Cinemanalyse, 9. Film des Zyklus „Welten“, 2017
Donnerstag, 14.12.2017, 20.00 (Bar ab 19.00), im Lichtspiel/Kinemathek, Sandrainstrasse 3, 3007 Bern. Einführung: Liliane Schaffner, Psychoanalyse am Werk

Zero Days, USA, 2016, 116 Minuten. Regie, Drehbuch: Alex Gibney. Produktion: Alex Gibney, Marc Shmuger. Darsteller: über 20 Interviewpartner aus den USA, Iran, Israel, Weissrussland, Grossbritannien und Deutschland. Sprecherin: Joanne Tucker.

Zum Abschluss unseres diesjährigen Zyklus bieten wir Ihnen eine Reise in die Cyberwelt an. Wir haben uns allerdings nicht für einen Film aus der Fantasy- oder Science-Fiction-Sparte entschieden, denn, was Alex Gibney mit seinem Dokumentarfilm beweist: Die Wirklichkeit ist oft fantastischer als die kühnste Fantasie.

At the time I was beginning my investigations, I thought it was a purely sort of technical story. I didn't understand at the time that it was something deeply fundamental about where we are heading, in terms of spying and cyber conflict. That didn't happen until we started the film. (Alex Gibney)

Definition

Als Zero Day Exploit bezeichnet man in der Computerwelt eine besondere Art der systematischen Ausnutzung von bis zum entscheidenden Moment unbekannten Sicherheitslücken in einem System. Zwischen dem Erkennen und der potenziellen Ausnutzung der Schwachstellen liegen Null Tage, der Angriff erfolgt demgemäss zu einem Zeitpunkt, da Soft- und Hardware noch nicht durch Sicherheitsmassnahmen geschützt werden konnten, was die besonders hohe Vulnerabilität von Systemen gegenüber solchen Angriffen erklärt.

Zero-Day-Exploits werden so lange wie möglich geheim gehalten. Sie werden unter Hackern auf dem Cyber-Schwarzmarkt entsprechend ihrem Wert gehandelt beziehungsweise den Programm-Herstellerfirmen zu hohen Summen angeboten. Ich zitiere Simonite: *Insbesondere seit staatliche Organe sich auch auf offensive Szenarien in einem Cyberwar vorbereiten, tritt auf dem Markt für Zero-Day-Exploits die Situation auf, dass legale staatliche und privatwirtschaftliche Akteure ein Interesse haben, Exploits zu kennen, um einerseits durch die Veröffentlichung von Patches Systeme abzusichern. Gleichzeitig haben dieselben oder im gleichen Auftrag handelnden Akteure das Bestreben, Exploits geheim zu halten, um sie für Angriffe auf feindliche Systeme nutzen zu können.*

Das Ganze spielt sich ab in einem Bereich von geheimen und halbgeheimen Aufdeckungs- und Verschleierungsszenarien, in denen die Grenze zwischen Legalität und Kriminalität auf gefährliche Art verwischt ist. Selbst dort, wo es um die Anwendung von gewissen Testmethoden geht, welche Sicherheitslücken im Voraus eruieren und dem Hersteller melden sollen, wird oft die Grenze des Erlaubten überschritten und/oder es wird gegen die Richtlinien von Herstellern verstossen.

Zum Film

Am 17. Juni gab Sergej Ulasen, ein Mitarbeiter der weissrussischen *VirusBlokAda*, nach einem Hinweis eines iranischen Kunden den Verdacht auf einen Computervirus bekannt. In den darauffolgenden Tagen und Wochen machten internationale Sicherheitsexperten die höchst beunruhigende Entdeckung, dass ein sich selbst replizierender Computerwurm unkontrolliert weltweite Verbreitung gefunden hatte – spätestens seit November 2007, wie sich nachträglich herausstellte. Aufgrund seiner technischen Brillanz und seiner Komplexität – *the most elegant, ingenious, elaborate and terrifying pieces of malware ever created* -, welche auf immense Entwicklungskosten rückschliessen liessen, wurde klar, dass hinter dem Phänomen *Stuxnet*, wie der Wurm inzwischen genannt wurde, am wahrscheinlichsten staatliche Institutionen standen; doch bis zum heutigen Tag hat sich niemand öffentlich dazu bekannt.

Stuxnet ging in die Geschichte ein, weil er die Büchse der Pandora hinsichtlich Cyberkrieg auftat. Zum ersten Mal wurde öffentlich bekannt, dass ein „virtueller Kampfstoff" gezielt eingesetzt worden war.

Recherchen ergaben, dass das Stuxnet- Schadprogramm vier Zero-Day-Exploits enthielt und darauf ausgerichtet war, von Siemens entwickelte Steuerungsanlagen vom Typ Simatic-S7, die weit verbreitet sind und in verschiedensten Industriezweigen zur Anwendung kommen, zu manipulieren. Es konnte weiter aufgezeigt werden, dass die Angriffe gehäuft in Iran auftraten, was zu der Hypothese veranlasste, dass die Zwischenfälle, durch welche Ende 2009 in der Atomanlage von Natanz circa tausend Zentrifugen ausser Dienst gestellt worden waren, auf Angriffe von Stuxnet zurückzuführen seien.

Gibney geht es im Film um die Aufklärung der Hintergründe rund um das Schadprogramm, sowohl was seine technische Entwicklung und seine Provenienz als auch was seine Rolle im komplexen, von Geheimhaltung geprägten politischen Kräftespiel im Nahen Osten angeht. Auf die Frage, welche Absicht ihn bei der Realisierung seines Films geleitet habe, weist Gibney auf seine grundsätzliche Pflicht als Dokumentarfilmer hin, als Aufklärer zu wirken. Er verfolge mit diesem Film das ausdrückliche Ziel, Fakten aufzudecken und Geheimnisse zu lüften, um damit eine öffentliche Diskussion anzuregen, besonders im Hinblick darauf, dass das Thema fundamentale politische Fragen aufwerfe, da wir uns in Sachen Cyber-Krieg in einem noch gänzlich unkontrollierten und unreglementierten Feld bewegen würden. Diese Absicht decke sich mit den Ansichten seiner Gesprächspartner im Film, welche sich letztlich trotz ihrer Geheimhaltungspflicht dazu entschlossen hätten auszusagen, weil sie sich mit der absoluten Informationsverweigerung ihrer Regierung nicht identifizieren könnten.

Für mich wirft der Film zudem grundsätzliche Fragen auf:

- Wie wirkt es sich aus, dass aufgrund der Folgen einer unkontrollierten digitalen Aufrüstung Überzeugungen, welche bis vor nicht allzu langer Zeit noch als

Verschwörungstheorien eingeschätzt und als solche dem Bereich des Wahns zugeordnet worden wären, zur neuen Alltagswirklichkeit werden?
- Wie reagieren wir auf die Zunahme an Komplexität und die damit zusammenhängende Fragilisierung unserer Existenz angesichts des exponentiellen Anstiegs der Menge an digitalen Daten?

Zero Days feierte am 11.2. 2016 seine Première bei den Internationalen Filmfestspielen in Berlin, wo er auch am Wettbewerbsprogramm teilnahm.

Der Regisseur:
Alex Gibney, 1953 geboren, ist ein aus den USA stammender Regisseur, Drehbuchautor und Produzent. Er hat in Yale Japanische Literatur studiert und anschliessend an der UCLA eine Filmschule absolviert. In seinen Dokumentarfilmen greift er mit Vorliebe sozial oder politisch heikle, häufig tabuisierte Themen auf, z.B. den Skandal um die Firmenpleite von Enron (2005), die systematische Anwendung von Folter durch die US-Armee (2007), den sexuellen Missbrauch in der Kirche (2012), die Geschehnisse um Julian Assange, Bradley Manning und Wikileaks (2013), die Praktiken von Scientology (2015). Seine Filme zeichnen sich aus durch minuziöse Recherchen und packende Inszenierungen, er wurde dafür mit zahlreiche Auszeichnungen bedacht, darunter 2008 einem Oscar für *Taxi to he Dark Side* und 2006 einer Oscar Nominierung für *Enron: The smartest guys in the room.* Das New York Times Magazine beschrieb ihn als *one of America's most successful and prolific documentary filmmakers.*

Eine iranische Anekdote:
Die Iraner verfügen – und dies nicht erst seit der Dauerbespitzelung durch ihre Geheimdienste und sonstigen Informanten – über ein unglaubliches Talent, heikle Inhalte metaphorisch zu umschreiben, um damit jegliches Risiko zu vermeiden, auf eine Aussage behaftet zu werden. Diese Technik wird sowohl im alltäglichen Diskurs als auch in der Kunst meisterhaft angewendet. Ich hatte dieses Jahr die Gelegenheit, den Iran zu besuchen. Auf dem Weg von Isfahan nach Kashan, wir fuhren sehr nahe an Natanz vorbei, wagte ich Reza, meinen iranischen Begleiter, auf Stuxnet anzusprechen. Seine Antwort fiel zögerlich und knapp aus: „Ach, der Versuch der Israeli, unser Atomprogramm zu schädigen… hat ihnen nicht viel gebracht.. im Gegenteil." Ich verstand dies als Bitte, ihm keine weiteren diesbezüglichen Fragen zu stellen. Etwa zehn Tage später, unterwegs im Zagros-Gebirge, erblickten wir auf dem Pfad eine Kakerlake. Reza erzählte, bis vor kurzem habe es im Iran nur sehr wenige davon gegeben, und wenn, dann nur kleine. Doch vor etwa zehn Jahren sei das Land regelrecht überschwemmt worden mit einer viel grösseren, viel gefährlicheren Kakerlaken-Art, die aus den USA und aus Europa eingeschleppt worden seien, versteckt in den Kartons mit den elektronischen Geräten, z.B. denjenigen von Siemens …
Ich bin mir bis heute nicht sicher, ob dies eine späte Antwort auf meine Stuxnet-Frage war.