehörte auch Mike Assante. Noch am Tag ihrer Ankunft traf sich die US-Delegation mit Angestellten der Firma Kyivenergo, dem städtischen Stromversorger und eines der drei Opfer des Hacker-Angriffs. Die detaillierten Schilderungen zogen sich über mehrere Stunden.

Der Virus hatte zwar kein „Script“ – in Computercode geschriebene Befehle –, um die Sicherungen des Netzwerks selbstständig zu kontrollieren. Dennoch mussten die Ingenieure des Stromversorgers am Nachmittag des 23. Dezember hilflos zusehen, wie eine Sicherung nach der anderen heraussprang und ein Gebiet von der Größe Massachusetts ins Dunkel getaucht wurde – gesteuert von den Rechnern ihres eigenen Netzwerks. Die Hacker hatten eine perfekte Kopie der Kontrollsoftware auf einem PC in einer weiter entfernten Einrichtung angelegt. Mithilfe dieses Klons wurde der Befehl zum Abschalten des Stroms gegeben.

Nachdem die Sicherungen ausgeschaltet und der Strom für Zehntausende Ukrainer abgeknipst worden war, begann die zweite Phase des Angriffs. Die Hacker hatten die Firm-

ware „Umwandler“ in den Umspannwerken überschrieben – winzig kleine Boxen in den Server-Schränken der Werke, die Internetprotokolle übersetzen, um eine Kommunikation mit älteren Geräten zu ermöglichen. Mit dem Umschreiben der Codes für diese Hardware – was wochenlange Vorbereitungen erfordert haben musste – konnten die Hacker die Geräte gewissermaßen einmauern und den wirklichen Administratoren die Kontrolle über die Trennschalter entziehen. Assante war zutiefst beeindruckt von solcher Gründlichkeit.

Und wieder hinterließen die Hacker ihre Visitenkarte: KillDisk, mit dessen Hilfe sie einige Computer des Unternehmens zerstörten. Der übelste Teil des Angriffs aber richtete sich gegen die Notstromversorgung der Kontrollstationen. Nicht nur die „normale“ Stromversorgung wurde ausgeschaltet, sondern auch der Strom für die Stromversorger, die nun ebenfalls im Dunklen saßen. Mit äußerster Präzision hatten die Hacker einen Stromausfall im Stromausfall arrangiert. „Die Botschaft lautete eindeutig: Wir können überall zuschlagen“, sagt Assante. „Die Angreifer müssen sich vorgekommen sein wie allmächtige Götter.“

Im August 2016, acht Monate nach dem ersten Weihnachtsstromausfall, kündigte Yasinsky seinen Job bei StarLightMedia. Es genügte ihm nicht mehr, ein einziges Unternehmen gegen Angriffe zu verteidigen, wenn doch die gesamte ukrainische Gesellschaft Ziel der Attacken war. Wenn man den Hackern etwas entgegensetzen wollte, dann war ein umfassenderer Ansatz notwendig. Die Ukraine brauchte eine kohärentere Antwort auf eine so skrupellose Gruppe wie Sandworm. „Das Problem ist nur, dass wir Guten Einzelkämpfer sind und die Bösen ganz und gar nicht.“ Yasinsky wurde Chef der Forschungs- und Forensikabteilung bei der Kiewer Firma Information Systems Security Partners (ISSP), zu dem Zeitpunkt noch ein kleiner Fisch in der Cyber-Security-Branche. Yasinsky machte sie zum Ersthelfer für die Opfer im Cyberkrieg gegen die Ukraine.

Kurz nachdem Yasinsky zu ISSP gewechselt hatte, erfolgte ein weiterer, noch umfassenderer Angriff. Zu den Opfern gehörten der ukrainische Rentenfonds, die Staatskasse, die Hafenbehörde, die Ministerien für Infrastruktur, Verteidigung und Finanzen, zum zweiten Mal auch das ukrainische Bahnunternehmen. Mitten in der Feriensaison legten sie über Tage hinweg das Online-Buchungssystem lahm. Wie 2015 kulminierten die Angriffe in einer KillDisk-Detonation auf der Festplatte des jeweiligen Opfers. Im Fall des Finanzministeriums wurden Terabytes an Daten gelöscht, gerade als das Ministerium seinen Haushalt für das kommende Jahr vorbereitete. Die neue Herbst-Winteroffensive der Hacker übertraf die des vorherigen Jahres um ein Vielfaches, großes Finale inklusive.

Die Botschaft lautet: „Wir können überall zuschlagen“

Am 17. Dezember 2016, just als Yasinsky und Familie den „Snowden“-Film schauten, hatte ein junger Ingenieur namens Oleg Zaychenko gerade die ersten vier seiner zwölfstündigen Schicht in Ukrenergos Übertragungsstation nördlich von Kiew hinter sich. In einem über und über mit beigen und roten Schaltkonsolen versehenen Kontrollraum

Bild nur in Printausgabe verfügbar

protokollierte er gerade mit Bleistift und Papier einen weitgehend ereignislosen Samstag. Dann schrillte der Alarm. Zwei der Kontrolllichter auf der rechten Seite seines Pultes wechselten von rot auf grün – die Stromkreise waren unterbrochen. Zaychenko griff zum Hörer seines altmodischen Tischtelefons und rief seinen Vorgesetzten in Ukrenergos Hauptquartier an, um ihm die routinemäßige Störung mitzuteilen. Unterdessen sprang ein weiteres Licht auf grün. Dann noch eines.

Während Zaychenko eilig die Situation erklärte, sprangen die Lichter weiter um: rot – grün, rot – grün. Erst acht, dann zehn, dann zwölf. Er solle schnellstens nachsehen, ob die Geräte physische Schäden aufwiesen, befahl sein Vorgesetzter. Als er sich die Jacke überwarf, fiel gerade der 20. und letzte Stromkreislauf aus. Lampen und Computerbildschirme erloschen, der gesamte Kontrollraum wurde dunkel.

Unter Normalbetrieb ist ein Umspannwerk – oft so groß wie ein Dutzend Fußballfelder – ein gigantischer brummender Dschungel aus elektrischen Geräten. Aber als Zaychenko in die eiskalte Nacht trat, herrschte geradezu unheimliche Stille. Von den drei riesigen Transformatoren, die etwa ein Fünftel der Stromversorgung der Hauptstadt liefern, war kein Brummen zu vernehmen. Wochen- und monatelang hatte Zaychenko routinemäßig seine Notfall-Checkliste abgearbeitet. Jetzt wusste er: Die Hacker hatten wieder zugeschlagen. Und dieses Mal mit noch sehr viel größerem Ehrgeiz.

Die Saboteure hatten nicht auf die Knotenpunkte gezielt, die gewissermaßen die Strom-„Kapillaren“ versorgen, sondern auf eine überlebenswichtige Arterie. Das Kiewer Umspannwerk lieferte mehr elektrische Leistung als alle 50 Verteilerstationen zusammen, die 2015 angegriffen worden waren. Glücklicherweise ließ sich

das System binnen einer Stunde wieder hochfahren, bevor Panik oder Unruhen ausbrechen konnten.

Stuxnet hat einen Nachfolger

Das war aber auch das einzig Positive. Cyber-Sicherheitsunternehmen, die den Angriff analysierten, stellten fest, dass die Technik der Hacker gegenüber 2015 deutlich weiterentwickelt war. Zum Einsatz kam jetzt eine hochgradig komplexe und anpassungsfähige Schadsoftware namens „CrashOverride". Dieses Programm wurde als automatisierte Waffe für die Sabotage von Stromnetzen entworfen. CrashOverride war in der Lage, die „Sprache" des Stromnetz-Kontrollsystems zu sprechen und damit direkte Befehle an die vernetzten Geräte zu schicken. Die Malware war so programmiert, dass sie das Netzwerk eines Betroffenen durchleuchten, potenzielle Ziele identifizieren und zu einer voreingestellten Zeit beginnen konnte, Stromkreisläufe gezielt zu unterbrechen, ohne dass eine Internetverbindung zu den tatsächlichen Hackern bestand. Es war seit Stuxnet die erste Schadsoftware, die dazu entworfen war, selbsttätig physische Infrastruktur zu sabotieren.

CrashOverride ist Experten zufolge eine wiederverwendbare und hochgradig anpassungsfähige Waffe, um auch andere Stromversorger lahmzulegen. Wegen der modularen Struktur der Malware kann die Protokollsprache der Kontrollsysteme von Ukrenergos einfach gegen eine andere ausgetauscht werden, die beispielsweise in anderen europäischen Ländern oder den USA verwendet wird. Marina Krotofil, Expertin für Sicherheit von industriellen Kontrollsystemen, beschreibt die Methoden der Hacker als gradliniger und viel effizienter als deren Vorgänger: „2015 benahmen sie sich wie eine brutale Straßenbande. 2016 bewegten sie sich elegant wie Ninjas." Dabei sind die Hacker vermutlich dieselben.

Auf der Grundlage von noch unveröffentlichten Analysen konnte Robert Lees Firma Dragos die Autoren von CrashOverride als Teil der Sandworm-Gruppe identifizieren. Und Sandworm hat laut Lee seit den ersten Attacken von 2014 erhebliche und äußerst beunruhigende Fortschritte gemacht. Die Hacker demonstrieren, dass sie fähig sind, kritische Infrastruktur anzugreifen und dabei ihre Technik mit jeder Angriffswelle noch zu verfeinern.

Eine anpassungsfähige und wiederverwendbare Waffe

Niemand weiß, wie und wo Sandworm das nächste Mal angreifen wird. Eine weitere Attacke könnte sich statt gegen Verteilungsstationen oder Umspannwerke gegen ein Kraftwerk richten. Geräte könnten nicht nur lahmgelegt, sondern zerstört werden. Schon 2007 hatte ein Forschungsteam um Mike Assante gezeigt, dass es möglich ist, physische Infrastruktur mit Hacks kaputtzumachen: Im so genannten Aurora-Experiment wurde allein durch digitale Befehle ein 2,25-Megawatt-Dieselgenerator – eine Maschine von der Größe eines Zimmers – so zerlegt, dass sie unter weißem und schwarzem Qualm zusammenbrach.

Ein Generator unterscheidet sich nicht wesentlich von den Maschinen, die in den USA Hunderte von Megawatt Strom an ihre Kunden liefern. Mit der richtigen Schadsoftware könnte man möglicherweise die Stromerzeugungsgeräte oder die schwer er-

setzbaren Transformatoren dauerhaft ausschalten, die als Rückgrat des amerikanischen Stromnetzes fungieren.

Neben Dragos hat sich auch das slowakische Institut ESET mit der Analyse von CrashOverride befasst. Demnach enthält die Schadsoftware möglicherweise schon jetzt ein Element für einen solch zerstörerischen Angriff. CrashOverride, vermuten die ESET-Experten auch, ist auf ein bestimmtes Siemens-Schutzgerät in Kraftwerken ausgelegt; eine Vorrichtung, die als Notschalter bei gefährlicher Überspannung fungiert. Falls es CrashOverride gelingt, diese Schutzvorrichtung stark zu beschädigen, könnte das Programm schon jetzt Stromnetze dauerhaft beschädigen.

Dienen die Cyber-Angriffe der Abschreckung?

Warum und wie genau aber würde ein Akteur wie Russland dem amerikanischen Stromnetz Schaden zufügen wollen? Ein Angriff auf amerikanische Versorgungsunternehmen würde mit Sicherheit sofortige und drastische Gegenmaßnahmen der USA nach sich ziehen.

Manche Experten für Cyber-Sicherheit vermuten, dass Russland darauf abzielt, die Cyber-Kapazitäten der USA in Schach zu halten. Es ginge also um Abschreckung. Die Angriffe auf die Ukraine wären eine klare Botschaft an die USA: Seht, was wir können, und wagt es nicht, uns oder einen Verbündeten wie den syrischen Machthaber Baschar al-Assad mit einem Virus wie Stuxnet anzugreifen.

Lee ist anderer Meinung: Sollte sich Russland in die Ecke gedrängt fühlen, zum Beispiel, wenn die USA gegen Moskaus militärische Interessen in der Ukraine oder Syrien handelten, dann könnten russische Hacker die amerikanische Versorgungsinfrastruktur angreifen, um Vergeltung zu üben.

Die Hacker-Angriffe auf das ukrainische Stromnetz waren äußerst raffiniert, lösten aber noch keine Katastrophe aus. Am Ende ging das Licht wieder an. Außerdem hätten amerikanische Stromkonzerne ihre Lehren aus den Ukraine-Attacken gezogen, meint Marcus Sachs, Verantwortlicher für den Bereich Sicherheit der North American Electric Reliability Corporation. Seit 2015 organisiert NERC Informationsveranstaltungen für Stromkonzerne, um sie widerstandsfähiger gegen Angriffe zu machen. Dazu gehört auch, die Fernsteuerung kritischer Systeme häufiger abzuschalten. Dennoch halten Experten, die Sandworm seit nunmehr drei Jahren beobachten, weitere Angriffe auf das US-Stromnetz nicht für völlig ausgeschlossen.

Vorbereiten auf die nächste Runde

Die Zentrale von Yasinskys Firma Information Systems Security Partners ist ein Flachbau inmitten eines Kiewer Industriegebiets. Yasinskys Büro ist dunkel, auf einem runden Tisch liegen riesige Netzwerkkarten, die Knotenpunkte und Verbindungen von verblüffender Komplexität zeigen. Jede Karte dokumentiert die Zeitleiste eines Sandworm-Angriffs. Seit fast zwei Jahren widmet Yasinsky den Großteil seiner Arbeit dieser Hacker-Gruppe. Es sei unmöglich, sagt er, die exakte Anzahl ukrainischer Einrichtungen zu kennen, die zum Ziel der Sandworm-Attacken geworden sind. Jede Schätzung sei mit großer Wahrscheinlichkeit eine Unterschätzung, und zu jedem bekannten Angriff komme mit hoher Wahrscheinlichkeit ein

Opfer, das die Cyber-Eindringlinge noch nicht entdeckt hat oder die Attacke nicht zugeben will.

Und die Eindringlinge machen immer weiter. Zwei Mitarbeiter Yasinskys sind während unseres Gesprächs damit beschäftigt, Schadsoftware zu analysieren, die das Unternehmen erst einen Tag zuvor über eine neue Salve von Phishing-Mails erhalten hat. Die Angriffe, sagt Yasinsky, folgen nunmehr einem jahreszeitlichen Rhythmus. In den ersten Monaten des Jahres schaffen die Hacker die Basis: Sie dringen unbemerkt in die Systeme ihrer Ziele ein und breiten sich aus. Am Ende des Jahres detonieren sie ihre digitale Bombe. Die Saat für eine erneute Dezemberattacke ist schon ausgebracht.

Sich auf die nächste Runde vorzubereiten, sagt Yasinsky, ist wie „für eine entscheidende Klausur zu lernen". Aber in dem größeren Masterplan der Hacker, glaubt er, ist die Ukraine seit drei Jahren einfach nur ein Übungsfeld für Cyber-Manöver. Selbst bei ihren zerstörerischsten Attacken hätten die Hacker noch deutlich weiter gehen können. Sie hätten nicht nur die Dateien des Finanzministeriums zerstören können, sondern auch deren Backups. Wahrscheinlich hätten sie Ukrenergos Umspannwerk längerfristig stören können. „Sie spielen immer noch mit uns", sagt er. Jedes Mal sind die Hacker abgezogen, bevor sie den maximalen Schaden anrichten konnten. Ganz, als wollten sie ihre tatsächlichen Möglichkeiten für eine zukünftige Operation geheimhalten.

Zahlreiche Cyber-Experten sind zum gleichen Ergebnis gekommen. Wo könnte man eine Armee aus Kreml-Hackern im digitalen Kampf besser ausbilden als in der rauen Atmosphäre eines heißen Krieges an Russlands Peripherie? „Sie machen ernst. Hier kann man Schlimmes anrichten, ohne Vergeltung oder Strafverfolgung fürchten zu müssen. Schließlich ist die Ukraine nicht Frankreich oder Deutschland", sagt Kenneth Geers vom NATO Cooperative Cyber Defence Center of Excellence.

Die Hacker testen, ob sie ohne Strafe davonkommen

Der Kreml hat sich in die ukrainischen Wahlen eingemischt und sah sich mit keinerlei Konsequenzen konfrontiert; daraufhin hat er ähnliche Taktiken in den USA und Frankreich angewandt. Russische Hacker haben ungestraft den Strom in der Ukraine abgeschaltet – die logische Kette lässt sich leicht zu Ende führen. „Die Hacker testen unsere Grenzen und ob sie ungestraft davonkommen", sagt Thomas Rid vom Londoner King's College. „Sie schubsen, und schubst man nicht zurück, dann lädt man sie geradezu ein, einen Schritt weiterzugehen."

Was wäre der nächste Schritt? Vielleicht noch ein Stromausfall. Oder eine gezielte Attacke auf die Wasserversorgung. „Bemühen Sie Ihre Fantasie", sagt Yasinsky trocken. „Der Cyber-Raum ist nicht das Ziel. Er ist ein Medium."

Andy Greenberg ist Autor der US-Ausgabe von *WIRED*. Dieser Beitrag beruht auf seiner Reportage „How an Entire Nation Became Russia's Test Labor for Cyber War" (Juli 2017).