tralisierung und gleichzeitige Ausbreitung der Macht auf alle Sphären des menschlichen Lebens haben es Kapital und Staat, so scheint es für den Moment, geschafft jeglichen anderen Horizont abzuschirmen als den der Reproduktion des Bestehenden. Diese Reproduktion, die soziale Reproduktion von Herrschaft ist wohl das haupsächliche Ziel der heutigen revolutionären Intervention. Manchmal, wenn Krawalle ausbrechen und sich eine Unzufriedenheit in den Straßen ausdrückt, wenn ansteckende Reaktionen sich gegen ein weiteres Verbrechen der Macht wehren, dann geht es darum weiter zu reichen, tiefer, fundermentaler: Es geht darum das anzugreifen, was den „normale Ablauf der Dinge“ garantieren soll.

Um zu den Sabotageaktionen gegen die Sendemasten zurückzukehren,...wir glauben, dass diese Aktionen einige wichtige Anhaltspunkte für Methoden des Kampfes und mögliche Bereiche der Intervention liefern. Die technologische Welt manifestiert sich permanent, 24/7. Wir resignieren und akzepzieren „unseren Platz“ in der Gesellschaft, den Platz von Schafen, die konsumieren, arbeiten und gehorchen. Aber diese Welt ist auch angewiesen auf eine vielzahl von Strukturen, welche sich überall um uns herum verteilt befinden und welche ziemlich einfach anzugreifen sind. Kein Militär und keine noch so starke Überwachung wird je in der Lage sein, diese Strukturen umfassend zu schützen.

Eine kurze Durchbrechung der alltäglichen Taubheit und Ausbeutung hervorzurufen bedeutet die Betonschicht aufzuknacken, die uns alle zerquetscht. Kein Warten auf einen magischen Moment, in dem „die Leute“ sich ihrer Situation bewusst werden und auf die Straße gehen; zu warten bedeutet nur das Spiel der Herrschaft mitzuspielen, während diese sich Tag für Tag ausbaut und festigt, sowohl auf einer materiellen Ebene (neue Gefängnisse, neue Polizeistationen, neue Industrie, neue Netzwerke der Kontrolle) als auch auf einer mentalen Ebene (Gehirnwäsche, jeglichen Gedanken an Revolte auslöschen, Reduktion des Lebens auf eine Wahre). Aus den Rissen heraus werden die Rebellen wissen wie sie etwas bewirken können. Ein neuer Horizont wird emporsteigen, ein Horizont der Freiheit und der sozialen Revolte.

Aus Hors Service, anarchistische Zeitschrift, Nr. 45, Brüssel

Schlechte Nachrichten aus der Welt der Technik

ein paar politische Überlegungen und technische Warnungen

Im autonomen Blättchen Nr. 15 gab der Artikel „Was bedeuten Snowdens Enthüllungen für eine widerständige Praxis“ einen Überblick über die bekannten Möglichkeiten von Geheimdiensten und Tipps für einen sichereren Umgang mit Computern u.a.. Ich will an dieser Stelle Einiges ergänzen bzw. neuere Erkenntnisse zusammenfassen. Da ich beim Zusammenstellen neuer Meldungen aus den Medien zu Sicherheitslücken und Angriffsmöglichkeiten merke, wie hilflos dieses Hinterherlaufen und Warnen ist, stelle ich den Warnungen einen Absatz zur politischen Einschätzung voran. Denn nach über einem Jahr „Überwachungsskandal“ wäre es eigentlich viel notwendiger darüber zu diskutieren, welche Wirkung Bespitzelung auf uns und die Möglichkeiten emanzipatorischer gesellschaftlicher Veränderungsprozesse hat, als immer neue Warnungen und immer kompliziertere Anleitungen für eine einigermaßen sichere Handhabung der Technik zu verfassen.

Politische Einschätzung?

Der grundsätzlichen Einschätzung, dass sich jede_r bei jeder spezifischen Nutzung selbst überlegen muss welche Art von Absicherung sie_er benötigt, ist zuzustimmen. Allerdings bin ich der Überzeugung, dass der Spielraum dabei immer enger wird bzw. dass immer mehr Aufwand und z.T. sehr spezifisches Wissen nötig ist um eine einigermaßen sichere Nutzung von Computern zu ermöglichen.

Dieses Wissen zu vermitteln ist zwar löblich, z.B. ist die Broschüre „TAILS – The amnestic incognito live system“ zu empfehlen (siehe Kasten), aber gleichzeitig scheint es mir nur für eine sehr kleine Zielgruppe relevant. Damit meine ich nicht, dass nur eine kleine Zielgruppe im Visier der Geheimdienste ist, es sollte klar geworden sein, dass mittlerweile global alle überwacht werden. Es geht darum, ganze Gesellschaften und ihre Entwicklungen zu kontrollieren. Obwohl also längst klar ist, dass jede_r bespitzelt wird und es dabei nur zweitrangig darum geht einzelne bei Straftaten zu erwischen, scheint sich nur eine kleine Zielgruppe wirklich dafür zu interessieren. Ein Grund dafür ist wohl, dass die Überwachung für die _den Einzelnen in den westlichen Demokratien nur äußerst selten zu direkt erlebbaren Konsequenzen führt. So habe ich den Eindruck, dass auch weite Teile der Linken sich der Auseinandersetzung verweigern und die Enthüllungen über Geheimdienstpraxen nichts daran geändert haben, dass Handys, Computer und Co bedenkenlos im Alltag aber auch zur politischen Aktivität genutzt werden. Die Masse an Warnungen bzw. Hinweisen was alles zu beachten ist, führt dazu, dass viele gleich kapitulieren, weil sie meinen sich das alles sowieso nicht aneignen zu können und hoffnungslos überfordert sind. Wobei kapitulieren in den meisten Fällen leider nicht heißt, die Finger davon zu lassen, sondern einfach keine oder nur sehr unzureichende Schutzmaßnahmen zu ergreifen – schließlich ist der Gegner

sowieso übermächtig und ein Schritthalten mit immer neuen technischen Lösungen schier unmöglich. Wer versteht denn wirklich die ganzen technischen Geräte und ihre Vernetzung, die sie_er ständig nutzt? Gleichzeitig scheint z.B. die subjektiv erlebte Notwendigkeit immer erreichbar zu sein und nicht sozial abgehängt zu werden größer, als die Gefahr permanent geortet oder sogar abgehört zu werden. Auch viele politische Gruppen schätzen z.B. das Mobilisierungspotential durch die Nutzung von Web 2.0 Angeboten weiterhin höher ein als die Gefahr, die sie den Leuten, die sie mobilisieren wollen, dabei zumuten.

Es gibt meiner Meinung nach mindestens vier wesentliche Faktoren, die dazu führen, dass auf die Enthüllungen der permanenten Bespitzelung nicht reagiert wird.

1. Das (technische) Terrain ist so komplex, dass es kaum jemand überblickt.

2. Die Geheimdienste werden als übermächtig angesehen, sodass Versuche sich zu schützen als hoffnungslos gelten.

3. Die eigene Relevanz wird herunter gespielt. Damit verbunden ist die Hoffnungslosigkeit gesellschaftlich wirklich was verändern zu können.

4. Die eigene Einbindung in Herrschaftsmechanismen, ihre Absicherung und Reproduktion wird nicht erkannt oder hingenommen. Entweder sind Andere schuld oder es gibt kein richtiges Leben im Falschen – so oder so wird es als legitim angesehen sich einzurichten in der Scheiße. Bzw. die eigenen Privilegien und das Profitieren von dem was diese Gesellschaft an Komfort bietet, werden nicht als Problem, sondern als etwas auf das man einen Anspruch hat, wahrgenommen.

Komische Einleitung für einen Text, in dem ich eigentlich nur einige aktuelle technische Warnungen zusammenfassen wollte. Ich belasse es dabei und hänge die technischen Warnungen hinten dran. Doch es würde mich sehr interessieren was andere dazu denken.

Technische Warnungen

Ich habe an dieser Stelle, neue Warnungen und Angriffsmethoden zusammengefasst. Ich erkläre aber nicht nochmal grundlegende Funktionsweisen oder Schutzmaßnahmen. Das folgende ist also dringend zu beachten, aber als eine Ergänzung und nicht als Ersatz zum Artikel im Blättchen Nr. 15 und auch zu der Broschüre mit der Anleitung für TAILS.

„TRUE-CRYPT ist nicht sicher“

Schon seit langem wurde kritisiert, dass Nutzer_innen der Verschlüsselungssoftware TRUE-CRYPT nicht nachvollziehen können, ob der öffentliche Quellcode auch wirklich mit den Binärdateien übereinstimmt, die das TRUE-CRYPT-Projekt anbietet. Dies sowie die Snowden-Enthüllungen, hatten einige Forscher_innen voriges Jahr veranlasst Spenden zu sammeln, um den Quellcode auf Hintertüren und Programmierfehler durchsuchen zu lassen. Das in diesem Zusammenhang geschaffene Open Crypto Audit Project (OCAP) engagierte daraufhin die Sicherheitsfirma iSec für den ersten Teil der Code-Überprüfung. Der erste Teil der unabhängigen Quellcode-Überprüfung des Verschlüsselungsprogramms TRUE-CRYPT ist abgeschlossen. Dabei kam heraus, dass der Code nach Einschätzung der Forscher_innen keine vorsätzlich eingebaute Hintertür enthält – er genügt allerdings auch nicht den gängigen Standards für das Programmieren von sicherheitsrelevanter Software. Alle entdeckten Probleme sähen nach unbeabsichtigten Fehlern aus. Das bezieht sich auf die von der Webseite des TRUE-CRYPT-Projektes heruntergeladene Version 7.1a des Programms. Gegenstand der Code-Überprüfung war sowohl der Quellcode als auch die von der Webseite erhältlichen Binärdateien. Insgesamt entdeckten die Forscher 11 Schwachstellen. Die gravierendste davon betrifft die Verschlüsselung der Volume Header. Laut den Forschern seien selbst mittelmäßig komplexe Passwörter durch diesen Prozess nicht sicher und erlaubten es einem_einer Angreifer_in, das verschlüsselte Volume zu knacken.

Der komplette Bericht kann als 32-seitiges PDF von der OCAP-Seite heruntergeladen werden. Dort wird auch der zweite Teil der Untersuchung veröffentlicht werden. ***opencryptoaudit.org/reports***

Die untersuchte Version 7.1a ist allerdings seit Mai 2014 nicht mehr von der offiziellen Homepage zu bekommen. Denn dort heißt es „WARNUNG: Die Nutzung von TRUE-CRYPT ist unsicher, da nicht behobene Sicherheitslücken vorhanden sein können“. Es gibt nur eine Warnung. Danach folgt eine ausführliche Erklärung, wie Nutzer_innen von TRUE-CRYPT zu BITLOCKER – ein Festplattenverschlüsselungsprogramm von Microsoft – wechseln können. Weitere Erklärungen beziehungsweise Hintergründe gibt es nicht, lediglich am Textende die erneute Warnung, dass TRUE-CRYPT unsicher sei. Die aktuell zum Download angebotene Version bietet nur einen eingeschränkten Funktionsumfang; es lassen sich lediglich bestehende Verschlüsselungen öffnen; da die Möglichkeit entfernt wurde, neue TRUE-CRYPT - Volumen anzulegen.

Außerdem wird es damit auch zukünftig keine Updates mehr geben – auch nicht im Fall von bekannt werdenden Sicherheitslücken. Trotzdem ist die emp-

Hefte zur Förderung widerständischer Praxis gegen den digitalen Zugriff

TAILS - The amnesic incognito live system

Anleitung zur sicheren Nutzung des TAILS-Live-Betriebssystems für politische Aktivist*innen bei der Recherche, Bearbeitung oder Veröffentlichung sensibler Dokumente (Juni 2014)

Mit den neueren Snowden-Veröffentlichungen vom März 2014 wissen wir leider mit Sicherheit, dass der US-Geheimdienst NSA in Zusammenarbeit mit dem britischen Partnerdienst GCHQ (und weiteren) für eine (maßgeschneiderte) Infiltration unserer Rechner keine menschlichen Hacker mehr benötigt, sondern automatisiert mit dem Spionageprogramm (Turbine) unbemerkt spezifische Schnüffel-Software auf unseren Rechnern installiert. Wir empfehlen angesichts dieser Angreifbarkeit über massenhaft infizierte Rechner, TAILS als unveränderliches (Live-Betriebssystem) für die Recherche, das Bearbeiten und Veröffentlichen von sensiblen Dokumenten zu benutzen. TAILS hinterlässt bei richtiger Nutzung keine Spuren auf dem Rechner - eure Festplatte bleibt unberührt. Ein eventuell (auf Betriebssystemebene) eingeschleuster Schadcode kann sich bei einer Live-DVD oder einem schreibgeschützten Live-USB-Stick als TAILS-Start-Medium nicht „festsetzen“ und euch beim nächsten Rechnerstart nicht mehr behelligen.

Die Broschüre beschreibt zwei Nutzungsmodelle für TAILS:

a) TAILS als Live-System auf einem Rechner mit Internetzugang
TAILS verwendet beim Surfen, Mailen und Chatten die Anonymisierungssoftware „Tor“ und verändert zusätzlich die sogenannte „MAC-Adresse“ eures Netzwerkadapters - was das ist und wozu das von Nutzen ist, erklärt euch die Einführung dieser Anleitung. Hier lernt ihr den Umgang mit den von TAILS zur Verfügung gestellten Programmen. Die Verbindung zum Netz erledigt ein weitgehend automatisierter und einfach zu bedienender Netzwerk-Manager. Die Oberfläche sieht sehr ähnlich aus wie bei eurem normalen Betriebssystem auf der Festplatte - egal ob ihr Windows, Mac-OS X oder ein Linux-Betriebssystem nutzt, ihr werdet euch bei TAILS schnell zurecht finden.

b) TAILS als autarke „Quasi-Schreibmaschine“ auf einem Rechner, bei dem Festplatte(n), WLAN- und Bluetooth- Adapter ausgebaut sind.
Hier lernt ihr den Umgang mit besonders sensiblen Dokumenten. Das kann die Bearbeitung von Texten, Fotos, Tonaufnahmen oder die Erstellung ganzer Bücher sein. Hier darf nichts schief gehen. Deshalb raten wir in solchen Fällen zu einem Rechner mit beschränkten Fähigkeiten (keine Festplatte, keine Internetverbindung, kein WLAN, kein Bluetooth), der euch zudem nicht persönlich zugeordnet werden kann.

Diese Anleitung erhebt den Anspruch, auch für Computer-Nicht-Expert*innen verständlich und nützlich zu sein. Ihr bekommt sie im Info-/Buchladen eures Vertrauens oder online unter ***capulco.nadir.org***

fohlene Verwendung von Bitlocker eine ganz schlechte Alternative. Niemand sollte zum Schutz ihrer_seiner Daten einem Hersteller wie Microsoft vertrauen, von dem man weiß, dass er bereits aktiv mit der NSA zusammen arbeitet. Da empfiehlt es sich schon eher, die neue unvollständige TRUE-CRYPT Version nicht zu installieren, sondern 7.1a weiter zu verwenden bzw. auf andere Programme umzusteigen. Mit GNU-PG, Open/LibreSSL, LUKS und so weiter gibt es eine ganze Reihe von vertrauenswürdigen Bausteinen. Allerdings gibt es bisher nichts was vom Funktionsumfang vergleichbar ist und auf den verschiedenen Betriebssystemen läuft. TAILS beinhaltet z.B. eine graphische Benutzeroberfläche um mit LUKS ganze USB-Sticks, SD-Karten oder Festplatten zu verschlüsseln. Einzelne Container lassen sich damit aber nicht erstellen und außerdem funktioniert LUKS nur für Linuxbetriebssysteme. (Die empfohlene TAILS Broschüre beinhaltet eine ausführliche Anleitung.)

Bei allen berechtigten Bedenken gegen TRUE-CRYPT ist noch anzumerken, dass es immer noch weit besser ist, als nicht zu verschlüsseln. z.B. hat der Berliner EA vor kurzem veröffentlicht, dass die Beschuldigten in einem mittlerweile eingestellten Verfahren wegen Angriffen auf Jobcenter Anfang Mai 2013, mittlerweile ihre zwischenzeitlich beschlagnahmten Datenträger wieder bekommen haben. Laut Akten war das Berliner LKA nicht in der Lage die TRUE-CRYPT Verschlüsselung zu knacken. Das hebt die Bedenken natürlich nicht auf und sagt auch nichts darüber aus was Geheimdienste drauf haben.

Erfolgreicher Angriff auf TOR-Anonymisierung

Dass die Anonymität, die TOR gewährt, angreifbar ist, wurde ja bereits in dem Artikel im autonomen Blättchen Nr. 15 ausführlich dargestellt. Nun gibt es erneut Beweise, dass dies auch geschieht und anscheinend einfacher ist als angenommen. Die Betreiber des Tor-Netzwerkes haben Anfang Juli 2014 eine Gruppe von Tor-Knoten entdeckt, die offenbar Nutzer_innen des Dienstes de-anonymisiert haben. Die Knoten waren vom 30. Januar bis zum 4. Juli aktiv und wurden jetzt stillgelegt. Unbekannte haben den bisherigen Erkenntnissen zufolge eine große Zahl von TOR-Knoten in das offene TOR-Netzwerk eingebracht. Auf Grund

ihrer Stabilität und guten Anbindung erhielten sie dort relativ schnell den Status „geeignet als Entry Guard“ (Guard) und „geeignet als Hidden Service Directory“ (HSDir). Damit hatten die Angreifer zwei kritische Positionen des TOR-Netzes besetzt; sie stellten zumindest zeitweise etwa 6,4 Prozent der Knoten. Auf Grund der TOR-internen Rotation ergab sich daraus eine beträchtliche Wahrscheinlichkeit, dass TOR-Nutzer_innen irgendwann mit diesen Trojaner-Knoten in Verbindung kamen. Ich erspare euch hier technische Details. Fest steht: Die Angreifer_innen konnten nicht die eigentlichen Nutzdaten mitlesen, sondern nur sehen wer welche Dienste anfragt. Die Art des Angriffs hatte aber zur Folge, dass auch alle anderen Betreiber_innen von TOR-Eingangsknoten IP-Adressen mit Diensten korrelieren konnten. Somit steht zu befürchten, dass über die Angreifer_innen hinaus weitere interessierte Parteien in den Besitz solcher Informationen gelangt sind.

Schon kurz vor diesem Angriff wurde bekannt, dass es möglicherweise eine Lücke im Dienst gibt. Worin genau sie besteht, ist aber noch nicht publik – Anwälte der Carnegie Mellon Universität haben den dazu angekündigten Vortrag bei der Hackerkonferenz Black Hat verhindert. Zwei Forscher der Uni wollten darüber referieren, wie jede_r mit relativ kleinem Budget TOR-Nutzer_innen enttarnen kann. Das TOR-Projekt weiß offenbar von dem Problem, vermutet einen Zusammenhang mit dem geschilderten aufgeflogenen Angriff und arbeitet an einer Lösung.
Dass das TOR-Netz für Geheimdienste von großem Interesse ist, zeigt auch eine weitere Meldung. Das russische Innenministerium hat eine Prämie von 3,9 Millionen Rubel (rund 83.000 Euro) für eine Technik ausgelobt, mit der Nutzer_innen des Anonymisierungs-Dienstes enttarnt werden können. Demnach können noch bis zum 13. August Vorschläge eingereicht werden, am 20. August soll ein_ Gewinner_in bekannt gegeben werden.

Aus meiner Sicht bleibt die Einschätzung aus dem Blättchen Nr. 15, trotz dieser Meldungen, aktuell. Das TOR-Netzwerk stellt auch für Geheimdienste eine Herausforderung da und es ist deshalb sinnvoll den Dienst zu nutzen, allerdings hat sich einmal mehr gezeigt, dass es angreifbar ist. Je nach Möglichkeit und Sicherheitsbedürfnis sind weitere Schutzmaßnahmen zu ergreifen. Im Blättchen Nr. 15 und der empfohlenen Broschüre zu TAILS sind einige erklärt. Bessere Anonymisierungswerkzeuge gibt es bisher nicht – es bleibt also nichts anderes übrig als die eigene Arbeitsweise ständig zu überprüfen, Nachrichten und Technikforen auf Hinweisen zu neuen Angriffsmethoden zu durchforsten und/oder wo es geht darauf zu verzichten Computer (mit Internetanschluss) zu verwenden. Zu den aktuellen Angriffen kann man sich detailliert auf der Homepage bzw. dem Blog des TOR-Projektes informieren (englisch). ***torproject.org*** und ***blog.torproject.org***. Deutschsprachige Nachrichten dazu findet man z.B. auf ***heise.de*** oder ***golem.de***

Daten sicher löschen - heißt Datenträger vernichten!

In dem Artikel im Blättchen Nr. 15 wird beschrieben wie Datenträger zu überschreiben sind. Die dort beschriebenen Programme und Methoden und auch die Grenzen bzw. Problem gelten ausschließlich für (alte) magnetische Festplatten. **Leider führen diese Software-Techniken, die einzelne Bereiche eines Datenträgers mit verschiedenen Datenmustern mehrfach überschreiben, z.B. bei USB-Sticks, nicht zum gewünschten Ergebnis!**

Physikalische Eigenschaften der Datenträgers erlauben es, den ehemaligen Inhalt einer Überschriebenen Speicherstelle zu rekonstruieren. Es geht dabei weniger um die Anzahl der Überschreibvorgänge als darum, dass sogenannte Flash-Speichermedien, wie z.B. USB-Sticks, SD-Karten, Compact-Flash-Karten und die neueren SSD-Festplatten (Solid-State-Disks) intern umkopieren (außerhalb der Kontrolle der_des Anwender_in). Dies geschieht wegen der besonders hohen Fehleranfälligkeit des Speichers und ist kein Ausnahmefall, sondern die Regel. Eine Überschreibeprozedur zum „sicheren“ Löschen einzelner Dateien „erwischt“ dann nur eine von mehreren Kopien. Eine der neueren Forschungsarbeiten bescheinigt sämtlichen Software-Löschtechniken, dass sie angewendet auf Flash-Speicher selbst beim Überschreiben des gesamten Speichermediums nur unzuverlässig funktionieren. **Das sichere Löschen von einzelnen Dateien gelang sogar mit keinem der getesteten Programme!**

Wenn Daten dauerhaft gesichert werden müssen, dann sollte es ein externer und komplett verschlüsselter Datenträger sein. Ein sicher verschlüsselter Datenträger ist der beste Schutz gegen (lesbare) Überreste. Sämtliche Löschprogramme wie z.B. WIPE, ERASER usw. sind zusätzlich nur brauchbar beim Überschreiben des gesamten Datenträgers. Datenträger mit hochsensiblem Inhalt müssen zusätzlich zerstört werden.

USB-Geräte können die Kontrolle über deinen Rechner übernehmen

Mit USB-Geräten gibt es allerdings, wie Ende Juli 2014 bekannt wurde, ein weiteres gravierendes Problem. Forscher_innen des Berliner Security Research Labs (SRLabs) haben es geschafft, die Firmware von USB-Microcontrollern nachzubauen und zu manipulieren. Diese Firmware kommt vom Hersteller und steuert die Funktionen der Geräte. In jedem USB-Gerät steckt ein Controller-Chip, der – vereinfacht ausgedrückt – zwischen dem USB-Gerät und dem PC vermittelt.

Dieser Chip (Microcontroller) arbeitet mit einer Firmware, die ihm sagt, was für ein Gerät er steuert – das kann ein USB-Stick sein, ein Smartphone, eine Tastatur, eine Webcam und vieles mehr. Bei der Angriffsmethode wird nun diese Firmware manipuliert. Das ist recht einfach möglich, da die meisten Controller gegen solche Manipulationen nicht geschützt sind. Sie werden für viele verschiedene Geräte genutzt und müssen deshalb leicht umprogrammiert werden können.

Die Forscher_innen schreiben: „*Wir nutzen die grundlegene Art aus, wie USB aufgebaut ist. Diese Lücken können nicht geschlossen werden. USB-Geräte - nicht nur Sticks - sind ein Infektionsrisiko für jeden Nutzer. Da einmal angegriffene Computer wiederum andere USB-Geräte infizieren können, kann sich ein solcher Angriff durchaus schnell verbreiten.*“

Ein manipuliertes USB-Gerät gibt sich dann einfach als etwas anderes aus, als es ist. Beispielsweise täuscht ein am PC angeschlossener USB-Stick vor, er sei eine Tastatur. Durch Tastatureingaben im Hintergrund führt er dann Befehle aus und installiert einen Trojaner, aktiviert die Webcam oder macht Screenshots vom Bildschirminhalt. Oder er protokolliert alle Tastatureingaben der_des Nutzer_in und kommt so an wichtige Passwörter. Weitere Beispiele gibt es viele: USB-Geräte können sich als Netzwerkkarte ausgeben und so allen Internetverkehr des PC abfangen oder ihn auf gefälschte Webseiten lenken; Oder einen Virus laden, mit dem das Betriebssystem noch während des Startens infiziert wird. Die_der Nutzer_in merkt von all dem nichts. Der USB-Stick kann vollkommen leer sein, es gibt keine verseuchte Datei, die ein Antivirenprogramm entdecken könne. Das Computer-Betriebssystem nimmt den Angriff nicht als Softwareattacke wahr, sondern glaubt, nur Tastenbefehle einer neuen Tastatur zu verarbeiten. So haben die Angreifer_innen den selben Zugriff wie der Nutzer_innen vor Ort. Die Methode ist auch deshalb so gefährlich wie erfolgversprechend, weil sie auf Windows-, Linux- und Apple-Rechnern gleichermaßen funktioniert. Die Schlussfolgerung der Forscher_innen ist drastisch: USB-Sticks sind nicht mehr vertrauenswürdig, wenn sie je mit einem unsicheren Computer in Kontakt gekommen sind. Damit sind die Datenträger zum schnellen Dateitausch praktisch ungeeignet.

Eine Lösung des Problems ist derzeit nicht in Sicht. Der gesamte USB-Standard müsste geändert und um Schutzvorkehrungen erweitert werden. Das wird aber zehn Jahre dauern, da die Standards von vielen Beteiligten entwickelt und beschlossen werden müssen. Auch einen Schutz gibt es nicht wirklich – Antiviren-Programme haben keinen Zugriff auf die Firmware von USB-Geräten. Um die Manipulation zu bemerken müsste man jeden Microcontroller jedes USB-Gerätes im Labor aufwendig untersuchen. Nutzer_innen können lediglich auf USB-Sticks verzichten und stattdessen SD-Karten verwenden. Diese können sich nicht als etwas anderes ausgeben. Bei anderen USB-Geräten gibt es bislang keine Alternativen.

Wir können daraus zwei Schlüsse ziehen: 1. USB-Sticks und andere Geräte nicht zwischen Rechnern mit verschiedenen Status hin- und hertragen. Wenn man, wie in der TAILS-Broschüre empfohlen, für besonders sensible Daten eine Rechner ohne Internetanschluss verwendet, dann macht es Sinn alle USB-Geräte, die man an einem solchen Rechner verwendet, nie an andere Rechner anzuschließen. 2. Für den Datentransfer zwischen verschiedenen Rechnern oder zum Booten eines Livebetriebssystems wie TAILS auf SD-Karten (natürlich nicht mit einem USB-Lesegerät/Cardreader) oder CD/DVD zurückgreifen.

Schluss

Was soll man dazu noch sagen? Klingt alles reichlich beschissen. Ansonsten steht das Wesentliche schon in der Einleitung. Was denkt ihr dazu?

anonym

Diese Broschüre ist der Versuch einige unterschiedliche Beiträge zu sammeln, die sich mit der Thematik der Anonymität auseinandersetzen. Der im Vordergrund stehende Streitpunkt dreht sich um die Frage, ob wir uns als Anarchisten, die angreifen und eine schnellst mögliche Umwälzung der bestehenden Gesellschaftsordnung herbeiführen wollen, zu den diffusen, wilden und unterschiedlichen Attacken, die wir praktizieren, bekennen wollen und unsere Motivationen und Ideen per Kommuniqués kommunizieren wollen. Man könnte diese Frage als nebensächlich betrachten, mir erscheint es allerdings so als ob eine Diskussion dieser Frage erst deutlich macht, wie wir kämpfen und kämpfen wollen und so von großer Bedeutung und immer von Aktualität ist. In diesem Sinne soll die Initiative diese Texte zusammenzustellen nicht eine Trennlinie zwischen vermeintlich unterschiedlichen anarchistischen Lagern ziehen, sondern viel eher Diskussionen anstoßen, die sich mit den angesprochenen Ideen und Kritiken beschäftigen und Verwirrungen aus dem Weg räumen.

editionirreversibel.noblogs.org
edition-irreversibel@riseup.net