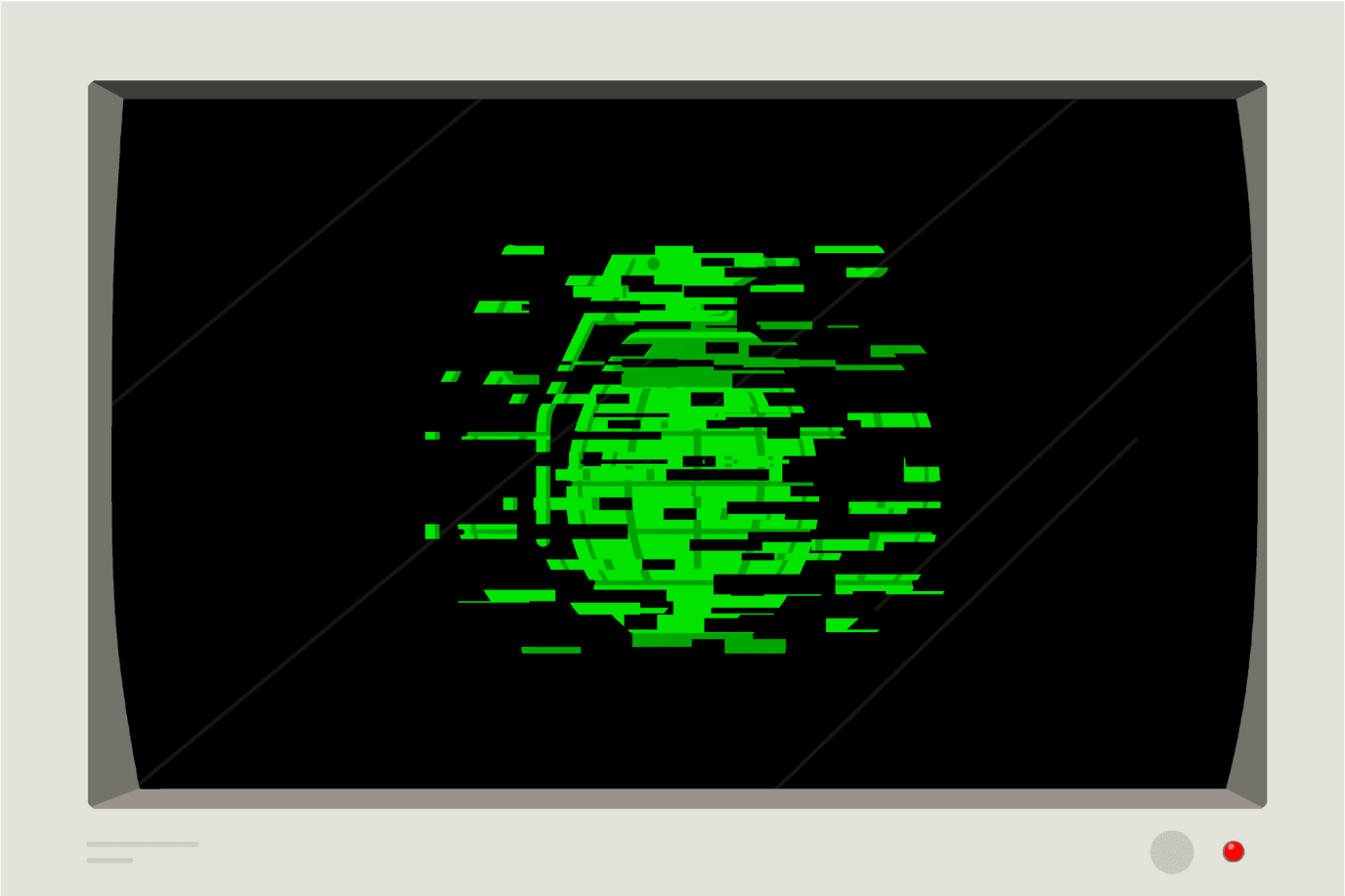

Wie Russland für den Cyber-Krieg aufgerüstet hat

Wie zettelt man einen Krieg nicht nur in der realen, sondern auch in der virtuellen Welt an? Russland hat dazu in den letzten Jahren viel Expertise gesammelt. Bevorzugter Übungsplatz für diese Cyber-Attacken: die Ukraine. Eine Analyse in sechs Akten.

Von Eva Wolfangel (Text) und Alexander Glandien (Illustration), 07.03.2022

Am Morgen dieses verhängnisvollen Dienstags war Wladimir Malezhik bester Dinge ins Büro in Kiews historisch bedeutendem Stadtteil Chokolivka gefahren. Schliesslich steht ein langes Wochenende bevor: Der Constitution Day (Tag der Verfassung) ist ein wichtiger Feiertag in der Ukraine. Als die ersten Kunden bei ihm anrufen an jenem 27. Juni 2017 und sich beklagen, dass ihre Daten verschlüsselt seien, denkt sich Cloud-Unternehmer Malezhik erstmal nichts dabei.

«Damals verging kein Tag ohne IT-Probleme», sagt er im Rückblick, an einem grauen Wintertag in Kiew, und schaut aus dem Fenster auf ein ebenso graues Industriegebiet. Malezhik hilft seinen Kundinnen mit seinem Backup-Service. «Immer wieder klickt jemand auf eine Phishing-E-Mail und alles ist verschlüsselt.» Doch der 27. Juni 2017 änderte alles. Was zunächst wie alltägliche IT-Probleme aussieht, entpuppt sich als massiver Cyber-Angriff, der als die verheerende NotPetya-Attacke und damit als Vorbotin eines Cyber-Kriegs in die Geschichte eingehen wird.

Knapp fünf Jahre nach dem 27. Juni 2017, im Winter 21/22: Erneut verschlüsselte und gelöschte Daten in mehreren Systemen der ukrainischen Regierung, von Banken und regierungsnahen Unternehmen. Kurz darauf der Einmarsch russischer Truppen. Kann man das, was gerade in der Ukraine geschieht, auch einen Cyber-Krieg nennen? Oder eher einen hybriden Krieg? Welche Rolle spielen digitale Angriffe auf das Land jetzt – und welche Kapazitäten hat Russland in diesem Bereich?

Russland hat sich jedenfalls lange auf einen Cyber-War vorbereitet, staatliche russische Akteure haben ihre Kapazitäten für Cyber-Angriffe in den vergangenen Jahren massiv ausgebaut. Sie können unterdessen viel mehr, als ein paar Websites lahmlegen – und sind damit unberechenbarer geworden. Gespräche über die jüngste Vergangenheit mit IT-Fachleuten aus der Ukraine zeigen: Das Land ist nicht nur regelmässig Opfer von Attacken, sondern auch Labor und Übungsplatz für die grösseren digitalen Angriffe, die die ganze Welt bedrohen.

Wer sich die Vorfälle der vergangenen acht Jahre genauer anschaut, kann dabei zusehen, wie die russischen Staatshacker ihre Kapazitäten immer weiter ausbauen: Angefangen bei gehackten Websites von Medien und Wahlkommissionen über das massenhafte Löschen von Daten bis zu den Blackouts durch Angriffe auf Energiewerke und eine lebensbedrohende Attacke auf eine petrochemische Fabrik in Saudiarabien. In den Computersystemen der Welt hat sich über die Jahre ein digitaler Feind eingenistet. Ob und wie heftig er als Nächstes zuschlägt: Niemand weiss es.

1. Akt: Angriff auf die Medien

Wer verstehen will, was im Cyberspace in der Ukraine geschieht, sollte mit Oleksii Yasinskyi von der ukrainischen Sicherheitsfirma ISSP in Kiew sprechen. Kaum einer hat die mutmasslich russischen Angriffe so intensiv verfolgt und analysiert wie der 46-jährige IT-Sicherheitsexperte – auch weil ihn seine Biografie immer wieder ins Zentrum dieser Angriffe geführt hat. Während die Welt erst angesichts der verheerenden NotPetya-Attacke darauf aufmerksam wurde, wozu russische Staatshackerinnen fähig sind, sah Yasinskyi entsprechende Zeichen schon viel früher: «Ab 2014 wurde die Ukraine der Spielplatz für russische Cyber-Angriffe», sagt er.

Einer der ersten eindeutig politisch motivierten Angriffe auf ukrainische Computersysteme findet wenige Tage vor den ukrainischen Präsidentschaftswahlen im Oktober 2014 statt: Ein Cyber-Angriff legt die Computersysteme der Zentralen Wahlkommission lahm. Eine prorussische Hacktivistengruppe namens CyberBerkut erklärt sich für den Angriff verantwortlich. Auch wenn das System rechtzeitig vor der Wahl wieder funktioniert, bleiben die Hacker offenbar weiterhin im System: Jedenfalls veröffentlichen sie am Wahltag ein Foto und verkünden, dass der rechte Kandidat Dmytro Yarosh die Wahl gewonnen habe – da sind die Wahllokale noch nicht einmal geschlossen. «Die Meldung wurde von den russischen Medien ausgeschlachtet», erinnert sich Yasinskyi, der damals noch in der

Sicherheitsabteilung des Telekommunikationsunternehmens Kyivstar arbeitete.

Kurz darauf wechselt Yasinskyi zu Starlight Media, dem grössten Medienunternehmen des Landes mit mehreren Fernsehsendern. Kaum dort, trifft er auf russische Angreiferinnen: 2015 verschaffen sich Eindringlinge Zugang zu den internen Systemen von Starlight Media, übernehmen deren Youtube-Kanal und veröffentlichen den Werbeclip eines Kandidaten der Kommunalwahlen. «Wir haben das sofort gestoppt, das Video war nur wenige Sekunden online», erinnert sich Yasinskyi. Doch der Angriff ist grösser, wie der Sicherheitsforscher feststellt: Yasinskyi findet eine massive Infektion des Unternehmens mit einer Schadsoftware namens «Black Energy». Diese wird dem russischen Geheimdienst zugeschrieben. Die Täter hatten versucht, all ihre Spuren sowie die Daten auf den Systemen des Medienunternehmens zu löschen, scheiterten aber aus unklaren Gründen. So konnte Yasinskyi den Angriff genauer analysieren und herausfinden, dass die Angreiferinnen schon seit mindestens sechs Monaten in den Systemen aktiv waren.

Es sind Versuche, die Demokratie des Landes zu destabilisieren. Das ist eine bekannte Strategie, die Fachleute auch rund um die US-Wahlen 2016 beobachtet hatten: Durch gefälschte Hinweise auf vermeintlichen Wahlbetrug und andere Unregelmässigkeiten soll Misstrauen verbreitet werden. Auch im Vorfeld der US-Wahlen 2020 gab es Einflussversuche, unter anderem in den sozialen Medien, wo mit falschen Nachrichten wohl Verwirrung gestiftet und dadurch die Demokratie geschwächt werden sollte. Eine Analyse des Tech-Konzerns Microsoft ergab, dass hinter den Angriffen auf US-Politiker 2016 und 2020 unter anderem die Gruppe «Fancy Bear» steckt: So nennen Sicherheitsforscher eine Hackergruppe des russischen Geheimdienstes GRU.

In diesen frühen Hacks zeigt sich, dass die russischen Angreiferinnen gut darin sind, Lücken zu finden – und dass viele Systeme nicht gut geschützt sind. Die Angriffe sind ein Anfang, nur mässig ausgefeilt. Und, wie die misslungene Spurenlöschung im System von Starlight Media zeigt, auch noch von Pannen begleitet.

2. Akt: Angriff auf die Elektrizitätswerke – aus der Ferne manuell

Im Jahr nach dem Angriff auf Starlight Media zünden die russischen Angreifer eine nächste Eskalationsstufe. 2015 und 2016, jeweils kurz vor Weihnachten, werden die Systeme einiger Elektrizitätswerke in der Ukraine gestört – und zwischen diesen beiden Angriffen ist eine deutliche Steigerung zu sehen. 2015 dringen die Hackerinnen mit der bewährten Black-Energy-Malware in die Systeme von drei Elektrizitätswerken ein. Sie übernehmen die Steuerungscomputer der Anlagen aus der Ferne, um händisch Teile der Systeme herunterzufahren.

Das funktioniert ähnlich wie mit dem Programm Teamviewer, mit dem man die Kontrolle über den eigenen Computer an eine Person in der Ferne übergeben kann. Ein solcher Angriff ist verhältnismässig einfach, weil die Angreifer die Tools der Ingenieurinnen nutzen – sie müssen lediglich genügend personelle Kapazitäten haben, um das dann in Echtzeit zu tun.

«Ich hatte gleich ein ungutes Gefühl», erinnert sich Marina Krotofil an die Tage vor Weihnachten 2015. Die deutsche Cybersicherheitsexpertin ukrainischer Herkunft analysierte den Vorfall damals als unabhängige

Sicherheitsforscherin. Sie hatte sich schon seit einigen Jahren mit Cyber-Attacken auf kritische Infrastrukturen beschäftigt und auch mit den lebensgefährlichen Folgen. Krotofil weiss: Hält so ein Stromausfall länger an, brechen die Trinkwasserversorgung und die Versorgung mit Lebensmitteln zusammen, das Telefonnetz fällt aus, auch Benzin wird schnell knapp. Damit fallen dann auch die Generatoren in Einrichtungen der Notfallversorgung aus, etwa in Krankenhäusern. Dazu kommt die bedrohliche Kälte im ukrainischen Winter. «Zum ersten Mal wurde das Leben von Menschen bewusst aufs Spiel gesetzt», sagt sie.

Die Störungen liessen sich relativ schnell beheben, indem Mitarbeitende der betroffenen drei Kraftwerke die Umspannwerke manuell wieder in Betrieb nahmen. Die Attacken, die zeitgleich begonnen hatten und von denen Experten annehmen, dass dafür Dutzende Angreiferinnen parallel beschäftigt waren, dauerten lediglich zwischen einer und sechs Stunden. Betroffen waren Millionen Menschen.

Selbst wenn der Angriff nicht besonders ausgefeilt war: Mit diesen Kapazitäten sei es möglich gewesen, einen deutlich grösseren Schaden anzurichten, sagt Krotofil. Offenbar sei das aber nicht das Ziel gewesen. Alles deutet laut der Sicherheitsforscherin darauf hin, dass die Angreifer – die US-Regierung ordnete die Attacken schliesslich Russland zu – einen Testlauf durchgeführt hatten. «Jede Armee kennt das, dass ab und zu Übungen gemacht werden», sagt Krotofil. Das zeige aber auch das Potenzial der Angreiferinnen, warnt sie. Denn wenn es allein zu Übungszwecken möglich ist, eine derart koordinierte Attacke auf drei Unternehmen zu starten, spreche das nicht nur für eine gewisse Expertise, sondern auch für entsprechende Kapazitäten und eine militärische Organisation: «Du brauchst drei Teams, die gleichzeitig einen komplexen Angriff starten, ohne eine Verspätung, ohne dass etwas schiefgeht.»

Die Angreifer dürften mit ihrer Übung zufrieden gewesen sein. Das ganze Land war kurzfristig in Angst und Schrecken. Und bei Krotofil lösten sie eine böse Vorahnung aus: Das ist erst der Anfang. Schon drei Wochen später bestätigen sich ihre Vorahnungen. Am 19. Januar 2016 bekommt sie eine E-Mail zugespielt, die angeblich vom staatlichen ukrainischen Stromversorger Ukrenergo verschickt wurde. Ihr Anhang enthält einen Computervirus, der sich in Computersystemen festsetzen und verbreiten kann. Die Angreiferinnen nehmen sich ein ganzes Jahr Zeit, um sich umzuschauen und einen Angriff zu planen, der jenen von 2015 in den Schatten stellen wird.

3. Akt: Automatische Schadsoftware im Elektrizitätswerk

Am 17. Dezember 2016 ist es so weit: Kurz vor Mitternacht fällt in grossen Teilen Kiews der Strom aus. Der IT-Sicherheitsexperte und Forscher Oleksii Yasinskyi ist diesmal selbst betroffen. Er erinnert sich an den Blick aus dem Fenster seines Wohnblocks, der ihn erschaudern liess: So schwarz hat er seine Heimatstadt Kiew noch nie gesehen: «Unser ganzer Wohnblock lag im Dunkeln, das ganze Viertel.» Das Stromunternehmen Ukrenergo meldet eine massive Cyber-Attacke.

Yasinskyi untersucht den Vorfall damals im Auftrag Ukrenergos. Er sieht, dass die Angreifer über lange Zeit intensiv Daten gesammelt und gelernt haben, wie das System funktioniert. Als er schliesslich tatsächlich entsprechende Befehle im Code findet, die offenbar mit der Steuerung von Industrieanlagen zu tun haben, schwant ihm: Das ist eine neue Stufe. Dies-

mal haben sich die Angreiferinnen nicht darauf verlassen, alles von Hand aus der Ferne zu steuern.

Auch Marina Krotofil ist alarmiert, als sie den Angriff analysiert. Im Gegensatz zu den Attacken ein Jahr zuvor brauchte es keine Menschen, die von irgendwo auf der Welt zeitgleich einen Angriff manuell steuerten. Die Schadsoftware konnte – einmal auf dem System angekommen – einen Angriff komplett automatisch ausüben. Die Angreifer brauchten dann nicht einmal mehr eine Internetverbindung. Wie eine Zeitbombe war sie aus der Ferne scharf geschaltet worden für diesen Moment, die Tage um Weihnachten, kurz vor Mitternacht.

Was sowohl Yasinskyi als auch Krotofil betonen: Der Schaden hätte sehr viel grösser ausfallen können. Dass der Strom in diesem Fall bereits nach einer Stunde wieder da war und die Angreiferinnen seither das ukrainische Stromnetz verschonen, sei kein Zufall. Und es bedeute nicht, dass sie nicht in der Lage wären, mehr Schaden zu verursachen. «Es war eine Übung», sagt Yasinskyi, «sie sind mit ihrem Spiel noch nicht fertig.»

Intermezzo: Angriff auf eine Chemiefabrik in Saudiarabien

Nach den Lehren im Energiesektor der Ukraine entwickelten die Angreifer offenbar ihre Fähigkeiten im sogenannten cyberphysischen Bereich weiter: Sie wurden immer besser darin, physischen Schaden anzurichten. Eine äusserst gefährliche Fähigkeit, wie sich im August 2017 zeigt.

In einer petrochemischen Fabrik in Saudiarabien fällt ein Sicherheitssystem aus – und wie eine genaue Analyse, unter anderem von Marina Krotofil, zeigt, ist auch hier ein ausgefeilter Cyber-Angriff die Ursache. Die Täter haben sich dafür seit langer Zeit in den Systemen der Fabrik bewegt und kennen diese wie ihre Hosentasche. Der Angriff, den die IT-Sicherheitscommunity «Triton» taufen wird, scheitert glücklicherweise an einem Fehler der Angreifer, der schliesslich auch zu ihrer Entdeckung führt. Wären sie nicht gestoppt worden, hätten sie Menschenleben gefährdet: Die Täterinnen hätten beispielsweise eine Explosion herbeiführen oder grosse Mengen giftiger Gase austreten lassen können.

Das US-Sicherheitsunternehmen Fireeye hat nach eigenen Angaben Spuren im Code gefunden, die zu einem staatlichen russischen Forschungsinstitut in Moskau führen. Fireeye betont aber, dass es keine konkreten Beweise gefunden hat, die eindeutig belegen, dass dieses Institut Triton entwickelt hat. Die US-Regierung hingegen scheint sich recht sicher zu sein – jedenfalls hat das amerikanische Finanzministerium im Oktober 2020 Sanktionen gegen das Institut verhängt.

Das US-Sicherheitsunternehmen Dragos bezeichnet die Gruppe hinter Triton als die «mit Abstand gefährlichste öffentlich bekannte Bedrohung», und gibt an, beobachtet zu haben, wie sie neue Ziele in den USA und Europa ausspioniert. Auch Sicherheitsforscherin Krotofil sieht immer wieder Spuren von Triton bei ihren Analysen in den Netzwerken kritischer Infrastrukturen – auch in Europa. Das heisse allerdings noch nichts Konkretes: «Das ist völlig normal, alle Angreifer scannen das Internet immerzu ab.» Sie suchen nach Lücken, vielleicht versuchen sie, einzelne Anlagen anzugreifen, vielleicht kommen sie sogar ein Stück weit, bewegen sich durch die Systeme. «Aber das heisst nicht, dass sie es schaffen, tatsächlich die Kontrollsysteme zu erreichen», sagt Krotofil, «denn das ist ein sehr langer, sehr aufwendiger Weg, ohne Garantie auf Erfolg.»

In Saudiarabien waren die Täterinnen kurz davor, eine Katastrophe auszulösen. Krotofil sieht Triton als eine bewusste und weitreichende Entscheidung Russlands, in den Cyber-War zu investieren. Dass die Angreifer auf der Suche nach neuen Zielen sind, bedeute zwar nicht, dass der nächste lebensgefährliche Angriff bereits vor der Tür steht. Aber sie bauten sich damit ein dauerhaftes Fundament für künftige Zwecke.

4. Akt: Die massive Cyber-Invasion

Der 27. Juni 2017 markiert den Tag der bislang grössten Cyber-Operation gegen die Ukraine. Das öffentliche Leben wird massiv ausgebremst und in einigen Fällen lahmgelegt. Auf einmal sind einige Regierungs- und Bankwebsites nicht mehr zu erreichen. Alles ist verschlüsselt. Die Erpresserinnen verlangten Lösegeld. Es ist der Tag, an dem Cloud-Unternehmer Malezhik in seinem Büro die Anrufe seiner Kunden entgegennimmt, die über verschlüsselte Daten klagen.

Es ist der Start der NotPetya-Attacke, die weltweit einen Milliardenschaden anrichten wird und hinter der – nach allem, was man weiss – der russische Geheimdienst steht. «Die ukrainische Regierung hatte kurz zuvor Sanktionen ausgesprochen gegen unzählige IT-Unternehmen aus Russland», erinnert sich Malezhik. Die Attacke gibt einen Vorgeschmack auf das, was im Cyber-War möglich ist. Am gleichen Morgen war ein Oberst des ukrainischen Militärgeheimdienstes ermordet worden – mitten in Kiew durch eine Autobombe. Kurz darauf zerstört NotPetya einen grossen Teil der IT-Infrastruktur des Landes.

Während Malezhik rätselt, wie er seinen Kundinnen helfen kann, ist der IT-Sicherheitsexperte Oleksii Yasinskyi auf dem Weg zur staatlichen Oschadbank in Kiew. Nach der anstrengenden Analyse der ausgefeilten Angriffe auf die Stromkonzerne wirkt das Problem erstmal wie ein üblicher Ransomware-Angriff krimineller Hacker. Doch als Yasinskyi bei der Bank ankommt, wird ihm klar: Das ist etwas Besonderes. Das Ausmass des Problems baut sich buchstäblich vor seinen Augen auf. In der Ecke eines Raumes stapeln sich die Laptops meterhoch, mit denen die Bankangestellten bis zu diesem Morgen gearbeitet haben – bis zeitgleich auf allen Bildschirmen die Nachricht auftauchte «Ups, Ihre Dateien sind verschlüsselt». Dazu: eine Lösegeldforderung. «Auf der anderen Seite des Raums haben IT-Mitarbeitende eilig einen neuen Laptop nach dem anderen ausgepackt und eingerichtet», erinnert sich Yasinskyi.

Die Techniker der Bank hatten gar nicht erst versucht, das Lösegeld zu bezahlen (zum Glück, wie sich später herausstellen wird). Dafür ist keine Zeit, wenn die zweitgrösste Bank des Landes paralysiert ist. Sie hatten einfach alle verschlüsselten Laptops eingesammelt und waren ausgeschwärmt, um in den umliegenden Technikgeschäften so viele neue Geräte wie möglich zu kaufen. Die Oschadbank hat mit ihren 6000 Filialen eines der grössten Filialnetze in der Ukraine, Millionen Kundinnen verlassen sich auf sie. Doch innerhalb weniger Minuten geht gar nichts mehr. Am Nachmittag bilden sich lange Schlangen an den wenigen funktionierenden Geldautomaten der Stadt.

Fachleute schätzen, dass beim Angriff mit NotPetya 10 Prozent aller Computer der gesamten Ukraine für immer verschlüsselt worden sind. Viele grosse Unternehmen sind betroffen, zentrale Infrastrukturen – mehrere Banken, zwei Flughäfen, die staatliche Eisenbahngesellschaft, sogar das Atomkraftwerk in Tschernobyl. Bald sind Laptops und Computer Mangel-

ware, viele Unternehmen brauchen Wochen, um ihre zerstörte Infrastruktur wiederherzustellen.

Yasinskyi kopiert sich die Logdateien aus den Systemen der Oschadbank und schaut sie sich im Büro genauer an. Andere Sicherheitsforscher analysieren derweil den Code aus Samples des Virus. Schnell war laut Yasinskyi klar, dass es sich um einen betrügerischen Virus handelte, der sich lediglich als Ransomware verkleidet hatte.

Die Bildschirm-Meldung mit der Forderung nach Lösegeld ist nur ein Trick, um die Opfer auf die falsche Fährte zu locken und die Gegenmassnahmen zu bremsen. «Die Dateien waren nicht so verschlüsselt, dass man sie mit einem Entschlüsselungscode hätte retten können», sagt Yasinskyi. Um ihre Verfolgerinnen weiter in die Irre zu führen, hatten die Angreifer zudem einige Teile einer damals sehr aktiven Schadsoftware in den Code kopiert: Petya war ein Verschlüsselungstrojaner, der damals häufig von Kriminellen genutzt wurde. Auch die Ransomware-Notiz auf den Bildschirmen war von dort kopiert. «Deshalb dachten alle zuerst, dass es sich um Petya handelt», sagt Yasinskyi. Der zentrale Unterschied war aber, dass sich die Daten nicht wieder entschlüsseln liessen. «Wir sagten deshalb: It is NOT Petya.» Seither heisst der Virus NotPetya.

Am Abend haben Yasinskyi und seine Kollegen ein klareres Bild: Es handelt sich um einen Computerwurm, der sich rasend schnell ausbreitet – unter anderem durch das Update einer Steuersoftware namens Medoc – und ausserdem seine Opfer täuscht. Die Daten sind nicht vorübergehend verschlüsselt, sie sind für immer verloren. Yasinskyi sieht, dass die Schadsoftware sich irgendwie die Anmeldedaten des Administrators aneignet – und damit lässt sie sich innerhalb eines Netzwerks nicht mehr aufhalten. Der Administratoraccount hat alle Rechte, mit ihm kann der Wurm andere Accounts übernehmen, alle Passwörter auslesen und sich bis in die hintersten Winkel eines Systems ausbreiten, was er in atemberaubender Geschwindigkeit tut. Die Folgen sind verheerend. Yasinskyis Arbeitgeber ISSP bezeichnet den Angriff am nächsten Morgen als «massive, koordinierte Cyber-Invasion».

Ich will es genauer wissen: Warum verbreitete sich der Wurm so schnell?

NotPetya verbreitete sich durch das Update einer Steuersoftware, die in der Ukraine so gut wie jeder nutzt: Medoc. Deshalb traf der Angriff auch internationale Unternehmen, die in der Ukraine Geschäfte machen wie Maersk oder Merck. Deren Systeme waren an jenem Tag im Juni 2017 innerhalb weniger Minuten für immer verschlüsselt. NotPetya ist damit auch einer der ersten Angriffe einer neuen Generation: Sogenannte Supply-Chain-Attacken infizieren Unternehmen über ihre Zulieferer – meist über eine verbreitete Software. Das macht diese Angriffe besonders effizient.

Einige westliche Firmen, die in der Ukraine Geschäfte machen, überlebten den Angriff nur knapp. Nach Schätzungen der US-Regierung belief sich der Gesamtschaden auf über 10 Milliarden US-Dollar. Allein das Pharmaunternehmen Merck erlitt einen Verlust über 870 Millionen US-Dollar, das Versandunternehmen FedEx 400 Millionen US-Dollar, der französische Industriekonzern Saint-Gobain 384 Millionen und der Logistikdienstleister Maersk 300 Millionen. Deutschland gilt als das Land, das nach der Ukraine am zweithäufigsten betroffen war mit 9 Prozent aller Infektionen.

Selten sind sich Sicherheitsforscherinnen so einig, wer dahintersteckte: Russland, genau genommen eine Elite-Hackergruppe des russischen Geheimdiensts GRU, die Sicherheitsforscher als «Sandworm» bezeichnen.

5 Akt: Die unauffälligen Schläfer

Einige Wochen nach dem NotPetya-Angriff, als alle bereits wieder zur Tagesordnung übergegangen sind, macht Yasinskyi weitere beunruhigende Entdeckungen. Ihm war schon zuvor ein seltsames Muster aufgefallen: Fast alle betroffenen Unternehmen hatten einige Computer, die auf rätselhafte Weise von der Attacke verschont geblieben waren. NotPetya hatte einen Bogen um sie gemacht. Zunächst hielt er das für Glück: «Man kann sein Netzwerk viel leichter wieder aufbauen, wenn noch etwas davon vorhanden ist.» Und das nutzten die Unternehmen dankbar. Jeder atmete auf, wenn ein Teil der Infrastruktur verschont geblieben war – ein Server etwa oder ein Computer mit nicht verschlüsselten Daten. Das war immerhin eine Basis für den Wiederaufbau.

Aber irgendwann entdeckt Yasinskyi eine auffällige Systematik: «Von den meisten Unternehmen sind etwa 90 Prozent der Computer verschlüsselt worden, aber 10 Prozent nicht.» Welche Eigenschaft hatten jene Geräte gemein, die verschont geblieben waren? Sie waren meist ebenfalls Teil des Netzwerks, der Wurm hätte sie erreichen können und müssen. Was hat NotPetya daran gehindert, diese Geräte zu infizieren?

Als sich Yasinskyi einige der nichtverschlüsselten Geräte genauer ansieht und auf deren Festplatten nach Spuren von NotPetya sucht, macht er eine unheimliche Entdeckung: Jedes von ihnen trug eine bestimmte Datei, nach der der Virus zunächst sucht, wenn er ein neues Gerät infiziert. Ist die Datei vorhanden, bleiben die Daten unverschlüsselt. Es ist ein Mechanismus, um manche Geräte bewusst auszunehmen. Die Täterinnen hatten ihn selbst eingerichtet. Yasinskyi dämmert es: «Es waren alle Geräte infiziert – aber nicht alle verschlüsselt.»

Die einzige Erklärung, die Yasinskyi dafür einfällt: So bleiben die Täter im System. Hätte NotPetya alle Geräte eines Unternehmens verschlüsselt, hätten die betroffenen Unternehmen diese komplett ersetzt – und damit eventuelle weitere verborgene Zugänge, die die Angreiferinnen eingebaut hatten, verschlossen. Wenn sie hingegen dafür sorgten, dass einige wenige Geräte erhalten blieben, konnten sie mittels gut versteckter Hintertüren im System bleiben und sich später durch das Unternehmensnetzwerk auch wieder auf andere Geräte ausbreiten.

Solche «Sleeper Agents», wie Yasinskyi sie nennt, hat er schon öfter gesehen: Angreifer versuchen, auch nach einer erfolgreichen Attacke unentdeckt im System zu bleiben, als unauffällige Schläfer. In gut versteckten Dateien, die kaum zu finden sind. Sie wollen einen Fuss in der Tür behalten für Spionage und künftige Attacken. Die Strategie der Angreiferinnen ist in der Regel erfolgreich, sagt Yasinskyi: «Die Wahrheit ist: Du wirst einen Angreifer nicht los in deinem System.»

Genau das scheint die russische Elite-Hackergruppe Sandworm seit Jahren zu machen, wie die Recherchen von Yasinskyi zeigen. Im schlichten Konferenzraum von ISSP projiziert er eine eng bedruckte Infografik auf den Bildschirm: darauf unzählige Cyber-Attacken, unter anderem jene von 2015 und 2016 auf ukrainische Energieversorger, jene auf Starlight Media 2015, diverse Attacken auf Ministerien wie das Finanzministerium in Kiew.

Darunter in leuchtend roten Feldern die Attacken von 2017: Xdata – eine Ransomware, die ebenfalls durch die Hintertür der Steuersoftware Medoc verbreitet wurde, NotPetya und einige weniger bekannte.

Zwischen ihnen finden sich Felder mit durchnummerierten «Medoc-Backdoors», das erste von April 2017. Yasinskyis Verdacht ist erschreckend: Bereits im April haben die russischen Angreiferinnen die Updates der Steuersoftware manipuliert und Angriffe durch diese verbreitet. Lange bevor NotPetya zuschlug. Wären diese Angriffe auf Medoc entdeckt worden, hätte NotPetya verhindert werden können.

Die Grafik wirkt wie die Waggons eines Zugs – erst eine überarbeitete Hintertür, dann ein Angriff. Der letzte Angriff in der Reihe ist NotPetya. Was, so fragt sich Yasinskyi im Dezember 2021, kommt wohl als Nächstes?

6. Akt: Die Löschattacke kurz vor dem Krieg

Am Nachmittag vor dem Einmarsch russischer Truppen in die Ukraine verbreitet sich eine sogenannte Wiper-Schadsoftware in zahlreichen ukrainischen Systemen. Insbesondere in denen von Unternehmen, die Vertragspartner der ukrainischen Regierung sind. Die Software ist laut Einschätzung von Sicherheitsexperten durchaus ausgefeilt. «Wiper» bedeutet eine Löschattacke: Damit werden Computerfestplatten und ganze Systeme gelöscht. In diesem Fall offenbar besonders gründlich. Die beiden Sicherheitsunternehmen ESET aus der Slowakei sowie Symantec aus den USA fanden die Schadsoftware auf Hunderten Systemen ihrer Kundschaft in der Ukraine und offenbar auch in den Nachbarländern Lettland und Litauen. Sicherheitsforscherinnen vergleichen den Löschalgorithmus unter anderem mit dem Angriff auf Sony Pictures 2014, bei dem innerhalb von wenigen Minuten weltweit ungefähr die Hälfte aller Daten von Sony gelöscht waren. Hinter diesem Angriff steckte Nordkorea. Im jetzigen Fall der Ukraine ist es sehr wahrscheinlich, dass staatliche russische Akteure die Urheber sind – entsprechende Analysen laufen noch.

Im Gegensatz zu «Hermetic Wiper», wie ESET den Löschangriff im Vorfeld des Einmarsches russischer Truppen nannte, haben die weit weniger ausgefeilten DDoS-Attacken (Angriffe mit dem Ziel, Websites im Internet unerreichbar zu machen) im Januar und Februar aus der Sicht von Sicherheitsforscherin Marina Krotofil nur eine geringe Rolle gespielt für die russische Angriffsstrategie: «Sie verfolgten keinen grösseren strategischen Zweck als die allgemeine Demoralisierung der Bevölkerung und die Einschüchterung der nationalen Cyber-Kräfte.» Aus ihrer Sicht sind die Angriffe von russischer Seite aber strategisch nicht besonders schlau: «Die kontinuierlichen Angriffe seit 2014 machten das Land mental und technisch widerstandsfähiger» – die Ukraine sei viel besser darauf vorbereitet, strategische Operationen zu vereiteln. Nicht zuletzt rückten die USA als Verbündete näher an die Ukraine und helfen auch in der digitalen Verteidigung. Das Weisse Haus hat mehrfach angekündigt, die Ukraine bei Cyber-Angriffen zu unterstützen und auch auf diese zu reagieren.

Epilog: Die Zukunft des Cyber-War

Was heisst das alles für die Gegenwart und die Zukunft des Cyber-War? Die russischen Aktivitäten sind nur bedingt einzigartig, betont Krotofil: «Viele Nationen bauen gerade ihre Kapazitäten für digitale Angriffe aus.» So wie auch in der analogen Welt Waffen und Kapazitäten bereitgehalten werden für den Fall eines Krieges. Ob analog oder digital – Angriffe seien in

der Theorie immer einfacher als in der Praxis: Bei Militäraktionen wie bei Cyber-Attacken kann Unvorhergesehenes geschehen – so wie beim Triton-Angreifer, der an irgendeinem Faktor in der Realität scheiterte, den er nicht bedacht hatte. Die Tatsache, dass Russland in derart komplexe Angriffe wie Triton investiere, sei aber auf jeden Fall sehr beunruhigend.

Spätestens mit Triton wurde ein Programm geschrieben, das den Angriff vollständig automatisiert. Das hebt die russischen Staatshackerinnen auf eine Stufe mit denen der USA und Israels. Die einzigen Nationen, die bisher – zumindest soweit öffentlich bekannt – in der Lage sind, derart ausgefeilte automatisierte Attacken auf Industrieanlagen auszuführen und dabei tief in deren Steuerung einzudringen. Die beiden Länder hatten 2010 mit Stuxnet einen berühmt gewordenen Angriff auf eine iranische Uranaufbereitungsanlage gestartet, der das dortige Atomprogramm stoppen sollte.

Aktuell nutzt das russische Militär nach dem Einmarsch eher seine Möglichkeiten vor Ort und aus dem Luftraum, um kritische Infrastrukturen in der Ukraine anzugreifen. Von daher stehen wenn, dann eher westliche Infrastrukturen im Fokus russischer Cyber-Angriffe. Russlands Präsident Putin hat mit markigen Worten angekündigt, jedem Angriff zu begegnen mit Konsequenzen, die die Angreifer «in ihrer Geschichte noch nie erlebt haben». Wer auch immer sich in die russischen Verhältnisse einmische, müsse mit entsprechenden Massnahmen rechnen. Angesichts der Sanktionen gegen Russland steigt die Gefahr russischer Cyber-Angriffe auf westliche Länder zur Vergeltung. «Es kann dadurch auch zu Ausfällen oder Einschränkungen bei kritischen Infrastrukturen wie etwa Strom und Wasser kommen», sagt Manuel Atug, ein deutscher Sicherheitsexperte für kritische Infrastrukturen.

Dabei ist es wichtig, wenn das Thema hybride Kriegsführung nun mehr Aufmerksamkeit bekommt, denn diese findet nicht nur in Kriegszeiten statt, im Gegenteil, erklärt Atug, der auch Sprecher der unabhängigen Arbeitsgruppe Kritis ist: «Der Zweck hybrider Kriegsführung ist es, im Vorfeld eines militärischen Eindringens beispielsweise die Kommunikation des Gegners mit digitalen Attacken lahmzulegen oder den Energiesektor anzugreifen, damit der Gegner schon vor dem Einmarsch geschwächt ist.» Solche Angriffe benötigten einen langen Vorlauf an Vorbereitung, und diese fänden in Friedenszeiten statt. Atug: «Cyber-Spionage – auch Aufklärung genannt – wird daher die ganze Zeit vorgenommen.»

Atug geht davon aus, dass sich staatliche Akteure wie Geheimdienste und Militärs verschiedener Länder auch in den kritischen Infrastrukturen Europas bewegen und diese ausspionieren. Sie dort zu finden, das sei nicht einfach: «Staatliche Akteure haben das Ziel, lange unentdeckt zu bleiben und spionieren zu können», sagt er. «Im Krieg werden diese Zugänge dann für offensive Angriffe mit cyberphysischen Auswirkungen eingesetzt.» Aus seiner Sicht sollte das verboten sein: «Es ist eine ernsthafte Bedrohung für die Zivilbevölkerung, ein erhebliches Risiko für die Aufrechterhaltung kritischer Infrastrukturen.»

Ob und wo es in den kommenden Wochen auch zu Angriffen auf westliche Infrastrukturen kommt, ist offen. Die Angreiferinnen sind zu gut versteckt. Sicher ist nur: Die russischen Staatshacker haben ihre Füsse in vielen Hintertüren – längst nicht mehr nur in der Ukraine, sondern auf der ganzen Welt.