FESTPLATTEN-VERSCHLÜSSELUNG

Es kommt immer wieder vor und gehört mittlerweile auch zur gängigen Praxis der Bullen, dass bei Hausdurchsuchungen Computer und Datenträger beschlagnahmt werden. Beispiele dafür sind die Ermittlungen gegen die vermeintlich existierende 'militante gruppe' in Deutschland, die Repression gegen die TierschützerInnen in Österreich seit 2008 oder die Hausdurchsuchungen im Vorfeld der Proteste gegen den Naziaufmarsch in Dresden im Februar 2010. Da heutzutage viel Kommunikation, Recherche und Arbeit mithilfe von Computern passiert, können die Repressionsbehörden einen Großteil des Lebens der BenutzerInnen rekonstruieren und ausforschen. Dies ist eine Gefahr für unsere politische Arbeit und unsere Strukturen.

Unverschlüsselte Festplatten sind gefährlich

Bei einer Standardinstallation werden bei den meisten Betriebssystemen die Daten unverschlüsselt auf die Festplatte geschrieben. Wenn die Bullen bei euch auftauchen und euren Computer mitnehen, können sie die Festplatte ausbauen und in einen anderen Computer einbauen und sich alle Daten ansehen, die auf dem Computer abgespeichert sind. Und das sind einerseits alle Dokumente die ihr abgespeichert habt (Flyer, Logos, Texte, Fotos ...) und andererseits auch Protokolle von Chatsitzungen, der Verlauf eures Browsers (also wann ihr welche Internetseiten angesurft habt) oder vielleicht auch alle eure Emails. Heutzutage werden bei der Arbeit im Netz so viele Daten auf eurem Computer zwischengespeichert (gecached), dass kein Mensch darüber einen Überblick haben kann. Bei AktivistInnen, die so unvorsichtig sind und Passwörter unverschlüsselt abspeichern, kann die Beschlagnahmung von Computern natürlich noch weitreichendere Folgen haben.

Hilft das Löschen von Daten?

Das Löschen solcher Daten hilft nichts. Wenn ihr eine Datei in den, auf den meisten Systemen vorhandenen, Papierkorb schiebt, ist sie nicht gelöscht sondern nur verschoben. Wenn ihr eine Datei wirklich löscht, dann ist die Datei auch nicht verloren, sondern es wird nur in einer Tabelle auf dem Dateisystem der Ort wo sich die Daten befinden als leer markiert. Es gibt genug Programme, mit denen diese Dateien wieder hergestellt werden können. Es gibt natürlich die Möglichkeit, den Speicherbereich, wo die ursprüngliche Datei lag, mit anderen Daten zu überschreiben. Besonders gründliche Programme machen das bis 35 mal mit zufälligen Daten. Jedoch wird dabei nur der Teil der Festplatte überschrieben, wo die Datei abgespeichert war- viele Programme speichern temporäre Sicherheitskopien der bearbeiteten Daten irgendwo anders ab. Der Defense Security Service des US-Verteidigungsministeriums weist in seinem Sicherheitsstandard von 2007 Software-Methoden zur Löschung von magnetischen Medien (also Festplatten, Disketten) als unzureichend aus. Als "streng geheim" eingestufte magnetische Datenträger müssen physisch zerstört werden.

Verschlüsselung ist ein Muss!

Das Verschlüsseln von Festplatten ist mittlerweile nicht mehr sehr aufwendig, jedoch von Betriebssystem zu Betriebssystem unterschiedlich. Meistens ist es so, dass die Festplatte beim Start des Systems mit einem Passwort 'freigeschaltet' wird, also der Datenstrom wird entschlüsselt. Bei jedem Schreibvorgang wird dann verschlüsselt, bei jedem Lesevorgang wird entschlüsselt. Im Zuge der Arbeit mit dem System merkt ihr nicht dass es verschlüsselt ist. Ein kleiner Nachteil ist jedoch, dass die Schreib- und Lesezugriffe ein wenig langsamer sind, als bei unverschlüsselten Festplatten. Dies liegt daran, dass beim Schreiben oder beim Lesen die Daten jedesmal durch den Prozessor ver- oder entschlüsselt werden müssen und das ist ein Rechenaufwand. Bei normaler Arbeit (mit Dokumenten, Internetsurfen, Layout, unaufwendige Bildbearbeitung) ist keine Verlangsamung zu spüren.
Festplattenverschlüsselung wirkt nur, wenn der Computer ausgeschaltet ist! Wenn der Computer eingeschaltet ist und die Bullen setzen sich davor, dann hilft die ganze Verschlüsselung nichts. Auch die Passwortabfrage von Bildschirmschonern kann umgangen werden. Also bevor sich jemand am Rechner zu schaffen macht am besten Netzstecker ziehen, bei einem Notebook zusätzlich den Akku entfernen.

Partitionen

Partitionen sind Teile einer Festplatte. Ihr müsst für euer Betriebssystem nicht die ganze Festplatte verwenden, sondern könnt diese unterteilen. So ist es zum Beispiel möglich, auf einem Teil Linux und auf dem anderen Teil Windows installiert zu haben. Oder ihr habt zusätzlich noch einen Teil der nur für Daten ist, die ihr sowohl unter Linux als auch unter Windows braucht.

Installation

Bei aktuellen Linuxdistributionen ist es bei der Installation schon möglich, die Verschlüsselung des ganzen Systems zu aktivieren. Da gebt ihr dann einfach ein Passwort ein, das dann jedes mal im Laufe des Systemstarts abgefragt wird. Die dabei verwendete Software heist dm-crypt und wird bei vielen Distributionen mit der Erweiterung LUKS eingesetzt. Bei Ubuntu gibt es auch noch die Möglichkeit mit encryptfs nur das eigene Verzeichnis zu verschlüsseln. Wie wir jedoch wissen, sollte das ganze System verschlüsselt werden. Bei Windows oder OS X müsst ihr auf die Software TrueCrypt zurückgreifen. Der Code von TrueCrypt ist zwar offen einsehbar und es ist gratis, jedoch ist die Software selber nicht Frei im Sinne der Free Software Foundation und ist deswegen bei vielen Linux Distributionen nicht dabei. Die Software TrueCrypt gibt es auch für Linux, jedoch ist es damit nicht möglich, unter Linux das ganze System zu verschlüsseln und die Installation ist auch nicht so einfach.
Die Linux Software dm-crypt mit der LUKS-Erweiterung kann übrigens mehrere Passwörter verwalten als auch auch mit Schlüsseldateien arbeiten. Dass kann sinnvoll sein, wenn mensch einen USB-Stick mit einer Schlüsseldatei zum 'aufschließen' von Festplatten verwenden will.

Auf Reisen

Wenn ihr eine Reise tut, dann informiert euch im Vorhinein über die Rechtslage der Länder in oder durch die ihr reist. Es ist nicht überall erlaubt, Festplatten zu verschlüsseln und in manchen Ländern ist es erlaubt euch rechtlich oder durch Folter zu zwingen, das Passwort herauszugeben (in der Kryptoanalyse wird das als 'Rubber-Hose Cryptoanalyse', also Analyse von Verschlüsselung mit dem Gummi-Schlauch bezeichnet, das bezieht sich auf das Auspeitschen mit Gummischläuchen um ans Passwort zu kommen). Manchmal kann es auch sinnvoll sein, einfach gar keine Daten mitzunehmen und sich dann die Daten per Post auf einer verschlüsselten Platte zuschicken zu lassen oder die Daten übers Netz nachzuladen.

Glaubhafte Abstreitbarkeit

Aufgrund der Repression ist es manchmal auch sinnvoll, glaubhaft versichern zu können, dass es keine wichtigen Daten gibt. Manche Umsetzungen von Verschlüsselung bieten die Möglichkeit, verschlüsselte Teile einer Festplatte zu 'verstecken', so dass sie für Außenstehende nicht als solches erkannt werden können. Sinnvoll kann es auch sein, zwei verschlüsselte Partitionen auf einer Festplatte zu haben, eine 'offizielle' und eine 'versteckte'- von der offiziellen kann dann im Falle von Repression das Passwort hergegeben werden, die andere bleibt jedoch versteckt.

Attacken auf Verschlüsselung

Verschlüsselung ist ein großes Thema in Kryptographie und Informatik, dementsprechend wird immer wieder versucht sie zu umgehen. Auch wenn die ganze Festplatte verschlüsselt ist, ist der Arbeitsspeicher nicht verschlüsselt und daraus kann möglicherweise auch im ausgeschalteten Zustand noch Information gewonnen werden. Natürlich sind auch Keylogger gefährlich, sowohl Hardware Keylogger, als auch Software Keylogger (zum Beispiel im BIOS, der untersten Systemebene der meisten Computer, sozusagen die Firmware). Eine weitere Gefahr stellt auch Schadsoftware auf Betriebssystemebene dar, also Manipulationen an Treibern oder Modulen, die zum Ziel haben, die Passwörter herauszufinden.

Oder gleich ohne Festplatte?

Eine Möglichkeit, wie ihr sicherlich keine Spuren auf einem Computer hinterlasst, ist es, ohne Festplatten zu arbeiten. Es gibt schon seit einigen Jahren Betriebssysteme auf CD, sogenannte Live-CDs. Dabei werden die Betriebssystemdaten von der CD gelesen und die Arbeit wird vollkommen im Arbeitsspeicher vollzogen. Bei einer solchen Lösung ist es am geschicktesten, die Festplatte abzustecken oder ganz auszubauen, damit nicht versehentlich Daten darauf abgespeichert werden. Der Nachteil dieser Methode ist die Langsamkeit, da von einem CD Laufwerk nicht so schnell gelesen werden kann, wie von einer Festplatte. Eine Empfehlenswerte Live CD ist der Ubuntu Privacy Remix (siehe Link am Ende des Flyers), eine weitere wäre The (Amnesic) Incognito Live System, das noch einen Schritt weitergeht und alle ausgehenden Netzwerkverbindungen über das Anonymisierungsnetzwerk TOR schickt.

TrueCrypt Software
http://www.truecrypt.org
Website des Ubuntu Privacy Remixes
https://www.privacy-cd.org
The (Amnesic) Incognito Live System
https://amnesia.boum.org/

tear the system down - bit. by. bit. mailto:bitbybit@riseup.net
technologie in linksradikalen kontexten irc://irc.indymedia.org/#bitbybit