Dietrich Meyer-Ebrecht

Zero Days

Dokumentarfilm über Geschichte und Hintergründe des Stuxnet-Angriffs

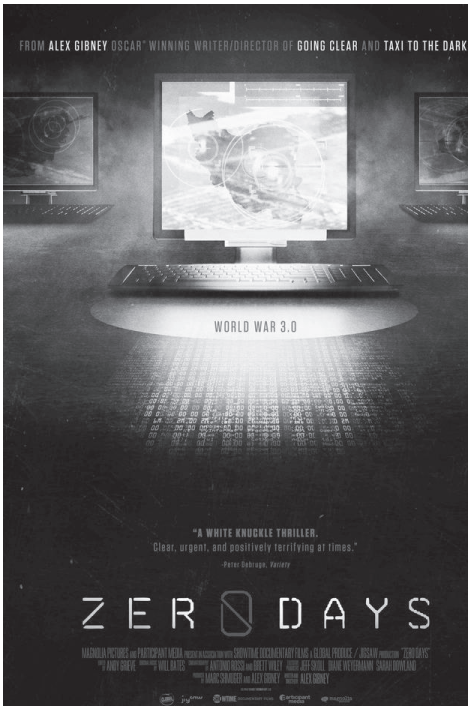
Dreimal habe ich mir den Film angeschaut. Jedes Mal eröffnete er mir mehr Details, jedes Mal war er wieder spannend bis zum Abspann. Und jedes Mal ging er mir tiefer unter die Haut. In *Zero Days* zeichnet der Regisseur und Oscar-Preisträger Alex Gibney die Geschichte der Entdeckung und Analyse des Computerwurms *Stuxnet* nach und versucht, die politischen und strategischen Hintergründe aufzudecken. Sein Publikum entlässt Gibney mit Denkanstößen, was Stuxnet für unsere Gesellschaft bedeuten kann und welche Folgen die durch Stuxnet offenbarte – technische, militärische, politische – Entwicklung für uns alle haben könnte. *Zero Days* ist ein gelungener Dokumentarfilm – unterhaltsam und spannend, dass er das Publikum erreicht und mitzieht, nicht ohne eine Position zu beziehen und eine Botschaft zu vermitteln. Er ist dabei ein anschauliches Beispiel, wie investigativer Journalismus geht.[1]

Wie ein Mosaik setzt Gibney den Plot aus Interviewschnitten zusammen, mit einem Minimum an Kommentar, und es ergibt sich am Ende ein schlüssiges Bild. So bringt Gibney die führenden Köpfe der Community, die sich mit der Aufdeckung der Rätsel um Stuxnet befasst hat, vor die Kamera und folgt mit Interviewschnitten der langwierigen Puzzlearbeit um die schrittweise Aufdeckung der Rätsel um Stuxnet. Politiker, Militärs, leitende Beamte, Journalisten lässt er zu Wort kommen, wenn es um Hintergründe und Folgen geht.

Am 17. Juni 2010 entdecken die „Woodpecker" der Computersicherheits-Unternehmen, zuerst in Weißrussland, einen neuen rätselhaften Typus von Schadsoftware im Internet. Sie nennen ihn *Stuxnet,* ein Amalgam aus zwei Codeschnipseln. Die Community der Sicherheitsanalysten, darunter führende Experten der Computersicherheits-Unternehmen Kaspersky Lab und Symantec, sind geschockt von der Komplexität dieser Schadsoftware. Für den *Dropper,* die für die Selbstausbreitung verantwortliche Softwarekomponente, werden vier Zero-Days genutzt – außergewöhnlich, wer kann sich einen derart hohen Aufwand leisten? Auch die *Payload,* die sich im Zielsystem aktivierende Softwarekomponente, überrascht bezüglich ihres Umfangs und ihrer Undurchschaubarkeit.

Die Zeichen verdichten sich, dass staatliche Akteure hinter dem Projekt stehen. In der *Payload* werden Hinweise auf PLC-Geräte gefunden, *Programmable Logic Controller* für die Steuerung von Maschinen und Geräten. Die Spur führt zu Siemens-Produkten. Offensichtlich identifiziert die *Payload* das Zielsystem anhand von Seriennummern für ein sehr gezieltes Zuschlagen. Die Seriennummern führen zu Zulieferern von Frequenzumrichtern und schließlich in den Iran. Aus US-Embargolisten kommt der Hinweis auf Anwendungen in nukleartechnischen Einrichtungen. Auf die Spur zum Ziel der Schadsoftware führt schließlich die Auswertung von Propagandafilmmaterial aus iranischen Atomforschungseinrichtungen: Entdeckt werden Korrespondenzen zwischen Zahlenmustern im *Payload*-Code und Gruppierungen der Urananreicherungszentrifugen in Anlagenplänen. Aber wer sind die Urheber? Was ist ihre Intention? Aus dem Off, „wo wir auch nachfragten, wir trafen auf eine Mauer des Schweigens, wir mussten uns andere Wege suchen".

Einen Ansatzpunkt liefert der Cyberwarfare-Experte David E. Sanger, Korrespondent der New York Times, mit einem Rückblick auf die Geschichte der politischen Beziehungen zwischen den USA und dem Iran. Ab 1959, unter Schah Reza Pahlavi, wird mit US-amerikanischer Unterstützung ein iranisches Atomforschungsprogramm aufgebaut. Die USA schenken dem Schah 1959 und 1967 jeweils einen Forschungsreaktor. Schon der Schah liebäugelt mit eigenen Atomwaffen. Nach 1979, dem Jahr der iranischen Revolution, wird Irans Streben nach eigenen Atomwaffen unüberhörbar. Der Iran treibt ihre Entwicklung voran, heimlich unterstützt von Pakistan. Die politische Situation im Nahen Osten wird zunehmend instabil. Israel sieht sich existenziell bedroht und bittet die USA um grünes Licht für Bombenangriffe auf iranische Nuklearanlagen. Die USA befürchten eine Eskalation, in die sie hineingezogen würden. Sie machen Israel das Angebot, einen „anderen Weg" zu finden. Die Militärs überzeugen Präsi-



Filmplakat, Magnolia Pictures[4]*: Zero Days (2016)*
Dokumentarfilm von Alex Gibney, 116 Minuten
Weitere Filmdaten: http://www.imdb.com/title/tt5446858/
Offizielle Filmseite: http://www.zerodaysfilm.com/

dent Bush von der Option eines Cyberschlags. Die Entwicklung wird im *Department of Defense* begonnen unter dem Codenamen „Olympic Games", später auf Drängen von Verteidigungsminister Gates in das neu geschaffene *US Cyber Command* verlagert. Beteiligt ist der israelische Geheimdienst.

Die Mauer des Schweigens. Bis heute gibt es zur Rolle der USA oder Israels keinerlei offizielle Erklärung, Aussage, Stellungnahme, Dementi. Nicht einmal ein Wort zur Existenz dieser Cyberwaffe. Selbst Sicherheitsorgane in den USA waren nicht informiert und glaubten an einen Angriff von außen, als Stuxnet auch heimische Systeme infizierte. Aber Washington sei nicht nur ein Ort der Geheimhaltung, sondern auch ein Ort der Lecks. Gibney findet seins. Vermutlich aus der Meisterklasse der NSA, der Abteilung TAO, zuständig für *Tailored Access Operations.* Vor die Kamera darf er diese Person (oder Personen?) natürlich nicht bringen. Ihre Aussagen lässt er von einer Schauspielerin mit verfremdeter Stimme sprechen, Aussagen über das Potenzial von Stuxnet, über die Rolle der NSA, über den schmalen Grat zwischen Ausspähung und Angriff – und über die Existenz einer noch weit mächtigeren Cyberwaffe für den Fall, dass die Verhandlungen mit dem Iran scheitern würden – *Nitro Zeus,* dazu bestimmt, die iranische Luftabwehr lahmzulegen und Teile des iranischen Stromnetzes auszuschalten.[2]

Dass die Existenz von Stuxnet aufgedeckt werden kann, verdanken wir dem israelischen Geheimdienst. Während man sich mit mehreren bestens getarnten Stuxnet-Vorversionen an den beabsichtigten Einsatz herantastet, modifizieren 2010 die Israelis die Software im Alleingang. Dabei unterläuft ihnen ein fataler Fehler, der zur Entdeckung führt – und die Zivilgesellschaft wird erstmals ganz konkret mit der potentiellen Bedrohung durch Cyberwaffen konfrontiert.

Stuxnet zerstört vermutlich um die tausend Zentrifugen in iranischen Nuklearanlagen. Die Produktion von angereichertem Uran wird, so die Kontrolleure der IAEA, ausgebremst – für ein Jahr. Danach nimmt sie erst richtig Fahrt auf. Der Iran baut seinerseits eine schlagkräftige Cyberwarfare-Einheit auf, Vergeltungsdrohungen richten sich an die USA. Im Iran vermutet man die Urheber folgenschwerer Cyber-Angriffe auf ein US-Unternehmen der Petrochemie und auf eine US-Bank. Zu den Folgen hat Ralph Langner, SPS-Sicherheitsberater, einen ausführlichen und lesenswerten Bericht veröffentlich.[3]

„Stuxnet hat die Büchse der Pandora geöffnet", O-Ton der anonymen Informantin. Oder Michael Hayden, „einmal ausgepackt, kann eine solche Waffe nicht mehr weggepackt werden". Die Zahl der Staaten und nichtstaatlichen Organisationen, die ein schlagkräftiges Cyberwaffen-Arsenal aufbauen, wird zunehmen, ebenso die nichtkalkulierbaren Risiken. Insider kommen zu Wort, die die Gefahren für die Gesellschaft noch über die der Atomwaffen stellen. Vor diesem Hintergrund appelliert der Terror-Experte Richard A. Clarke engagiert für einen Cyberwaffen-Bann. Auch wenn heute die praktische Unmöglichkeit einer Waffenkontrolle prophezeit wird. „Es hat 30 Jahre gedauert, und es wurde für unmöglich gehalten, aber heute haben wir wirksame Verbote von biologischen Waffen und Chemiewaffen und einige brauchbare Verträge für eine Atomwaffenkontrolle. Auch bei Cyberwaffen wird es Zeit brauchen. Aber es wird sich nur etwas bewegen, wenn wir anfangen!"

Ein hervorragender Einstieg in die Cyberpeace-Debatte, für öffentliche Veranstaltungen, für den Unterricht in Schulen und Ausbildungsstätten … könnte der Film sein, wenn die sprachliche Verständlichkeit nicht so schwierig wäre: Die Interviews werden auf Englisch geführt, und die Interviewten sind keine geschulten Sprecher (der Genderpunkt ist hier nicht nötig, bezeichnenderweise), sie sprechen teils sehr schnell, in knappen Sätzen, mit starkem Akzent, in Slang- und Fachtermini. Hinzu kommt die eigentlich unnötige und störende Verfremdung der Stimme der Schauspielerin. Ist man nicht im angelsächsischen Sprachraum unterwegs, zudem vielleicht auch mit den Fachbegriffen nicht vertraut, wird man ohne wiederholtes Abhören den Feinheiten der Aussagen kaum folgen und viele Zusammenhänge nicht erfassen können. Jedoch, durch eine Synchronisation oder überlagerte Kommentierung würde dem Film die Authentizität verloren gehen, und davon lebt der Film. Deswegen ist der Film doch unbedingt zu empfehlen. Auch für Veranstaltungen, wenn er moderiert, an wichtigen Stellen kommentiert und natürlich diskutiert wird.

> *"The title ZERO DAYS refers on one level to the multiple soft-ware vulnerabilities that made Stuxnet possible, as well as the infinite software vulnerabilities that will fuel the attacks of the future. But it is also a potent metaphor for this moment in time. We don't have a patch for this problem yet. From this moment forward, we're going to have to reckon with this new challenge of the potential of cyberwar. These are our 'Zero Days.' We're starting from zero. What are we going to do going forward?" — Alex Gibney*[5]

Zusätzliche Empfehlung der Redaktion: ZERO DAYS VR[6]

> *"How do you make a documentary where the lead character is code – where code could speak for itself? […] The true story of a clandestine mission hatched by the US and Israel to sabotage an underground Iranian nuclear facility told from the perspective of Stuxnet, a sophisticated cyber weapon, and a key NSA informant. Audiences experience the high stakes of cyber warfare placed inside the invisible world of computer viruses." – Scatter*[7]

Anmerkungen und Referenzen

1 *Vorgestellt am 17. Februar 2016 auf den Internationalen Filmfestspielen Berlin*

2 *Sanger DE, Mazetti M (16. Februar 2016) U.S. Had Cyberattack Plan if Iran Nuclear Dispute Led to Conflict. New York Times.* https://www.nytimes.com/2016/02/17/world/middleeast/us-had-cyberattack-planned-if-iran-nuclear-negotiations-failed.html

3 *Langner R (2017) Stuxnet und die Folgen. Langner Communications GmbH, Hamburg.* https://www.langner.com/wp-content/uploads/2017/08/Stuxnet-und-die-Folgen.pdf

4 Magnolia Pictures (2016) Zero days. Complete press kit. http://www.magpictures.com/resources/presskits/ZERODAYS.zip

5 *Magnolia Pictures (2016) Zero days; Final press notes.* http://www.magpictures.com/resources/presskits/zerodays/ZERODAYSfinalnotes.doc

6 *ZERO DAYS VR.* https://www.zerodaysvr.com/

7 *Scatter (Januar 2018) Zero days VR. Press kit.* https://www.zerodaysvr.com/s/1801_ZeroDays_PressKit.pdf