AUSZUG AUS:
LEIPZIGER KAMERA - INITIATIVE GEGEN ÜBERWACHUNG (HRSG.)
KONTROLLVERLUSTE
INTERVENTIONEN GEGEN ÜBERWACHUNG
256 SEITEN | 18 EUR [D] | ISBN 978-3-89771-491-5
UNRAST VERLAG, MÜNSTER, MÄRZ 2009
HTTP://WWW.UNRAST-VERLAG.DE/UNRAST,2,308,7.HTML

SCHRITTE ZU EINEM SICHER(ER)EN COMPUTERSYSTEM

VON COMPUTERGRUPPE H48

1. EINLEITUNG

Die folgenden Hinweise sind dazu gedacht, ein nach unserem Wissen möglichst abgesichertes Computersystem zu basteln und darüber hinaus auf eine Sensibilisierung beim Umgang mit persönlichen Daten hinzuwirken. Oppositionelle Aktivistinnen sehen sich mit einer Vielzahl von Überwachungs-, Kontroll- und Repressionsmaßnahmen konfrontiert. Eine Möglichkeit, mit den entstehenden Sicherheitsprobleme umzugehen, liegt sicherlich im Rückgriff auf ›konventionelle‹ Medien: also persönliche Treffen, gemeinsame Briefkästen etc. Aber kaum jemand möchte sich den technischen Errungenschaften vollkommen verschließen. Allerdings kann bereits das Verschlüsseln von E-Mails als verdächtig wahrgenommen werden, da dies bisher nur eine geringe Anzahl von Leuten gewohnheitsmäßig praktiziert. Erhöht sich die Anzahl derjenigen, die Verschlüsselung anwenden, so kann dieses Verdachtsmoment nicht mehr so leicht konstruiert werden, und diejenigen, die wirklich ›Verschlüsselnswertes‹ zu verschicken haben, werden geschützt. Eine Verbesserung der Sicherheit im Zusammenhang mit elektronischer Kommunikation ist in vielerlei Hinsicht also kein individuelles Problem, sondern lediglich mit einer kollektiven Anstrengung zu erreichen. Aus dieser Maßgabe erklärt sich auch das Selbstverständnis unserer kleinen, noch im Aufbau befindlichen Tech-Gruppe: Wir bieten für Laien verständliche Hilfestellung – vor allem bei sicherheitsrelevanten Themen. In diesem Text finden sich keine detaillierten Anleitungen, sondern lediglich Anregungen, was alles verbessert werden könnte. Anleitungen und *HowTos* gibt es zuhauf im Internet, und im Zweifelsfalle bietet es sich ohnehin an, eine Person hinzuzuziehen, die bereits über Erfahrung im Umgang mit der Technik verfügt.

2. BEDROHUNGSSZENARIO

MITLESEN VON E-MAILS

Eine E-Mail passiert auf ihrem Weg zu ihrer Empfängerin eine Vielzahl von Servern und Routern im Internet. An jeder dieser Stellen ist es ein Leichtes, Kopien anzufertigen oder die Inhalte der E-Mails zu manipulieren. Dagegen hilft das Verschlüsseln und Signieren von E-Mails.

SURFEN IM NETZ

Bei jedem Abruf einer Seite im Internet wird die persönliche IP-Adresse übermittelt, die wiederum an die Anschlussinhaberin rückgebunden werden kann. Das ist vor allem datenschutzrechtlich relevant, da so personenbezogene Datensätze angelegt werden können, z.B. für die Erstellung von Interessensprofilen zum Zwecke der ›zielgerichteten‹ Werbung. Aber auch sicherheitsrelevante Fragen können sich daraus ergeben: Das BKA benutzte beispielsweise nach der Verhaftung der mutmaßlichen Mitglieder der militanten gruppe (mg) die eigene Internetpräsenz als *honeypot* und überprüfte sämtliche IP-Adressen derjenigen, die die BKA-Informationsseite zur militanten gruppe (mg) besuchten. Auch bei mindestens einer der unter Verweis auf § 129a gerechtfertigten Hausdurchsuchungen vom 9. Mai 2007 wurden Aufzeichnungen des Surfverhaltens als ein Verdachtsmoment angeführt. Um sich zu schützen, bietet sich die Verwendung von Anonymisierungsdiensten an.

REKONSTRUKTION SOZIALER NETZWERKE

Die Bedeutung dieses Punktes wird häufig unterschätzt, doch dürfte es für Ermittlungsbehörden weit interessanter und einfacher sein, soziale Netzwerke und damit die Organisation politischer Bewegungen zu durchleuchten, als den Inhalt einzelner E-Mails zu durchforsten. Seit Einführung der Vorratsdatenspeicherung werden sämtliche ›Verbindungsdaten‹ gespeichert. Das ermöglicht den Behörden, E-Mail-Adressen bestimmten Personen zuzuordnen oder IP-Adressen zurückzuverfolgen. Sich dagegen zu wehren, ist kompliziert. Eine Möglichkeit ist die Verwendung von so genannten Remailern, die die Absenderin einer E-Mail verschleiern können. Außerdem können vertrauenswürdige E-Mail-Provider außerhalb Europas benutzt werden.

ONLINEDURCHSUCHUNG

Die so genannte ›Onlinedurchsuchung‹ oder auch der ›Bundestrojaner‹ sind ein medienträchtiges Thema geworden. Dennoch ist nicht viel über den Trojaner bekannt, was eine effektive Gegenwehr schwierig macht. Allgemein gesprochen handelt es sich um die heimliche Installation von Schadsoftware auf den Rechnern ›verdächtiger‹ Personen, mit der Festplatteninhalte und Passwörter ausspioniert werden sollen. Dagegen helfen kann eine allgemein sichere Konfiguration des Systems (Firewall, Virenscanner). Allerdings ist es für die Ermittlungsbehörden auch möglich, in Zusammenarbeit mit Service-Providern Downloads zu manipulieren und Firewall- und Virenscannerschutz zu umgehen.

HEIMLICHE MANIPULATION & HAUSDURCHSUCHUNG

Gegen das heimliche Eindringen und Manipulieren von Rechnersystemen durch Ermittlungsbehörden gibt es keinen Schutz. Selbst in ein komplett verschlüsseltes System können winzige Hardwareteile eingebaut werden, die als *keylogger* fungieren und Eingaben aufzeichnen, die über die Tastatur vorgenommen werden. Wird Hardware in einer ›normalen‹ Hausdurchsuchung beschlagnahmt, lassen sich die Inhalte durch verschlüsselte Festplatten schützen.

3. TECHNISCHE GEGENWEHR

WAHL DES BETRIEBSSYSTEMS

Computersicherheit fängt selbstredend bei der Wahl des Betriebssystems an und eine erste Empfehlung ist: Finger weg von Windows! Neben allen politischen, philosophischen oder pragmatischen Gründen, die gegen Windows sprechen (Monopolstellung, Gängelung durch *Digital Rights Management,* Anfälligkeit für Viren und Spyware, zentralistische Organisation usw.), gibt es eine Tatsache, die jede ernsthafte Auseinandersetzung mit Windows unter Sicherheitsaspekten verbietet: Windows ist nicht *quelloffen*. Grundsätzlich werden Programme zunächst in einer Programmiersprache verfasst, die menschenlesbar ist. Bevor ein Programm aber vom Computer verwendet werden kann, muss es in binäre Form, also quasi in ›Computersprache‹ übersetzt werden. Die eigentlichen Programmabläufe sind dann für den Menschen kaum mehr nachvollziehbar. Beim Ausführen von Windows kann alles Mögliche passieren: Der Media-Player telefoniert beispielsweise gern mal unbemerkt nach Hause, was sich wiederum nur über eine Firewall feststellen lässt. Was genau der Media-Player in diesen Momenten versendet, bleibt jedoch unklar: Es könnte sich um eine harmlose Aktualisierungsanfrage handeln, aber auch um das private Outlook-Adressbuch. Dasselbe gilt für alle anderen Programme, die lediglich im Binärformat vorliegen. Somit ist unter Sicherheitsgesichtspunkten die große Unbekannte Windows als Erstes aus der Gleichung zu eliminieren.

Im Unterschied zu Windows wird GNU/Linux und die freie Software stets zusammen mit dem Quellcode ausgeliefert. So kann weitgehend ausgeschlossen werden, dass ungewollte Funktionen implementiert sind. Auch so genannte *backdoors* (geheime Hintertürchen), durch die Programmiererinnen einer Software Zugang zum System erhalten können, sind unter GNU/Linux unwahrscheinlich. Darüber hinaus ist GNU/Linux robuster und weniger anfällig für Attacken von außen.

SYSTEMVERSCHLÜSSELUNG

Es ist mittlerweile sehr einfach, ein Computersystem nahezu komplett zu verschlüsseln: Debian und Ubuntu (beides GNU/Linux-Distributionen) bringen einen Installer mit, der einem alle Arbeit abnimmt. Für die Benutzung ergeben sich außer der Eingabe eines Passwortes keinerlei Änderungen. Die angewendete Verschlüsselung kann als sicher gelten. Unter Windows lässt sich eine Komplettverschlüsselung mittels der Software TrueCrypt realisieren. Für eine solche Verschlüsselung sprechen eine Reihe von Gründen. Angefangen mit dem Schutz der persönlichen Daten bei Verlust des Laptops (Benutzernamen-/Passwortabfrage beim Systemstart stellt keine Sicherheit der Daten dar!) bis hin zu bei einer Hausdurchsuchungen entwendeten Festplatten gibt es viele denkbare Szenarien. Aber Achtung: Während des Betriebs liegen alle Daten in entschlüsselter, also ungeschützter Form vor – Festplattenverschlüsselung schützt nicht vor Onlinedurchsuchungen oder ähnlichen Angriffen! Auch eine Teilverschlüsselung der Festplatte ist kaum ausreichend, die meisten Programme legen während des Betriebs Kopien in verschiedenen Bereichen der Festplatte an, z.B. im Auslagerungsspeicher. Selbst wenn diese zwischenzeitlichen Kopien automatisch gelöscht werden, lassen sie sich mit einfachen Methoden wieder rekonstruieren.

E-MAIL TEIL I: VERSCHLÜSSELN UND SIGNIEREN

Das Verschlüsseln und Signieren von E-Mails ist auf allen Systemen leicht umzusetzen. Die vermutlich am weitesten verbreitete Möglichkeit ist die Kombination aus Thunderbird als Mailclient, GnuPG

als Verschlüsselungssoftware und Enigmail als Plugin für Thunderbird. Auf jedem Server, den eine E-Mail auf ihrem Weg in die Inbox der Empfängerin passiert, kann sie mitgelesen oder manipuliert werden. Daher stellen sich bei der E-Mail-Kommunikation grundsätzlich zwei Probleme: Die Privatsphäre und die Authentizität.

Das Public-/Private-Key-Verfahren adressiert beide genannten Probleme: Wer verschlüsselte E-Mails senden und empfangen will, generiert sich auf dem heimischen Rechner ein Schlüsselpaar. Der öffentliche Schlüssel kann an alle verschickt werden. Der private Schlüssel ist zusätzlich mit einer Passphrase geschützt und befindet sich selbst in nochmals verschlüsselter Form auf der eigenen Festplatte.

Zur Verschlüsselung einer E-Mail wird der öffentliche Schlüssel der Kommunikationspartnerin benötigt. Mit diesem Schlüssel wird die Nachricht verschlüsselt; das Ergebnis ist ein unleserlicher Zahlen- und Buchstabensalat. Durch Eingabe der Passphrase wird die E-Mail entschlüsselt und erscheint im Klartext. Mit diesem Verfahren ist der Inhalt der Mail auf seiner Reise durchs Netz gut geschützt.

Um die Authentizität der E-Mail zu gewährleisten, wird im Prinzip dasselbe Verfahren verwendet, nur andersherum. Bevor die E-Mail verschickt wird, generiert das E-Mail-Programm aus dem Inhalt der Mail und dem privaten Schlüssel der Absenderin eine Prüfsumme, die beim Senden mitübermittelt wird. Das E-Mail-Programm der Empfängerin kann eine mathematische Beziehung zwischen dem Text der Mail, der Prüfsumme und dem öffentlichem Schlüssel überprüfen. Damit kann die Empfängerin feststellen, dass die E-Mail von der entsprechenden Kommunikationspartnerin kommt und am Inhalt der Mail nichts manipuliert wurde.

SICHERHEIT IM NETZ I: VIRENSCANNER, FIREWALLS & SCRIPTE

Wer mit Windows im Internet unterwegs ist, sollte in jedem Fall einen aktuellen Virenscanner (bspw. AntiVir) und eine Firewall-Software (bspw. ZoneAlarm) benutzen. Unter Linux ist beides nicht zwingend erforderlich, da Viren hier fast keine Rolle spielen. Die Sicherheitsarchitektur macht es Schadsoftware generell schwerer, und außerdem stellt Linux aufgrund seiner geringeren Verbreitung bisher kein attraktives Ziel dar. Da sich letzterer Punkt in Zukunft ändern könnte, gibt es auch für Linux Virenscanner-Software wie beispielsweise ClamAV. Anders sieht es aus mit so genannten Scripten. Viele Internetseiten benutzen beispielsweise die Programmiersprache Javascript. Diese Scripte werden zusammen mit der Internetseite heruntergeladen und auf dem heimischen Rechner ausgeführt. Im Prinzip sind Scripte also kleine Programme. Im schlimmsten Fall handelt es sich bei ihnen um Schadsoftware, die programmiert wurde, um Informationen zu gewinnen oder weitere Programme von außen nachzuladen. Es ist also generell ratsam, Scripte zu blockieren. Unter Firefox bietet es sich an, das Add-on NoScript zu installieren. Dieses blockiert zunächst alle Scripte und erlaubt das Ausführen des Programmcodes nur auf expliziten Wunsch. Es empfiehlt sich, Software nur aus vertrauenswürdigen Quellen zu beziehen und vor der Installation die Integrität der Software mittels eines *Prüfsummenalgorithmus* zu testen.

SICHERHEIT IM NETZ II: ANONYM SURFEN MIT TOR

TOR (*The Onion Router*) ermöglicht das anonyme Surfen im Netz. Die Metapher der ›Zwiebel‹ im Namen verweist auf das zugrunde liegende Funktionsprinzip. Wird mittels TOR im Internet gesurft, so werden die versandten Pakete durch mindestens drei verschiedene Router des TOR-Netzwerkes geschickt. Der Inhalt ist dabei mehrfach und für jeden beteiligten Router

einzeln verschlüsselt: Der erste Router kann nur die erste Verschlüsselungsschicht entschlüsseln, welche lediglich die nötigen Informationen enthält, um den zweiten Router anzusprechen. Dieser wiederum entschlüsselt die zweite Verschlüsselungsschicht und reicht die Information an den dritten Router weiter, welcher wiederum die Anfrage an den entsprechenden Internetserver weiterreicht. Für jeden der beteiligten Router ist also nur die Adresse des Routers, von dem die Anfrage kam, und die Adresse des Routers, an den die Nachfrage weitergeleitet wird, sichtbar. Auf dem Rückweg der Daten passiert dasselbe. Der Weg durch das TOR-Netzwerk hindurch wird dabei zufällig ermittelt. Auf diese Weise ist für Dritte nicht zu ermitteln, welche Information von wem abgerufen wird. Der oben erwähnte *honeypot* des BKA wäre z.B. wirkungslos. An der Gegenstelle der Kommunikation (z.B. ein Webserver) lässt sich lediglich feststellen, dass eine Verbindung über das TOR-Netzwerk aufgebaut wurde, nicht jedoch deren Urheberin.

Größtes Problem bei der Nutzung bleibt die Verringerung der Geschwindigkeit, ansonsten ist die Verwendung von TOR ziemlich einfach. Benötigt wird lediglich die TOR-Software und das Plugin Torbutton für den Firefox.

E-MAIL TEIL II: REKONSTRUKTION SOZIALER NETZWERKE

Für Ermittlungsbehörden ist es ein leichtes, soziale Netzwerke zu analysieren, indem der E-Mail-Verkehr überwacht wird. Dabei sind die Inhalte der Kommunikation vernachlässigbar. Die Vorratsdatenspeicherung schafft die Voraussetzungen für die Auswertung der Kommunikation der letzten sechs Monate eines ›verdächtigen‹ E-Mail-Accounts. Mittels eines einfachen Programms ließe sich so eine Datenbank sämtlicher Kontakte samt Häufigkeit der Kommunikation anlegen. Passiert dies zeitgleich mit mehreren miteinander in Kontakt stehenden Accounts, ergibt sich ein recht exaktes Bild darüber, wer wem etwas mitzuteilen hat. Was dies für Rückschlüsse auf die eigene politische Praxis ermöglicht, sei an dieser Stelle der Beurteilung der Leserin überlassen.

Sich gegen solche Angriffe zu wappnen, ist schwer. Als erste Maßnahme bietet es sich an, einen vertrauenswürdigen E-Mail-Provider außerhalb der EU zu wählen. Es kann zwar dennoch nicht ausgeschlossen werden, dass Ermittlungsbehörden an die entsprechenden Daten gelangen, jedoch ist der administrative Weg weitaus komplizierter. Kann auf die direkte Kommunikation via E-Mail nicht verzichtet werden, empfiehlt es sich, ein gesichertes Message-Board bei einem vertrauenswürdigen Provider im Ausland zu benutzen. Wird dieses Board ausschließlich über anonymisierte Verbindungen (TOR) angesurft und bleibt es lediglich einer kleinen Gruppe von Menschen bekannt, so ist die Kommunikation zu einem gewissen Grad vor ungewollten Zugriffen gesichert. Eine weitere Möglichkeit stellt die Verwendung von Remailern dar. Dies sind Programme, die die Absenderin einer E-Mail verbergen. Einige Remailer löschen lediglich alle Angaben zum Absender (bspw. Cypherpunk-Remailer), weswegen es unmöglich ist, auf diese E-Mails zu antworten. Andere Programme nutzen wie TOR das Prinzip des Onion-Routings (bspw. Mixmaster-Remailer), um Anonymität herzustellen. Bei diesen ist es möglich, Antworten auf gesendete Nachrichten zu erhalten und dennoch einen hohen Grad an Anonymität sicherzustellen. Allerdings ist die Verwendung von Remailern mit der derzeit zur Verfügung stehenden Software nicht trivial und erfordert gewisse Erfahrung im Umgang mit der Materie.

4. SCHLUSS

Die meisten der hier vorgeschlagenen Maßnahmen lassen sich mit entsprechender Hilfe innerhalb eines Nachmittags in die Tat umsetzen. Das Entscheidende folgt allerdings danach: der überlegte Umgang mit aller elektronischen

Kommunikation. Denn bei allen technischen Mitteln bleibt eine mögliche Schwachstelle immer auch die Nutzerin selbst. Vielleicht hilft es, sich stets zu vergegenwärtigen, dass das Internet und E-Mail nicht einfach nur ein tolles und einfaches Kommunikationsmedium sind. Sie stellen gleichzeitig auch ein Kontroll- und Überwachungssystem dar. Gegenwehr kann daher nur eine kollektive Aufgabe sein. Aufmerksamkeit ist generell dann geboten, wenn Daten übermittelt werden, die es Außenstehenden (theoretisch) ermöglichen, Verbindungen zwischen sonst isoliert nebeneinanderstehenden Datensätzen herzustellen. Anonymisierungssoftware oder Remailer zielen deshalb darauf ab, solche Verbindungen zu erschweren. Bei aller technischer Umsicht sei noch auf die notwendige Sensibilität im Umgang mit den privater Daten, beispielsweise auf community-websites wie Facebook oder studiVZ hingewiesen.

Auch das planvolle Sammeln großer Datenmengen (*Datamining*) oder das massenhafte Auswerten von Suchanfragen seitens der Suchmaschinenanbieter (Google) sollte stets bedacht werden, ebenso wie jene reale Welt jenseits des Internets, wo sich durch biometrische Verfahren oder RFID-Chips ein neues Netz der Kontrolle ausbreitet. All diese Veränderungen vollziehen sich auf dem scheinbar neutralen Gebiet technischen Fortschritts. Die Herausforderung besteht darin, diese Entwicklungen zu verstehen, streitbar zu machen und unter Umständen auch zu bekämpfen, und zwar ohne in einseitige Dämonisierung zu verfallen, die die feststellbaren emanzipatorischen Potentiale leugnete. Und ebenso sollte die Eingebundenheit und die Technisierung des persönlichen Alltags Gegenstand kritischer Reflexion bleiben.

AUTOR _ INNEN

Die Computergruppe h48 (https://computergruppe.h48.de) beschäftigt sich mit Themen aus der Schnittmenge linker Politik und Telekommunikation. Sie arbeitet praktisch und hilft Gruppen und Einzelpersonen bei sicherheitstechnischen Problemen.

LINKS

■ **Software-Links** ■ debian.org: Eine universell einsetzbare Linux-Distribution. ■ ubuntu.org: Eine besonders für Desktop-Rechner optimierte Linux-Distribution. ■ mozilla-europe.org/de/products/thunderbird: Der Thunderbird-Mailclient. ■ gnupg.org: Der GNUPrivacy Guard. Standardverschlüsselungssoftware unter Linux. ■ torproject.org: The Onion Router zum anonymen Surfen im Netz. ■ truecrypt.org: Die plattformübergreifend funktionsfähige Verschlüsselungssoftware. ■ clamav.net: ClamAV-Virenscanner für Linux. ■ **Links zur dunklen Seite der Macht** ■ tinyurl.com/5c8bko, tinyurl.com/5bc5on, tinyurl.com/5w4sdu, tinyurl.com/6xyy9v: Die Seiten der Bundesnetzagentur mit den wichtigsten Infos zur Vorratsdatenspeicherung. ■ netlaw.de/gesetze/tkg.htm: Hier findet sich das Telekommunikationsgesetz (TKG), in dem auch die Vorratsdatenspeicherung festgeschrieben ist. ■ **Eher technische Links zum Weiterlesen** ■ hp.kairaven.de: Eine Vielzahl von Anleitungen und Artikel rund um Privatsphäre und Sicherheit. ■ andrebacard.com/remail.html: Die Remailer-FAQ (englisch). ■ wiki.ubuntuusers.de: Großes Wiki rund um Ubuntu-Linux. Erste Adresse für allerlei technische Anleitungen. ■ help.riseup.net/security/measures: »Simple Measures for Email Security« bei riseup.net (englisch).

ANMERKUNGEN

Ein *honeypot*, zu deutsch ›Honigtopf‹, bezeichnet eine Falle. So sollen beispielsweise durch ein absichtlich unsicher konfiguriertes System Angreiferinnen angezogen werden (wie Insekten vom Honig), um diesen auf die Schliche zu kommen.

Freie Software bezeichnet nach der Definition des GNU-Projektes Software, die von den Nutzerinnen für jeden Zweck benutzt und den eigenen Ansprüche angepasst werden kann. Des Weiteren sind Kopien von Freier Software ausdrücklich erlaubt, sodass man seiner Nächsten weiterhelfen kann, das Programm zu verbessern. Die Verbesserungen können der Öffentlichkeit zur Verfügung gestellt werden, damit die ganze Gemeinschaft von ihnen profitiert. Der Zugang zum Quellcode ist dafür Voraussetzung.

Der Begriff *freeware* bezieht sich dagegen lediglich darauf, das die betreffende Software kostenlos angeboten wird.

Ein *Prüfsummenalgorithmus* (englisch: *checksum*) ist ein mathematisches Verfahren, mit dem die Integrität einer Datei überprüft werden kann. Dabei berechnet ein Algorithmus eine Prüfsumme von einer beliebigen Datei. Sollte die Datei manipuliert worden sein, würde sich auch diese Prüfsumme verändern. Daher finden sich auf vielen Downloadseiten neben den eigentlichen Downloads auch Prüfsummen, mittels derer die Dateien nach dem Download nochmals überprüft werden können.

Bei der *PGP-Verschlüsselung* wird ein Schlüsselpaar verwendet. Dies besteht aus einem öffentlichen und einem privaten Schlüssel, die sozusagen ineinander greifen. Nachrichten, die mittels des öffentlichen Schlüssels verschlüsselt wurden, können nur unter Zuhilfenahme des privaten Schlüssels wieder entschlüsselt werden.

Eine *Signatur* ist im Kontext von E-mail-Verschlüsselung mittels GnuPG eine Prüfsumme, die die Authentizität einer Nachricht sicherstellt. Die Senderin einer E-Mail generiert mittels des privaten Schlüssels und des Inhalts der geschriebenen Mail eine Prüfsumme, die an die Empfängerinnen mitübermittelt wird. Die Empfängerinnen können mittels des öffentlichen Schlüssels der Senderin überprüfen, dass der Inhalt der Mail nicht manipuliert wurde.