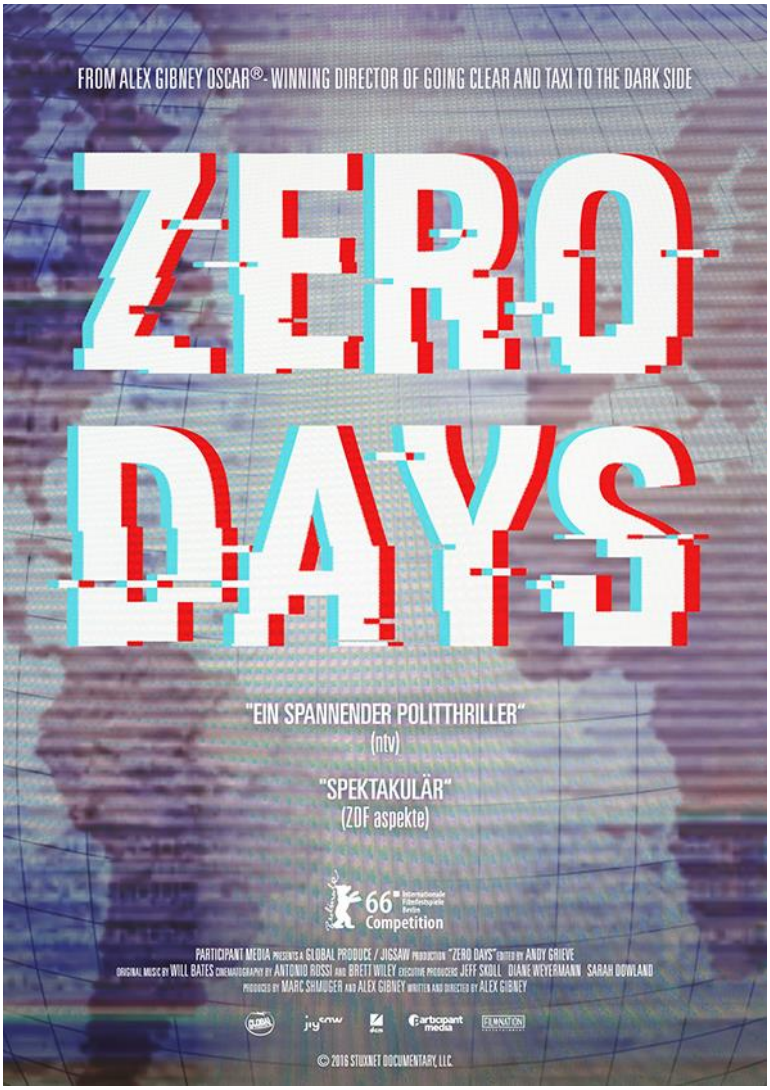


Presseheft

Ein Film von Alex Gibney

Laufzeit: 116 Minuten

Ab 01.09.2016 in ausgewählten Kinos
& ab 06.09.2016 digital erhältlich

Pressefotos und -material finden Sie unter www.filmpresskit.de zum Download

Betreuende Presseagentur:
RUBI PUBLIC RELATIONS
Uhlandstr. 127
10717 Berlin
Tel.: 030/88623930
eMail: info@rubi-pr.com

Verleih:
DCM Film Distribution GmbH
Schönhauser Allee 8
10119 Berlin
030/885 974-0
what@dcmteam.com
www.dcmworld.com

define(Inhalt)

Kurzinfo 1
10 Dinge, die ZERO DAYS erstmals enthüllt 2
Regisseur Alex Gibney über ZERO DAYS 4
Hintergründe des Cyberwars 6

  Die Entstehung von Stuxnet 6
  Cyberwar: Ein Krieg, über den niemand spricht 7
  Die Zukunft des Krieges: Was als nächstes passiert 8

Lexikon der Fachbegriffe 9
Über den Filmemacher 10
Credits 11

Kurzinfo

2010 machen Sicherheitsexperten eine unheimliche Entdeckung. Ein hochkomplexer Computerwurm namens STUXNET verbreitet sich mit noch nie gesehener Aggressivität auf der ganzen Welt. Was die Forscher noch nicht ahnen: Sie sind auf den geheimen Prototypen einer neuen Generation von Kriegswaffen der CIA und des Mossads gestoßen. Cyberwaffen, deren reale Zerstörungskraft allein mit der von Atombomben vergleichbar ist – und deren Verbreitung außer Kontrolle gerät…

Der hochspannende und alarmierende Doku-Thriller ZERO DAYS von Oscar-Preisträger Alex Gibney (TAXI ZUR HÖLLE, GOING CLEAR) enthüllt die Hintergründe des World War 3.0. Gibney spricht mit Drahtziehern, Whistleblowern und Politikern und zeigt auf, dass STUXNET nur der Anfang ist. Unbemerkt von der Weltöffentlichkeit setzen Militärs und Geheimdienste Cyberwaffen in einem Krieg ein, für den bisher keine internationalen Konventionen und Regeln gelten.

Mit ZERO DAYS durchbricht Alex Gibney das Schweigen der Politik und stößt eine der wichtigsten Debatten unserer Zeit an.

„Von nun an werden wir mit der Herausforderung eines potentiellen Cyberwars rechnen müssen. Dies ist unser Nullpunkt. Wie werden wir weiter damit umgehen?“

– ALEX GIBNEY, Regisseur

10 Dinge, die ZERO DAYS erstmals enthüllt

Dank der Whistleblower erhielt Alex GIbney einen völlig neuen Blickwinkel auf die Stuxnet-Operation – interner Deckname: „Olympic Games“ – und auf die neue Welt der Cyber-Waffen insgesamt. Wovon die breite Öffentlichkeit durch ZERO DAYS zum ersten Mal erfährt:

01_ **Die USA haben keine ausreichenden Vorkehrungen getroffen, um sich gegen Cyber-Angriffe zu verteidigen**. Sie verfolgen stattdessen eine Offensivstrategie und setzen darauf, dass allein die Drohung eines Vergeltungsschlags mögliche Gegner davon abhalten wird, ihr virtuelles Kriegsarsenal gegen die USA zu richten. Dieser Plan ging bisher jedoch nicht auf. Russland, China, der Iran und Nordkorea haben Cyber-Angriffe gegen die USA gefahren und verfügen vermutlich über Tausende heimliche Zugänge zu Computernetzwerken. Dampit können möglicherweise Schlüsselbereiche der US-amerikanischen Infrastruktur in Mitleidenschaft gezogen werden: Stromnetze, Kläranlagen, Verkehrssysteme, Klimaanlagen usw.

02_ **Obwohl „Olympic Games“ ein Gemeinschaftsunternehmen der USA und Israels war, konnten beide Staaten die Cyberwaffen ihren jeweiligen eigenen Ansprüchen anpassen und individuell zum Einsatz bringen.** Zu Animositäten und Spannungen kam es, als der Mossad – gedrängt von einem ungeduldigen Bibi Netanyahu – ohne Rücksprache mit den USA eine aggressive Version des Wurms aufsetzte, die sich über die ganze Welt verbreitete. Dadurch wurden die Beziehungen zwischen den USA und Israel schwer belastet und grundsätzlich in Frage gestellt.

03_ **Nach „Olympic Games“ entwickelte die NSA noch weitaus wirkungsvollere Cyberwaffen.** Eine Operation, in der solche Systeme zum Einsatz kamen, trug den Namen „Nitro Zeus“ (erstmals enthüllt in ZERO DAYS) und hatte das Potential, die komplette Luftabwehr des Iran außer Gefecht zu setzen und die zentralen iranischen Stromnetze teilweise auszuschalten. In den Worten eines unserer Informanten: „Das Science-Fiction-Szenario eines Cyberwar ist Wirklichkeit geworden.“

04_ **Das Cyber-Commando innerhalb des US-Verteidigungsministeriums zeigte einen bemerkenswerten Mangel an Weitsicht oder überhaupt Interesse daran, was das mögliche Ausmaß der Zerstörung durch ihre Waffen anging**. Wenn die wichtigsten Kraftwerke erst einmal ausgeschaltet seien, hieß es in einer Quelle, könnten sie nicht mehr so ohne weiteres „wieder hochgefahren werden. Es ist wie bei Humpty Dumpty... viele Menschen sterben.“ Bei der Diskussion von Angriffszielen im Iran wandten Juristen des Außenministeriums ein, Cyber-Attacken würden Krankenhäuser außer Betrieb setzen und hätten somit eine hohe Anzahl von Todesfällen zur Folge. Das Verteidigungsministerium ignorierte solche Bedenken.

05_ **„Olympic Games“ war eine CIA-geführte Operation**. Bei jedem Angriff stand ein CIA-Beamter hinter den Computer-Operatoren der NSA und erteilte diesen die Einsatzbefehle.

06_ **Als der Iran für Stuxnet Vergeltung nahm und seinerseits Cyber-Aktionen gegen amerikanische Banken durchführte, war die US-Regierung sich zwar darüber im Klaren, verzichtete jedoch auf Gegenmaßnahmen.** Der Grund: Die Rechner, die das „Botnet“ kontrollierten (ein Netzwerk privater Rechner, die mit Schadsoftware verseucht sind), befanden sich außerhalb der USA. Das Außenministerium hatte Sorge, dass ein befreundeter Staat mit in den sich ausbreitenden Cyber-Konflikt hineingezogen würde. Dies macht eines der Dilemmas des Cyber-Kriegs deutlich: Die Zuordnung ist problematisch, das Risiko „falscher Flaggen“ und irrtümlicher Gegenschläge, die zu einem weltweiten Cyber-Krieg führen könnten, ist virulent und nimmt immer weiter zu.

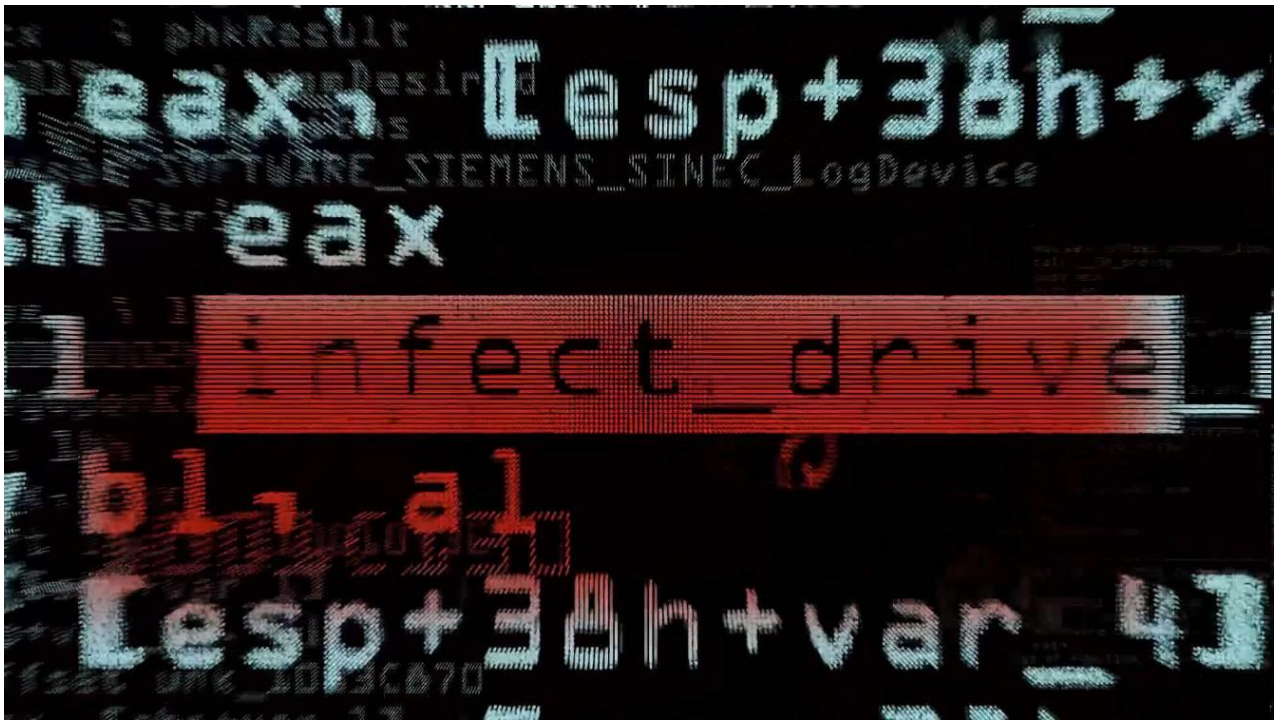
07_ **Der Stuxnet-Wurm arbeitete autonom. Kein Operator gab ihm einen Einsatzbefehl.** Stuxnet war so programmiert, dass er, hatte er sein Ziel innerhalb der Anlage in Natans einmal identifiziert, Angriffe auf eigene Faust durchführte, gänzlich ohne menschliches Zutun. Eine wachsende Zahl von Cyber-Waffen funktioniert nach diesem Muster.

08_ **Das Versteckspiel um offensive Cyberwaffen und der Wirkungskraft behindert nicht nur die demokratische Auseinandersetzung, sie ist auch ein Sicherheitsrisiko.** Tatsächlich waren unsere Informanten auch deswegen bereit auszupacken, weil sie in der Geheimhaltung selbst eine enorme, auch existenzbedrohliche Gefahr sehen.

09_ **Die Aufdeckung von „Nitro Zeus“ warf ein neues Licht auf das Atomabkommen der Obama-Regierung mit dem Iran.** Während viele Kritiker unkten, Obama habe aus einer Position der Schwäche heraus verhandelt, ist – im Anbetracht von “Nitro Zeus” – das Gegenteil wahrscheinlich. Die USA wissen, dass sie bei einem iranischen Verstoß gegen das Abkommen in der Lage sind, das gesamte Land nahezu zum Stillstand zu bringen.

10_ **Gibneys Informanten haben bestätigt, dass staatlich ausgeführte, aggressive Cyber-Operationen seit Stuxnet Alltag sind**. (O’Muchu und Chien von Symantec unterstreichen ebenfalls, dass die Zahl staatlicher Cyber-Attacken in den letzten Jahren exponentiell zugenommen hat.) Der einzige Grund, warum wir nicht mehr über Cyberwaffen wissen, ist die Geheimhaltungsstrategie der Regierungen sowie die Unfähigkeit der Medien, darüber zu berichten. Doch solche Waffen werden entwickelt und eingesetzt – von uns und gegen uns – jeden Tag.

Regisseur Alex Gibney über ZERO DAYS



„Was tun, wenn deine Regierung einen globalen Krieg anzettelt und niemandem davon erzählt?“ Diese Frage verfolgte mich, als ich ZERO DAYS drehte, einen Film über das Menetekel einer neuen Generation von geheimen Cyberwaffen.

Ich arbeitete ursprünglich an einem kleineren Film, der dem Computerwurm „Stuxnet“ nachging, mit dem die USA und Israel die Zentrifugen in der iranischen Urananlage Natans unterminieren und lahmlegen wollten. Dabei stieß ich auf eine streng geheime Operation, an der die CIA, die NSA, das US-Militär und der israelische Geheimdienst Mossad beteiligt waren. Deren Mission war es, versteckte Cyberbomben zu entwickeln und einzusetzen, mit denen es möglich war, verheerende Angriffe auf zentrale Bereiche der zivilen Infrastruktur zu unternehmen: die Elektrizität ausschalten, die Wasserversorgung kontaminieren sowie Autos, Züge und Flugzeuge in tödliche Waffen verwandeln. Was dieses Science-Fiction-Szenario, das den Verlust von Millionen Menschenleben bedeuten konnte, noch beängstigender machte: Es konnte eintreten ohne den kleinsten Hinweis auf die Drahtzieher dahinter.

Als ich mit dem Projekt startete, wusste ich, dass sich Stuxnet (ein sich selbst replizierender Wurm) über die ganze Welt verbreitet hatte. Die Geheimhaltung der Operation war gescheitert. Doch trotzdem schwieg jeder US-Offizielle, mit dem ich darüber sprechen wollte, oder bestritt sogar, dass eine solche Operation überhaupt jemals existiert habe. Gerechtfertigt wurde das Schweigen von allen Beteiligten im Namen der nationalen Sicherheit. Oder wie es Michael Hayden, der frühere Chef der CIA und der NSA, ausdrückte: Eine verdeckte Operation „wandert automatisch in die Darüber-wird-nicht-geredet-Schublade“.

Doch Stuxnet war nicht irgendeine Geheimoperation. Sie markierte eine neue Qualität der Bedrohung. Erstmals in der Geschichte überschritt ein Wurm die Schwelle zwischen der virtuellen Realität der Einsen und Nullen und der physischen Welt. Stuxnet übernahm die Kontrolle über Maschinen und befahl ihnen, sich selbst zu zerstören. Dann gelang der Code in die ganze Welt und konnte so von anderen Nationen, von Kriminellen und Terroristen für ihre eigenen Zwecke benutzt und umprogrammiert werden. Ein solches Geheimnis für sich zu behalten, war so, wie wenn es nach Hiroshima geheißen hätte: „Was für eine Bombe?“

Den Gipfel der Absurdität erreichte das Ganze, als ich erfuhr, dass das Homeland Security-Department wegen Stuxnet die höchste Alarmstufe aktiviert hatte. Die NSA hatte andere Regierungsbehörden nicht darüber

informiert, dass sich die Waffe, die wir selbst in Stellung gebracht hatten, nun gegen das eigene Land richtete. Wir stießen auf einen Feind – und der waren wir selbst.

Während offizielle Stellen die Gefahren zu vertuschen suchten, deren Urheber sie waren, hielten wir nach anderen Informationsquellen Ausschau. Zunächst nahmen wir zu den Cyber-Detektiven Liam O'Murchu und Eric Chien von der Antiviren-Firma Symantec Kontakt auf, die als erste das System hinter Stuxnet aufgedeckt hatten. Sie zerlegten für uns die Waffe, damit wir ihre Funktions- und Wirkungsweise verstehen konnten.

Danach fuhren wir nach Moskau – der Hauptstadt der Cyberkriminalität und Hauptsitz des russischen Cyberwaffen-Programms – sowie nach Israel, dem Schlüsselpartner der USA bei der Entwicklung von Stuxnet. In Tel Aviv und Jerusalem erfuhren wir in Gesprächen mit Politikern, Journalisten und – hinter vorgehaltener Hand – Agenten des Mossad, dass Stuxnet ganz und gar nicht als Malware für Computer konzipiert worden war. Der Wurm war vielmehr Bestandteil einer viel umfangreicheren Operation, in die der Mossad, die CIA und das US Cyber Command involviert waren. Zu ihr gehörten verdeckte Aktionen – teilweise gegen US-amerikanische Firmen wie Microsoft gerichtet –, die Liquidierung von iranischen Wissenschaftlern sowie virtuelle Waffensysteme von einer Massenvernichtungskraft, gegen die Stuxnet ein Computerspiel war.

Mit diesem Detail- und Geheimwissen kehrten wir in die USA zurück und konnten einige Leute innerhalb der NSA und der CIA davon überzeugen, mit uns zu reden – unter der Bedingung, dass wir keinesfalls ihre Identität preisgaben. Inzwischen kam heraus, dass die Obama-Regierung mehr Whistleblower strafrechtlich verfolgt hat als alle Vorgängerregierungen zusammen. Wir mussten also alles daran setzen, unsere Quellen zu schützen.

Wir nahmen daher Interviews nur auf Rekordern auf, die nicht WLAN-tauglich waren, transkribierten sie ausschließlich auf elektrischen Schreibmaschinen und vernichteten danach die Datenkarten. Wir benutzten ein Codesystem, mit dem wir unsere Informanten kennzeichneten, und verschlüsselten in ihren Aussagen all jene Sätze, die die Ermittler möglicherweise zu ihrer Enttarnung geführt hätten. Zudem verwendeten wir DepthKit, ein Video-Tool, mit dem menschliche Körper in digitale Modelle umgewandelt werden können und erschufen daraus einen Cyber-Whistleblower, dessen „gehacktes" Aussehen zur Animation des Stuxnet-Codes passte.

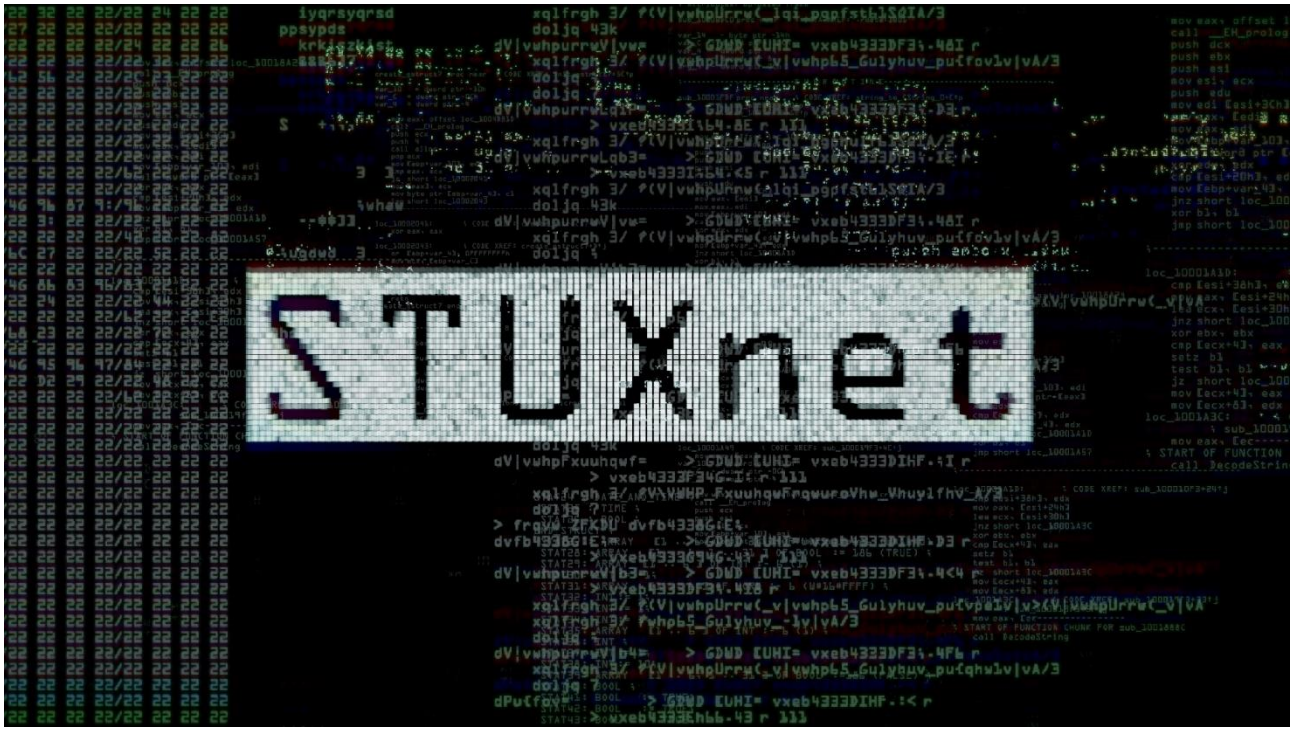
In den animierten Darstellungen von Stuxnet verwendeten wir lediglich Ausschnitte des Codes, mit denen es nicht möglich ist, den Wurm zu rekonstruieren. Allerdings hatte unser Co-Produzent Javier Botero keinerlei Probleme, sich den kompletten Code zu beschaffen, was die strenge Geheimhaltung der offiziellen Stellen umso absurder macht.

Alex Gibney, April 2016 – New York City

Die Hintergründe des Cyberwars

Cyberwar ist etwas, das im Verborgenen vor sich geht. Wie bei einem Computervirus nehmen wir sie erst wahr, wenn sie an die Oberfläche kommt und Schaden anrichtet. Ein Grund, warum wir so wenig über das Thema wissen, ist, dass unsere Regierung uns gar nicht wissen lassen will, welche offensiven Cyber-Operationen sie in unserem Namen durchführt. Zudem entzieht sich diese Art der Kriegsführung unserer Kontrolle, weil sie so ganz anders ist als kriegerische Konflikte, wie wir sie bisher kannten. Doch Cyber-Waffen sind genauso schlagkräftig wie konventionelles Kriegsgerät – und unser mangelndes Bewusstsein macht sie umso schlagkräftiger.

Die Entstehung von Stuxnet



Die Geschichte von Stuxnet basiert auf einem nahezu unlösbaren Rätsel: Wie konnte Stuxnet in die iranische Nuklearanlage in Natans eindringen, die sich in über 21 Metern Tiefe befindet, umgeben von Betonmauern, beschützt von Überwachungstürmen und Flugabwehrgeschützen – und deren Computer zu keiner Zeit mit dem Internet verbunden waren? „Sie haben Maschinen nicht nur lahmgelegt“, sagt Gibney, „sie haben Maschinen vielmehr so umprogrammiert, dass sie sich destruktiv verhalten. Und was noch erschreckender ist: Gleichzeitig signalisierten die Maschinen dem Bedienungspersonal, dass alles in Ordnung sei. Stuxnet operierte völlig autonom und war jedem menschlichen Zugriff entzogen. Einmal losgelassen, konnte der Wurm nicht mehr eingefangen werden.

Entdeckt wurde Stuxnet Mitte 2010 von dem weißrussischen Antiviren-Experten Sergey Ulasen. Er war von iranischen Kunden um Hilfe gebeten worden, die besorgt waren wegen einer Reihe von rätselhaften Computerabstürzen. Ulasen teilte seine Entdeckung mit anderen Antiviren-Experten, die die Spur von Stuxnet aufnahmen. Zu ihnen gehörten Eric Chien und Liam O’Murchu von Symantec (USA), Eugene Kaspersky und Vitaly Kamluk von Kaspersky Labs (Russland) und Ralph Langner (Deutschland). Chien und O’Murchu nannten die Schad software „Stuxnet“, eine Wortschöpfung, die sich aus den wiederkehrenden Schlüsselbegriffen des Softwarecodes “stub” und “Mrxnet.sys.” zusammensetzte.

Der Wurm nutzte zahlreiche, selbst den Herstellern bisher unbekannte Sicherheitslücken (*zero day*-exploits) aus, um sich weiterzuverbreiten, was Hinweise auf seine Herkunft gab: Der Stuxnet-Wurm war zu groß, zu komplex und zu perfekt programmiert, als dass er das Werk von herkömmlichen Hackern oder Kriminellen hätte sein könnte – es bedurfte zu seiner Entwicklung der Mittel, Manpower und Zeit, die nur ein Staat aufbringen konnte.

Nach einer eingehenden Analyse fanden die Sicherheitsexperten heraus, dass der Wurm so konstruiert war, dass er nur einen Angriff startete, wenn er eine bestimmte Windows-Software für eine speicherprogrammierbare Steuerung (Programmable Logic Controller, PLC) aufspürte. Dieses Gerät wird zur Steuerung von Industriemaschinen, einschließlich Zentrifugen von Nuklearanlagen, eingesetzt. Genau genommen war Stuxnet so gebaut, dass er nur die PLCs von zwei Anbietern attackierte, von denen einer seinen Sitz im Iran hatte, einem Land, in dem Symantec 60 Prozent aller weltweit mit Stuxnet infizierten Rechnern ausmachte.

Die Frage, welches Land oder welche Länder ein Interesse daran haben könnten, das iranische Nuklearprogramm zu sabotieren, führte zu zwei offensichtlichen Verdächtigen. Gibney und sein Team konnten bis ins Detail belegen, was jahrelang vermutet wurde – dass Israel und die USA die Drahtzieher hinter dem Ganzen waren. Gibney fand zudem heraus, dass Chiens und O'Murchus „Stuxnet" in Wirklichkeit eine gigantische Militäroperation namens „Olympic Games" war, die in den USA von CIA, der NSA und dem US-Cyber Command und in Israel vom Mossad und der verdeckten Cyber-Abteilung Unit 8200 durchgeführt wurde.

Cyberwar: Ein Krieg, über den niemand spricht

Gibneys Versuche, die Erfinder von Stuxnet vor die Kamera zu bringen, prallten gegen eine Wand des Schweigens, da jede Information zu dem Wurm strengster Geheimhaltung unterliegt. Gibney: „Es ist wie in dem Märchen 'Des Kaisers neue Kleider' – Stuxnet existiert, jeder weiß, dass die USA und Israel dahinter stecken, doch niemand darf das Offensichtliche aussprechen." Die Gründe liegen auf der Hand: Das US-Justizministerium hat bewiesen, dass es jeden Informanten mit der ganzen Härte des Gesetzes verfolgen würde.

Dieses rigorose juristische Durchgreifen führte dazu, dass jeder Dialog praktisch unmöglich ist. Und es sind ja nicht nur spezielle Details der Operation, über die nicht gesprochen werden darf, der gesamte Komplex ist tabu. Jede Debatte zu so einem wichtigen Thema wie der virtuellen Kriegsführung wird dadurch im Keim erstickt. Die Executive Producerin Sarah Dowland sieht noch größere Kräfte am Werk als die bloße Angst vor Strafverfolgung: „Ich denke, niemand will etwas zugeben, weil jede kleinste Bekenntnis zur Folge hätte, dass die Öffentlichkeit noch mehr wissen möchte. Das ist nicht nur bei Stuxnet so, sondern bei allem, das im Verborgenen passiert. Wir sollen einfach keine Fragen stellen."

Bereits die Ambition und Ausführung der Stuxnet-Technologie ist so Ehrfurcht einflößend wie verstörend. Was die Geschichte aber zu einem wirklichen Drama macht, ist die Tatsache, wie diese Operation unterhalb des Radars der Weltöffentlichkeit ablaufen konnte. Es wird angenommen, dass sich Israel von den USA unabhängig machte und den Code der Software so veränderte, dass er sich über den kompletten Globus verbreitete.

Die Entscheidung, Stuxnet zu entwickeln, wurde relativ hastig getroffen, sodass keine Zeit war, sich mit den langfristigen Folgen des Programms zu befassen. Gibney: „Jemand hätte daran denken müssen, dass ein so fahrlässiger Umgang mit dieser Waffe dazu führen würde, dass sie in die falschen Hände gerät und wie ein Bumerang wieder zurückkommt. Aber alle waren so berauscht von der kurzfristigen technischen Lösung, dass niemand einen Gedanken an die mögliche Katastrophe verschwenden wollte."

Die Zukunft des Krieges: Was als nächstes passiert

Stuxnet ist nun eine mächtige Open-Source-Waffe, frei verfügbar für alle unsere Feinde, die sie studieren, umprogrammieren und neu ausrichten können auf egal welche Infrastruktur. „Der IS könnte sich jederzeit eine Kopie von Stuxnet besorgen“, sagt Gibney. „Ob sie schon die nötigen Programmierer haben, die Spione, um Sachen zu schmuggeln, den Nachrichtendienst, der herausfinden könnte, welche Kontrollen es gibt, steht natürlich auf einem anderen Blatt.“ Gibney weiter: „Zum jetzigen Zeitpunkt ist ein Cyberkrieg für Staaten wahrscheinlich die wirksamere Waffe als für eine Terrororganisation wie den IS. Doch haben Hacker Zugriff darauf? Ja, haben sie. Wir haben im Grunde weltweit Hackern die Blaupause für das Manhattan-Projekt geliefert.“

Jetzt, wo der Damm gebrochen ist, gibt es kein Zurück mehr. Michael Hayden, der frühere Chef der NSA und des CIA sagt im Film, es gebe nun eine „neue Normalität“. Gibney: „Mit ihrer Entscheidung, Angriffe gegen wichtige Infrastrukturen zu fahren, etablierten die USA einen neuen moralischen Codex. Es ist nicht so, wie Hayden behauptet, „dass man nur das Licht ausschaltet.“ Es dauert Wochen, Monate, manchmal sogar Jahre, bis eine Infrastruktur nach einem Cyber-Angriff wieder instandgesetzt ist. In der heutigen Zeit kann die Beeinträchtigung der Trinkwasserversorgung und des Verkehrssystems, von Kraftwerken, Krankenhäusern und Stromnetzen einen verheerenden und großflächigen Verlust von Menschenleben bedeuten. Der Knock-out von Infrastrukturen ist kein hypothetisches Ereignis, vor dem man in der Zukunft Angst haben muss. Es gibt Berichte aus vielen Ländern – insbesondere aus der Ukraine mit ihrem fortdauernden Cyberkrieg –, in denen Hacker Festplatten mit Wahlergebnissen zerstört oder staatliche Behörden bis zu den höchsten Stellen empfindlich getroffen haben.

ZERO DAYS, der Titel des Films, bezieht sich auf die vielen Sicherheitslücken, die Stuxnet erst ermöglicht haben, ebenso wie auf die unendlich vielen Sicherheitslücken, die zu zukünftige Attacken einladen werden. ZERO DAYS ist auch eine starke Metapher für dieses Zeitmoment. Gibney: „Von nun an werden wir mit der Herausforderung eines potentiellen Cyberwars rechnen müssen. Dies ist unser Nullpunkt. Wie werden wir weiter damit umgehen?“

Lexikon der Fachbegriffe

Computerwurm

Ein Computerwurm ist eine schädliche Software, die sich selbst nach ihrer Ausführung viervielfältigen und weiterverbreiten kann – und das sogar von selbst, ohne dass eine Interaktion des Benutzers notwendig ist. Im Gegensatz zu Viren warten Würmer nicht passiv darauf, von einem Anwender auf einem neuen System verbreitet zu werden, sondern versuchen, aktiv in neue Systeme einzudringen. Daher verbreiten sich Würmer deutlich effizienter als Viren.

Computervirus

Eine Computervirus ist eine schädliche Software Ein Virus verbreitet sich, indem es sich selbst in noch nicht infizierte Dateien kopiert und diese so anpasst, dass das Virus mit ausgeführt wird, wenn das Wirtsprogramm gestartet wird.

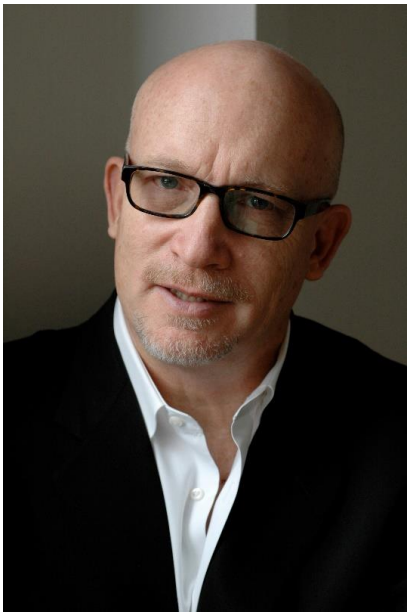
Stuxnet

Stuxnet ist ein Computerwurm, der gezielt von der USA und Israel entwickelt wurde, um das iranische Atomprogramm unentdeckt zu sabotieren. Stuxnet verbreitet sich eigenständig und unkontrolliert weiter und verwischt dabei seine eigenen Spuren.

Zero Day

„Zero Days“ sind vom Hersteller unentdeckt gebliebene Sicherheitslücken in Software. Hacker, die solche Lücken entdecken, können dadurch unmittelbar angreifen, ohne dass der Hersteller die Zeit (=zero days) hat, Gegenmaßnahmen zu entwickeln.

Über den Filmemacher



Alex Gibney wurde als „der wichtigste Dokumentarfilmer unserer Zeit“ (Esquire) und als „einer der herausragendsten amerikanischen Filmemacher“ (Indiewire) bezeichnet.

Er ist bekannt für seine filmisch brillanten, fesselnden und äußerst aufschlussreichen Dokumentarfilme und gewann den Academy Award®, den Emmy, den Grammy, den Peabody Award, den DuPont-Columbia Award, den Independent Spirit Award sowie den The Writers Guild of America Award, um nur einige aufzuzählen. 2013 wurde Gibney mit dem International Documentary Association’s Lifetime Achievement Award ausgezeichnet.

Meilensteine seiner Karriere sind der Dokumentarfilm-Oscar für TAXI ZUR HÖLLE, die Academy Award®-Nominierung für ENRON: THE SMARTEST GUYS IN THE ROOM sowie – als Executive Producer – die Oscar-Nominierung für NO END IN SIGHT.

Sein Dokumentarfilm DIE ARMSTRONG LÜGE über den spektakulären Absturz von Lance Armstrong stand 2014 auf der Shortlist für den Academy Award®. Er war zudem 2014 für den BAFTA Award nominiert ebenso wie WE STEAL SECRETS: DIE WIKILEAKS GESCHICHTE.

Kürzlich stieg Alex Gibney mit seiner Produktionsfirma Jigaw Productions auch ins TV-Seriengeschäft ein mit dem Debütprojekt „Death Row Stories“ für CNN, bei dem er zusammen mit Robert Redford als Executive Producer fungierte. Die zweite Staffel der Serie erscheint diesen Sommer. Gibneys Firma produzierte auch „Edge of Eighteen“ für Al Jazeera America und befindet sich gerade in der Produktion von drei neuen Serien: Für Amazon „The New Yorker Presents“ über das altehrwürdige Magazin The New Yorker, für Netflix eine vierteilige Doku-Reihe sowie für den Sender A&E eine neue Serie, die im Sommer bekanntgegeben wird.

2015 erhielt Gibney einen Peabody Award für MR. DYNAMITE: THE RISE OF JAMES BROWN, einen Dokumentarfilm für HBO, der den Aufstieg des „hardest working man in show business” erzählt.

Zu Gibneys letzten Filmen zählen GOING CLEAR: SCIENTOLOGY AND THE PRISON OF BELIEF, der 2015 seine Premiere in Sundance feierte und mit bis heute 6,5 Millionen Zuschauern der meistgesehene Film bei HBO seit zehn Jahren ist; SINATRA: ALL OR NOTHING AT ALL, ein zweiteiliges Biopic über Frank Sinatra, erstmals auf HBO ausgestrahlt im April 2015; und STEVE JOBS: THE MAN IN THE MACHINE, der im März 2015 auf dem Filmfestival SXSW Film uraufgeführt wurde und im Herbst 2015 in die US-amerikanischen Kinos kam.

Gibneys Filme GOING CLEAR: SCIENTOLOGY AND THE PRISON OF BELIEF und SINATRA: ALL OR NOTHING AT ALL waren 2015 für acht Emmy Awards nominiert und gewannen davon drei für Outstanding Writing for Nonfiction Programming, Outstanding Directing for Nonfiction Programming und Outstanding Documentary or Nonfiction Programming.

Credits

Written and Directed by ALEX GIBNEY

Produced by
MARC SHMUGER
ALEX GIBNEY

Executive Producers
JEFF SKOLL
DIANE WEYERMANN

Executive Producer SARAH DOWLAND

Cinematographers
ANTONIO ROSSI
BRETT WILEY

Original Music WILL BATES

Editor ANDY GRIEVE

Co-Editor HANNAH VANDERLAN

Co-Producer JAVIER ALBERTO BOTERO

Associate Producer GRACE FARDELLA

Design and Visual Effects
FRAMESTORE
TECHNICOLOR POSTWORKS SPECULAR PROJECTS

Researchers
SOLVEJ KRAUSE
CHARLOTTE KAUFMAN

Featuring
(in alphabetical order)

COLONEL GARY D. BROWN
ERIC CHIEN
RICHARD A. CLARKE
GENERAL MICHAEL HAYDEN
OLLI HEINONEN
CHRIS INGLIS
VITALY KAMLUK
EUGENE KASPERSKY
EMAD KIYAEI
RALPH LANGNER
ROLF MOWATT-LARSSEN
SEÁN PAUL McGURK
YOSSI MELMAN
LIAM O'MURCHU