CONSTANZE KURZ UND FRANK RIEGER

CYBERWAR – DIE GEFAHR AUS DEM NETZ

Constanze Kurz und Frank Rieger

CYBER WAR

DIE GEFAHR AUS DEM NETZ

**Wer uns bedroht
und wie wir uns wehren können**

C. Bertelsmann

Verlagsgruppe Random House FSC® N001967

1. Auflage September 2018

Umschlag: Büro Jorge Schmidt, München
Umschlagmotiv: © deepadesigns/shutterstock
Gestaltung und Satz: Uhl + Massopust, Aalen
Gesetzt aus der Sabon
Druck und Bindung: GGP Media GmbH, Pößneck
Printed in Germany
ISBN 978-3-570-10351-7

www.cbertelsmann.de

Dieses Buch ist auch als E-Book erhältlich.

Inhalt

Einleitung

Das Schlachtfeld ist überall

Wir leben in einer durchdigitalisierten Welt. Unsere Abhängigkeit von Mobiltelefonen, Internet, Computern ist total. Auch wenn man selbst ohne vernetzte Geräte lebt: Der Strom aus der Steckdose, das Geld aus dem Automaten, die vollen Regale im Supermarkt, die Bahn zur Arbeit, die Fußballübertragung im Fernsehen, die Produktion von Autos und Maschinen – praktisch alle Aspekte des Lebens funktionieren nur, wenn Computer und Netze störungsfrei ihren Dienst verrichten. Fast alle diese Systeme, von denen die moderne Welt abhängt, weisen Schwachstellen, Angriffspunkte, Verwundbarkeiten auf. Früher war deren Ausnutzung nur ein Hobby für neugierige Hacker oder ein Mittel zum Zweck für Onlinekriminelle. Heute sind es jedoch Staaten, die mit ihren ungleich größeren Ressourcen den systematischen Angriff auf die Fundamente der digitalen Welt vorbereiten und auch erproben.

Kriegführung im digitalen Raum ist nicht gänzlich anders als bisherige Formen kriegerischer Auseinandersetzung, hinzukommen jedoch weitere Dimensionen wie Cyberspionage, Desinformations- und Einflussoperationen sowie strategische Aktivitäten zur Erringung von vorteilhaften Positionen. Ob es sich überhaupt um einen militärischen oder geheimdienstlichen Angriff handelt (und nicht etwa um normale Onlinekriminalität), wer der Urheber und was

das eigentliche Ziel einer Attacke ist – nicht einmal auf die grundlegenden Fragen eines Konfliktes gibt es verlässliche Antworten.

Trotzdem – oder genau deswegen? – überschlagen sich Militärs und Geheimdienste seit einigen Jahren dabei, eigene Einheiten für Cyberangriffe aufzubauen. Es wird um Budgets und Befugnisse gerangelt und vor allem um talentiertes Personal geworben. Als durch die Enthüllungen von Edward Snowden ab Sommer 2013 klar wurde, wie umfangreich die Fähigkeiten der Amerikaner und Briten auf dem Gebiet der Cyberspionage sind, war die Begierde erst recht geweckt.

Computer und Netze sind die essenziellen Informationslebensadern der modernen Gesellschaften. Angriffe gegen sie können Teil einer umfassenderen Aggressionsstrategie sein. Deswegen tönen bei jedem Anzeichen eines größeren Cyberangriffs in den Lagezentren die Alarmsirenen: Wer weiß schon, ob es sich nicht um einen Vorstoß im Rahmen einer groß angelegten Offensive handelt, deren weitere Elemente man nur noch nicht gesehen hat? Die Grenzen und Mittel von Kriegen im Digitalzeitalter sind schwer auszumachen. Geschickte Kombinationen von Infrastrukturstörungen, Netzwerkangriffen und Trojanern im Konzert mit Desinformation (»Fake News«), Wahlbeeinflussung und politischen Aktionen können eine große Wirkung entfalten und eine Gegenwehr schwer machen.

Um eine Übersicht über das Treiben der verschiedenen Akteure und ihre Interessenlagen zu bekommen, wollen wir einen Blick hinter die Kulissen werfen. Dazu hilft es, sich vor Augen zu führen, wie sich die digitale Welt verändert hat, seit die Netze und Computer zu Schlachtfeldern geworden sind, auf denen sich allerhand potente Akteure tummeln.

Um verständlich zu machen, warum unsere Software und Hardware so verwundbar sind, werden wir erklären, welche Schwachstellen digitale Angreifer typischerweise ausnutzen und wie sie beim Bau ihrer Cyberwaffen vorgehen.

Zwar umweht der Mythos des Hackers den Cyberraum, doch die Praxis des Hackens hat in der Realität nur noch wenig zu tun mit den Darstellungen, die man aus Filmen oder Vorabendserien kennt. Die IT-Sicherheitsbranche hat sich längst professionalisiert und folgt den Regeln des Marktes, der mit den Geldern von Kriminellen, Geheimdiensten oder Militärs befeuert wird. Welche weiteren verschiedenen Akteure mit welchen Motiven ihren Anteil an der heutigen IT-Sicherheitsmisere haben, werden wir ebenfalls beleuchten.

Natürlich ist der Zeitpunkt des Buches fünf Jahre nach Beginn der Enthüllungen von Edward Snowden nicht zufällig. Nicht nur, weil es aus den Papieren, die er ans Licht der Öffentlichkeit gebracht hat, qualitativ und quantitativ viel Neues über die Praktiken der Geheimdienste zu lernen gab, sondern auch, weil nach Bekanntwerden dieser brisanten Informationen eine neue Diskussion beginnen konnte. Denn was nicht mehr zu leugnen ist, bedarf eben der Rechtfertigung. Im Nachgang des Snowden-Erdbebens kann heute ehrlicher über die strategischen Interessen der digitalen Angriffsmächte, allen voran der Vereinigten Staaten, gesprochen werden.

Staatlich finanzierte Cyberoperationen sind untrennbar verbunden mit dem irreführenden Begriff »Fake News«. Wir widmen daher ein Kapitel unseres Buches dem Komplex Desinformation und Einflussoperationen, in denen erhackte Informationen, Leaks und die destruktive Nutzung sozialer Medien eine zentrale Rolle spielen.

Der Begriff »Cyber« ist allein stehend im Englischen ein Synonym geworden für alles Digitale, zugleich aber vom amerikanischen Militär übernommen und allzu kriegerisch umgedeutet worden. Uns hat es zunächst widerstrebt, dem Buch den Titel »Cyberwar« zu geben. Denn er bringt zwangsläufig den Krieg in unsere zivilen Netze. Doch wenn man ehrlich auf die derzeitige Situation blickt, kommt man nicht umhin, die Anzeichen der kriegerischen Handlungen zu sehen: die immensen Summen für die digitalen Angriffe, der professionalisierte Waffenbau, die Strategien und Taktiken sowie die Militärs selbst als Akteure. Dabei ist es kein Zufall, dass die aktuellen Ausformungen des »Cyberwars« sich entlang der Kriege entwickeln, die mit konventionellen Waffen ausgetragen werden. Mehr noch, digitale und konventionelle Kriege wachsen immer stärker zusammen.

Auch wenn es vielen heute so vorkommen mag: Mit den derzeitigen katastrophalen Sicherheitsbedingungen von Hard- und Software muss sich niemand dauerhaft abfinden. Deswegen unterbreiten wir zum Schluss des Buches Vorschläge, wie man eine bessere und weniger verwundbare digitale Welt bauen könnte, in der die grassierende IT-Vertrauenskrise nach und nach überwunden werden kann. Dass allerdings der aktuelle Zustand in der IT-Sicherheit überwunden werden muss, ist eine Notwendigkeit. Diskutiert werden muss daher nicht das Ob, sondern nur noch das Wie.

Alarmstufe 2

Ein Cyberangriff und seine Folgen

Berlin, Ostersonntag, der 9. April 2023

Der Morgen ist kühl und feucht. Trotzdem sitzt Fjodor Bernhart auf dem Fahrrad. Er wird den ganzen Tag vor Monitoren verbringen und es bestenfalls kurz zur Kantine ins Nachbargebäude schaffen, deshalb braucht er die Bewegung am Morgen und Abend, egal wie das Wetter ist. Am Pförtnerhaus seiner Behörde hat sich eine Schlange gebildet, die Kollegen der Frühschicht im Gemeinsamen Cyber-Lagezentrum Deutschland sehen schon etwas genervt aus. Offenbar gibt es ein Problem mit der Zugangskontrollanlage. Der Pförtner wirkt zunehmend verzweifelt. Die Mutmaßungen von drei Dutzend Behörden-Nerds, was denn nun das Problem sein könnte, helfen auch nicht weiter.

Direkt vor Fjodor stehen zwei jüngere Beamte in der Schlange, einer spielt auf seinem Telefon einen Song vor und erzählt, wie er ihm gestern den Feierabend vermasselt hat. Als das Lied in seinem Musikstream lief, spielte plötzlich sein Auto verrückt. Die Fenster gingen auf, die Heizung stellte sich auf Maximalleistung, und der Bordassistent versuchte, nacheinander die Kontakte aus seinem Telefonbuch anzurufen, während auch noch der Warnblinker aktiviert wurde. Das alles passierte, erklärt der Autobesitzer dem Kollegen, weil der Song, so zumindest die erste Erkenntnis,

neben einem sehr eingängigen Beat aus darin versteckten, nur für Maschinen hörbaren Sprachkommandos bestehe. Diese wiederum manipulieren die inzwischen überall in Autos verbauten Assistenzsysteme. Die beiden beschließen herauszufinden, wie viele andere Autofahrer das gleiche Problem hatten und ob die großen Musikstreaminganbieter das Lied schon von ihren Plattformen verbannt haben. Immerhin erledigen die Kollegen schon mal ihre Arbeit, bevor sie am Arbeitsplatz sind, denkt sich Fjodor beim Zuhören, während die Schlange immer länger wird.

Nach ein paar Minuten wird klar, dass die elektronische Zugangskontrolle wohl nicht so bald wieder in Gang zu setzen sein wird. Fjodor ist der ranghöchste Beamte, der hier auf Einlass wartet, also lässt er sich vom Pförtner das Festnetztelefon geben und verhandelt mit dem Schichtleiter der privaten Sicherheitsfirma, die das Gelände bewacht. Danach dürfen die Mitarbeiter nach Sichtkontrolle der Dienstausweise hereingelassen werden. Noch während sich die Schlange abbaut, beginnen erst Fjodors Telefon und wenig später auch die Geräte fast aller anderen Kollegen zu brummen und zu vibrieren. Die Schritte werden schneller, alle joggen zu der großen Betonhalle, in der das Lagezentrum gerade erst letzten Winter eröffnet worden ist.

Cyberalarm, Stufe 3. Das bedeutet, dass mehrere große oder wichtige Systeme betroffen sind, aber keine landesweite kritische Infrastruktur. Herbert Ganz, ein graubärtiger Zyniker, der seit Jahrzehnten im Staatsdienst ist und von dem es heißt, er sei früher beim BND gewesen, aber wegen irgendeines Skandals zum Cyber-Lagezentrum weggelobt worden, ist der Schichtleiter der Nachtschicht. Er brieft Fjodor kurz: Seit 5:45 Uhr, also genau zum Eintreffen der Frühschicht, die um sechs Uhr beginnt, zeigten die

Monitoring-Systeme mehrerer Internetprovider einen massiven Anstieg der übertragenen Datenmengen, zum Teil bis an die Kapazitätsgrenzen.

Es gibt schon reihenweise Warnungen, dass Banken und öffentliche Einrichtungen nicht erreichbar sind, auch Nutzer im Internet berichten darüber, zumindest soweit die Social-Media-Seiten noch funktionieren. Man wisse noch nichts Genaues, so Ganz in seinem Briefing, die automatischen Meldesysteme hätten aber reagiert und einen Stufe-3-Alarm ausgelöst. Er würde Fjodor empfehlen, nach Freiwilligen aus der Nachtschicht zu fragen, die noch dableiben könnten, das Ganze sehe für ihn nach einem größeren Ding aus. Er selbst müsse jetzt aber leider los, schließlich ist Ostern und die Familie …

Fjodor zögert kurz und folgt dann dem Ratschlag. Er stellt sich vor die große Monitorwand des Lagezentrums und bittet um Ruhe. »Wir haben es hier offenbar mit einem umfangreicheren Problem zu tun. Wenn das noch weiter eskaliert, kann es sein, dass wir, um genügend Personalstärke zu haben, Stufe 2 ausrufen müssen. Dann war es das ohnehin mit Ostern. Wer also noch dienstfähig ist und es irgendwie einrichten kann hierzubleiben, hebt bitte die Hand. Ich lasse Feldbetten in Konferenzraum 3 aufstellen, wenn Sie sich zwischendurch kurz hinlegen wollen. Und die Kantine wird gleich Kaffee und belegte Brötchen herüberbringen.« Gemurmel macht sich breit. Das klingt ernst. Knapp die Hälfte der Nachtschicht, meist jüngere Mitarbeiter ohne familiäre Verpflichtungen, hebt die Hand und bleibt zu einer zweiten Schicht.

Fjodor fährt fort: »Wir gehen nach dem gleichen Muster vor wie bei der Notfallübung im Februar. Zuerst Statusberichte von den Industrie-CERTs und den Providern einho-

len. Die Verbindungsbeamten nehmen Kontakt zu ihren Lagezentren bei BKA, Bundeswehr CNO, BSI, ZITiS, Verfassungsschutz, BND und NATO auf, ob dort schon eine Einschätzung vorliegt oder jemand eine Idee hat, was eigentlich los ist. Um die EU-Cyberkoordinationsstelle kümmere ich mich.« Fjodor nickt mit dem Kopf Richtung Presseteam: »Social-Media- und News-Monitoring auf das Stichwortmuster für Denial of Service und Hinweise auf neue Trojaner fokussieren, falls die Feeds noch erreichbar sind.« Wieder an alle gerichtet und mit Blick auf die Uhr fährt er fort: »Telefonkonferenz um sieben Uhr mit allen deutschen Behörden, danach Bericht an Innenministerium und Kanzleramt.« Wieder Richtung Presseteam, aber mit besonderer Betonung: »Frau Stolz, Presseanfragen bis auf Weiteres ohne konkrete Details beantworten: Wir wissen Bescheid und kümmern uns um das Problem. Rufen Sie bitte auch die Sprecher der anderen Behörden an, damit keiner mit halb garen Spekulationen aus der Reihe tanzt. Wenn irgendwo etwas Relevantes zu erfahren ist, kurze Zusammenfassung auf den Lageschirm. An die Arbeit!«

Die Meldungen kommen nun in schneller Folge. Das Problem betrifft nicht nur Deutschland, sondern praktisch die gesamte EU, Großbritannien, die Vereinigten Staaten, Australien und halb Asien. Die Übertragungskapazitäten der Internet Exchanges, an denen die großen Provider zusammengeschaltet werden, sind am Limit. Google, Facebook, YouTube und Twitter sind nur noch sporadisch und mit viel Glück erreichbar. Die Mobilfunknetze sind völlig überlastet, internetbasierte Festnetztelefone vollständig ausgefallen. Die Behördennetze funktionieren nur noch teilweise, Onlinebanking ist nicht mehr möglich, und Geldautomaten sind ausgefallen. Die Medien berichten inzwi-

schen pausenlos, auch wenn sie nichts Substanzielles zu sagen haben.

Noch während der Telefonkonferenz mit den Lagezentren der anderen Behörden erhöht Fjodor um 7:10 Uhr die Alarmstufe auf 2. Stufe 1 ist für den Ausfall der Energieversorgung reserviert, die scheint jedoch noch ohne größere Probleme zu funktionieren. Der Krisenstab im Kanzleramt ist zusammengerufen worden. Weil über die Mobilfunknetze kaum noch Daten durchgehen, stößt die Alarmierung der Techniker allerorten auf große Schwierigkeiten. Fjodor hat auf dem kurzen Dienstweg die Feldjäger der Bundeswehr und die Bundespolizei, deren Funksysteme noch funktionieren, dazu herangezogen, wenigstens die von den verschiedenen Bundesbehörden an sein Lagezentrum abgestellten Mitarbeiter einzusammeln.

Der öffentliche Nahverkehr und die Bahn laufen zum Glück noch einigermaßen problemlos, auch wenn niemand mehr Fahrkarten an den Automaten kaufen oder in den Apps nachsehen kann, wann die Züge eigentlich fahren. Onlinezahlung ist so gut wie unmöglich, da kaum noch Internetverbindungen aufgebaut werden können. Damit fallen auch Taxi-Apps, Car-Sharing-Dienste oder das Ausleihen von Fahrrädern über Onlineplattformen aus.

Das Computer Emergency Response Team (CERT) beim Bundesamt für Sicherheit in der Informationstechnik (BSI) liefert schließlich um kurz vor halb acht einen ersten Hinweis darauf, was eigentlich gerade geschieht: Eine Vielzahl unterschiedlicher Digitalgeräte – Computer, Internetrouter, Fernseher, Mobiltelefone, »intelligente« Lautsprecher, vernetzte Produktionsmaschinen, aber auch Autos und internetbasierte Festnetztelefone – hat nahezu zeitgleich um 5:45 Uhr angefangen, Verbindungen zu allen möglichen

Servern im Netz aufzubauen und viele Daten zu übertragen. Die Anfragen an die Server weisen keine gemeinsame Charakteristik auf, die es erlauben würde, den Datenverkehr zu filtern, sie sehen für sich betrachtet eigentlich ganz normal aus. Sie kommen von überall her und gehen in alle Himmelsrichtungen. Es gibt kein konkretes identifizierbares Ziel, wie es normalerweise bei solchen Denial-of-Service-Angriffen der Fall ist.

Um neun Uhr beginnt die Krisensitzung im Bundeskanzleramt. Nicht alle Behörden und Ministerien sind mit ihren Chefs vertreten, viele sind im Osterurlaub, einige im Ausland. Die Videokonferenz-Verbindungen, auf denen normalerweise die Lagezentren der Behörden zugeschaltet werden, funktionieren nur teilweise. Als Erstes werden das Innenministerium, die Bundespolizei und die Bundeswehr angewiesen, mit ihren Fahrzeugen und Hubschraubern die wichtigen Fachkräfte in ihre Dienststellen zu bringen. Dies gilt auch für die Internetanbieter und IT-Sicherheitsfirmen, mit denen das BSI zusammenarbeitet. Der Cyber-Notstand wird intern ausgerufen.

Die erste Bilanz im Kanzleramt fällt gemischt aus. Der plötzliche Ausfall des Internets scheint keine größeren Verkehrsunfälle oder Ähnliches verursacht zu haben, Opfer sind bisher keine zu beklagen, das ist die gute Nachricht. Die Stromversorger melden, dass zwar der Stromhandel lahmgelegt ist und die Steuerung von Solar- und Windenergie versagt hat, aber die konventionellen Kraftwerke funktionieren. Außer den riesigen Mengen Datenverkehr hatten sie keine Anzeichen von Angriffen feststellen können. Die Tankstellen funktionieren zumindest für Barzahler noch. Durch das lange Wochenende sind die Supermärkte geschlossen, um die Lebensmittellogistik muss man sich

also erst einmal keine Gedanken machen. Weil es noch früh am Morgen des Ostersonntags ist, sind noch keine Panikhandlungen zu verzeichnen, allerdings ist klar, dass es dazu kommen wird, sobald immer mehr Menschen aufwachen und bemerken, dass kaum noch etwas funktioniert.

Ein großes Problem sind die massenweise gestrandeten automatischen Lieferdrohnen. Um endlich die mit Kleintransportern zugestauten rechten Spuren in den Innenstädten freizubekommen und der notleidenden deutschen Autoindustrie wieder auf die Beine zu helfen, hatte die Regierung vor zwei Jahren eine aggressive Förderung von rollenden Auslieferdrohnen ›Made in Germany‹ beschlossen. Während der Vorweihnachtszeit Ende letzten Jahres hatte das Programm schon Wirkung gezeigt: Die Lieferdrohnen waren schlagartig hochpopulär geworden, nicht nur, weil es weniger Staus gab, sondern vor allem durch die Ausdehnung der Lieferzeiten in den späten Abend und über das gesamte Wochenende – die Roboterfahrzeuge haben schließlich keine Familie und keine Gewerkschaft.

Nun standen die Lieferdrohnen jedoch nutzlos in der Gegend herum und versperrten Straßen und Gehwege, viele machten dabei auf der Suche nach einer Netzverbindung nervtötende Geräusche. Immerhin gab es noch keine Berichte über Plünderungen oder Gewaltanwendungen gegen die Geräte. Das Innenministerium hatte alle Bundesländer vorsorglich um maximale Polizeipräsenz auf den Straßen gebeten. In als besonders gefährdet eingestuften Vierteln sollen möglichst schnell Beamte aus den Einsatzhundertschaften der Bundespolizei auf Patrouille gehen, um Randalen und Einbrüchen vorzubeugen. Der Cyber-Notstand wird langsam zum echten Ausnahmezustand.

»Wer war das? Hat sich schon irgendjemand dazu be-

kannt?«, lautet die erste Frage des Geheimdienstministers im Kanzleramt, nachdem die Statusberichte vorgetragen wurden und die vorbeugenden Maßnahmen gegen Unruhen und Plünderungen angeordnet sind. »Wir gehen von einem staatlichen oder terroristischen Angriff aus. Die Kollegen bei den Amerikanern denken das Gleiche. Einen solchen Angriff gab es noch nie, das sprengt alle Dimensionen!«, meldet sich Frauke Ebehard, die stellvertretende BND-Chefin und Zuständige für Cyberfragen zu Wort. Dieser Einschätzung schließt sich der Verfassungsschutz an. Das Innenministerium ist nur durch einen parlamentarischen Staatssekretär vertreten, der eigentlich für Flüchtlingsfragen zuständig ist und deshalb liebend gern seiner untergeordneten Behörde, dem BSI, das Wort überlässt. »Wir wissen bisher noch nichts über die Urheber. Die Kollegen in der Slowakei meldeten gerade, dass es ihnen gelungen ist, die Schadsoftware auf einem DSL-Router zu isolieren, die Analyse läuft aber gerade erst, und wir haben noch keine Ergebnisse. Wir versuchen das Gleiche, aber es wird ein paar Stunden dauern, bis wir irgendwas sagen können. Vom Umfang des Angriffs her würden wir aber auch von einem staatlichen Ursprung ausgehen.«

Während die Telefonkonferenz noch läuft, flimmert auf Al Jazeera ein Bekennervideo des »Nation of Islam Cyber Jihad« über die Bildschirme. »Wie sieht der BND das? Ist das glaubwürdig?«, will der Geheimdienstminister wissen. Frau Ebehard vom BND versucht es mit einer Antwort: »Wir haben das jetzt natürlich noch nicht analysieren können, aber diese Gruppe hat nach unserer Kenntnis bisher nichts weiter gemacht, als ein paar Medien-Webseiten anzugreifen. Das sieht so ganz aus dem Bauch heraus eher nach Trittbrettfahrerei aus, aber wir werden dem nachgehen und

die befreundeten Geheimdienste in der Region anfragen.« Der Geheimdienstminister fragt in die Runde: »Wen haben wir sonst, der so was anrichten könnte?« Die BND-Frau sagt mit matter Stimme: »Unsere Lageeinschätzung in der Reihenfolge der Gefährlichkeit führt Russland, China, Iran, Nordkorea und danach ein paar kleinere Staaten auf. Wir holen gerade noch die Meinung der Partnerdienste ein.«

Der Vertreter der Bundeswehr, Generalmajor Schmal, meldet sich zu Wort: »Die NATO-Cyberzentrum-Krisensitzung findet um zehn Uhr statt, wir sind gerade dabei, die Pläne für Gegenschlagsoptionen für die wichtigsten Verdächtigen zu eruieren und dann mit den Partnern abzustimmen. Ein solcher Angriff kann nicht ohne Antwort bleiben!« Die Staatssekretärin aus dem Justizministerium hebt die Hand: »Ich sehe ja noch ein, dass wir die Bundeswehr heute hinzugebeten haben, aber – mit Verlaub – wir wissen doch bisher gar nicht, was geschehen ist. Was reden Sie da von Angriffen und offenbar einer militärischen Antwort?« Danach setzt ein kurzes Schweigen ein, das der Geheimdienstminister mit der Bemerkung unterbricht, dass die Frau Staatssekretärin vielleicht erst Rücksprache mit der Ministerin halten solle, ehe sie versuche, Optionen von vorneherein auszuschließen.

Fjodor, der bisher außer seinem Statusreport nichts gesagt hat, bringt eine Idee vor, die eine Kollegin ihm kurz vor der Konferenz geschickt hat: »Wir werden mit den Internetanbietern und den Partnerbehörden in den anderen EU-Staaten versuchen herauszubekommen, welche Länder weniger oder gar nicht betroffen sind. Vielleicht hilft das ja bei der Eingrenzung der Verdächtigen. Dazu bräuchten wir aber auch eine Priorisierung auf den BND-Überwachungspunkten und Hilfe von den deutschen Botschaften.« – »Machen

Sie das, so schnell es geht«, weist der Kanzleramtsminister an. »Frau Ebehard, sehen Sie zu, dass das Lagezentrum alle Unterstützung bekommt, die es braucht!« Die stellvertretende BND-Chefin wiegt den Kopf: »Wir haben da ein paar Probleme, viele unserer ausländischen Ausleitungspunkte sind auch über das Internet angebunden und liefern derzeit nicht. Die NSA hat das gleiche Problem, sie versuchen gerade, auf Satelliten auszuweichen, um das zu umgehen.« – »So geht es uns auch«, meldet sich das Außenministerium, »wir erreichen unsere Botschaften gerade fast nur auf Kurzwelle und …« – »Dann eben nachfragen, in welchen Ländern das Internet gerade noch geht und wo nicht, das sollte darüber ja wohl möglich sein!«, fällt ihm der Geheimdienstminister ins Wort. Der barsche Tonfall verbirgt kaum seine Verunsicherung.

Nächster Tagesordnungspunkt: Was kann kurzfristig getan werden, um die Lage in den Griff zu bekommen? Das BSI empfiehlt, die Bürger über den Rundfunk dazu aufzufordern, den Datenmodus ihrer Mobiltelefone zu deaktivieren, oder die Geräte ganz auszuschalten und zugleich die Provider anzuweisen, die Internetanschlüsse in den Haushalten lahmzulegen, um die Menge des Datenverkehrs wenigstens so weit zu reduzieren, dass die grundlegenden Funktionen noch gewährleistet oder wieder angefahren werden können. Die Datenübertragung im Mobilfunk vollständig zu deaktivieren, würde das Chaos nur noch verschlimmern, da sowohl Behörden als auch die Industrie darauf angewiesen sind. Die Hoffnung ist, dass die Bürger durch das Ausschalten ihrer Geräte die Netze wieder für die wichtigen Dinge benutzbar machen.

Deutschland ist schließlich dabei aufzuwachen und soll dann möglichst rasch offline gehen. Der Vertreter des Wirt-

schaftsministeriums merkt an, dass man keine gesetzliche Grundlage sehe, nach der man private Unternehmen dergestalt anweisen könnte. Das Kanzleramt will davon nichts hören. Dann solle sein Haus gefälligst eine finden, schließlich habe man genau dafür ja das BSI-Gesetz geändert. »Jetzt ist die Zeit zum Handeln, nicht für juristische Erbsenzählerei!«, beendet der Geheimdienstminister die Konferenz.

Um 14 Uhr tagt die nächste Krisensitzung. Der Netzwerkverkehr ist nach den Aufrufen im Radio und der Abschaltung der meisten Internetanschlüsse zwar zuerst etwas abgefallen, aber nicht weit genug, weil viele Menschen nach dem Aufwachen natürlich zuerst einmal ihre Telefone und Tablets angeschaltet haben, kein funktionierendes Internet zu Hause mehr vorfanden, ins Mobilfunknetz gingen und das Problem damit wieder verschlimmerten. Sprachtelefonie ist in den Mobilnetzen praktisch nur noch für die glücklichen Besitzer einer SIM-Karte mit Behördenpriorität möglich. Das neue 5G-Netz, angeblich konstruiert für gigantische Datenübertragungsraten, ist längst unter der Last von Dutzenden Millionen Endgeräten zusammengebrochen, die nach dem Einschalten alle sofort so viele Daten senden, wie sie nur irgendwie können.

Konventionelle Radioempfänger gibt es in vielen Haushalten nicht mehr. Ob Fernsehen, Hörfunk, Zeitungen, Nachrichtenseiten – der Medienkonsum hat sich fast vollständig ins Netz verlagert, auf das nun kaum noch zugegriffen werden kann. Viele private TV-Sender sind nicht mehr zu empfangen, da auch sie ihre Übertragung zu den Senderstandorten über das Internet abwickeln. Wer doch noch Nachrichten empfangen kann, hört, dass der Tonfall der Sprecher längst in den Katastrophenmodus gewechselt

ist, den man bislang nur von der Berichterstattung über den GAU eines Atomkraftwerks kannte. Niemand weiß, was genau geschehen ist. Da es bislang nur eine kurze offizielle Meldung des BSI gibt, die wenig Informationen liefert, schießen die Spekulationen ins Kraut. Echte und selbst ernannte Experten füllen das Informationsloch mit allerhand Unsinn und Mutmaßungen, aber auch einigen sinnvollen Verhaltenshinweisen: Internetgeräte ausschalten, Radio oder, falls er noch funktioniert, Fernseher anmachen.

Nach wie vor werden die Server im Internet permanent mit Anfragen bombardiert, die Router sind allerorten überlastet. Die Internetprovider versuchen, was sie können, sind aber nun mit der Lage überfordert. Auch die meisten Behörden und Unternehmen sind betroffen: Statt eigener fester Leitungen haben sie sich auf verschlüsselte Virtual Private Networks durch das Internet verlassen, die nun natürlich kaum noch funktionieren.

Nachmittags wird das Lagebild langsam etwas klarer. Es gibt einige Länder, die weniger betroffen sind oder aus denen kein Netzwerk-Störverkehr kommt: Russland, Weißrussland, Thailand, Taiwan, Japan sowie einige kleinere Staaten wie die britischen Überseegebiete. China hat die Verbindungen ins Ausland weitgehend gekappt. Trotz der stark eingeschränkten Kommunikation, die eine internationale Kooperation beeinträchtigt, gibt es erste Analysen der Schadsoftware. Offenbar ist die Infektion über Monate erfolgt, sie betrifft praktisch alle Plattformen der modernen Informationsgesellschaft.

Dem Cyberzentrum der holländischen Behörden ist es gelungen, einen Infektionsprozess zu beobachten. Was sie darüber berichten, ist beängstigend: Die Schadsoftware suchte nach neuen Geräten im Netz, identifizierte

das Betriebssystem und die darauf laufende Software und lud von Servern im Netz die passenden Einbruchswerkzeuge nach. Dabei war sie in den vergangenen Monaten so intelligent, langsam vorzugehen, sodass ihre Verbreitung bisher nicht aufgefallen war. Die NSA schickt an ihre Partnerdienste einen vertraulichen Bericht, wonach der Trojaner auch Einbruchsmethoden angewendet hat, die »uns bekannt, aber nicht öffentlich sind«. Mehr Details gibt die amerikanische Behörde jedoch nicht preis. An diesem Ostersonntag um fünf Uhr morgens stoppten die Neuinfektionen. 45 Minuten später schaltete die Software in den Angriffsmodus und begann, massiven Netzwerkverkehr zu generieren.

Das Cyber-Koordinationskomitee der NATO hatte sich am Vormittag auf 15 Uhr vertagt, um mehr Informationen abzuwarten. Die Cyber-Offensivkräfte aller Verbündeten wurden angehalten, ihre Optionen für Gegenschlagsoperationen gegen die üblichen Verdächtigen zu prüfen. Die US-Präsidentin tritt um 14.30 Uhr vor die Presse und verkündet, was die NSA ihren Partnerdiensten wenige Minuten zuvor per Eildepesche mitgeteilt hat: Die US-Dienste gehen davon aus, dass Russland hinter dem Angriff steckt. Über das Rote Telefon, die eigentlich zur Deeskalation im Falle eines drohenden Atomkrieges etablierte direkte Leitung vom Weißen Haus in den Kreml, habe sie den russischen Präsidenten gerade aufgefordert, den Angriff sofort zu beenden, sonst müsse Russland mit schwerwiegenden Konsequenzen rechnen.

Die Außenministerien der NATO-Staaten haben zeitgleich die russischen Botschafter in ihren Ländern einbestellt und die gleiche Nachricht übermittelt. Russland hält auf allen Kanälen dagegen: Man habe mit der Cyberatta-

cke nichts zu tun und werde jede Aggression des Westens »robust« beantworten. Aus der Satellitenüberwachung der westlichen Dienste kommt die Nachricht, dass unmittelbar nach dem Anruf der US-Präsidentin die russische Armee aus ihren Kasernen in weit verstreute Bereitstellungsräume ausrückt, viele Atom-U-Boote auslaufen und die Marine die Häfen verlässt. Die Atomstreitkräfte sind ohnehin schon im erhöhten Alarmzustand.

Quellen des Mossad auf unteren Ebenen des russischen Militärs haben zwar auch keine Anhaltspunkte für eine russische Urheberschaft des Angriffs, berichten aber, dass Russland mit einem Kriegsausbruch rechnet. Das wird als Zeichen dafür interpretiert, dass die Operation auf allerhöchster Ebene geplant und gesteuert worden sein muss, in der keiner der westlichen Dienste zuverlässige Informanten hat. NATO und EU mobilisieren ihre schnellen Reaktionskräfte. Die Armeen der NATO-Staaten bereiten die Aktivierung ihrer Reserven vor. Die US-Streitkräfte gehen auf Alarmstufe DEFCON 3 und bereiten sich auf DEFCON 2 vor.

Die Telefonkonferenz der NATO-Regierungschefs kommt auf der Basis ihrer Geheimdiensterkenntnisse zu dem Schluss, dass es an der Zeit ist für einen »Warnschuss«, der in Form eines konzertierten Cyberangriffs auf die russischen Regierungsnetze, die Medien und die Bankeninfrastruktur erfolgen soll. Weiterhin sollen das russische Telefonnetz lahmgelegt und russische Internetfirmen aus dem Netz geschossen werden. Aus Sorge vor einer militärischen Eskalation und Angst, die Zugänge zu verlieren, die für die digitale Spionage und das Abhören der russischen Regierungskommunikation wichtig sind, werden das Mobilfunknetz im Raum Moskau und alle militärischen Systeme auf

eine Tabu-Liste gesetzt, die keinesfalls angegriffen werden sollen. Man will schließlich nicht noch blinder werden, als man ohnehin schon ist.

Die Zielplaner setzen sechs Uhr abends Moskauer Zeit als Beginn des Angriffs fest, jedes Land hat eine Liste der Ziele eingereicht, die es angreifen kann, um Dopplungen zu vermeiden. In der Abteilung Cyber Network Operations (CNO) der Bundeswehr herrscht hektische Betriebsamkeit, die Verteidigungsministerin ist trotz Ostern persönlich anwesend. Die Cyberkrieger stehen vor einem komplizierten Problem: Um die zugewiesenen Ziele in Russland zu attackieren, muss man irgendwie eine Netzverbindung zu ihnen bekommen. Mithilfe des Kanzleramts und der NATO werden deshalb verschiedene europäische Netzwerkanbieter verpflichtet, direkten Zugang zu ihren Glasfaserleitungen nach Russland zu ermöglichen. Nicht alle stehen jedoch Gewehr bei Fuß, sie haben ohnehin mit ihren Oster-Rumpfmannschaften alle Hände voll zu tun. Manche stellen Nachfragen und verlangen formale Anordnungen des Innenministeriums. Nicht alle sind bereit, sich lediglich auf Zuruf zum Handlanger der Bundeswehr zu machen.

Die CNO-Kommandos der Bundeswehr packen nach einer kurzen Ansprache der Ministerin ihre Sachen und machen sich auf den Weg zum militärischen Teil des Flughafens Frankfurt/Main, von wo sie nach Gdansk, Tallin, Kiew, Stockholm und Helsinki geflogen werden. Zwei Teams bleiben in Frankfurt. Über die dortige Fastline-Glasfaser werden sie versuchen, direkt Smolensk anzugreifen. Zur Koordination haben sie Satellitentelefone bekommen. Die Stimmung ist hochgradig angespannt, auf dem Hauptschirm sind alle Indikatoren zu sehen, die darauf hinweisen könnten, dass auch Russland seine Außenverbindungen

gekappt hat. Doch bisher sieht alles gut aus, die Leitungen stehen noch.

Kurz nach 20 Uhr rennt der Leiter der Schadsoftware-Analyseabteilung des BSI, Franz Blau, so schnell ihn seine Beine tragen durch die endlos langen, trostlosen Behördenflure des Bundesamts in Bonn. In der Nachrichtenzentrale angekommen, lässt er sich per Videoschaltung sofort mit dem Cyber-Lagezentrum verbinden. Ein privater Sicherheitsforscher, der gelegentlich Hinweise an die Behörde schickt, hat ohne Zutun der Behörden ein Exemplar der Schadsoftware analysiert und sich durch die diversen Schichten gegraben, die darin eine Analyse erschweren sollen. Was er gefunden hat, ändert die Lage grundlegend, erklärt Blau hektisch, sobald die Leitung steht: Punkt Mitternacht wird die Schadsoftware aufhören, Netzwerkverkehr zu senden, und sich dann selbst deaktivieren.

Ungläubige Verwunderung macht sich breit. »Sind wir uns absolut sicher, dass das so ist?«, will Fjodor zuerst wissen. Auf dem Bildschirm ist deutlich zu sehen, wie nervös Blau ist, der Schweiß rinnt ihm von der Stirn. »Wir haben die Analyse noch nicht selbst nachvollziehen können, aber wir kennen den Forscher. Und wir haben Folgendes getestet: Die infizierten Geräte und Mobiltelefone, denen wir auf die Schnelle eine falsche Uhrzeit vorgegaukelt oder eingestellt haben, hörten hier bei uns im Labornetz tatsächlich auf zu senden. Danach haben sie nicht wieder angefangen!«

Fjodor entscheidet schnell: »Sofort den BSI-Kurzbericht an alle Behörden, die NATO und die Partnerdienste schicken, als FLASH-Nachricht! Das Kanzleramt soll sofort Kontakt zu den Amerikanern aufnehmen. Frau Schwarz, machen Sie mir eine Leitung zur Bundesnetzagentur, vielleicht können die Provider ja die zentralen Uhren in ihren

Netzen nach vorne drehen! Und wir brauchen eine Pressemitteilung, die so schnell wie möglich über den Rundfunk geht und die Leute auffordert, die Uhren vorzustellen und dann ihre Geräte zu rebooten!« Hektische Aktivität bricht aus. Vielleicht gibt es ja eine Möglichkeit, doch noch ohne einen Krieg aus dieser Situation herauszukommen.

1. April 2023, Tarifa, Spanien

Es ist ein sonniger Vorfrühlingstag. Die Sonne brennt an diesem schönen Nachmittag schon so stark, dass es lohnt, im Halbschatten zu sitzen, um keinen Sonnenbrand zu bekommen. Von der Terrasse hat man einen guten Blick auf die Schiffe, die zur Meerenge von Gibraltar steuern. Die Runde aus knapp einem Dutzend Männern und einigen wenigen Frauen, die sich hier auf einen Sonnenuntergangs-Drink versammelt hat, kennt sich seit Jahren, wenn auch nicht mit realem Namen.

Einem aufmerksamen Beobachter würde auffallen, dass niemand ein Telefon in der Hand hat, auch Smartwatches sind nicht zu sehen, man bevorzugt gediegene mechanische Zeitmesser. Genauer gesagt befindet sich kein einziges Stück Elektronik in ihrer Nähe. Sie alle sind Veteranen der Cryptocoin-Szene, die den europäischen Winter am südlichsten Punkt Spaniens verbracht haben. In den letzten Monaten haben sie an einem großen Projekt gearbeitet: Wenn es Erfolg hat, wird es dafür sorgen, dass sie den nächsten Winter in Luxusresorts verbringen können, in der Südsee oder wo auch immer es ihnen gefällt.

Der Plan, der ihnen endlich zu richtig großem Reichtum verhelfen soll, ist im Detail komplex, aber im Grunde

eigentlich ganz einfach. In etwas mehr als einer Woche, am Ostersonntag, wird »Pay« gestartet, ein revolutionärer neuer Cryptocoin. Es soll eine neue kryptografische Währung werden, mit der ein Konsortium der größten Internetfirmen, Kreditkartenunternehmen, Banken und Anbieter von digitalen Dienstleistungen endlich ein universelles Zahlungsmittel etablieren will. »Pay«-Coins werden schon an den großen Börsen gehandelt, die Erwartungen sind riesig.

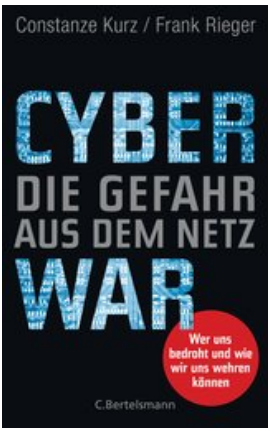
Der Kurs ist in den letzten Monaten praktisch durchgehend gestiegen, schon vor dem eigentlichen Start, ab dem man dann mit der neuen Währung alles Mögliche von Zeitungsartikeln über Softwarelizenzen bis zu Uber-Fahrten bezahlen kann. Die Investoren glauben daran, dass durch die Marktmacht des Konsortiums schnell alle anderen Kryptowährungen für praktische Anwendungen in die Irrelevanz gedrängt werden. Die entspannte Runde in Tarifa will auch ein Stück von diesem gigantischen Kuchen abhaben und ist willens, dafür zu ungewöhnlichen Mitteln zu greifen.

Ihr Plan beruht darauf, den Kurs der Kryptowährung an den diversen Börsen, an denen sie gehandelt werden, kurzzeitig drastisch nach unten zu manipulieren. Dafür wollen die Mitglieder der Runde die automatischen Algorithmen, die aus Gründen der Zeitersparnis inzwischen direkt auf den Systemen der Börsen laufen, in einen Panikverkaufsmodus zwingen. Sobald der Kurs drastisch sinkt, wollen sie möglichst viele »Pay«-Coins für einen Bruchteil ihres Wertes aufkaufen. Um einen noch größeren Hebel zu bekommen, werden zusätzliche Optionen zur Anwendung kommen.

Damit eine echte, tief greifende algorithmische Panik entsteht und man verhindert, dass menschliches Eingreifen die Panikverkäufe verhindert, muss dazu aber etwas Unerhörtes geschehen: Das Internet muss für ein paar Stunden

C.Bertelsmann

UNVERKÄUFLICHE LESEPROBE



Constanze Kurz, Frank Rieger

Cyberwar – Die Gefahr aus dem Netz
Wer uns bedroht und wie wir uns wehren können

ORIGINALAUSGABE

Gebundenes Buch mit Schutzumschlag, 288 Seiten, 13,5 x 21,5 cm
ISBN: 978-3-570-10351-7

C. Bertelsmann

Erscheinungstermin: Oktober 2018

Die unterschätzte Gefahr: wie Cyberattacken jeden einzelnen von uns bedrohen

Wir sind abhängig vom Internet. Der Strom aus der Steckdose, das Geld aus dem Automaten, die Bahn zur Arbeit, all das funktioniert nur, wenn Computer und Netze sicher arbeiten. Doch diese Systeme sind verwundbar – und werden immer häufiger gezielt angegriffen. Deutschland mit seiner stark vernetzten Industrie und Gesellschaft, mit seiner hochentwickelten und deshalb umso verwundbareren Infrastruktur hat die Gefahr aus dem Netz lange ignoriert. Erst durch die wachsende Zahl und die zunehmende Massivität der Cyberangriffe sind Politik, Wirtschaft und Bürger aufgewacht. In ihrem ebenso spannenden wie aufrüttelnden Buch sagen die Computersicherheitsexperten Constanze Kurz und Frank Rieger, wer uns bedroht und was wir tun müssen, um unsere Daten, unser Geld und unsere Infrastruktur zu schützen.

Der Titel im Katalog