4. Backdoors

Ein Phänomen, das ein nicht zu unterschätzendes, aber oft leises Problem für die Sicherheit innerhalb digitaler Kulturen darstellt, und in der vorliegenden Untersuchung bisher nur am Rande gestreift wurde, sind Backdoors. Backdoors, auch Hintertüren genannt, sind vor allem im Kontext der vorliegenden Publikation von besonderem Interesse, da die anspruchsvolleren unter ihnen an der Intersektion von IT-Sicherheit und Kryptographie anzusiedeln sind, und ihre Analyse daher die Erkenntnisse der beiden vorangegangenen Kapitel vereint. An Backdoors lassen sich Fragen nach der Sicherheit vernetzter Computer diskutieren, die in den beiden vorangegangenen Kapiteln bereits jeweils als einem negativen Sicherheitsbegriff folgend definiert wurde. Der erste Teil dieses Kapitels wird zunächst eine informatische Definition von Backdoors vorstellen. Fragen, die dabei im Vordergrund stehen, sind: Welche Phänomene werden als Backdoor bezeichnet? Was macht eine Backdoor zu einer Backdoor? Muss immer eine Absicht hinter einer Backdoor stecken, oder können Backdoors auch unabsichtlich entstehen? Diese Fragen werden anhand von zwei Backdoors erörtert: einer verhältnismäßig trivialen *hard-coded credentials*-Backdoor und der im Zuge der Snowden-Enthüllungen zu großer Bekanntheit gelangten kleptographischen Backdoor im Pseudozufallsgenerator *DUAL_EC_DRBG*. Diese Fallbeispiele wurden ausgewählt, da sie im innerfachlichen Diskurs der IT-Sicherheit recht bekannt sind, und somit über eine gute Quellenlage verfügen, was durchaus nicht der Regelfall für Backdoors ist.

Der zweite Teil des vorliegenden Kapitels widmet sich skizzenhaft den mit Backdoors verbundenen Metaphern der Tür, der Hintertür und des Geheimnisses, und wie diese das Phänomen der Backdoor innerhalb digitaler Kulturen situieren. Im Anschluss daran wird mit der Backdoor-Schadsoftware *Back Orifice* das Verhältnis von informatischen zu menschlichen Hintertüren untersucht – also das Verhältnis von Backdoors zum Anus, sowie der homopho-

be Subtext dieses Metaphernzusammenhangs. Dieser in der Informatik eher ignorierte Zusammenhang wird unter Bezugnahme auf Guy Hocquenghem, einem Vertreter der Gay Theory der 1970er Jahre, ins Sprechen gebracht. Im Anschluss daran werden mit Leo Bersani und Paul B. Preciado zwei mögliche Lesarten von *Back Orifice* angeboten, mit denen die im vorangegangenen Kapitel herausgearbeitete Homophobie, die den IT-Sicherheitsdiskurs über die HIV/AIDS-Metaphorik informiert, denaturalisiert und/oder umgedeutet werden kann.

4.1 Was sind Backdoors?

Unter dem Stichwort »backdoor« werden in der zweiten Ausgabe des *Oxford English Dictionary* drei mögliche Bedeutungen in zwei Kategorien aufgelistet: »1.) a) A door at the back of a building or enclosure, as opposed to the front-door; a secondary or private entrance. b) back-door trot (figurative); also spec., diarrhœa,[1] dialect. 2.) figurative; also attributive = Unworthily secret, clandestine« (Oxford English Dictionary 1989). Hier besteht bereits ein Zusammenhang zwischen den hinteren, von öffentlichen Orten wie einer Straße aus nicht einsehbaren Orten der Hintertüren von Häusern, von privaten Eingängen, und der Idee der Heimlichkeit oder des Verbergens. Eine informatische Bedeutung wird nicht aufgeführt, obwohl in der Online-Ressource auch jüngere Aktualisierungen des Wortes vermerkt sind. Auch im Duden kommt diese Bedeutungsdimension nicht vor: Es gibt keinen Eintrag zu »Backdoor«, und unter dem Lemma »Hintertür« werden als Bedeutungen lediglich »1. hintere [Eingangs]tür (besonders eines Hauses, Gebäudes)« sowie »2. versteckte Möglichkeit, etwas auf nicht [ganz] einwandfreien Wegen und Umwegen zu erreichen, sich einer Sache zu entziehen« (Dudenredaktion 2018) gelistet. In der Open Access-Variante des *Oxford Dictionary* namens *Lexico* findet sich nach den bereits genannten Erklärungen auch eine kurz gehaltene informatische Bedeutung: »A feature or defect of a computer system that allows surreptitious unauthorized access to data« (Lexico 2021a). Eine Backdoor im informatischen Sinne kann also ein Feature oder ein Defekt sein, das oder der einen heimlichen und

1 Über den Bedeutungszusammenhang des Ausdrucks »back-door trot« als Bezeichnung für Durchfall wird eine Beziehung des Wortes Backdoor zum Anus/Rektum hergestellt, auf die später noch eingegangen wird.

unautorisierten Zugang zu Daten ermöglicht. Der Informatiker David Ferbrache (1992, 3) gibt in seinem Handbuch *A Pathology of Computer Viruses* folgende knappe Definition:

> »A software feature programmed by the original designer which will permit him [sic!] to carry out operations denied to normal users of the software (e.g. a login program which will accept the designer's hard-wired password irrespective of the contents of the system password file).«

Während Ferbrache die Frage nach dem un/autorisierten Zugriff ausspart, fällt die Definition im *Jargon File*, dem Wörterbuch der Hacking Culture, etwas ausführlicher aus. Dort wird darauf hingewiesen, dass der Zugang zu Daten nicht immer unautorisiert erfolgen muss, beispielsweise könnte ein_e Techniker_in eine Fernwartung mittels Backdoor durchführen. Unter dem Lemma »back door« ist dort nachzulesen:

> »A hole in the security of a system deliberately left in place by designers or maintainers. The motivation for such holes is not always sinister; some operating systems, for example, come out of the box with privileged accounts intended for use by field service technicians or the vendor's maintenance programmers. Syn. trap door; may also be called a wormhole.«[2] (The Jargon File o.J.b)

Elementarer Teil dieser Definition ist die Absicht, die hinter einer Backdoor stecken muss. Während über die treibenden Motive keine Aussage getroffen wird, muss doch mindestens eines vorhanden gewesen sein, denn ohne eine Intention des_der Autor_in wird eine gegebene Sicherheitslücke laut *Jargon File* jedenfalls nicht als Backdoor klassifiziert. Im *Jargon File* (ebd.) heißt es weiter: viele Backdoors »lurked in systems longer than anyone expected or planned«, und dass nur wenige Backdoors zu größerer Bekanntheit gelangt seien. Auf welche Art eine Backdoor in ein System kommen kann, beantwortet die Definition des *Bundesamts für Sicherheit in der Informationstechnik* (BSI o.J.a), die folgendermaßen lautet:

> »Eine Backdoor ist ein üblicherweise durch Viren, Würmer oder Trojanische Pferde installiertes Programm, das Dritten einen unbefugten Zugang (›Hin-

2 Die Bezeichnung *trap door* ist außerhalb des Jargon File eher in umgangssprachlichem Gebrauch, aber nicht in wissenschaftlicher Literatur zu finden. *Trap door* bezieht sich in letzterer eher auf mathematische Vorgänge, die schwer oder nicht reversibel sind (vgl. Diffie/Hellman 1976, 652). *Wormhole* hat sich als Synonym nicht durchgesetzt.

> tertür‹) zum Computer verschafft, jedoch versteckt und unter Umgehung der üblichen Sicherheitseinrichtungen. Backdoors werden oft für Denial-of-Service-Angriffe benutzt.«

Diese Definition folgt grundsätzlich der Richtung der bereits besprochenen, besteht allerdings erneut auf einen unautorisierten Zugang, der durch eine Backdoor entsteht. Während die bisher aufgeführten Definitionen von Backdoors im informatischen Sinne zwar einen gemeinsamen Kern besitzen, unterscheiden sie sich doch in ihrer Schwerpunktsetzung, und ergeben erst in ihrer Aneinanderreihung ein ganzheitlicheres Bild. Eine umfassende Definition dessen, was eine Backdoor im informatischen Sinne sein könnte, die aus einem wissenschaftlichen Kontext kommt, ist erstaunlich schwer zu finden. Der Begriff wird eher in populärwissenschaftlichen Glossaren auf IT-Dienstleistungswebseiten erläutert als in Fachliteratur, obwohl er ständig verwendet wird.[3] Es scheint also innerhalb von IT-Sicherheit als wissenschaftlicher Disziplin eher ein intuitives Wissen davon zu geben, was eine Backdoor ist, eine Art Gebrauchsdefinition. Ferbrache (1992, 3) bemerkt dazu bereits Anfang der 1990er Jahre: »A feature of the anti-virus community has been the adoption of a wide range of (often conflicting) terminology […]«. Diesen Umstand der ausbleibenden und/oder ungenauen Definitionen adressieren auch Sam Thomas und Aurélien Francillon (2018, 93) nahezu 30 Jahre später in ihrem Aufsatz *Backdoors: Definition, Deniability and Detection*: »The term ›backdoor‹ is generally understood as something that intentionally compromises a platform, aside from this, however, there has been little effort to give a definition that is more rigorous.« Im Wesentlichen führen sie zwei Gründe für das bisherige Ausbleiben einer rigorosen Definition an. Zum einen nennen sie die Vielgestaltigkeit von Backdoors: »[…] backdoors can take many forms, and can compromise a platform by almost any means; e.g., a hardware component, a dedicated program or a malicious program fragment.« (Ebd.) Zum anderen sei eine generalisierende Definition auch aufgrund weniger bekannter und damit auch dokumentierter Backdoors schwer aufzustellen: Bei komplizierteren Backdoors habe man mit einem »sheer lack of real-world samples« (ebd.) zu kämpfen, wohingegen die bisher dokumentierten Fälle eher simpel seien und hauptsächlich darauf basierten, dass User_innen »certain static data, e.g., hard-coded credentials« (ebd.) eingeben. Solche Varianten seien zwar bereits wissenschaftlich aufgearbeitet worden, decken laut Thomas und Francillon

3 Gesucht wurde sowohl nach »backdoor« als auch nach »back door« und »Hintertür«.

(vgl. ebd.) jedoch nur einen kleinen Teil der möglichen Fälle ab. Ein Beispiel für *hard-coded credentials*[4] als Backdoor wäre folgender Fall: Änderungen am BIOS[5] eines Computers, also der Einheit, die den Computer funktionsfähig macht, können in der Regel nur nach Eingabe eines Passworts vorgenommen werden. Dieses Passwort lässt sich in den meisten Fällen von den User_innen selbst setzen, es gibt aber auch einige Standardpasswörter für verschiedene BIOS-Modelle, die auch unabhängig davon, ob die Nutzer_innen des jeweiligen Computers ein anderes Passwort eingestellt haben, noch funktionieren. Im Lauf der Zeit wurden verschiedene Passwortlisten im Internet veröffentlicht (vgl. Caloyannides 2004, 251), die es beispielsweise Hacker_innen leicht machten, unautorisiert an verschiedensten Computern Änderungen vorzunehmen.[6] Ein aktuelles Beispiel ist das *Mirai*-Botnet,[7] das erstmals 2016 in Erscheinung trat, und im selben Jahr zu internationaler Bekanntheit gelangte, da der *Mirai*-Quellcode für einen großskaligen Angriff verwendet wurde. *Mirai* suchte online nach Internet of Things-Geräten mit einem ARC-Prozessor. Auf diesem läuft eine Linux-Variante als Betriebssystem, und falls die Standardwerte für User_innenname und Passwort nicht verändert wurden, konnte *Mirai* das Gerät infizieren (vgl. Cloudflare o.J.b). Infizierte Geräte suchten selbständig nach weiteren Geräten, um auch diese mit Schadsoftware zu bespielen (vgl. BSI o.J.b). All dies geschah ohne das Wissen und/oder Einverständnis der Besitzer_innen – also *heimlich*. Zu internationaler Bekanntheit

4 Als »credentials« werden Zugangsdaten bezeichnet, die sowohl User_innennamen als auch Passwörter umfassen. »Hard-coded« bedeutet in diesem Zusammenhang, dass diese Daten fest im Code eines jeweiligen Systems hinterlegt sind, und nicht verändert und/oder entfernt werden können, ohne die Software selbst zu verändern.

5 Das BIOS (kurz für *Basic Input Output System*) vermittelt zwischen Hard- und Software, da es die Hardwarekomponenten eines Computers ansteuert (vgl. Schimpf et al. 2001, 75–76). Da das BIOS spezifisch auf eine jeweilige Hardware zugeschnitten ist, muss es das Betriebssystem nicht sein.

6 Auf diesen Listen finden sich nicht nur (erwartbarer Weise) die Namen der Herstellerfirmen, sondern auch absurdere Passwörter: Mehrere BIOS-Modelle der Firma *Award* können unter anderem mit dem Passwort »LKWPETER« (entweder ausschließlich in Groß- oder in Kleinbuchstaben) entsperrt werden (vgl. Caloyannides 2004, 251).

7 Als Botnet bezeichnet man ein Netzwerk aus verschiedenen Endgeräten, die mittels Schadsoftware verbunden und dann für Cyberangriffe instrumentalisiert werden. Durch die Verbindung einer großen Anzahl an Geräten (die dann als *Bots* oder manchmal auch als *Zombies* bezeichnet werden) zu einem Netzwerk werden großskalige Angriffe möglich, wie bspw. Distributed Denial of Service-Angriffe.

gelangte *Mirai*, da es mehrere hunderttausend Internet of Things-Endgeräte (darunter beispielsweise Videorecorder, Webcams, Router, Kühlschränke etc.) verbinden und eine Distributed Denial of Service-Attacke auf den DNS-Provider *Dyn* ausführen konnte, im Zuge derer weite Teile des Internets für mehrere Stunden nicht mehr zu erreichen waren (vgl. Kühl/Breitegger 2016; Schneier 2018). Zentral für die Möglichkeit, ein so riesiges Botnet aufzubauen, war ebenfalls die Tatsache, dass viele IoT-Geräte über unveränderliche *hard-coded credentials* verfügen, die als Backdoor fungiert haben, über die sich *Mirai* Zugang zu den Geräten verschaffen konnte (vgl. Weidenbach/vom Dorp 2020, 17–18).

Obgleich Thomas und Francillon (2018, 93) wiederholt von »backdoor-like functionality« sprechen, denken sie Backdoors nicht als bloße Modi oder Funktionsweisen, sondern durchaus als spezifische strukturierte Objekte, die aufgrund ihrer Vielgestaltigkeit erst durch eine Betrachtung aus verschiedenen Blickwinkeln und auf verschiedenen Ebenen trennscharf zutage treten. Zu diesem Zweck entwickeln sie ein komplexes Klassifizierungssystem, das im Weiteren schrittweise vorgestellt wird.[8] Das System fokussiert sich ausschließlich auf informationstechnologische Aspekte, stellt aber für die weiterführenden Betrachtungen eine gute Basis dar. Um die Definition nachvollziehen zu können, ist zuvor etwas Begriffsarbeit notwendig: Die Autoren setzen den Begriff *platform* als höchste Abstraktionsebene eines gegebenen Geräts, das mit einer Backdoor versehen werden soll, und ein *system* als die höchste Abstraktionsebene einer Einheit innerhalb einer *platform* (vgl. ebd., 95). Ein *system* kann beispielsweise ein Programm, ein bestimmter Teil einer Software- oder eine Hardwarekomponente sein (vgl. ebd.). Um dies anhand eines bereits bekannten Beispiels zu veranschaulichen: Ein PC wäre die *platform*, innerhalb derer das *system* BIOS den Ansatzpunkt für eine *hard-coded credentials*-Backdoor bildet. Der erste Teil der umfassenden und rigorosen Definition, die Thomas und Francillon (ebd., 98, Herv. i.O.) aufstellen, lautet folgendermaßen:

> »***Backdoor***. An *intentional* construct contained within a system that serves to compromise its expected security by facilitating access to otherwise privileged functionality or information. Its implementation is identifiable by its

8 Ein elementarer Teil von Thomas' und Francillons theoretischem Framework ist es auch, ein System zur Entdeckung von Backdoors bereitzustellen. Da dieser Part für die hier angestellten Überlegungen nicht relevant ist, wird er ausgeklammert.

> decomposition into four components: *input source*, *trigger*, *payload*, and *privileged state*, and the intention of that implementation is reflected in its complete or partial (e.g., in the case of bug-based backdoors) presence within the DFSM and AFSM, but not the EFSM of the system containing it.«

Die vier genannten Komponenten stellen laut den Autoren die Minimalbedingungen dafür dar, ein Phänomen als Backdoor zu klassifizieren (vgl. ebd.). Sie beschreiben gleichzeitig den zeitlichen Ablauf der Funktionsweise einer Backdoor: Aus einer *input source* (Eingabequelle) muss ein *trigger* (Auslöser) kommen. Wenn der *trigger* erfolgt ist, wird der *payload* (die funktionsgebende Software) ausgeführt, wonach sich das *system* im *backdoor-activated state* befindet, was bedeutet, dass die Entität,[9] die die Backdoor aktiviert hat, nun höhere Privilegien innerhalb des Systems hat als vorher, weswegen dieser Zustand auch als *privileged state* bezeichnet wird (vgl. ebd., 97). Die Frage nach der Intentionalität wird bei Thomas und Francillon durch die Modellierung verschiedener Betrachtungsperspektiven gelöst. Sie schlagen vor, dass ein gegebenes *system* von zwei entgegengesetzten Positionen betrachtet werden könne: die der Endanwender_innen und die der Entität, die die Backdoor implementiert hat (vgl. ebd., 96). Um innerhalb dieser Gegenüberstellung präzise Aussagen treffen zu können, definieren sie vier verschiedene Sichtweisen oder Versionen desselben *systems*: 1.) die Version der Entwickler_innen (developer) *DFSM*, 2.) die tatsächliche (actual) Version *AFSM*, die beispielsweise eine käuflich zu erwerbende Software ist, 3.) die von Endnutzer_innen erwartete (expected) Version *EFSM*, und 4.) die Version, die durch *Reverse Engineering*[10] erstellt wurde *RFSM* (vgl. ebd.).[11] Thomas und Francillon verwenden

---

9 Der Verständlichkeit halber wird »entity« mit Entität übersetzt, da es sich dabei sowohl um einzelne Entwickler_innen als auch um Institutionen handeln könnte, um Zufälle, Bugs oder Hacker_innen, oder um Geräte mit Schadsoftware (wie bspw. im Fall von *Mirai*).

10 Als *Reverse Engineering* wird ein Vorgang bezeichnet, bei dem eine Software, deren Quellcode unbekannt ist, anhand des ausführbaren Programms nachprogrammiert wird, sodass dieselbe Funktionalität entsteht. Da es mehrere Möglichkeiten gibt, eine konkrete Funktionalität zu erzeugen, können sich der Originalquellcode und der *Reverse Engineering*-Quellcode deutlich voneinander unterschieden.

11 Das Kürzel FSM steht für *finite state machine*, also einen *Endlichen Automaten*. Ein endlicher Automat zeichnet sich dadurch aus, dass er eine endliche Menge an Zuständen annehmen kann und zu jedem gegebenen Zeitpunkt in einem genau definierten Zustand existiert (vgl. Schimpf et al. 2001, 45–46). Nach einer Eingabe, die eine Zustandsveränderung auslöst, nimmt der Automat einen neuen Zustand aus der Menge zur Ver-

dieses Modell, um den zeitlichen Ablauf der Funktionsweise von Backdoors vereinfacht zu veranschaulichen. Dieser lässt sich exemplarisch anhand des bereits eingeführten BIOS-Beispiels nachvollziehen: Innerhalb der *platform* PC befindet sich das *system* BIOS. Das BIOS befindet sich in Zustand A. Aus der Eingabequelle Tastatur (*input source*) erfolgt nun ein *trigger* (z.B. die Passphrase »LKWPETER«), woraufhin der *payload* ausgeführt wird, und das System die Zugriffsrechte verändert. Das BIOS befindet sich im Anschluss daran in Zustand B, im *privileged state*, in dem die vor dem Computer sitzende Person mit Admin-Rechten auf das BIOS zugreifen und sensible Einstellungen verändern kann. Ob eine Backdoor nun mit Absicht in ein System integriert wurde oder nicht, lässt sich Thomas und Francillon (ebd., 106) folgend mit einem vergleichenden Blick verschiedener Versionen des gegebenen Systems feststellen. Sie schlagen drei Abstufungen vor: Eine mit Absicht eingebaute »*Intentional Backdoor*« muss ihnen zufolge mindestens teilweise in der Entwickler_innenversion (DFSM) nachweisbar sein, und der Übergang von *trigger* zu *payload* muss explizit im Quellcode erkennbar sein. Eine »*Deniable Backdoor*« wäre zum Beispiel ein Bug, der eine für User_innen unerwünschte Funktionalität bereitstellt. Diese Backdoor sei von einem rein technischen Standpunkt aus von einer unabsichtlichen Sicherheitslücke nicht zu unterscheiden, eine dahinterstehende Absicht könne jedoch aus einer gesellschaftlichen Betrachtung heraus vermutet werden. Sie kann in der DFSM nicht definitiv nachgewiesen werden, ist jedoch in der AFSM und der RFSM präsent. Eine »*Accidental vulnerability*« hingegen verfüge zwar über eine Backdoor-ähnliche Funktionalität, wird von Thomas und Francillon nicht mehr als Backdoor klassifiziert, da es weder technische noch soziale Anzeichen für eine Intentionalität gebe. Diese letzte Variante ist in der AFSM und eventuell in der RFSM, aber nicht in der DFSM präsent. Keine Backdoor oder Sicherheitslücke ist jemals in der von Endnutzer_innen erwarteten (expected) Version EFSM vorzufinden – ansonsten wäre der jeweilige Mechanismus einfach eine Funktionalität unter anderen (vgl. ebd., 107) und die Komponente der Heimlichkeit nicht mehr gegeben. Eine *hard-coded credentials*-Backdoor ist Thomas und Francillon (ebd., 106) zufolge immer eine mit Absicht eingebaute Backdoor – an dieser Stelle lässt sich hinzufügen, dass das zwar grundsätzlich stimmt, da diese auf jeden Fall von den Entwickler_innen hinterlegt worden sein muss. Dennoch lässt sich die Intention nicht genau klassifizieren: In manchen Fällen kann

---

fügung stehender Zustände an. Ein simples Beispiel für einen endlichen Automaten wäre eine Verkehrsampel.

eine solche Backdoor angelegt worden sein, um die Software im Entwicklungsprozess schnell bearbeiten zu können, und es wurde lediglich vergessen, diesen Zugang zu entfernen, als das Produkt veröffentlicht wurde. So liegt zwar eine Absicht vor, die aber nicht grundsätzlich darauf abzielen muss, die Entwickler_innen gegenüber den Endanwender_innen in einer privilegierten Position zu halten, und die sich ggf. lediglich auf die DFSM bezieht, aber nicht auf die anderen Versionen, da sie hätte entfernt werden sollen – dies wurde auch bereits in der Definition des *Jargon File* angesprochen. Zusammenfassend lassen sich Backdoors unter Rückgriff auf Thomas' und Francillons Klassifizierungssystem also als Phänomene beschreiben, die die erwartete Sicherheit eines Systems kompromittieren, indem sie den Zugang zu Informationen oder Funktionen, die auf einer höheren Ebene als die eines Standardnutzer_innenkontos liegen, erleichtern. Backdoors müssen mindestens über die vier Komponenten *input source*, *trigger*, *payload* und *privileged state* verfügen. Sie müssen mit Absicht angelegt worden sein, was sich über partiale Perspektiven aus der Sicht von Entwickler_innen und Nutzer_innen auf ein gegebenes System nachweisen lässt. Auf diesem Wege nicht nachweisbare Backdoor-ähnliche Phänomene werden nicht als Backdoor klassifiziert. Im Folgenden soll nun anhand der kleptographischen Backdoor in DUAL_EC_DRBG eine Backdoor vorgestellt werden, die auf einem kryptographischen Verfahren basiert. Die Funktionsweise dieser Backdoor steht in starkem Kontrast zu einer *hard-coded credentials*-Backdoor, was illustrativ für die Spannweite der Materialitäten von Backdoors verstanden werden kann.

4.1.1 Die kleptographische Backdoor in DUAL_EC_DRBG

> »Random numbers are critical for cryptography: for encryption keys, random authentication challenges, initialization vectors, nonces, key-agreement schemes, generating prime numbers and so on. Break the random-number generator, and most of the time you break the entire security system. Which is why you should worry about a new random-number standard that includes an algorithm that is slow, badly designed and just might contain a backdoor for the National Security Agency.« (Schneier 2007)

Mit diesen Worten beginnt ein im November 2007 erschienener Artikel des Security-Experten Bruce Schneier im Magazin *Wired*, in dem Schneier eine mögliche Backdoor in einem Pseudozufallszahlengenerator namens DUAL_EC_DRBG bespricht. Schneiers Ausführungen beziehen sich auf einen im

August 2007 von Dan Shumow and Niels Ferguson, zwei bei *Microsoft* angestellten Kryptographen, gehaltenen Vortrag auf der *Crypto conference* in Santa Barbara. Der kurze Vortrag mit dem Titel *On the Possibility of a Back Door in the NIST SP800-90 Dual Ec Prng*[12] fand in einer informellen *rump session*[13] statt und sorgte für Aufsehen. Ihren Ausführungen zufolge war die Möglichkeit einer mathematischen Backdoor in DUAL_EC_DRBG gegeben (vgl. Bernstein et al. 2015, 8). DUAL_EC_DRBG wurde 2005 durch das *National Institute of Standards and Technology* (NIST) erstmals publiziert (vgl. ebd., 5) und 2007 durch dasselbe ratifiziert (vgl. Sullivan 2014). Das Akronym löst sich folgendermaßen auf: DRBG bezeichnet einen *Deterministic Random Bit Generator*, also einen deterministischen Algorithmus, der Zufallszahlen erzeugt. DUAL_EC steht dafür, dass die Erzeugung der Zufallszahlen auf elliptischen Kurven (Elliptic Curves) geschieht, und zwar mittels zweier (DUAL) Punkte *P* und *Q*, die beide auf derselben Kurve liegen (vgl. Bernstein et al. 2015, 8). Wer die Konstanten *P* und *Q* erzeugt hat, so Shumow und Ferguson, könne anhand einer Pseudozufallszahl, die durch DUAL_EC_DRBG berechnet wurde, auf die zukünftig folgenden Ergebnisse des Algorithmus schließen (vgl. ebd.). Wie Bernstein, Lange und Niederhagen (ebd.) resümieren: »obviously a security disaster.« Dennoch ließ diese Aussage auch zunächst einige Dinge ungeklärt. Bezugnehmend auf die Ergebnisse von Shumow und Ferguson konstatiert Schneier (2007), es sei trotz der mathematisch bewiesenen Möglichkeit, dass DUAL_EC_DRBG eine Backdoor enthalte, unmöglich, mit Sicherheit zu sagen, ob ein sogenannter »skeleton key«, also ein Generalschlüssel, tatsächlich existiere. Darüber hinaus weist Schneier darauf hin, dass es nicht nur unmöglich sei, mit Sicherheit zu sagen, *ob* jemand im Besitz dieses Generalschlüssels sei, sondern darüber hinaus auch, *wer* ihn besitze – die NSA, NIST oder ein_e andere_r Akteur_in? Und obwohl es darüber hinaus technisch möglich sei, DUAL_EC_DRBG so zu implementieren, dass die bekannte Backdoor ausgeschlossen werde, plädiert Schneier (ebd.) dafür, »[to] not […] use Dual_EC_DRBG under any circumstances.« Nach einer kurzen Abwägung verschiedener Details des Falles schreibt Schneier (ebd.) weiter: »If this story

12 Das Akronym PRNG bezeichnet einen *Pseudo Random Number Generator* – also einen Algorithmus zur Generierung von Pseudozufallszahlen. PRNG und DRBG werden im vorliegenden Fall oft synonym verwendet, wobei DRBG etwas spezifischer ist als PRNG.

13 *Rump sessions* oder auch *lightning talks* sind ein beliebter Teil technisch-mathematischer Konferenzen und zeichnen sich durch ihren prägnanten (oft haben die Vortragenden nur wenige Minuten Zeit) und informellen Charakter aus.

leaves you confused, join the club.« Dieser Verwirrung wird im Folgenden auf den Grund gegangen, denn mittlerweile ist der Fall DUAL_EC_DRBG von Daniel Bernstein, Tanja Lange und Ruben Niederhagen, auf deren Ergebnisse ich mich in diesem Unterkapitel maßgeblich beziehen werde, ausführlich aufgearbeitet worden.

Sicherheit und Zufall

Wie kommt eigentlich Verschlüsselung in Software? In der Regel entwickeln Kryptograph_innen Verschlüsselungsverfahren in der Form von Algorithmen, die auf derzeit schwer oder nicht lösbaren mathematischen Problemen basieren. Softwareentwickler_innen implementieren diese Algorithmen dann in Kryptographie-Bibliotheken[14] (englisch: cryptography libraries), um die bis dahin nicht anwendungsbezogene Mathematik[15] in eine Art Software-Baustein auf dem Weg zur Einbindung in spezifische Anwendungen zu verwandeln. Wieder andere Softwareentwickler_innen bauen dann diese Bibliotheken in ihre Programme ein (vgl. Bernstein et al. 2015, 3–4). DUAL_EC_DRBG ist ein solches, in der Kryptographie-Bibliothek *BSAFE* der Firma *RSA Security* enthaltenes, kryptographisches Modul.

Zeitgenössische Kryptographie beruht, wie bereits in Kapitel 2 ausführlich dargestellt, auf dem *Kerckhoffs'schen Prinzip*, das (stark verkürzt) besagt, dass die Sicherheit eines kryptographischen Verfahrens allein von dem verwendeten Schlüssel abhängen dürfe, und dass alle weiteren Komponenten des Verschlüsselungsvorgangs bekannt sein können müssen. Die Wahl eines guten Schlüssels ist daher umso wichtiger – denn wer den Schlüssel kennt oder erraten kann, kann auch die Verschlüsselung brechen. In digitalen Medien muss aus diesem Grund auch der Art, wie ein Schlüssel erzeugt wird, besondere Aufmerksamkeit geschenkt werden. An diesem Punkt kommt der

14 Bekannte Bibliotheken sind u.a. *OpenSSL*; *BSAFE* von *RSA Security* oder *SChannel* von Microsoft.

15 In Gesprächen mit dem Kryptographen Benedikt Auerbach machte dieser mir klar, dass die Aufgabe von Kryptograph_innen oftmals darin besteht, mathematische Verfahren zu entwickeln, die keinerlei Bezug zu Fragen der Implementierung haben. Diese sei ein nachgelagertes Problem, das andere Fachbereiche betreffe. Aus einer um Nachhaltigkeit bemühten Perspektive ergibt dies durchaus Sinn: Software verändert sich stetig, und würden Verschlüsselungsverfahren speziell auf bestimmte Anwendungsfälle zugeschnitten werden, wäre an Langlebigkeit nicht zu denken. Darüber hinaus erleichtert eine solche strikte Aufteilung der Zuständigkeiten, also eine Modularisierung verschiedener Teile derselben Software, die Fehlersuche.

Zufall ins Spiel: Computer verwenden Random Bit Generators (auch als Random Number Generators bezeichnet), um eine lange, zufällige Zahlenreihe zu erzeugen, die dann beispielsweise zur Schlüssel- oder Passwortgenerierung verwendet wird. Die Form des Zufalls, die hier gefordert ist, ist nicht derselbe Zufall, den man beispielsweise mit dem einmaligen Werfen eines sechsseitigen Würfels verbindet: Statistisch gesehen sind die Häufigkeiten gewürfelter Zahlen vorhersagbar, und jede stochastisch berechenbare Zufälligkeit wäre nachteilig für ein kryptographisches System, dessen komplette Sicherheit von dieser einen Komponente abhängt (vgl. Cloudflare o.J.a). Gesucht wird also eine Sorte nicht mittels Wahrscheinlichkeitsberechnung kalkulierbaren Zufalls, der als »true randomness« (Bernstein et al. 2015, 3) bezeichnet wird. Solche nicht vorhersagbaren Zufallszahlen sind in logikbasierten rechnenden Umgebungen schwer zu finden, daher wird das bisschen »true randomness« (ebd.), das in einem Computer gefunden werden kann,[16] mittels eines Algorithmus, der als Pseudozufallszahlengenerator bezeichnet wird, ›gestreckt‹. Dieser Algorithmus ist insofern deterministisch, als alle Ergebnisse des Pseudozufallszahlengenerators berechnet werden können, wenn der tatsächlich zufällige Input bekannt ist (vgl. ebd.). Daher wird der tatsächlich zufällige Input, auch als *seed* bezeichnet, stets geheim gehalten. Um aus Ergebnissen des Pseudozufallszahlengenerators keine Rückschlüsse auf den *seed* ziehen zu können, entspricht der Algorithmus des Pseudozufallszahlengenerators einer Einwegfunktion (vgl. Sullivan 2014). Im Fall von DUAL_EC_DRBG erfolgt die Berechnung von Pseudozufallszahlen auf sogenannten *elliptischen Kurven*. Diese verfügen über die mathematische Besonderheit, dass zwei beliebige Punkte *P* und *Q* auf einer gegebenen Kurve miteinander addiert einen Wert ergeben, der ebenfalls auf der Kurve liegt. Dies erlaubt es, die Multiplikation eines Punktes *P* mit einer ganzen Zahl *Z* als eine *Z*-fache Addition des Punk-

16 *True randomness* bei Computern wird oft durch die Eingaben von User_innen erzeugt, bspw. durch Bewegungen der Maus oder durch Tastatureingaben. Doch auch andere Dinge außerhalb des Computers können zu tatsächlichen Zufallszahlen werden: Die Firma *Cloudflare* verwendet eine Wand aus ca. 100 Lavalampen, da die Formen, die das Wachs in ihnen annimmt, nicht vorhersagbar sind. In regelmäßigen Abständen wird ein Foto von der Wand gemacht. Da digitale Fotos auch als Zahlenkolonnen ausgegeben werden können, entspricht jedes Bild einer tatsächlich zufälligen Zahlenreihe (vgl. Cloudflare o.J.a).

tes *P* mit sich selbst zu definieren.[17] Diese Multiplikation lässt sich schnell berechnen, ist allerdings auch eine Kandidatin für eine Einwegfunktion – ihre Umkehrung in Polynomialzeit berechnen zu können würde bedeuten, dass das diskrete Logarithmusproblem auf elliptischen Kurven gelöst worden wäre (vgl. ebd.). Die in DUAL_EC_DRBG mathematisch beweisbare Backdoor hängt mit genau dieser Einwegfunktion zusammen, und den zuvor erwähnten zwei Punkten *P* und *Q*, die beide auf derselben elliptischen Kurve liegen, und als Konstanten in die Berechnung von Pseudozufallszahlen eingehen, indem sie mit einem *seed* jeweils in eine Einwegfunktion eingesetzt werden. Die Backdoor in DUAL_EC_DRBG besteht darin, dass, wer die Beziehung der Konstanten *P* und *Q* zueinander kennt, oder genauer: wer weiß, wie *P* aus der Multiplikation von *Q* gewonnen werden kann, in der Lage ist, von einer durch DUAL_EC_DRBG erzeugten Zahl aus alle weiteren Pseudozufallszahlen, die DUAL_EC_DRBG produzieren wird, zu errechnen (vgl. Bernstein et al. 2015, 8, 12). Dem Framework von Thomas und Francillon folgend, besteht zu diesem Zeitpunkt der Analyse eine *deniable backdoor*: Shumows und Fergusons Überlegungen wurden anhand der AFSM angestellt, und die EFSM enthielt selbstverständlich keine Backdoor, denn immerhin wurde DUAL_EC_DRBG vom *National Institute of Standards and Technology* veröffentlicht und ratifiziert. Mathematisch nachweisbar ist, dass es möglich wäre, anhand der Kenntnis der Beziehung der Konstanten *P* und *Q* zueinander mittels eines einzigen Outputs aus DUAL_EC_DRBG alle weiteren Outputs zu berechnen. Es ist jedoch nicht zwingend notwendig, *P* und *Q* auf eine Weise zu erzeugen, die eine Backdoor generieren würde. Unklar ist also, ob diese mathematische Backdoor in der DFSM vorhanden ist, also ob die Entwickler_innen von DUAL_EC_DRBG tatsächlich über diesen Generalschlüssel verfügen.

Tatsächlich eine *deniable backdoor*?

Shumow und Ferguson waren sehr darum bemüht, ihrem Fund keine Intentionalität zu unterstellen. Entsprechend liest sich die vorletzte Folie ihrer Präsentation:

> »WHAT WE ARE NOT SAYING: NIST intentionally put a back door in this PRNG

17 P+P+P=Q entspricht 3xP=Q. Es handelt sich hier um das mathematische Verfahren der sog. Gruppenoperation, das aus Gründen der Verständlichkeit entweder als Addition oder Multiplikation beschrieben werden kann.

> WHAT WE ARE SAYING: The prediction resistance of this PRNG (as presented in NIST SP800-90) is dependent on solving one instance of the elliptic curve discrete log problem. (And we do not know if the algorithm designer knew this before hand [sic!].)« (Shumow/Ferguson 2007)

Thomas und Francillon (2018, 106) verweisen in ihrer Definition einer *deniable backdoor* darauf, dass im Fall einer technisch nicht nachweisbaren Backdoor in der DFSM stattdessen »from a non-technical perspective«, also aus einer Betrachtung politischer Zusammenhänge, einer Entität eine Intentionalität unterstellt werden könne. Aus heutiger Perspektive hätten Shumow und Ferguson guten Gewissens eine Intentionalität unterstellen können, allerdings nicht NIST, sondern der NSA: In dem 2006 von NIST veröffentlichten Dokument namens SP 800–90 für DUAL_EC_DRBG werden keine Erfinder_innen des Pseudozufallszahlengenerators benannt (vgl. Bernstein et al. 2015, 6). Als die Autor_innen des Dokuments, Elaine Barker und John Kelsey, eine Anfrage bezüglich eines möglichen Kommentars zu DUAL_EC_DRBG erhielten, leitete Elaine Barker diese Mail an Mitarbeiter_innen der NSA weiter, mit dem Hinweis, dass diese die Frage beantworten könnten (vgl. ebd.), woraus deutlich hervorgeht, dass die NSA für die Entwicklung von DUAL_EC_DRBG verantwortlich ist. Aus einem 2014 veröffentlichten Mailwechsel zwischen John Kelsey (NIST) und Don Johnson (NSA) aus dem Jahr 2004, in dem Kelsey nach dem Ursprung der Konstanten *P* und *Q* fragt, ist weiterhin ersichtlich, »that NSA had ›generated (*P, Q*) in a secure, classified way‹ […] and that it ›would be reasonable to allow other users to generate their own (*P, Q*)‹.« (Ebd., 9) In einem Appendix zu SP 800–90 riet NIST jedoch explizit davon ab, eigene Konstanten zu erzeugen, um die Integrität der Verschlüsselung nicht mit unter Umständen falsch gewählten Konstanten zu beschädigen (vgl. ebd.). Bernstein, Lange und Niederhagen (ebd., 10) resümieren: »In hindsight it is quite amazing how blindly NIST trusted NSA.« Doch damit noch nicht genug. Anfang 2005 brachte die kanadische Firma *Certicom* zwei Patente auf den Weg: eines für die Verwendung der DUAL_EC_DRBG-Backdoor für *key escrow*,[18] und eines für eine

18 Unter *key escrow* versteht man das Hinterlegen eines Schlüssels für ein Kryptosystem bei einer Regierung oder einem Geheimdienst etc. Bernstein et al. (2015, 20) bezeichnen dies als »deliberate back door«. Bei *key escrow* besteht jedoch immer die Gefahr des Missbrauchs des hinterlegten Schlüssels. Eine mögliche Lösung für dieses Problem kommt vom David Chaum. Das von ihm vorgestellte System »Privategrity« beinhaltet ein *key escrow*-Verfahren, bei dem der Schlüssel, mit dem eine Kommunikation entschlüsselt werden kann, in neun Teile gesplittet wird und jedes Teil in einem anderen

Modifikation von DUAL_EC_DRBG, die *key escrow* unmöglich macht (vgl. ebd., 20). Anhand dieser beiden Patente lässt sich belegen, dass *Certicom* bereits im Jahr 2005 von der Backdoor im DUAL_EC_DRBG wusste, und die NSA spätestens im April 2005 ebenfalls über die Backdoor informiert war (vgl. ebd.). Darüber hinaus waren die Unterlagen für die Patentierung inklusive Beispiele für den Exploit von DUAL_EC_DRBG im Juli 2006 im Internet auffindbar – und das nur einen Monat nach der Standardisierung von DUAL_EC_DRBG als SP 800–90 durch NIST (vgl. ebd.). Darum bemüht, Aufsehen ob dieser Patente und der Backdoor in DUAL_EC_DRBG zu vermeiden, listete auch *Certicom* zwei Namen vermutlich unbeteiligter Personen als Erfinder der Patente.

Tatsächlich sollte es noch bis kurz nach den Snowden-Enthüllungen dauern, bis die Standardisierung und Verwendung von DUAL_EC_DRBG international größeres Aufsehen erregte. Aus einem Bericht vom 06.09.2013 in der Zeitung *The Guardian*, die über mehrere Artikel hinweg die von Edward Snowden bereitgestellten Dokumente journalistisch aufarbeitete, geht hervor, dass die NSA gemeinsam mit dem britischen Geheimdienst GCHQ seit einigen Jahren systematisch an einer Schwächung kryptographischer Systeme arbeitete, um abgefangenen Traffic entschlüsseln und mitlesen zu können. Das entsprechende Projekt trägt den Titel *Bullrun* (das britische Äquivalent trägt den Namen *Edgehill*) und ist Teil des SIGINT-Programms (vgl. Ball et al. 2013), das dem offensiven Teil der NSA zugeordnet ist. Das Ziel von SIGINT wird in internen Dokumenten der NSA folgendermaßen beschrieben:

> »The SIGINT Enabling Project actively engages the US and foreign IT industries to covertly influence and/or overtly leverage their commercial products' designs. These design changes make the systems in question exploitable through SIGINT collection (e.g., Endpoint, MidPoint etc.) with foreknowledge of the modification. To the consumer and other adversaries, however, the systems' security remains intact.« (National Security Agency 2012, 115)

Land liegt (vgl. Greenberg 2016). Nur wenn alle Schlüsselparteien von der Notwendigkeit einer Entschlüsselung überzeugt sind, fügen sie ihre Teile zu dem vollständigen Schlüssel zusammen und entschlüsseln die Kommunikation. Auf diese Weise möchte Chaum einen leichtfertigen Gebrauch des Master-Schlüssels verhindern, aber gleichzeitig Regierungen die Möglichkeit geben, Terrorismus zu bekämpfen (vgl. ebd.) – ein scheinbar ausgewogener Kompromiss aus Privacy und Security.

Anhand dieser Absichtserklärung lässt sich erneut die von Thomas und Francillon vorgenommene Differenzierung der Nachweisbarkeit von Backdoors in DFSM und EFSM beobachten: die Backdoors sollen, wenn möglich, nur in der DFSM enthalten, und im besten Fall auch dort nicht explizit nachweisbar sein. Ball, Borger und Greenwald (2013) weisen darauf hin, dass *Bullrun* explizit darauf abzielt, »to ›insert vulnerabilities into commercial encryption systems‹.« In den Dokumenten werden zwar keine Firmen explizit benannt (vgl. Menn 2013), jedoch ist durch eine Meldung der Nachrichtenagentur Reuters nur wenige Monate nach Bekanntwerden von *Bullrun* ersichtlich, dass die NSA 10 Millionen US-Dollar an die Firma *RSA Security* zahlte, um DUAL_EC_DRBG zum standardmäßig voreingestellten Pseudozufallszahlengenerator in *RSAs* Kryptographie-Bibliothek *BSAFE* zu machen (vgl. Ars Staff 2013; Menn 2013; Sullivan 2014).[19] Bernstein, Lange und Niederhagen (2015, 2) bemerken dazu: »The surprise for the public cryptographic community was not so much this confirmation of what had already been suspected, but rather that NSA's backdooring of Dual EC was part of an organized approach to weakening cryptographic standards.« Auf ein Element der Politiken dieses organisierten Vorgehens wird im folgenden Abschnitt eingegangen.

»NOBUS«

»You look at a vulnerability through a different lens if even with the vulnerability it requires substantial computational power or substantial other attributes and you have to make the judgment who else can do this?«, sagte Michael Hayden, ein ehemaliger Direktor der NSA, auf dem *Washington Post Cybersecurity Summit* im Oktober 2013, rund einen Monat nachdem im *Guardian* über *Bullrun* berichtet wurde. Er führte weiter aus:

> »If there's a vulnerability here that weakens encryption but you still need four acres of Cray computers[20] in the basement in order to work it you kind of think »NOBUS« and that's a vulnerability we are not ethically or legally compelled to try to patch – it's one that ethically and legally we could try to

19 Dies bedeutet zwar nicht, dass irgendjemand zu dessen Verwendung verpflichtet wäre – Softwareentwickler_innen, die sich nicht mit Kryptographie auskennen, würden aber vermutlich den ihnen vorgeschlagenen Standard verwenden, da sie keine informiertere Entscheidung treffen können. Genau diese Kompetenz sollte ihnen durch die Existenz von Kryptographie-Bibliotheken immerhin abgenommen werden.

20 »Cray computers« ist eine Bezeichnung für Supercomputer, die auf den Markennamen des bekanntesten Herstellers derselben verweist.

exploit in order to keep Americans safe from others.« (Hayden in Peterson 2013)

Die Abkürzung »NOBUS« steht für »nobody but us« und bezieht sich in Haydens Statement konkret auf die monetären und rechnerischen Ressourcen der NSA im Vergleich zu denen anderer Akteur_innen. Diese Einschätzung kann als eine Auslegung von David Kahns (1967, 753) Aussage verstanden werden, das Verhältnis von Kryptographie zu Kryptanalyse sei maßgeblich von Zeit geprägt: Mit dem Zusammenwachsen von Kryptologie und Informatik treten Rechenleistung und monetäre Ressourcen in eine Wechselbeziehung zu verfügbarer Zeit. Die NSA-interne Klassifizierung von Sicherheitslücken gelte, so fügt Hayden erläuternd hinzu, sowohl für bereits existierende, aus zufälligen Fehlern entstandene, absichtlich implementierte oder nachträglich zu Überwachungszwecken eingesetzte Sicherheitslücken (vgl. Peterson 2013). Doch bei DUAL_EC_DRBG handelt es sich um einen Sonderfall, bei dem sich Kryptographie und Kryptanalyse nicht im konventionellen Sinne gegenüberstehen: Der erste Schritt besteht, Adam Young und Moti Yung (1997) folgend, in »Using Cryptography Against Cryptography«. Diese Tagline ist ein Teil des Titels von Youngs und Yungs Paper über *Kleptographie*. Kleptographie definieren Young und Yung (ebd., 63) als »the ›study of stealing information securely and subliminally‹«,[21] und exemplifizieren: »The kleptographic attacker can steal the secrets securely, and in an exclusive and subliminal manner.« Während Youngs und Yungs Konzept der Kryptovirologie, wie in Kapitel 3 bereits besprochen wurde, die Möglichkeit beschreibt, mittels Verschlüsselung einen Angriff auszuführen, bei dem den Angegriffenen Zugang versperrt und Daten vor ihren Besitzer_innen erpresserisch zurückgehalten werden können, beschreibt Kleptographie die Möglichkeit, Kryptographie gegen sich selbst zu wenden, sodass eine verwendete Verschlüsselung für alle außer der kleptographisch operierenden Entität sicher und vertrauenswürdig erscheint. Bezugnehmend auf eine ihrer früheren Arbeiten beschreiben Young und Yung dies anhand eines mit dem Akronym SETUP benannten Algorithmus. SETUP steht für »Secretly Embedded Trapdoor with Universal Protection«, und ein solcher Algorithmus »can be embedded within a cryptosystem to leak encrypted secret key information to the attacker in the output of that cryptosystem.« (Ebd., 64) Der SETUP-Algorithmus wird als einem

21 Bei Kleptographie lassen sich durchaus Anklänge an steganographische Verfahren bemerken.

gegebenen kryptographischen System zugehörig beschrieben, es erfolgt also weder ein Angriff durch ein Außen, noch muss eine zusätzliche (und ansonsten verräterisch überflüssige) Komponente in ein *system* integriert werden, die die zu schützenden Informationen preisgibt. Es ist also die Implementierung von SETUP selbst, die »in conjunction with the internal cryptographic tools, *generates* opportunities for leaking information.« (Ebd., 63, Herv. i.O.) Dies führt zu einer Situation, in der, ähnlich wie bei DUAL_EC_DRBG, nur die Entität, die die Beziehung der Konstanten *P* und *Q* zueinander kennt, den Output des Pseudozufallszahlengenerators entschlüsseln und zukünftige Kombinationen berechnen kann. Im Fall einer kleptographischen Backdoor kann also nur die Entität, die SETUP implementiert hat, auch etwas mit den geleakten Informationen anfangen, da diese verschlüsselt sind. Mehr noch: Nur die Entität, die SETUP implementiert hat, weiß überhaupt, dass ein *system* Informationen preisgibt. Basierend auf diesem Konzept lässt sich die *deniable Backdoor* in DUAL_EC_DRBG durch das Vorgehen der NSA als *kleptographische* Backdoor einstufen. Die Backdoor in DUAL_EC_DRBG ermöglicht es der NSA also, Daten »in an exclusive and subliminal manner« zu stehlen, da sie – in Schneiers (2007) Worten – den »skeleton key« besitzen, diese Sicherheitslücke aber für andere Akteur_innen aufgrund des diskreten Logarithmusproblems auf elliptischen Kurven nicht ausnutzbar ist. Ob dies auch »securely« geschieht, ist vom Blickwinkel abhängig: Da kein_e NSA-Agent_in sich dafür in eine physisch gefährliche Situation begeben muss, und die Daten für alle nicht eingeweihten Akteur_innen weiterhin verschlüsselt sind, könnte man davon ausgehen, dass die NOBUS-Politik der NSA in kleptographischen Backdoors ihr volles Potential entfaltet, und maximale Überwachung bei maximaler Sicherheit gewährleistet. Diese Auffassung lässt sich angesichts rezenter Cyberangriffe wie *WannaCry* allerdings auch als schlichtweg falsch beschreiben: Die Sicherheitslücke *EternalBlue* in *Windows*' SMB-Protokoll war der NSA zum Zeitpunkt von *WannaCry* bereits seit einigen Jahren bekannt, wurde jedoch im Zuge der NOBUS-Einschätzung nicht publik gemacht, um sie weiter ausnutzen zu können. Auf diese Weise konnte die NSA zwar über einige Jahre hinweg operieren, aber schlussendlich schadete diese Sicherheitslücke, als sie durch die *Shadow Brokers* im Internet veröffentlich wurde, auch den Vereinigten Staaten massiv – der von Hayden formulierte Anspruch »to keep *Americans* safe from others« (Peterson 2013, Herv. MS) wurde also in letzter Konsequenz nicht eingelöst. Ein ähnliches Schicksal könnte auch eine kleptographische Backdoor treffen: Würde der geheime Schlüssel, mit dem *Q* generiert wurde (vgl. Bernstein et al. 2015,

8–9), gestohlen und veröffentlicht werden, würde die Backdoor nicht mehr exklusiv der NSA zur Verfügung stehen. Einmal veröffentlicht, wäre die Ausgabe jeder einzelnen DUAL_EC_DRBG-Instanz mit den Standardwerten für *P* und *Q* vorhersagbar (vgl. Schneier 2007).

Die absichtliche Schwächung kryptographischer Infrastrukturen durch aktives Eingreifen oder durch gezielte Passivität ist jedoch kein neues Phänomen. Bruce Schneier (2018) legt in *Click here to kill everybody* dar, dass bereits seit den 1990er Jahren immer wieder Verschlüsselung von verschiedenen geheimdienstlichen Organisationen als unüberwindbare Hürde zur Verfolgung krimineller Akteur_innen diskursiviert wurde. Die wiederholt zur Rechtfertigung solcher Forderungen vorgebrachten Akteur_innen »terrorists, drug dealers, pedophiles, and organized crime« bezeichnet Schneier (ebd.) aufgrund des repetitiven Diskurses scherzhaft als die »Four Horsemen of the Internet Apocalypse«. Er plädiert, wie viele andere Wissenschaftler_innen aus den Bereichen IT-Sicherheit und Kryptographie, sowie FLOSS[22]-Aktivist_innen, für kompetentere Ermittlungsstrategien statt der Ausweitung technologischer Kompetenzen der Geheimdienste. Denn, so Schneiers (ebd.) Argument:

> »While in theory it would be great […] there's no way to design this securely. It's impossible to build a backdoor mechanism that only works in the presence of a legal warrant, or when a law enforcement officer tries to use it for legitimate purposes. Either the backdoor works for everyone or it doesn't work for anyone.«

4.2 Von Türen, Hintertüren und Schlüsseln

Nachdem im vorangegangenen Unterkapitel zwei Arten von Backdoors, sowie ein informatisches Framework für die Bestimmung von Backdoors besprochen wurden, wird im Folgenden auf die in dem Begriff »Backdoor« als Metapher enthaltene Tür eingegangen. In Kapitel 3 wurde IT-Sicherheit vor allem in Bezug auf Sicherheit vor Schadsoftware besprochen, doch die Herstellung von Sicherheit bei Computern verfügt noch über einen weiteren

22 Das Akronym FLOSS steht für Free, Libre and Open Source Software und fasst so unterschiedlich lizensierte Software, deren Quellcode in jedem Fall frei einsehbar ist, zusammen.

Bereich. Wie Parikka (2016, 3) ausführt, basieren »security and computer protection […] on *control*, *inspection*, and *integrity*.« Während *inspection* und *integrity* mit dem Auffinden von Schadsoftware und unautorisierten Veränderungen innerhalb eines Computers befasst sind, kommt *control* eine umfassendere Rolle zu: »As the key concept of computer security, it has meant controlling access to systems, as well as functions, resources, and the moving and sharing of data.« (Ebd.) Das offensichtlichste Beispiel für die Herstellung von Sicherheit durch *control* ist an *access control*, also Zugangs- oder Zugriffskontrolle orientiert: Bei der Verwendung eines Computers ist der_die User_in in den meisten Fällen mit Lese- und Schreibrechten für die meisten Dateien auf der Festplatte ausgestattet. Um alle Dateien, darunter auch die, die die Programme und Funktionen des Computers ausmachen, lesen und bearbeiten zu dürfen, wird in der Regel ein Passwort abgefragt. Dies soll verhindern, dass aus Versehen oder von unbefugten Personen oder Programmen Änderungen am System vorgenommen werden und dieses dadurch in einen Zustand veränderter oder reduzierter Funktionalität versetzt wird, oder dass jemand unrechtmäßigen Zugang zu Informationen erlangt. Bei den Betriebssystemen *Microsoft Windows*, *MacOS* und *Ubuntu* ist dies das Passwort, das der_die User_in auch verwendet, um sich in seinem_ihrem Account anzumelden: Der_die User_in muss nachweisen, dass er_sie autorisiert ist, Änderungen an bestimmten Dateien vorzunehmen.[23] Die Abfrage eines Passworts vor dem *Betreten* eines bestimmten Bereichs ist ein Vorgang der Authentifizierung: Das Passwort fungiert also wie eine Losung, wie ein *Schlüssel*, wie ein geteiltes *Geheimnis* zwischen User_in und Computer, mit dem eine Person nachweisen kann, dass sie wirklich über die Berechtigung verfügt, einen abgegrenzten Bereich zu betreten, dort Dokumente anzusehen und zu bearbeiten. Bei Sicherheit als Zugangskontrolle funktioniert die Frage nach dem Passwort wie eine *Tür*, das Passwort wie der dazugehörige *Schlüssel*: Der Authentifizierungsmechanismus steht wie eine Tür zwischen zwei Bereichen, gewährt bei korrekten Eingaben den Übertritt in einen geheimen oder privaten Bereich, und bringt diesen, ebenso wie ihr öffentlicheres Gegenstück gleichsam durch die Grenzziehung erst hervor.

23 Das Betriebssystem *Debian* hingegen verlangt standardmäßig ein anderes Passwort als das des_der User_in, und differenziert auch explizit zwischen *user* und *root user*, wobei Root-User_innen Lese- und Schreibberechtigungen für alle Bereiche des Computers haben.

Türen und Hintertüren

In seinem Aufsatz *Türen. Zur Materialität des Symbolischen* widmet sich Bernhard Siegert (2010) aus kulturtechnischer Perspektive den Beziehungen zwischen Menschen und Türen als Objekten des Alltags. Die vorliegende Publikation hat sich bereits methodisch gegen eine kulturtechnische Herangehensweise positioniert, dennoch lässt sich Siegerts Text an dieser Stelle für die Analyse von Backdoors produktiv machen. Siegert legt anhand von unterschiedlichen Türsorten eine Art Motivgeschichte der Tür vor: Glastüren, Drehtüren und Schiebetüren, sowie die *Porte de Duchamp*[24] werden bedacht, lediglich Hintertüren erwähnt er leider nicht. »Türen«, so schreibt Siegert (ebd., 153–154), seien »Operatoren symbolischer, epistemischer und sozialer Prozesse, die mithilfe der Differenz zwischen innen und außen Rechtssphären, Geheimnissphären und Privatsphären generieren, wodurch sie den Raum so artikulieren, dass er zum Träger kultureller Codes wird.« Diese Definition versteht Türen als Elemente der Differenzgenerierung. Angesichts der im vorangegangenen Kapitel herausgearbeiteten immunologischen Struktur des IT-Sicherheitsdiskurses scheint sich die Metapher der Tür damit zunächst nur allzu passend als eine weitere Spielart der »frontier-based concepts« (Taylor 2001, 38) neben Metaphern der Landnahme und des Immunsystems begreifen zu lassen. Dieser Eindruck mag jedoch täuschen: Obwohl Siegert sich nur in stark verkürzter und nahezu naiver Weise über Türen digitaler Medien äußert,[25] schwingt jedoch ein Prinzip des Digitalen in seinen Betrachtungen mit: die Binarität. Dies ist beispielsweise dort erkennbar, wo er zu der Tür Duchamps schreibt: »Die Tür als digitales Medium bezieht sich auf die Passage von Körpern.« (Siegert 2010, 160) Nun ließe sich argumentieren, dass die Tür Duchamps ohnehin mit Binarität befasst, und Siegerts Analyse daher äußert treffend sei. Doch auch an anderer Stelle orientiert er sich an naturwissenschaftlichem Wissen, und überträgt dieses auf die Betrachtung von Türen aus Holz, beispielsweise in seiner Betrachtung eines Auszugs aus

24 Die *Porte de Duchamp* ist ein Entwurf des Künstlers Marcel Duchamp, die mit drei Räumen operiert, von denen sie stets zwei miteinander verbindet und einen dritten schließt (vgl. Siegert 2010, 158–159).

25 Siegerts (2010, 165) Behauptung, dass »in den virtuellen Architekturen des Cyberspace, des Internet […] die Differenz von innen und außen dekonstruiert und permanent aufgeschoben« würde, muss als das Festhalten an einer nicht eingelösten Utopie des Internets eingestuft werden. Die vorliegende Publikation sollte – neben zahllosen weiteren – mittlerweile mehr als deutlich gemacht haben, dass die Differenz von Innen und Außen gerade in digitalen Kulturen bis heute grundlegend ist.

Robert Musils Geschichte *Türen und Tore*. In dem von ihm zitierten Ausschnitt Musils schreibt dieser über die Rolle von Türen für die un/gleiche Verteilung von Wissen, die in neueren Häusern nicht mehr gegeben sei, da die Wände dieser so dünn seien, dass man nicht mehr an der Tür zu lauschen brauche – man könne bereits alles durch die Wände hören (vgl. ebd., 163). Siegert (ebd.) hält jedoch an der Rolle der Tür als Differenz generierend fest, wenn er schreibt:

> »So lange Türen ihre Rolle spielten als Operatoren der Differenz zwischen innen und außen schufen sie auch – mithilfe der Differenz zwischen öffentlich und privat – eine Asymmetrie im Wissen. Türen produzieren ein Informationsgefälle. Sie spielen daher eine unverzichtbare Rolle in der Produktion thermodynamischen bzw. informationstheoretischen Wissens. […] Solange Türen ihre informatische Funktion erfüllen, halten sie ein Energie- bzw. Wissensungleichgewicht aufrecht, das ein Anwachsen der Entropie im Gesamtsystem nahezu unvermeidlich macht. Auf diese Weise dienen Türen der Wissenszirkulation […].«

Die Tür kann, wenn sie, wie hier bei Siegert, digital und damit binär gedacht wird, entweder geöffnet oder geschlossen sein, eine halboffene Tür kann es nicht geben. Damit erweist sich die Tür mehr als eine Verabsolutierung von Differenz denn als eine aushandelnde Differenzgenerierung, die im Gegensatz zum Immunsystem nicht die Logik der Steigerung, sondern die der Binarität verkörpert. In der Übertragung der Tür als Metapher für informatische Formen der Regulierung von Informationsaustausch, so lässt sich anhand von Siegert feststellen, büßt die Tür die Möglichkeit ein, angelehnt zu werden, nur halb geschlossen zu sein, und wird zu einer binären Unterscheidungsmaschine, die entweder geöffnet oder geschlossen ist, Zutritt gewährt oder verweigert. So schreibt auch Bruno Latour (1996, 69) in *Ein Türschließer streikt*: »Im Jargon der Informatik: Eine Tür ist ein ausschließendes ODER, niemals ein UND«. Dies gilt bei Computern für Türen in Hardware (sog. Gates, dt.: Gatter) und in Software. Was passiert aber mit der Binarität, wenn es nicht nur eine Tür gibt? An dieser Stelle kommt die Hintertür ins Spiel, denn mit einer Reihe von Türen lassen sich, um zunächst in einer technischen Beschreibungsweise zu bleiben, differenziertere Schaltungen erzeugen, ähnlich einem gemischten Stromkreis, der aus Reihen- und Parallelschaltungen konstruiert ist. ›Türen‹ bei Computern erzeugen Ein- und Ausschlüsse binärer Art, die von heimlich angebrachten weiteren Türen störend erweitert werden können. So wirken beispielsweise kleptographische Backdoors an der Aufrechterhaltung

der grundsätzlichen Struktur des Informationsgefälles dadurch mit, dass sie einen Zugang zu einem geschützten Bereich ermöglichen, und diesen Zugang wiederum selbst mittels kryptographischer Verfahren schützen – dennoch verändern sie das Informationsgefälle zugunsten der User_innen, die durch die Backdoor gewissermaßen ›eintreten‹. So bringen Backdoors die vorgegebene Unterscheidung von Innen und Außen in Gefahr, weil sie eine zweite Eintrittspforte schaffen, wo nur eine sein sollte. An der Binarität der Tür-Metapher in der Informatik ändert dies allerdings nichts.

Schlüssel und Geheimnis

Zu den Türen und Hintertüren gehört, wie eingangs erwähnt, auch stets ein *Schlüssel*, das heißt, ein Passwort, ein *Geheimnis*. Das Geheimnis, oder vielmehr, das Verraten eines Geheimnisses, hat vor allem in den letzten Jahren durch zahllose Whistleblower_innen und Enthüllungen eine prominente Position in digitalen Kulturen eingenommen. Timon Beyes und Claus Pias (2014, 111) weisen in ihrem Aufsatz *Transparenz und Geheimnis* darauf hin, dass es unter den gegebenen Umständen sinniger sei, digitale Kulturen »nicht, oder nicht primär, in Potential und Problematik der Transparenz (und korrespondierender Leitbegriffe wie Partizipation und Öffentlichkeit) zu denken, sondern im Zeichen des Geheimen, der fundamentalen Intransparenz und des Arkanums.« Die Autoren führen die privilegierte Stellung des Geheimnisses auf die Vormachtstellung der modernen Kybernetik seit 1945 zurück, die eine neue Form von Zeitlichkeit etabliert habe (vgl. ebd., 114), die durch die fortschreitende Digitalisierung unserer Lebenswelt zur Normalität geworden sei. Sie fassen Algorithmen, die als *black box* operieren, als Kennzeichnungsmerkmal dieser neuen Zeitordnung, die die Zukunft nicht mehr offenhalte, sondern schließe – als Paradigmenwechsel führen sie anhand der Klimaforschung an, nicht mehr die Natur sei das Geheimnis, das es zu entschlüsseln gelte, sondern die Datenverarbeitung (vgl. ebd., 116). In einer Umkehrbewegung rücken Beyes und Pias (vgl. ebd., 112) mit Bezug auf Eva Horn anstelle von Transparenz Partizipation und Öffentlichkeit in den Vordergrund:

> »Die Frage ist nicht, was geheim gehalten wird, sondern was überhaupt verraten werden kann, und was – indem es zum Objekt des Verrats werden kann oder nicht – den Stellenwert und die Logik des Geheimnisses in verschiedenen Kulturen und zu verschiedenen Zeiten ausmacht.«

Kryptologie kommt in Beyes' und Pias' Paper nicht vor, dennoch lässt sich basierend auf den bisher erfolgten Überlegungen anmerken, dass nicht nur

die Kybernetik und die durch sie entstandenen Algorithmen für die von Beyes und Pias diagnostizierte Verschiebung verantwortlich zu zeichnen haben. Die Geschichte der Kryptologie, und damit auch die spätestens seit der Entschlüsselung der Enigma mit ihr verknüpfte Geschichte der IT-Sicherheit, drehen sich um die Möglichkeit der Geheimhaltung und damit, in derselben Umkehrbewegung, um die Frage danach, was überhaupt verraten werden kann. Die Verwaltung des Geheimen, die von so vielen Autor_innen als eine Militärgeschichte erzählt wird, da sie eng mit Belangen der Kriegsführung verbunden war, betrifft in nicht unmittelbaren Kriegssituationen vermittelt über Geheimdienste die Relationen von Staaten zueinander, aber auch die von Bürger_innen zu ihren Staaten (vgl. Sprenger 2016). Kryptographie nach dem Kerckhoffs'schen Prinzip lässt sich zugespitzt formuliert als die Verwaltung von Geheimnissen (Plaintext) mittels Geheimnissen (Schlüsseln) beschreiben. Backdoors lassen sich in diesem Sinne als Tropen verstehen, die Teil dieser komplexen Relationen sind, und mit denen der Status des Geheimnisses verändert werden kann, wie anhand von DUAL_EC_DRBG expliziert wurde. Darüber hinaus veruneindeutigt sich das Vokabular selbst an den Stellen, wo die verschiedenen Metaphern, die zur Beschreibung des Phänomens herangezogen werden, sich überlappen: Eine *hard-coded credentials*-Backdoor besteht, wie bereits ausgeführt, darin, dass in einem gegebenen System eine Art General*schlüssel* hinterlegt wird, mit der eine Entität sich immer Zutritt zu diesem verschaffen kann. Die Hinter*tür* kann also auch darin bestehen, ein *Schlüssel* zur Vordertür zu sein. Das nun folgende Unterkapitel widmet sich der sexualisierten Dimension der Backdoor-Metapher, die in den vorherrschenden Diskursen der Informatik übersehenen oder als Ausnahme abgetan wird, und wie diese mit *Gay Theory* ins Sprechen gebracht werden kann.

4.3 ›In through the back door…‹: Mögliche Umdeutungen

In der bereits zitierten aktuellen Online-Ausgabe des *Oxford English Dictionary* wird darauf verwiesen, dass der Eintrag »backdoor« noch nicht für die dritte Ausgabe des OED bearbeitet wurde. Allerdings wird eine weitere Bedeutung als »Draft Addition« aufgeführt: »*slang*. The anus, the rectum« (Oxford English Dictionary 2021). Der erste gelistete Verwendungsnachweis für diesen Wortsinn reicht bis ins Jahr 1613 zurück, zu dem Theaterstück *The Insatiate Countess*

von John Marston.[26] In einer Szene des Stücks unterhalten sich zwei weibliche Nebencharaktere, Thais und Abigail, über ihre zukünftigen Ehemänner. Diese kommen aus zwei verfeindeten Familien und wollen die bestehende Familienfehde selbst in der ›doppelten‹ Hochzeitsnacht aufrechterhalten (beide Paare sollen am selben Tag heiraten). Statt ihre Fehde im Kampf auszutragen, beschließen die Männer allerdings, die Frau des jeweils anderen zu verführen. Thais und Abigail, die befreundet sind, möchten diesen Plan mit ihrem eigenen durchkreuzen: Indem sie die Häuser tauschen, soll in der doppelten Hochzeitsnacht jede von ihnen mit ihrem jeweiligen Ehemann Sex haben. Teil des Gesprächs sind folgende Zeilen:

> »*Abig*. […] The hour for both to come, is six; a dark time, fit for purblind lovers; and with cleanly conveyance by the nigglers our maids, they shall be translated into our bed-chambers: your husband into mine, and mine into your's.
> *Thais*. But, you mean they shall come in at the back-doors.
> *Abig*. Who? our husbands? nay, an they come not in at the fore-doors, there will be no pleasure in't. But, we two will climb over our garden-pales, and come in that way; (the chastest that are in Venice will stray, for a good turn;) and thus wittily will we be bestowed: you into my house, to your husband; and I into your house, to my husband; and, I warrant thee, before a month come to an end, they'll crack louder of this night's lodging than the bedsteads.« (Marston 1820, 31–32)

Abigails Bemerkung, »nay, an they come not in at the fore-doors, there will be no pleasure in't«, lässt sich sowohl auf die Tatsache beziehen, dass die beiden Männer dahingehend getäuscht werden sollen, dass sie durch die Vordertür in das jeweilige Haus eintreten können, um symbolisch die Oberhand behalten zu haben (die Heimlichkeit des Eintretens durch die Hintertür wird hier zugunsten einer offen sichtbaren Dominanzgeste ausgetauscht), als auch darauf, dass Abigail eine pikante Bemerkung darüber macht, dass anale Penetration im Gegensatz zur vaginalen keine Freude bereite. Eine Hintertür findet sich in diesem Dialog also sowohl an Häusern als auch an Körpern – beide werden damit jeweils als geschlossene Systeme konstituiert, mit einer Hülle (Haut/Wände), die das Innere klar von dem Äußeren abgrenzt. Eine ähnliche Mehrdeutigkeit und sexualisierte Zweideutigkeit wird dem Begriff

26 Unter den Verwendungsnachweisen finden sich weiterhin diverse Umgangssprachen-Wörterbücher sowie ein Männer-Lifestylemagazin (vgl. ebd.).

Backdoor auch im *Urban Dictionary*[27] attestiert, beispielsweise in Eintrag Nummer 9, der folgende Erklärungen listet: »1. dishonest 2. the anus 3. a malicious computer program installed to allow access by hackers and other malware«. Der 5. Eintrag präzisiert: »Refers to a person's anus in the context of anal intercourse.« Als Beispielsatz wird dort angegeben: »Sally likes it in the back door.« Auch der folgende Eintrag gibt einen ähnlichen Beispielsatz: »Tom fucked Glenda, up the back door«. In einem weiteren Beitrag wird Backdoor als »smelly brown hole« erläutert und mit dem Beispielsatz »Oi bitch do you take it up the back door« versehen. Weitere Beispielsätze beinhalten »She has a big backdoor«, »Her Back Door is so damn sexual, I just wanna grab it!«, »She has a fine back door.« Kurz, das Wort Backdoor bezeichnet im Urban Dictionary in den meisten Fällen: »A Person's Ass, mostly a female.« (Urban Dictionary o.J.). Auffällig an dieser Auflistung, aber auch am ersten Verwendungsnachweis in *The Insatiate Countess* ist, dass Backdoor als Anus, vor allem im Zusammenhang mit Analsex, in erster Linie Frauen, und auch explizit heterosexuellem Sex zugerechnet wird. Wird diese Praxis in *The Insatiate Countess* noch eindeutig abgewertet, so ist sie im *Urban Dictionary* schon nicht mehr so eindeutig negativ konnotiert, wobei an dieser Stelle auch darauf verwiesen sei, dass die meisten Beispielsätze über Frauen sprechen, und nicht aus ihrer Sicht. Expliziter Genuss seitens der Frau wird nur in einem Beispiel erwähnt. Penetrativer Analsex jenseits von als heterosexuell zu lesenden Konstellationen oder Frauen in der penetrierten Position kommt in den bisherigen Beispielen nicht explizit vor. Dies rahmt penetrativen Analsex zwar als heterosexuelle Sexualpraktik, allerdings nur durch den Ausschluss analer Penetration von Männern. Dies lässt sich durchaus als ein Symptom heteronormativer Diskurseffekte begreifen, die sich, wie bereits gezeigt wurde, auch im Bereich der IT-Sicherheit finden. Mit der folgenden Diskussion der Software *Back Orifice*, die den Zusammenfall von Backdoor und Anus expliziert, soll die ansonsten auf der Ebene des Subtexts verbleibende Homophobie der Metaphern des IT-Sicherheitsdiskurses, die bereits in den Ausführungen zur HIV/AIDS und Schadsoftware angerissen wurde, fokussiert und politisiert werden. Es stellt sich also die Frage, wie dieser Subtext, wie Fragen nach Lust, Begehren und Liebe, die bestenfalls in den Beispielen (und anekdotischen

27 Das *Urban Dictionary* ist ein Wörterbuch für Umgangssprache, sowie explizit auf digitale Kulturen bezogene sprachliche Phänomene. Es folgt einem ähnlichen Prinzip wie Wikipedia: Jede_r kann Bedeutungen beisteuern – moderiert wird allerdings weniger als bei Wikipedia.

Witzen), aber nicht in den wissenschaftlichen Schriften der IT-Sicherheit selbst thematisiert werden (vgl. Bergermann 2018, 339), ins Sprechen gebracht werden können. An dieses Unterfangen schließt sich eine weitere Frage an: Was wird sag- und denkbar, wenn die sexualisierten Zweideutigkeiten des IT-Sicherheitsdiskurses mit scheinbar randständigen Phänomenen wie *Back Orifice* in das Zentrum der Analyse gestellt werden? Diesen Fragen wird in einem argumentativen Dreischritt nachgegangen: Zunächst wird anhand eines kurzen Überblicks über *Back Orifice* die naheliegende Lesart als homophober Witz erläutert. Diese wird im nächsten Schritt kritisiert, und unter Rückgriff auf Positionen der Gay Theory zur Bedeutung des Anus und den mit ihm verbundenen Praktiken in westlichen Kulturen umgedeutet. Als dritter und letzter Schritt wird versucht, mit Queer Computing einen Gegenentwurf zum bestehenden negativen Sicherheitsbegriff der IT-Sicherheit zu entwerfen, um die dort vorhandenen Ausschlüsse nicht zu reproduzieren.

4.3.1 *Back Orifice*

Anfang August 1998 stellte die US-amerikanische Hackergruppe *Cult of the Dead Cow* auf der Hacker_innenkonferenz DEFCON (6) ein Programm namens *Back Orifice* vor. *Back Orifice* wurde offiziell als Fernwartungssoftware (englisch: remote administration tool) für *Microsoft Windows 95* angekündigt – aber »[d]aß die Intention eine andere ist, ergibt sich schon aus dem Namen«, wie auf *heise.de* im August 1998 zu lesen ist: »Back Orifice (hintere Öffnung) übersetzt man hier am besten mit ›Hintertür‹, denn das Programm macht es fast zum Kinderspiel, Schindluder mit Windows-PCs zu treiben.« (Himmelein 1998) Die Verwendung von Fernwartungssoftware ermöglicht es, einen Computer von einem zweiten Computer aus fernzusteuern, sowie die auf ihm vorhandenen Dateien auszulesen. Software dieser Art wird daher in erster Linie zu ihrem namensgebenden Zweck der Wartung aus der Ferne eingesetzt, beispielsweise wenn die Computer eines Unternehmens durch ein weiteres Unternehmen auf dem neuesten Stand gehalten oder von Schadsoftware gereinigt werden sollen. *Back Orifice* wurde allerdings nicht in einem solchen kommerziellen Setting und in gegenseitigem Einvernehmen eingesetzt, sondern eher als Scherzprogramm verwendet und ohne das Wissen der jeweiligen Personen, denen ein Streich gespielt werden sollte, auf ihrem Computer installiert. ›Hintere Öffnung‹ als Übersetzung für *Back Orifice* ist gemessen an der Verwendung des Wortes *orifice* im Englischen allerdings eine etwas zahme Übersetzung, denn *orifice* bezeichnet nicht einfach irgendwelche, sondern

spezifisch Körperöffnungen: »An opening, particularly one in the body such as a nostril or the anus« (Lexico 2021b). Computer werden, so lässt sich als erste Beobachtung festhalten, durch diese Benennung der Software einmal mehr als Körper konfiguriert. Der Name der Software ist neben diesem Wortspiel auch eine Anspielung auf das vier Jahre zuvor erschienene Produkt *Microsoft BackOffice Server*, ein Softwarepaket für Firmenkund_innen, das die Servervariante von *Microsoft Windows NT* und später *Windows 2000* sowie weitere Programme enthielt (vgl. Wikipedia 2016). In einer Pressemitteilung mit dem Titel *Running a Microsoft Operating System on a Network? Our Condolences* auf ihrer Webseite lassen *Cult of the Dead Cow* vermuten, der Urheber von *Back Orifice*, ein unter dem Pseudonym *Sir Dystic* bekannter Hacker (vgl. Wikipedia 2017), habe *Back Orifice* als eine Art pädagogische Hacking-Maßnahme im Kampf gegen »Microsoft's Swiss cheese approach to security« (Cult of the Dead Cow 1998a) geschaffen.

Anfang der 2000er Jahre warnte auch das Rechenzentrum der Ruhr-Universität Bochum vor *Back Orifice* (vgl. RUB RZ 2002), stellte eine kurze Anleitung zur Verfügung, wie *Back Orifice* zu löschen sei und verlinkte eine Webseite mit weiterführenden Informationen. Während diese Webseite durchaus sehr detailliert Auskunft über *Back Orifice* gibt, sind die Titel der einzelnen Einträge spannend: Von *The Back Orifice »Backdoor« Program. YOUR security is at risk* (Little 1999) bis zu *Almost All The Ways to Find Your Back Orifice* (Little 1998) wird deutlich, dass *Back Orifice* in den Augen des auf seiner Webseite zunächst anonym bleibenden Verfassers nicht nur Computer, sondern auch User_innen direkt betrifft, die er als »›orificed‹ people« (Little 1999) bezeichnet, die er vor *Back Orifice* gerettet habe. Die Gleichsetzung und Verbindung menschlicher und maschinischer Körper wurde bereits im vorangegangenen Kapitel ausführlich diskutiert. Die Übertragung der Gefahr von Computer auf User_innen lässt sich als ein Effekt der *Personal Systems Hygiene-* und *Safe Hex*-Diskurse werten, und mit Parikka (2016, 116) weiterhin als typisch für den IT-Sicherheitsdiskurs einordnen, in dem Computer, aber auch User_innen als »frequently gendered and sexualized with rhetorics of rape and other images of vulnerability« erscheinen. Während es naheliegend ist, aufgrund dieser Übertragung in *Back Orifice* einen langen, homophoben Witz zu sehen, und Analysen des Sexismus innerhalb der Hacking Culture (siehe exemplarisch Taylor 2001), sowie die bisherigen Erkenntnisse über den IT-Sicherheitsdiskurs eine solche Intentionalität nahelegen würden, soll an dieser Stelle eine Umdeutung versucht werden. Mit dem in der Übertragung dieser Rhetoriken von Computern auf Menschen entstandenen Ausdruck

»›orificed‹ people« wird eine weitere Dimension sicht- und adressierbar, die über die Unannehmlichkeiten dysfunktionaler Computer hinausgeht, und im Spannungsfeld dieser Übertragung besprochen werden soll: Dass eine Grenzverletzung im Bereich der IT-Sicherheit mit der Metapher eines geöffneten Körpers beschrieben wird, ist nach den bisherigen Ausführungen erwartbar. Weshalb aber verknüpft sich eine Grenzverletzung im Bereich der IT-Sicherheit und der damit einhergehende Verlust von Privatsphäre spezifisch mit der Metapher eines geöffneten Anus? Welche (negativen) Konnotationen verbinden sich mit der Bezeichnung »›orificed‹ people«? Sind nicht alle Menschen per se *orificed*, das heißt, verfügen nicht alle Menschen über Körperöffnungen, über einen Anus? Und sind nicht alle Computer erst durch (die Standardisierung ihrer) Anschlussstellen, also durch ihre Öffnungen in Hard- und Software überhaupt steuerbar? Was macht Backdoors als Figurationen innerhalb dieser Kultur so bemerkenswert? Die in der Vermischung der offenen Hintertür im Computer mit dem (offenen) Anus sichtbar werdende Verknüpfung von Penetriertwerden und einer dadurch implizierten Passivierung, die als Verlust von Sicherheit und Macht gefasst wird, soll im Folgenden befragt werden.

4.3.2 Über den Anus

Für die Diskussion des Anus abseits von heteronormativer Theoriebildung, die in der *Gay Theory* ihren Anfang nahm, werden an dieser Stelle drei Ansätze besprochen, die sich mit Analsex in einer heteronormativen, und damit homophoben Gesellschaft auseinandersetzen, aber zu unterschiedlichen Schlüssen und Konsequenzen kommen. Der erste ist Guy Hocquenghems Anfang der 1970er Jahre erschienenes Buch *Le désir homosexuel*, in dem ausgehend von der durch Hocquenghem wahrgenommenen konservativ-psychoanalytischen Ausrichtung der damaligen Gesellschaft anale Penetration als eindeutig schwule Sexualpraktik kontextualisiert, sowie der Zusammenhang des Anus und der Formation von Subjektivität und Privatheit expliziert wird. Das Projekt Hocquenghems ließe sich als der Versuch beschreiben, den von der Psychoanalyse (fehl)informierten Diskurseffekten einer kapitalistischen Gesellschaft zu entkommen, allerdings nicht, indem er die Psychoanalyse gänzlich verwirft, sondern über eine genaue Lesart und Auseinandersetzung mit ihr, sowie des Topos der Paranoia, die einen privilegierten Schauplatz für die Analyse von Homosexualität darstellt. Der zweite hier diskutierte Ansatz findet sich in Leo Bersanis Aufsatz *Is the Rectum a Grave?*, mit dem die

Diskursivierung des penetrativen Analsex homosexueller Männer im Zuge der AIDS-Krise noch einmal genauer betrachtet werden soll. Auch Bersani bezieht sich auf die Psychoanalyse, zieht aber andere Konsequenzen als Hocquenghem. Seine Forderung ist nicht, die bestehenden Strukturen zu zerschlagen, sondern den mit analer Penetration verknüpften Machtverlust, der als Passivierung diskursiviert wird, in seiner Negativität aufzuwerten. Abschließend wird anhand von zwei Texten Paul B. Preciados, *Anal Terror. Notes on the First Days of the Sexual Revolution* und *Kontrasexuelles Manifest*, eine metaphorische Umdeutung von *Back Orifice* vorgenommen. Preciado baut seine Argumentation auf Hocquenghems Analyse auf, und kommt so ebenfalls zu der Forderung, dass die heteronormative Gesellschaftsordnung zerschlagen werden müsse. Anale Penetration ist für Preciado dabei das Mittel der Wahl, denn er begreift diese als eine Praktik, mit der Körper von sexueller Orientierung und Geschlechtsidentität gelöst werden können. Preciado geht es also im Gegensatz zu Bersani nicht um eine Aufwertung der Passivität im Sinne einer Erfahrung des Machtverlusts, sondern um die Einebnung der Differenz von aktiv und passiv, und damit auch des Machtgefälles. Da Preciado in *Anal Terror* mit einem stark an die Informatik angelehnten Vokabular arbeitet, wird dieser Text als Brücke genommen, um eine Umdeutung der homophob lesbaren Metaphorik von *Back Orifice* vorzunehmen.

Sexualisierung, Paranoia, Kapitalismus

Guy Hocquenghems Buch *Le désir homosexuel*, das 1972 in Frankreich erschien, kann von heute aus betrachtet als erstes in einer Reihe von Werken gesehen werden, die eine Form des Wissens und der Wissensproduktion darstellen, die die Grundlage der Queer Theory bildet (vgl. Preciado 2015, 140). Das Buch wurde in den letzten Jahren erneut in zahlreiche Sprachen übersetzt und mit Begleittexten und einordnenden Vorworten versehen. Gemeinsam mit der spanischen Veröffentlichung mit dem Titel *El deseo homosexual* im Melusina Verlag im Jahr 2000 wurde auch ein Aufsatz Paul B. Preciados mit dem Titel *Terror anal: Apuntes sobre los primeros días de la revolución sexual* veröffentlicht, der mit Hocquenghems Text in einen Dialog tritt.[28] *Anal Terror. Notes on the First Days of the Sexual Revolution*, so der englische Titel von Preciados Essay, ist eine kurze und polemisiert zugespitzte Geschichte des Anus als Schauplatz der Herstellung von Körpern, Geschlecht und sexueller Orientierung. *Le désir homosexuel* war eine für die damalige Zeit in mehrfacher Hinsicht revolutionäre

28 Im Folgenden werden die englischen Übersetzungen beider Texte verwendet.

Schrift: Hocquenghem schrieb über Homosexualität und homosexuelles Begehren, ohne dieses zu pathologisieren. Preciado (ebd., 126) weist darauf hin, dass nicht nur der Inhalt, sondern auch die Form des Texts von damals ungekannter Schlagkraft war: »There are no apologies, excuses, or justifications in Hocquenghem's text. They're lacking because he no longer wants to be the good boy […].«[29] Mit Roland Barthes ordnet Preciado (ebd.) Guy Hocquenghems Buch als »textual terrorism« ein, da es das erste Buch war, in dem ein offen schwuler Mann die Verbindung von Kapitalismus und Heterosexualität untersuchte. Hocquenghem, Gründungsmitglied der *Front Homosexuel d'Action Révolutionnaire* (FHAR), arbeitet sich an der Freud'schen Psychoanalyse ab: an den Effekten der Normalisierung ihres Wissens in der Breite der kapitalistischen Gesellschaft[30] sowie den Verdrehungen, die dieses Wissen dabei erfährt. Die kapitalistische Gesellschaft, so Hocquenghem (1993, 50), »manufactures homosexuals just as it produces proletarians, constantly defining its own limits: homosexuality is a manufactured product of the normal world.« Die mit dem Begriff Homosexualität konstruierte abstrakte Kategorie des Begehrens erlaube es, Machtrelationen auch auf die Subjekte auszudehnen, die ansonsten außerhalb des Gesetzes stünden, und sei damit Teil einer Gesellschaft, die fortschreitend Menschengruppen klassifiziere und ihnen einen sozialen Status zuschreibe (vgl. ebd., 51). Elementarer Teil der Arbeit Hocquenghems ist die Denaturalisierung von Homosexualität als eine über Begehren konstruierte Identitätskategorie, indem sie als Diskurseffekt beschreibbar wird.

»The problem is not so much homosexual desire«, beginnt Hocquenghem (ebd., 49) seine Überlegungen, »as the fear of homosexuality: why does the mere mention of the word trigger off reactions of recoil and hate?« Er folgert, dass es diskursive Strategien geben müsse, die diese »reactions of recoil and hate« auslösen, und nimmt sich auf der Suche nach diesen zunächst der »Anti-Homosexual Paranoia« (ebd., 55) an. Die gesellschaftliche Diskursivierung von Homosexualität, beobachtet Hocquenghem (ebd., 56), sei »the fruit of the paranoia through which a dominant sexual mode, the family's reproductive

29 Peter Rehberg (2019, 101) bemerkt in seinem Essay *Energie ohne Macht. Christian Maurels Theorie des Anus im Kontext von Guy Hocquenghem und der Geschichte von Queer Theory*, es habe eine »Domestizierung von Queer« stattgefunden, die er unter anderem der Übersetzungspraxis zurechnet: »Mit der Übersetzung ins Deutsche hat die Kategorie Queer somit auch das Anstößige und Verletzende, das ihr im Englischen anhaftet, verloren.«

30 Zentral für Hocquenghems Betrachtungen zum Kapitalismus ist Gilles Deleuzes und Félix Guattaris nahezu zeitgleich erschienenes Buch *Capitalisme et schizophrénie. L'anti-Œdipe* (dt.: *Anti-Ödipus: Kapitalismus und Schizophrenie*).

heterosexuality, manifests its anxiety at the suppressed but constantly recurring sexual modes.« Diese Angst vor Homosexualität, konstatiert er, sei eine Umkehrung von Freuds Konzept der Paranoia,[31] denn »Freud's famous ›persecutory paranoia‹ is in actual fact a paranoia that *seeks to persecute.*« (Ebd., Herv. i.O.) Er schreibt weiter:

> »The reversal of meaning which Freud's concept has undergone in this respect is enlightening. Freud states that persecutory paranoia is generally connected with the repression of the libido's homosexual component. Social man's fear of his own homosexuality induces in him a paranoiac fear of seeing it appear around him.« (Ebd.)

Freuds paranoider Wahn, der also eigentlich ein *verfolgender* ist, wird in einer Umkehrbewegung von der Gesellschaft in eine Paranoia umgedeutet, die sich *verfolgt* fühle. Die Herstellung von Homosexualität als Identitätskategorie gehe daher mit ihrer Unterdrückung durch die Mehrheitsgesellschaft einher (vgl. ebd., 55). Dies wiederum manifestiere sich in einer homophoben Paranoia:

> »The attitude of what is commonly called ›society‹ is, in this respect, paranoiac: it suffers from an interpretative delusion which leads it to discover all around it the signs of a homosexual conspiracy that prevents it from functioning properly.« (Ebd.)

Was Hocquenghem hier als »homosexual conspiracy« benennt, lässt sich auch heute noch wiederfinden, beispielsweise in der Kontroverse um den Bildungsplan 2015 des Landes Baden-Württemberg, im Zuge derer eine Petition mit dem Titel *Zukunft – Verantwortung – Lernen: Kein Bildungsplan 2015 unter der Ideologie des Regenbogens* gestartet wurde, mit der verhindert werden sollte, dass auch LGBTQI*-Themen und -Lebensentwürfe im Schulunterricht behandelt werden (vgl. o.A. 2013). Die Unterdrückung von Homosexualität führe gleichzeitig zu einer »spontaneous sexualisation of all relationships with a homosexual« (Hocquenghem 1993, 55), die schließlich in der Angst münde, von of-

31 Freud diagnostizierte Daniel Paul Schrebers Paranoia als Resultat verdrängter Homosexualität: »Die Eigenart der Paranoia (oder der paranoiden Demenz) müssen wir in etwas anderes verlegen, in die besondere Erscheinungsform der Symptome, und für diese wird unsere Erwartung nicht die Komplexe, sondern den Mechanismus der Symptombildung oder den der Verdrängung verantwortlich machen. Wir würden sagen, der paranoische Charakter liegt darin, daß zur Abwehr einer homosexuellen Wunschphantasie gerade mit einem Verfolgungswahn von solcher Art reagiert wird.« (Freud 1955, 295)

fen schwulen Männern vergewaltigt zu werden. Hocquenghem (ebd., 55–56) wendet also die psychiatrische Definition von *persecutory paranoia*, die Homosexuellen zuschrieb, sich bedroht oder verfolgt zu fühlen, mit einer genauen Freudlektüre zurück in ihr (ursprüngliches) Gegenteil und kommt so zu dem Schluss, dass der vorherrschende homophobe Diskurs vielmehr selbst ein Ergebnis der Verdrängung anderer Formen von Sexualität durch die dominante reproduktive Heterosexualität sei. Ebendiese *persecutory paranoia* ist beispielhaft in der Petition gegen den baden-württembergischen Bildungsplan 2015 zu erkennen, in der beklagt wird, dass

> »die ethische Reflexion der negativen Begleiterscheinungen eines LSBTTIQ-Lebensstils, wie die höhere Suizidgefährdung unter homosexuellen Jugendlichen, die erhöhte Anfälligkeit für Alkohol und Drogen, die auffällig hohe HIV-Infektionsrate bei homosexuellen Männern, […] die deutlich geringere Lebenserwartung homo- und bisexueller Männer, das ausgeprägte Risiko psychischer Erkrankungen bei homosexuell lebenden Frauen und Männern« (o.A. 2013)

fehle, wobei Lehrer_innen gleichzeitig gezwungen würden, »Coming-out zu neuen ›sexuellen Orientierungen‹ pädagogisch [zu] propagieren« (ebd.). Die von Hocquenghem beschriebene homosexuelle Verschwörung als »interpretative delusion« zeigt sich hier darüber hinaus in der Vermutung, es handle sich beim Bildungsplan 2015 um eine »pädagogische, moralische und ideologische Umerziehung an den allgemeinbildenden Schulen« (ebd.). Anhand dieses Beispiels wird deutlich, wie Hocquenghem mit Paranoia als zentralem Konzept operiert, das, wie Eve Kosofsky Sedgwick (2003, 126) in ihrem Aufsatz *Paranoid Reading and Reparative Reading, or, You're So Paranoid, You Probably Think This Essay Is About You* schreibt, damit zur »uniquely privileged site for illuminating not homosexuality itself, as in the Freudian tradition, but rather precisely the mechanisms of homophobic and heterosexist enforcement against it« wird. Über diese Umkehrbewegung könne Hocquenghem somit erklären, schreibt Sedgwick (ebd.) weiter, »not how homosexuality works, but how homophobia and heterosexism work – in short, if one understands these oppressions to be systemic, how the world works.«

In Hocquenghems (1993, 93) Lesart, die die von der Psychoanalyse (fehl)informierte Pathologisierung, aber auch die davor dominante Kriminalisierung von Homosexualität in Betracht zieht, sind diese beiden Modi der Verwerfung von Homosexualität verbunden mit der Herausbildung des Kapitalismus als dominanter Gesellschaftsform westlicher Zivilisation. Hocquenghem geht

insbesondere auf Freuds Konzept der *analen Phase* ein, die in einer nach Plan verlaufenden Entwicklung eines Kindes von der *genitalen Phase* abgelöst werden müsse. In letzterer ereigne sich Freud zufolge der Ödipuskonflikt, durch den Kinder sowohl Heterosexualität erlernten als auch Moral. In der Überwindung der analen Phase ereignet sich Hocquenghem (ebd., 96) folgend die von Freud formulierte »formation of the person«: Indem der Anus mit dem erfolgreichen Erwerb von Kontinenz als Lustzentrum überwunden werde, seien alle mit dem Anus verbundenen Funktionen »excremental« geworden. Bezugnehmend auf Deleuze und Guattari verknüpft Hocquenghem (ebd.) dies mit der Formation von Privatheit: »The anus has no social position except sublimation. The functions of this organ are truly private; they are the site of the formation of the person. The anus expresses privatisation itself.« Basierend auf zwei psychoanalytischen Fallanalysen[32] der Verbindung von Homosexualität und Paranoia mit besonderem Fokus auf den Anus konstatiert Hocquenghem (ebd., 98–99) unter Rückgriff auf Deleuze und Guattari, Kontrolle über den Anus sei die Vorbedingung für die Fähigkeit, Güter zu besitzen, also in die Ordnung des Kapitalismus einzutreten. Denn Geld, das zuerst in dem privaten Besitz einer Person liegen müsse, um schließlich auf dem Markt zirkulieren zu können, sei mit dem Anus als privatestem Teil des Körpers verbunden (vgl. ebd., 96–97). Vor diesem Hintergrund betrachtet, erscheinen informatische Backdoors in ihrer Zweideutigkeit als Hintertür und Anus, und die mittels Backdoors herstellbaren Grenzverletzungen als homophobes Motiv innerhalb eines heterosexistisch kodierten Systems: Bei *Back Orifice* wird die Verknüpfung analen Penetriertwerdens mit dem Verlust

32 Hocquenghem (1993, 98–99) führt einerseits einen durch den ungarischen Psychoanalytiker Sándor Ferenczi beschriebenen Fall eines bis zu einer operativen Entfernung einer Analfistel in seiner Gemeinde sehr aktiv gewesenen Bauern an, der nach der Operation einen paranoiden Verfolgungswahn entwickelte und sich aus dem Gemeindeleben ins Private zurückzog. Ferenczi diagnostiziert, die Operation durch männliche Ärzte habe eine latente, bis dahin sublimierte Homosexualität zutage gefördert, die nun dafür verantwortlich sei, dass der Bauer einen paranoiden Wahn entwickelt habe, und sich von anderen Männern fernhalte, obwohl er bis dahin ein angesehenes Mitglied der Gemeinde gewesen sei. Das zweite Fallbeispiel ist Sigmund Freuds Analyse des Falls Schreber, der konstitutiv für das Konzept von Paranoia in der Freud'schen Psychoanalyse ist, und in dem Freud verdrängte Homosexualität als Auslöser für Daniel Paul Schrebers paranoiden Wahn ausmachte. Die Unterdrückung der möglichen Verwendung des Anus als Lustzentrum spielt in beiden Analysen eine tragende Rolle, da diese Sublimierungsleistung das gesellschaftliche Ansehen beider Männer bedinge.

von Sicherheit und Privatheit deutlich ausbuchstabiert. Der geöffnete Anus eignet sich, Hocquenghem und Preciado folgend, wie keine andere Körperöffnung für diese Metapher. Die Verbindung des Anus mit dem Privaten, führt Hocquenghem (ebd., 97) weiter aus, bindet gleichsam den Phallus an die Öffentlichkeit: »The constitution of the private, individual, ›proper‹ person is ›of the anus‹; the constitution of the public person is ›of the phallus‹.« Mit Preciado (2015, 125) lässt sich zuspitzen, dass mit dieser Verwerfung des Anus der Penis als »despotic signifier« erschien, und der Phallus als »affordable mega-$-porno-fetish of the new Disney-heterosexual-land.« Körper, deren Anus im übertragenen Sinne ›offen‹ geblieben war – Preciado (ebd.) zählt dazu die Körper von Frauen und »fag bodies« – wurden konsequenter Weise von Machtpositionen ausgeschlossen und aus der Öffentlichkeit verbannt.

Penetrativer Analsex und Passivität

Zusätzlich zur Bedeutung des Anus sowie der notwendigen Überwindung der analen Phase, um in die kapitalistische Ordnung eintreten zu können, macht Hocquenghem (1993, 98) deutlich, dass Homosexualität für die Psychoanalyse nicht bloß an den Anus als Lustzentrum, sondern spezifisch an anale Penetration geknüpft sei: »Homosexuality primarily means anal homosexuality, sodomy.« Zur (bis heute) mit Analsex diskursiv verbundenen Passivierung der anal penetrierten Person konstatiert er:

> »Experience has proved the thesis that effeminate men are attracted to masculine ones and vice-versa to be quite absurd. The categorisation of so-called passive sodomy as ›effeminate‹ is not even based on the material reality of homosexual relationships, where men who are considered most masculine are surely not necessarily, nor even in the majority of cases, the ›male‹ partners.« (Ebd., 118–119)

Hocquenghem geht nach dieser Anmerkung ausführlicher auf psychoanalytische Positionen zur Objektwahl und -beziehung ein, um die Verbindung von Homosexualität und dem Weiblichen zu dekonstruieren, was an dieser Stelle jedoch nicht verfolgt werden soll. Stattdessen lässt sich hier mit Bersani (1987, 212) anschließen, der die Idee der Passivierung durch Penetration historisiert. Selbst in Kulturen, die Homosexualität per se nicht ablehnend gegenüberstanden, wie beispielsweise im antiken Rom oder der islamischen Kultur zur Zeit des Mittelalters wurde die Position des anal penetrierten Mannes abgewertet (vgl. ebd.). Mit Foucault schreibt Bersani (ebd.) über die explizite Verknüpfung von Penetration und Passivität im antiken Griechen-

land: »A general ethical polarity in Greek thought of self-domination and a helpless indulgence of appetites has, as one of its results, a structuring of sexual behavior in terms of activity and passivity, with a correlative rejection of the so-called passive role in sex.« Die damit einhergehende »legal and moral incompatibility between sexual passivity and civic authority« (ebd.) traf vor allem auf erwachsene Männer zu, und Bersani (ebd., Herv. i.O.) formuliert pointiert: »In other words, the moral taboo on ›passive‹ anal sex in ancient Athens is primarily formulated as a kind of hygienics of social power. *To be penetrated is to abdicate power*.« Im Verlauf seines Aufsatzes geht es Bersani allerdings nicht darum, die Passivität, also den Machtverlust, des_der Penetrierten in eine Aktivität umzudeuten, sondern vielmehr in ihrer Negativität zu rehabilitieren. Bezugnehmend auf Simon Watneys Formulierung des *Rektums als Grab* schreibt Bersani (ebd., 222): »[…] if the rectum is the grave in which the masculine ideal (an ideal shared – differently – by men *and* women) of proud subjectivity is buried, then it should be celebrated for its very potential for death.« Dieser Satz lässt sich folgendermaßen verstehen: Die privilegierte Position, die im Phallozentrismus dem Penis vor dem Anus (und der Vagina) zukommt, so führt Bersani (ebd., 217, Herv. i.O.) weiter aus, sei »not primarily the denial of power to women (although it has obviously also led to that, everywhere and at all times), but above all the denial of the *value* of powerlessness in both men and women.« Powerlessness bezieht sich an dieser Stelle weder auf Sanftheit noch auf Passivität, sondern auf Freuds Bemerkung, dass für das Empfinden sexueller Lust die Organisation des Selbst für eine kurze Zeit unterbrochen werden müsse (vgl. ebd.). Dieser Akt des »self-shattering« (ebd.) sei es, der Sexualität mit Machtpositionen, spezifisch mit Machtverlust, verknüpfe. Im letzten Kapitel wurde bereits ausführlicher auf die von Bersani analysierte Verbindung von homosexuellem Analsex, imaginierter und realer Promiskuität sowie pathologisierter weiblicher Sexualität eingegangen, bei der anale Penetration als eine Praktik »associated with women but performed by men« (ebd., 220) imaginiert werde, was in letzter Konsequenz homosexuelle Männer selbst zum Zeichen der HIV-Infektion, und damit des unausweichlichen Todes mache. Zusammengedacht mit dem Potential des »self-shattering« wohnt homosexuellem Analsex Bersani zufolge also eine Negativität inne, die er allerdings nicht umdeuten möchte, in der Hoffnung, dass sich auf diese Weise die Homophobie der Gesellschaft bekämpfen ließe. Bersanis Einsatz besteht vielmehr in der genau gegensätzlichen Bewegung: Wenn das Rektum als Grab des männlichen Ideals, und der damit verbundenen Machtposition imaginiert wird, dann besteht Bersani

(ebd., 222) zufolge die befreiendere Haltung darin, es »for its very potential for death« zu zelebrieren.

Was könnte dies für die Betrachtung von *Back Orifice* bedeuten? In einer affirmativen Lesart ließe sich *Back Orifice*, und damit im übertragenen Sinne das anale Penetrieren von Computern, nicht als homophober Witz, sondern vielmehr als ein lustvoller Umgang mit dem »potential for death« von Backdoors begreifen. *Back Orifice* auf dem eigenen Computer zu entdecken, könnte bedeuten, die damit einhergehende Machtlosigkeit zu genießen. Die Möglichkeit, mittels *Back Orifice*, oder Backdoors im Allgemeinen in vernetzte Computer einzudringen, ließe sich somit als lustvoller Akt einstufen, der dem in Teilen homophoben IT-Sicherheitsdiskurs mit exakt dem begegnet, was er verwirft.

Sex(ualität) als Technologie

Preciados Anliegen lässt sich quer zu Bersanis begreifen, insofern es Preciado nicht darum geht, die mit analem Penetriertwerden verbundene Machtlosigkeit aufzuwerten, sondern die Dynamiken abzuschaffen, die überhaupt erst ein solches Machtgefälle innerhalb von Sexualität erzeugen. Mit Preciado stellen sich also folgende Fragen: Wie könnte die Konzeptionalisierung analen Penetriertwerdens als passivierend der heteronormativen Deutungshoheit entzogen werden? Könnte das Praktizieren analen Penetriertwerdens, sofern es von Menschen aller Geschlechter und sexuellen Orientierungen durchgeführt würde, seinen Status im gegebenen System und dieses selbst verändern, da seine Beschreibungskategorien bereits in ihrer deskriptiven Funktion als unbrauchbar markiert werden?

Preciado widmet sich diesen Fragen mit scharf polemisierenden wissenschaftlichen Texten, sowie Anleitungen zu konkreten Arten, Sex zu haben: Ein radikales Programm, das er *Kontra-Sexualität* tauft. Das Anliegen von Kontra-Sexualität, formuliert Preciado (2003, 10), »handelt nicht von der Erschaffung einer neuen Natur, sondern vom Ende einer Natur, die als Ordnung verstanden wird und die Unterwerfung von Körpern durch andere Körper rechtfertigt.« Diese Position wird, wenn auch nicht ganz so explizit, ebenfalls im Aufsatz *Anal Terror* formuliert, in dem Preciado (2015, 138) »anal politics« als »counter-biopolitics« bezeichnet. Hocquenghems *Homosexual Desire* begreift Preciado (ebd.) dabei als »an instruction manual to render functional an anti-systemic orifice installed in each and every body: the ANUS.« Gleichzeitig erfolgt eine Erweiterung des Körperbegriffs, der nicht mehr nur den menschlichen/weiblichen/männlichen/rassifizierten Körper umfasst, sondern den Körper als »relational, vulnerable platform, socially and historically constructed, whose

limits are constantly redefined« (ebd.) denkt. Preciados (2003, 14) Anliegen umfasst dabei mit dem erweiterten Körperbegriff auch »die Sex- und Genderverhältnisse, die zwischen Körpern und Maschinen entstanden sind.« Kontra-Sexualität realisiere sich über die von Preciado thematisierten, ausschließlich nicht-prokreativen Sexpraktiken,[33] mittels derer eine Herstellung von Körpern, die außerhalb der heteronormativen, naturalisierten Differenz binärer Geschlechterrollen sowie Begehrensstrukturen stehen, erfolgen könne (vgl. ebd., 11, 36–49). Im Zentrum kontrasexueller Praktiken steht dabei notwendigerweise ein Verständnis von »Sexualität als Technologie«, das

> »die unterschiedlichen Elemente des Systems Sex/Gender – also ›Mann‹, ›Frau‹, ›homosexuell‹, ›heterosexuell‹, ›transsexuell‹ ebenso wie deren Praktiken und sexuellen Identitäten – als Maschinen, Produkte, Werkzeug, Apparate, Gadgets, Prothesen, Netze, Anwendungen, Programme, Verbindungen, Energie- und Informationsströme, Unterbrechungen und Unterbrecher, Schlüssel, Zirkulationsgesetze, Grenzen, Zwänge, Designs, Logiken, Ausstattungen, Formate, Unfälle, Abfälle, Mechanismen, Gebrauchsweisen, Umwidmungen …« (ebd., 11)

denkbar macht. Der Anus als Lustzentrum wird dabei »das transitorische Zentrum einer Arbeit kontrasexueller Dekonstruktion«, da er durch seine Unbrauchbarkeit für prokreativen Sex »außerhalb der durch die sexuelle Differenz erzwungenen anatomischen Grenzen liegt« und in ihm »die Rollen und die Register als universal umkehrbar erscheinen« (ebd., 18–19): Unabhängig von Sex- und Genderkonfigurationen haben alle Körper einen penetrierbaren Anus, und können alle Körper penetrieren. Der Anus könne damit als eine Art Gleichmacher der Körper begriffen werden, über den heteronormative Beschreibungs- und Herstellungsweisen derselben dekonstruiert werden können: Er »konstituiert einen Raum technologischer Arbeit; er ist eine Fabrik der Wiederherstellung des kontrasexuellen Körpers.« (Ebd., 19)

Bioports und Buttplugs

An dieser Stelle soll mit Preciado erneut ein Blick auf die technische Funktionsweise von *Back Orifice* geworfen werden, um das Programm mit dem Konzept der Kontra-Sexualität zu lesen. *Back Orifice* besteht aus zwei Komponenten:

33 Einige Praktiken listet Preciado im *Kontrasexuellen Manifest* in Form von Handlungsanweisungen auf, die strukturell an Fluxus-Scores erinnern.

Einem Server, der auf dem Ziel-PC installiert werden muss, und einem Programm, das auf dem PC installiert sein muss, von dem aus der Ziel-PC gesteuert werden soll. Ist der *Back Orifice*-Server einmal auf einem Computer mit *Microsoft Windows 95* installiert, kann von einem zweiten Computer aus eine direkte Verbindung aufgenommen und der erste Computer komplett ferngesteuert werden, und das mit mehr Benutzerrechten als eingeloggte User_innen haben, die direkt vor dem Zielcomputer sitzen – dies ist der bereits bekannte *privileged state*, den Thomas und Francillon als elementaren Teil einer funktionierenden Backdoor beschrieben haben. Von dieser Position aus können Hacker_innen beispielsweise Dialogfenster erscheinen lassen, die einen von ihnen geschriebenen Text beinhalten, oder aber Tastatureingaben mitschneiden oder den Speicher des Zielcomputers auslesen, um hier nur einige Anwendungsmöglichkeiten der Software zu nennen (vgl. Cult of the Dead Cow 1998a). *Back Orifice* lässt sich durch seine geringe Größe als Payload in anderer, unauffälliger Software verstecken (vgl. Little 1998), die dann als Trojaner fungiert, und wurde so durch Softwaretausch, also Software EXchange – im Jargon File mit dem Akronym »SEX« (The Jargon File o.J.c) abgekürzt – zwischen Freund_innen, Bekannten oder über das Usenet und das Internet verbreitet, beispielsweise über öffentlich zugängliche FTP-Server, sogenannte *public directories*, und, um hier ›im Jargon‹ zu bleiben: »*pubic directories*« (The Jargon File o.J.d). Um den eigenen PC vor *Back Orifice* zu schützen, wurden gemeinhin alle Tipps genannt, die auch schon aus den Praktiken zur Prävention vor Computerviren bekannt sind – empfohlen wurde, sich ein rudimentäres Wissen über die Funktionsweise von Computersystemen anzueignen, sowie keine Programme aus unbekannten und/oder ggf. nicht vertrauenswürdigen Quellen zu installieren (Little 1999), also die komplette Bandbreite dessen, was unter *Personal Systems Hygiene* und *Safe Hex* verhandelt wird. Kam es trotz aller Vorsichtsmaßnahmen dennoch zu einer Installation von *Back Orifice*, so wurde der Server bei jedem Neustart des befallenen Computers automatisch gestartet und ausgeführt. Es ist nicht leicht, *Back Orifice* zu bemerken und zu schließen, da es nicht in der Liste der laufenden Prozesse auftaucht. Daher ist es zunächst auch schwierig zu bestimmen, ob auf einem Computer *Back Orifice* installiert ist oder nicht – Thomas und Francillon folgend weist also die *EFSM* (wenigstens auf den ersten Blick) keine Spuren der Backdoor auf. Ein Hinweis kann aber in den Netzwerkverbindungen erkennbar sein: Um die Fernsteuerung eines Computers zu ermöglichen, etabliert *Back Orifice* eine verschlüsselte Verbindung zu dem Computer eines_einer Hacker_in, von dem aus es gesteuert werden soll, indem es

Ports des Zielcomputers ›öffnet‹ und auf ihnen ›lauscht‹.[34] ›Lauscht‹ ein Programm auf einem Port, so bedeutet dies, dass es über den betreffenden geöffneten Port Daten empfangen kann – im Fall von *Back Orifice* wird der Computer dadurch fernsteuerbar. Preciados (2015, 164) Beschreibung des Anus als »bioport«, der nicht nur ein Symbol sei, sondern »an insertion port through which a body is open and exposed to another or others«, sowie die Fernsteuerbarkeit des Zielcomputers nach der Öffnung eines Ports, den ich hier analog zum Anus lese, greift die bereits besprochenen Dynamiken der Passivierung des_der anal Penetrierten auf. Auch das Logo von *Back Orifice* ist in diesem Zusammenhang bemerkenswert: Es nimmt die Form eines Schlüssels auf, dessen Reite gleichzeitig der weit geöffnete Anus eines minimalistisch dargestellten, weißen Hinterns mit Beinansatz ist. Es sind keine Geschlechtsmerkmale erkennbar, und die Figur des Schlüssels taucht erneut als stilisiertes O im Schriftzug *Back Orifice* auf, der rechts von dem Hintern angeordnet ist, und weist so ein zweites Mal auf die Öffnung, das Loch, den geöffneten (Bio-)Port, den Anus hin.

Back Orifice-Logo

Quelle: https://adesinio.tripod.com/Multimedia/Back_orifice_logo.gif&sp=d370 [16.12.2018, Link mittlerweile inaktiv].

34 Ports regeln – vereinfacht gesagt – die verschiedenen Ebenen, auf denen eine Verbindung zweier Computer miteinander zustande kommen kann, indem sie Verbindungen mit unterschiedlichen Transportprotokollen wie TCP, UDP oder Telnet unterschiedliche Nummern zuweisen, etwa wie bei einem Adresszusatz. Ports stellen also die Endpunkte vernetzter Kommunikation dar, die Verbindung zwischen ihnen etabliert den Trans-Port von Datenpaketen. Im Englischen (und teilweise auch im Deutschen) ist der Begriff mehrdeutig und bezeichnet sowohl die bereits beschriebenen Verbindungen, als auch einen Hafen, sowie Anschlussstellen technischer Geräte, wie beispielsweise beim USB-Port, oder Anschlussstellen menschlicher Körper, wie sie beispielsweise zur Verabreichung von Chemotherapie verwendet werden.

Auch die zahlreichen Wortspiele, die *Back Orifice* umgeben, arbeiten an den Verquickungen mit – die Plug-Ins, also installierbare Erweiterungen, die nicht standardmäßig zur Software gehören, werden als »Buttplugs« bezeichnet (Cult of the Dead Cow 1998b) – und remediatisieren so das Motiv des *Plug-Ins*. Die ›Buttplugs‹ haben sprechende Namen wie beispielsweise *ButtSniffer* (ein *packet sniffer)*, oder *Butt Trumpet* (versendet heimlich die IP-Adresse des Computers, auf dem der BO-Server installiert ist, an eine einstellbare E-Mail-Adresse, vgl. ebd.). Die Namen der Entwickler_innen *DilDog* und *Sir Dystic*, sowie ein weiteres Plug-In mit dem Namen *Silk Rope* (vgl. ebd.) spielen auf Dildos sowie S/M-Praktiken an. Letztere betrachtet Preciado (2003, 19) als Vorbild für Kontra-Sexualität, da sie in den oft mit ihnen einhergehenden expliziten Verträgen auch die impliziten Verträge der heteronormativen Gesellschaftsordnung sichtbar machten. Auch der von Preciado formulierte kontrasexuelle Vertrag ist am Vorbild von S/M-Verträgen orientiert. Das unter dem Begriff Kontra-Sexualität formulierte Programm zur Verwischung und Auslöschung von Geschlechterdifferenzen durch die Aufwertung analer Penetration legt Preciado (2015, 164) zufolge die Gleichheit heterosexuell-männlich kodierter Körper mit anderen Körpern offen, und »dissolves the opposition between hetero and homosexual, between active and passive, penetrator and penetrated. It displaces sexuality from the penetrating penis to the receptive anus, thus erasing the segregative lines of gender, sex, and sexuality.«

Es wird nicht bei der Passivierung *eines* Computers (und den dazugehörigen User_innen) durch *einen* anderen (und den dazugehörigen User_innen) bleiben. Der kontrasexuelle Vertrag gilt für menschliche Körper, und für maschinische fast umso mehr: Obgleich sich die Hardwarekomponenten von Computern stark unterschieden können, so werden diese Differenzen durch die auf ihnen laufende Software gewissermaßen überschrieben, und die jeweiligen Geräte so aneinander angeglichen, dass sie miteinander kommunizieren können. Dennoch sind diese technischen Zusammenhänge, wie gezeigt werden konnte, informiert von Geschlechterdifferenzen biologischer Körper. Wenn Preciado bemerkt, Sex sei eine »Technologie heterosozialer Herrschaft, die den Körper auf erogene Zonen reduziert« (Preciado 2003, 14) und die Geschlechterdifferenz konsequent als »Hetero-Partionierung des Körpers« (ebd., 15) liest – beim vorliegenden Beispiel ließe sich vielleicht treffender von der Hetero-*Partitionierung* des (maschinischen) Körpers sprechen – dann liegt ein transgressives Potential in Backdoors. Diese können, bewusst implementiert, »electronic information exchange as electrifying heterosexual intercourse« (Chun 2006, 12) denaturalisieren, sowie neue Arten

von Verbindungen offenbaren, die nicht der intendierten Logik der Maschine entsprechen, die auf reibungslose Funktionalität und Effizienz ausgelegt ist.

Der Anus, und damit im vorliegenden Fall die Backdoor, kann Preciado folgend als Gleichmacher begriffen werden: Wie anhand der bisher geschilderten Fallbeispiele deutlich geworden ist, kann jedes System eine Backdoor haben. Hat die heteronormative Lesart und Konstruktion von Computern und Computernetzwerken auch geschichtlich konkrete Hardware-Dispositive informiert, wie Wendy Chuns Beispiel der Werbekampagne eines brasilianischen Internetanbieters mit verschiedenen ›männlichen‹ und ›weiblichen‹ Steckern verdeutlicht (vgl. ebd., 12–14), so ist die Backdoor als Anus als Ort der Verwischung dieser sexuellen Differenz gerade in Bezug auf zunehmend ubiquitär werdende, vernetzte digitale Systeme spannend: Alles kann eine Backdoor haben, auch Systeme, die nicht physisch mittels eines Datenträgers oder Kabels, also mit einer Steckverbindung penetriert werden können. »The anal machine rises up before the heterosexual machine«, schreibt Preciado (2015, 165) – aber wie eine solche Maschine genau aussehen könnte, ist (noch) unklar.

Nachgedanken

Die Umdeutungen von *Back Orifice* mit Bersani und Preciado sind aufgrund der Vielgestaltigkeit von Backdoors nicht beliebig auf andere Backdoors übertragbar. Dennoch bieten sie eine Möglichkeit, anders über Sicherheit vernetzter Computer nachzudenken: Entweder könnte, wie mit Bersani herausgearbeitet, eine Lust an der Unsicherheit entwickelt werden, die gleichermaßen ein befreiendes Moment hat, da sie Nutzer_innen von der Steigerungslogik der Herstellung von Sicherheit enthebt. Oder, wie mit Preciado aufgezeigt wurde, eine Denaturalisierung der heteronormativen Diskursivierung von Computerhardware und Software, die vielleicht zu neuen Formen von *Computation* führen könnte. Sowohl mit Bersani als auch mit Preciado lässt sich die höchst spekulative, aber dennoch spannende Frage stellen, ob IT-Sicherheit anders gedacht werden könnte als bisher. Dieser Frage wird im folgenden Kapitel anhand des noch jungen QueerOS/*Queer Computation*-Diskurses nachgegangen.