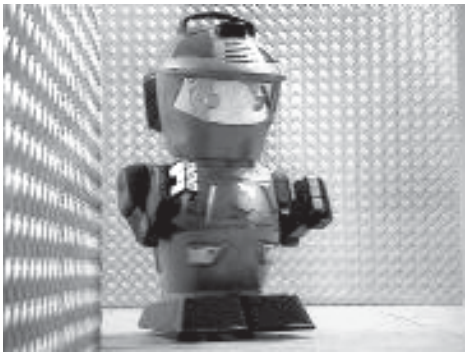
Sicher durchs Netz

Tipps für den Umgang mit Computersicherheit und Internetüberwachung

www.interkomm.tk



Sicher durchs Netz?

Stell dir vor, dein Telefon wird vom Staat abgehört - ohne dass ein formeller richterlicher Beschluss notwendig wäre und irgend jemand je davon erfährt. Stell dir außerdem vor, alle deine Briefe werden vom Verfassungsschutz aufgerissen und gelesen. Und stell dir schließlich vor, dass die Polizei unbemerkt in deine Wohnung eindringen und dort deine Unterlagen durchwühlen darf.
Was sich auf den ersten Blick nach einer Szene aus einem orwellschen Science-Fiction-Roman anhört ist bereits zum größten Teil Wirklichkeit - zumindest wenn es um die elektronische Kommunikation geht.
Anhand der Verbindungsdaten - Stichwort „Vorratsdatenspeicherung" - kann nachvollzogen werden, wer zu welchem Zeitpunkt welche Internetseiten aufruft. Denn das Internet ist keineswegs anonym, sondern dein Computer kann bis zur Telefonbuchse zurückverfolgt werden.
Die aktuelle Diskussion über den legalen Einsatz von staatlichen „Trojanern" (Spionagesoftware, die den Computer wie ein Computervirus infizieren und ausspionieren soll) lässt auch befürchten, dass ungesicherte Computer bald so zugänglich sind wie eine Wohnung mit offener Haustür.
Seit Januar 2005 haben die staatlichen Repressionsorgane außerdem die Möglichkeit, auf die kompletten E-Mail-Daten bei deinem E-Mail-Provider zuzugreifen. Sie können so verfolgen, wer mit wem kommuniziert und was die Kommunikationsteilnehmer sich mitzuteilen haben. Und wenn wir mal ehrlich sind, kann das für den Staat ganz schön interessant sein. Da wird in der Linken auf der einen Seite z.B. über die Bespitzelung des Berliner Sozialforums diskutiert. Dass aber die meisten über E-Mail verschickten Bündnisprotokolle nicht unbedingt uninformativer sind als die Aufzeichnungen von informellen Geheimdienstmitarbeitern, scheint eher wenig zu stören.

„Wer nichts zu verbergen hat, hat nichts zu befürchten", so lautet ein Argument, das häufig von Politikern ins Feld geführt wird. Natürlich braucht ein Staat eine Rechtfertigung für seine Überwachungsmaßnahmen. Aber letztlich geht es vor allem um Prävention und Schutz vor der eigenen Bevölkerung und um Einschüchterung.
Auch wenn die in letzter Zeit grassierenden Überwachungsmaßnahmen, ebenso wie die zunehmenden Grundrechtseinschränkungen, häufig mit einem „Kampf gegen den Terror" oder der „organisierten Kriminalität" gerechtfertigt werden, macht es sie nicht besser. Es wäre naiv zu denken, dass solche Technik nicht auch gegen die Linke angewandt wird. Wie ein Blick in die Berichte der Verfassungsschutzämter oder die bereits erwähnte Bespitzelung des Berliner Sozialforums zeigt, sind selbst zivilgesellschaftliche Initiativen von der Überwachung nicht ausgenommen. Zudem muss man noch nicht einmal im Verdacht stehen, unmittelbar strafrechtlich relevante Dinge zu verantworten zu haben.
So scheint die Überwachung der Linken eher eine Art präventive Aufstandsbekämpfung darzustellen, auf die bloße Gefahr hin, dass soziale Bewegungen doch einmal wieder an Einfluss gewinnen und Unmut über bestehnde Verhältnisse äußern könnten, der von größeren Teilen der Bevölkerung geteilt wird.
In ihrem Überwachungswahn und dem Schüren einer Sicherheitshysterie, mit der sich so gut wie jede Maßnahme rechtfertigen lässt, scheinen die Repressionsorgane von einer regelrechten Paranoia getrieben zu sein. Darauf mit einer Paranoia vor Verfolgung und Überwachung zu antworten, scheint die Sache auch nicht besser zu machen. Stattdessen kommt es darauf an, sich diesem Problem bewusst zu werden und mit der Situation vernünftig umzugehen.
In diese Richtung ein wenig Aufklärungsarbeit zu leisten ist Anliegen dieser Broschüre. Sie ist praxisorientiert geschrieben, d.h. sie beschränkt sich nicht darauf, auf Probleme aufmerksam zu machen, sondern bietet einen Überblick über Handlungsmöglichkeiten. Dabei geht es um einfache Maßnahmen, wie man sich beim Umgang mit Computertechnik vor staatlicher Überwachung schützen kann. Die Anwendung der beschriebenen Programme setzt kein Fachwissen voraus, ist für jede und jeden umsetzbar, der oder die überhaupt einen Computer bedienen kann und muss eigentlich Standard im Ungang mit moderner Technik sein.
Denn statt sich drauf zu verlassen, dass, „wer nichts zu verbergen, auch nichts zu befürchten hat", sollte man lieber auf Nummer sicher gehen: „Wer sich schützt hat weniger zu befürchten" ist die angemessenere Antwort auf den Sicherheitswahn.

Inhalt:

Sicheres Surfen im Internet

Um sich vor Überwachung und Angriffen aus dem Internet schützen zu können, ist zuerst ein Grundverständnis für dessen Funktionsweise und Problembereiche notwendig. Diese werden nun kurz aufgezeigt. Anschließend wird erläutert, wie man sich konkret im Internet schützen kann.

a) Problembereich Anonymität und Verbindungsdaten:

Beim Verbinden mit dem Internet wählt sich der Computer per Modem-, ISDN-, Netwerkkarte oder (DSL-)Router bei einem Internet Service Provider (ISP) ein. Dabei wird die Telefonnummer sowie die eindeutige Kennung (die MAC-Adresse) des Einwahlgerätes z.B. Modem oder DSL-Router an den Provider übertragen. Gleichzeitig bekommt der Computer bzw. Router eine eindeutige IP-Adresse (z.B. 200.10.8.5) zugewiesen.

Wenn man eine Internetseite aufruft, E-Mails versendet oder andere Internetdienste nutzt, wird immer diese IP-Adresse zur Kommunikation übermittelt, sie ist praktisch wie ein elektronischer Fußabdruck. Es ist auch möglich, im Internet nach bestimmten IP-Adressen zu suchen. Anhand der IP-Adresse kann der Computer bis zum Internetprovider zurückverfolgt werden. Außerdem können Surfverhalten und die übertragenen Daten (z.B. E-Mails oder Downloads) ausspioniert werden.

Die Internetprovider durften bisher Verbindungsdaten nur zu Abrechnungszwecken kurzfristig speichern. Ein Beschluss des EU-Parlaments von Dezember 2005 soll die Provider (und Telefonanbieter) jedoch dazu verpflichten, die Verbindungsdaten zwischen 6 und 24 Monate zu speichern (die genaue Umsetzung dieses Beschlusses ist den einzelnen Mitgliedsstaaten überlassen, in Deutschland soll das Gesetz Ende 2007 mit 6 Monaten umgesetzt werden).

Zu den Verbindungsdaten gehört beispielsweise wer mit welchem Computer im Internet direkt kommuniziert und dabei welche Dienste (z.B. Surfen oder E-Mail) nutzt und wie lange diese Verbindung besteht. Durch die nachträgliche Zuordnung von IP-Adresse auf den Telefonanschluss und das Einwahlgerät ist es für die staatlichen Repressionsorgane möglich, z.B. das Surfverhalten einzelner Internetbenutzer zu überwachen oder festzustellen, wer wann an wen eine E-Mail verschickt hat. Die genauen Inhalte der E-Mail lassen sich bereits seit Anfang 2005 überwachen.

Für die Zukunft ist zusätzlich geplant, die MAC-Adresse zusammen mit der IP-Adresse beim Surfen zu übertragen. Somit wird die Überwachung, welcher Computer auf welche Seite zugreift, nicht nur für staatliche Behörden noch einfacher.

Im Internet gibt es keine Anonymität: Verbindungsdaten sind wie ein digitaler Fußabdruck. Der Datenverkehr kann von Lauschern an jedem Knotenpunkt gelesen werden.

b) Problembereich Abhören des Datenverkehrs

Daten werden im Internet normalerweise unverschlüsselt, d.h. im Klartext, übertragen. Durch die netzförmige Struktur des Internets lässt sich nie genau vorhersagen, über welchen Weg bzw. über welche Knotenpunkte die Datenpakete übertragen werden. Werden nun ein oder mehrere zentrale Knotenpunkte überwacht, hat ein Lauscher theoretisch uneingeschränkten Zugriff auf alle Daten und kann diese lesen oder im schlimmsten Fall sogar verändern.

Geheimdienste betreiben auf der ganzen Welt Horchposten, die zentrale Knotenpunkte des Datenverkehrs überwachen. Mit einigem Aufwand können auch Hacker Zugriff auf private Daten bekommen, wenn sie sich Zugang zu zentralen Netzwerken verschaffen. Eingeschränkt werden die Überwachungsmöglichkeiten der Repressionsorgane vor allem durch die immensen Datenmengen, welche tagtäglich über das Internet übertragen werden. Deshalb ist eine flächendeckende und lückenlose Überwachung des Internets in absehbarer Zeit nicht möglich.

Außerdem ist es für den Staat ein leichtes, E-Mails mitzulesen oder automatisiert nach bestimmten Schlüsselwörtern zu durchsuchen. Insbesondere durch die gesetzliche Verpflichtung der E-Mail-Provider, auf eigene Kosten spezielle Überwachungseinrichtungen zum Abhören des E-Mail-Verkehrs vorzuhalten, kann äußerst effektiv überwacht werden.

c) sicheres Surfen ganz praktisch

Es wird also recht schnell deutlich, dass es im Internet so etwas wie Anonymität kaum gibt und dass der Datenverkehr von Internetbenutzern recht leicht abgehört werden kann. Dennoch gibt es Möglichkeiten sich dagegen zu schützen:
Dabei ist zu unterscheiden zwischen verschlüsselten Internet*seiten*, auf die man zugreift, und einer verschlüsselten Anonymisierung, die man *selbst vornimmt*.

Verschlüsselte Internetseiten

Im Internetalltag gibt es häufig Fälle, in denen wichtige persönliche Daten übermittelt werden, die aber auch persönlich, sprich geheim, bleiben sollen. Bekannte Beispiele sind das Online-Banking oder die Abwicklung des Zahlungsverkehrs mittels Kreditkarte.
Hierfür wurde das so genannte HTTPS-Protokoll erfunden. Wenn du auf eine verschlüsselte Seite gehst, erscheint in der Adresszeile des Browsers (z.B. Firefox oder Internet Explorer) z.B. „https://www.online-banking.de". Außerdem wird unten auf dem Monitor in der Statuszeile ein kleines Schloss angezeigt.
Verschlüsselte Seiten arbeiten mit elektronischen Schlüsseln. Diese werden vor der Kommunikation zwischen Internetseite und Benutzer ausgetauscht und sind notwendig, um die verschickten Benutzerdaten entschlüsseln zu können. Damit ist sichergestellt, dass niemand Unbefugtes die übermittelten Daten lesen kann. Vor allem kleinere Projekte verwenden unzertifizierte Schlüssel. Das bedeutet, dass nicht für die Sicherheit des Schlüssels garantiert werden kann und der Benutzer auf die besuchte Seite vertrauen muss. Deshalb erscheint bei solchen Seiten häufig eine zusätzliche Warnmeldung auf dem Bildschirm, die auf diesen Sachverhalt hinweist.
Auch verschlüsselte Internetseiten sind nicht anonym. Wenn du also z.B. bei Indymedia einen Artikel schreibst, kann zwar nicht nachvollzogen werden, was drin steht, aber die Tatsache, dass du etwas zu einer bestimmten Zeit geschrieben hast schon! Und wenn man die Zeit der Verschickung mit den Veröffentlichungen vergleicht, lässt sich evtl. auch der zugehörige Text ausfindig machen.

Verschlüsselte Internetseiten verhindern, dass Unbefugte den Datenverkehr abhören können. Durch anonyme Proxies lässt sich zudem nicht mehr nachvollziehen, wer mit wem kommuniziert hat.

Anonymität und Verschlüsselung im Internet

Die Anonymisierung und Verschlüsselung der Internetzugriffe kann erreicht werden, indem sich die Computer der Nutzer nicht direkt mit der gewünschten Internetseite verbinden, sondern ihre Verbindungen verschlüsselt über mehrere Umwege schalten. Dazu wählst du mit deinem Computer einen Proxy-Server, der die Anfrage an ein Netz von „Umwege-Computern" weiterleitet. Diese nacheinander geschaltenen Computer leiten deine Daten weiter und senden das Ergebnis an dich zurück. Dadurch lässt sich nicht mehr nachvollziehen, von wem die übermittelten Daten ursprünglich stammen bzw. welche Internetseiten aufgerufen wurde. Wenn jemand deinen Anschluss oder Datenverkehr abhört, lässt es sich somit nicht nachvollziehen, welche Daten du an welche Internetseiten schickst, sondern nur, dass du Kontakt zu solch einem Proxy aufgenommen hast; wohin die Daten danach gehen, lässt sich nicht rekonstruieren.
Wenn jemand umgekehrt einzelne Internetseiten abhört, lässt sich nicht nachvollziehen, wer darauf zugegriffen hat (sprich: wo die Daten herkommen); der Inhalt der Daten selbst lässt sich jedoch schon einsehen (außer die Seite verwendet die oben beschriebene https-Verschlüsselung). Das ist z.B. dann problematisch, wenn du ein Kontaktformular einer Seite mit deinem richtigen Namen ausfüllst und diese Seite überwacht wird.

Für die Installation von Proxy-Servern auf dem Computer gibt es zwei besonders verbreitete Projekte: eins heißt JAP (Java Anon Proxy) und kommt von der TU Dresden (http://anon.inf.tu-dresden.de/), das andere nennt sich Tor (http://tor.eff.org/). Die Software kann kostenlos herunter geladen und installiert werden. Anschließend muss lediglich im Browser (z.B. Firefox oder Internet Explorer) der Proxy eingetragen werden. Wie das genau funktioniert, ist auf der Internetseite sehr ausführlich beschrieben.
Großer Nachteil: Das anonyme Surfen im Internet schränkt in der Regel die Geschwindigkeit ein. Manche Seiten funktionieren nur ohne Proxies. Allerdings kann der Proxy bei Bedarf jederzeit im Browser deaktiviert werden.
Neben dieser Variante des anonymen Surfens gibt es auch Internetseiten, über die man sich anonym auf andere Seiten weiterleiten lassen kann. Hierzu wird einfach eine Internetadresse in einem Webformular eingegeben und die gewählte Seite öffnet sich im neuen Fenster. Wie sicher solche Anonymisierungsseiten sind, ist aber schwer zu sagen.

Das Problem mit E-Mails

Eine Mail nimmt nicht den direkten Weg vom Absender zum Empfänger, sondern es liegen viele Stationen bzw. Netzwerkknoten dazwischen, die vorher nicht festgelegt werden können. An jedem dieser Knotenpunkte kann man eine Mail abfangen, lesen, kopieren oder gar inhaltlich verändern.
Seit dem 1. Januar 2005 sind E-Mail-Dienstleister ab 1.000 Kunden in Deutschland gesetzlich dazu verpflichtet, Abhöreinrichtungen auf eigene Kosten zu installieren. Die staatlichen Repressions- und Überwachungsorgane sind somit in der Lage, jederzeit ganz legal fremde E-Mails zu lesen. Sogar der E-Mail-Anbieter bekommt von der Überwachung gar nichts mehr mit. Außerdem ist es möglich, E-Mails nach bestimmten Schlüsselwörtern, Empfängern, Absendern etc. automatisch zu filtern und so ohne wenig Aufwand Menschen zu überwachen und auszuspionieren - auch nachträglich noch.
Insbesondere das Überwachen von Mailinglisten z.B. zum 1. Mai, zu G8, Sicherheitskonferenz etc. dürfte im Interesse des Staates liegen. Da viele Menschen ohne groß nachzudenken dort ihre richtigen Namen angeben, sind Mailinglisten für den Verfassungsschutz mindestens so interessant wie Namenslisten.
Dazu kommt, dass inzwischen viele politische Gruppen und Bündnisse ihre Protokolle o.ä. per E-Mail verschicken. Ob sich entsprechende Stellen noch die Mühe machen, diese auszudrucken und abzuheften oder gleich digital speichern, spielt keine Rolle. Auf jeden Fall war es für die Schnüffler früher wesentlich schwieriger tieferen Einblick in die Arbeitsweise und Aktivitäten unterschiedlicher Zusammenhänge zu erlangen, während die Linke heute sehr freizügig mit Informationen umgeht. Aber nun zur E-Mail selbst:

Es lässt sich nicht vorhersagen, auf welchem Weg eine E-Mail ihr Zeil erreicht. Die verschiedenen Teile einer E-Mail sind so gut vor Unbefugten geschützt, wie eine Postkarte.

Die Bestandteile einer E-Mail

Eine E-Mail besteht aus 3 Teilen:

Der „Header“ (Kopfzeile)

Im Header werden Informationen wie die IP-Adresse oder das E-Mail-Programm des Absenders gespeichert. Außerdem die E-Mail-Adresse vom Absender und die aller Empfänger (außer der BCC-Empfänger) sowie der Betreff der E-Mail. Da sich dieser Bereich nicht verschlüsseln lässt, gibt es auch kaum Möglichkeiten den E-Mail-Header zu schützen. Wichtig ist es vor allem, mit dieser Tatsache richtig umzugehen:

- Es lässt sich zurückverfolgen, wer von wo eine E-Mail versendet hat. Daher ggf. anonym surfen.
- Überlege, welche E-Mail-Adresse du zum Senden verwenden willst. Steht dein richtiger Name in der E-Mail-Adresse (z.B. petra.meier@email.de) oder hört sich die Adresse schon irgendwie komisch an (antifahool@aol.com) oder verwendest du eine unverdächtige Adresse? Verwende für politische und private Dinge unterschiedliche E-Mail-Adressen und wechsel deine Adresse ab und zu. Ein E-Mail-Provider im möglichst fernen Ausland schützt zumindest vor den euopäischen Überwachungsstandards.
- Achte darauf, was du in den Betreff schreibst. Oft wird dieser nach bestimmten Schlüsselwörtern wie „Demo“ durchsucht.

Der „Body“ (Nachrichtentext)

Hier steht der eigentliche Nachrichtentext praktisch wie auf einer Postkarte; viele Leute können ihn mitlesen, wenn sie dies wollen. Die einzige Möglichkeit, sich davor zu schützen, ist die Verschlüsselung der Nachricht, also die Unkenntlichmachung des Textes durch ein mathematisches Verfahren. Zusätzlich lässt sich eine Nachricht unterschreiben (signieren). Nur dadurch ist gewährleistet, dass die Nachricht auch vom richtigen Absender verschickt wurde.

Die „Attachments“ (Datei-Anlagen/Anhänge)

Beim Verschicken von Dateien werden diese als Anlage an die E-Mail angehängt. Willst du verhindern, dass Unbefugte diese Dateien öffnen können, musst du jede Datei einzeln verschlüsseln. Bei mehreren oder größeren Dateien empfiehlt es sich, diese mit Programmen wie WinZIP in einer einzigen Datei platzsparend zu komprimieren und diese anschließend zu verschlüsseln. Zusätzlich kannst du diese Dateien auch signieren. Das ganze funktioniert wie das Verschlüsseln eines Nachrichtentextes im Body und wird im folgenden genauer beschrieben.

E-Mails verschlüsseln

Wenn es um Verschlüsselung von E-Mails und Dateien oder anderen Schutzmechanismen am Computer geht, fällt häufig das Schlagwort PGP bzw. GPG. Es handelt sich hier um zwei gleichwertige Computerprogramme unterschiedlicher Hersteller, die verschiedene Werkzeuge zur Verfügung stellen, um private Daten vor unbefugtem Zugriff zu schützen. Es reicht aus, sich für eines der beiden Programme zu entscheiden. Aus diesem Grund erfolgt eine kurze Beschreibung, um die Auswahl für eines der Programme zu erleichtern. Danach werden Installation, Einrichtung und Funktionsweise beider Programme beschrieben.

Unterschiede zwischen PGP und GPG

PGP (Pretty Good Privacy) ist ein kommerzielles Programm zum Schutz privater Daten. Es gibt eine kostenlose Freeware-(Trial)-Version. Diese bietet folgende Funktionen:
- Ver- und Entschlüsseln sowie Signierung und Überprüfung von E-Mails und Dateien.
- Dauerhaftes Löschen von Dateien und Säubern der Festplatte.

Die kostenpflichtige Variante (ca. 100 Euro) bietet zudem die Möglichkeit, die ganze Festplatte zu verschlüsseln. Alternativ gibt es hierfür das kostenlose Programm TrueCrypt für Windows; in MacOS X ist mit FileVault und dem Festplattendienstprogramm bereits eine Festplattenverschlüsselung ins Betriebssystem integriert.

GPG (Gnu Privacy Guard) verfügt über dieselben Funktionen wie die Freeware-Version von PGP. Obwohl PGP als sicher gilt, hat GPG drei Vorteile:
- Es ist nicht kommerziell, d.h. herstellerunabhängig.
- Es sind keine umständlichen Lizenzmodelle oder Registrierungen notwendig.
- Der Quellcode ist OpenSource, d.h. frei einsehbar. Somit ist gewährleistet, dass keine Fehler oder Hintertürchen eingebaut sind, um die Verschlüsselung zu umgehen.

Der Nachteil von GPG ist allerdings ein geringerer Komfort bei der Installation und Bedienung der Software, weshalb für Menschen mit geringen Computerkenntnissen PGP dennoch die bessere Wahl sein kann.

Das Schlüsselpaar: Öffentlicher Schlüssel dient zum Verschlüsseln. Mit dem privaten Schlüssel + Passwort kann der Empfänger Daten entschlüsseln. Den privaten Schlüssel niemals weitergeben.

Generelle Funktionsweise von PGP/GPG

Um PGP/GPG richtig verwenden zu können, ist es wichtig zu verstehen, wie die Verschlüsselung dort überhaupt funktioniert.
Bei beiden Programmen werden „asymmetrische" Verfahren wie RSA oder DSS eingesetzt. Asymmetrisch bedeutet, dass es für jede Person zwei unterschiedliche Schlüssel gibt: einen zum *Verschlüsseln* und einen zum *Entschlüsseln* : Öffentlicher Schlüssel und Privater Schlüssel (public key und private key). Beide Schlüssel zusammen ergeben ein *Schlüsselpaar* (key pair). Wie dies ganz konkret in PGP/GPG geht, werden wir später sehen. Hier folgt eine allgemeine Erklärung.

Das Schlüsselpaar: privater und öffentlicher Schlüssel

Der erste Schritt besteht darin, ein Schlüsselpaar zu erstellen. Dazu werden neben Schlüsseltyp und Schlüsselgröße dein Name (ist dann der Schlüsselname), deine E-Mail-Adresse und ein Passwort (siehe Kapitel Problemzone Passwörter) benötigt. Daher solltest du für jede deiner E-Mail-Adressen ein eigenes Schlüsselpaar erstellen und ggf. einen unverdächtigen Namen angeben. Dann hast du je Schlüsselpaar zwei Schlüssel:

Der ***private*** **Schlüssel** (private key block) dient zusammen mit dem Passwort (passphrase) zum Entschlüsseln von Nachrichten, die deine Freunde dir schicken. Er tritt nur zusammen mit dem öffentlichen Schlüssel, also nie alleine, auf und darf nicht weitergegeben werden. Der private Schlüssel lagert auf deinem Computer und dient dazu, zusammen mit dem Passwort des Schlüsselpaares Nachrichten zu entschlüsseln, die auf den Namen des Schlüsselpaares verschlüsselt wurden.

Der ***öffentliche*** **Schlüssel** (public key block) ist ebenfalls Teil des Schlüsselpaares und dient deinen FreundInnen zum Verschlüsseln von Nachrichten an dich. Er kann einzeln exportiert werden (in Textform oder als PGP/GPG-Datei) und muss an deine FreundInnen weitergegeben werden, damit sie dir verschlüsselte Nachrichten senden können. Viele

Leute und Gruppen stellen diesen Schlüssel auch auf ihre Homepage oder laden ihn auf sogenannte Keyserver hoch, wo sie von allen PGP/GPG-BenutzerInnen wieder heruntergeladen werden können. Ein öffentlicher PGP/GPG-Schlüssel in Textform sieht etwa so aus:

```
-----BEGIN PGP PUBLIC KEY BLOCK-----
Version: PGP 8.0.1
mQGiBBLR5y9r6kEAKAjncLltDRBuwwpBU2bwJMTyyaI41fguZYyy8R7
G1KPx8rJCuFQdg8sxxEt08EZ1B0NmaCq8kL+zOYTPwcLYyanvTIySZR
t5T7K/RzZsOLgx//nbxBuNYXqI7MYhhPviptslyEIlXPKGKT6AZ6WCx
9A+5RjPGMreZKSItPuj6k5LrR1zxRO+/3VuEMu5zpvRYJzW0KC65Z1e
o98GbpqNTLyck042XMBo4JgHrrsDrHPWytGD4ht9ONKz4RU3lNXUp94
79ZLokATAQYEQIADAUCEv5aMwUbDAAAAAAKCRBzP++oElh/9VD5AKDd
-----END PGP PUBLIC KEY BLOCK-----
```

Zusammenfassung:
Nachdem du deinen öffentlichen Schlüssel an deine Freunde geschickt hast, können sie dir verschlüsselte Nachrichten schicken. Diese kannst du mit deinem privaten Schlüssel (welchen du niemals weitergeben solltest) und dem Passwort entschlüsseln.
Um deinen Freunden verschlüsselte Nachrichten schicken zu können, benötigst du deren öffentliche Schlüssel. Wenn du z.B. mit xy verschlüsselt kommunizieren möchtest, musst du dir den öffentlichen Schlüssel von xy schicken lassen und auf deinem Computer in PGP/GPG importieren. Die Nachrichten an xy kannst du dann damit verschlüsseln.
Das hört sich am Anfang kompliziert an, ist aber sehr einfach: Praktisch funktioniert das so, dass du in PGP/GPG eine Liste mit all deinen PGP/GPG-FreundInnen hast, aus der du den öffentlichen Schlüssel des Empfängers auswählst, wenn du eine Mail schreiben willst. Umgekehrt müssen alle deine FreundInnen deinen öffentlichen Schlüssel besitzen, ansonsten können sie dir nicht zurückschreiben. Mit dem öffentlichen Schlüssel kann *nur* verschlüsselt werden. Die Entschlüsselung der Dateien kann *nur* durch die Person erfolgen, die den privaten Schlüssel hat und das Passwort des Schlüsselpaares kennt.

Installation von PGP/GPG

PGP (Windows und Macintosh):
Wenn du nicht die Möglichkeit hast, dir die Vollversion des Programms von Feunden brennen zu lassen, dann gehe auf die Seite http://www.pgp.com. Dort gibt es einen Link „PGP Desktop 30-Day Trial". Auf der folgenden Seite müssen ganz unten die Lizenzbedingungen akzeptiert werden. Anschließend musst du dich mit E-Mail-Adresse etc. registrieren, dein Betriebssystem auswählen (Windows oder Mac OS X) und bekommst eine E-Mail mit dem Link auf das Installationsprogramm (ca. 15 MB).
Nachdem du das Installationsprogramm gestartet und den Lizenzcode eingegeben hast, werden die Dateien auf deinen Computer kopiert. Am Ende wirst du evtl. gefragt, ob du einen Schlüssel einrichten möchtest. Du kannst an dieser Stelle auf „Abbrechen" klicken. Wir werden später erläutern, was es mit den Schlüsseln auf sich hat und wie sie sich einrichten lassen.

GPG (je nach Betriebssystem):
- Bei den meisten LINUX-Distributionen ist GPG bereits vorinstalliert (siehe LINUX-Keyserver: Startmenü...).
- Für Windows: auf http://www.winpt.org gehen und „graphical installer with WinPT and GPG" anklicken. Anschließend das Installationsprogramm ausführen. Am Ende wirst du nach einem Verzeichnis für die Schlüsseldateien gefragt. Wähle Eigene Dateien in deinem Benutzerverzeichnis z.B.: „c:\dokumente und einstellungen\benutzerverzeichnis\eigene dateien" oder tippe einfach einen Verzeichnisnamen ein, z.B.: „c:\gpg\"
- Für Mac OS X auf http://macgpg.sourceforge.net gehen, dort findest du alle 3 Programmteile:
  GNU Privacy Guard herunterladen (ca. 4 MB) und installieren. Achte darauf, dass du die für dein Betriebssystem passende Version herunterlädst (im Finder auf das Apfel-Menü gehen und „über diesen Mac" auswählen und du siehst, welches Mac OS du verwendest). Anschließend solltest du für eine komfortable, grafische Oberfläche noch „GPG Keychain Access" und „GPG Tools" (ganz unten je ca. 1 MB) herunterladen. Beide Programme werden auf dem Desktop als .ZIP bzw. als .DMG gespeichert. Diese öffnen und dann das Programm auf die Festplatte in „Programme" kopieren (keine Installation notwendig).

Schicke den öffentlichen Schlüssel an deine Freundinnen und Freunde und besorge dir deren öffentliche Schlüssel. Installiere entweder PGP oder GPG

Praktische Anwendung von PGP/GPG

Wie wir gesehen haben, funktioniert PGP/GPG wie eine Geldkassette mit einem speziellen Schloss: zum Abschließen reicht der öffentliche Schlüssel, zum Aufschließen braucht man den privaten Schlüssel und das Passwort. Unterschlägt jemand die Geldkassette während ihrem Transport, kann er sie nicht öffnen. Nachdem du eines der Programme auf dem Computer installiert hast, folgt nun die praktische Anwendung:

Schlüsselverwaltung starten:

Je nach der verwendeten Version von PGP/GPG und dem Betriebssystem hast du im Startmenü (Windows oder Linux) oder im Programm-Ordner (Macintosh) ein neues Programmsymbol (ein Schloss oder Schlüssel) das einen der folgenden Namen trägt:

- Bei PGP: „PGP“, „PGP Keys“, „PGP Desktop“ oder so ähnlich
- Bei GPG:. „GPG Schlüsselbund“ (Mac), „WINPT-Key-Manager“ (Windows) oder so ähnlich.
- Bei GPG unter Linux: KGPG unter Dienstprogramme starten. Erscheint dann unten als Symbol in der KDE-Leiste.

Wenn du das Symbol gefunden hast, dann starte das Programm.

Schlüsselpaar erstellen:

In dem Fenster, was sich öffnet wenn du das Programm startest, gibt es den Eintrag „Datei/Neuer PGP-Schlüssel“, „new key“, „neu“ oder so ähnlich. Den wählst du aus. Bei einigen PGP/GPG-Versionen wird gefragt, ob du einen „Experten-Modus“ öffnen willst. Den kannst du ohne Bedenken auswählen. Du musst folgende Felder ausfüllen:

- Deinen Namen bzw. einen Phantasienamen
- Die E-Mail-Adresse, für die das Schlüsselpaar gelten soll
- Passwort (brauchst du später zum Entschlüsseln von eingehenden Nachrichten). Vgl. Kapitel über sichere Passwörter
- Bei Schlüsselgröße solltest du 2048 eintragen.
- Ablaufdatum: Du kannst wahlweise einstellen, dass dein Schlüssel nur bis zu einem bestimmten Tag gültig ist. Du wirst dadurch quasi gezwungen deinen Schlüssel gelegentlich neu zu erstellen, was die Sicherheit erhöht. Der Nachteil ist, dass du den Schlüssel wieder neu an alle FreundInnen verschicken musst. Du kannst diesen Eintrag also auch unverändert stehen lassen, dann gibt es kein Ablaufdatum.
- Die übrigen Felder kannst du so lassen wie sie sind.

Manche Versionen von PGP/GPG fragen am Ende, ob sie den generierten öffentlichen Schlüssel an den „Keyserver“ übermitteln sollen. Falls du noch am ausprobieren bist, solltest du dies nicht machen (überspringen).
Wenn du deinen öffentlichen Schlüssel an einen Keyserver übermittels, lagert er im Internet. Der Vorteil ist, dass alle deine Freunde diesen Schlüssel dort herunterladen können und du ihn nicht an alle schicken musst. Wenn du den Schlüssel von jemand anderes brauchst, kannst du auf einem Keyserver nach dem Schlüssel suchen und brauchst ihn dir nicht schicken zu lassen. Es gibt verschiedene Keyserver, die du von dem Menüeintrag „keyserver“ in PGP/GPG anwählen kannst.

Schlüsselübersicht:

Nachdem das Schlüsselpaar generiert wurde, müsste es in der Schlüsselübersicht des Programms erscheinen. Du kannst nun den Schlüssel markieren und über „export“ deinen öffentlichen Schlüssel aus dem Schlüsselpaar exportieren, d.h. als Datei separat speichern. Am besten speicherst du den öffentlichen Schlüssel in einem bestimmten Ordner z.B. eigene Dateien, dann kannst du immer diese Datei weitergeben und musst den Schlüssel nicht ständig neu exportieren, wenn ihn jemand von deinen Freunden braucht. Unter „import“ kannst du die Schlüssel-Dateien von deinen Freunden importieren. Die meisten PGP/GPG-Versionen unterscheiden in der Übersicht z.B. durch unterschiedliche Symbole zwischen eigenen Schlüsselpaaren und öffentlichen Schlüsseln von Freunden.

Schlüsselverwaltung: Hier lassen sich die Schlüssel erstellen, bearbeiten und löschen. Außerdem gibt es eine Übersicht mit allen erstellten und importierten Schlüsseln.

Schlüssel sichern/Backup:

Gelegentlich wird PGP/GPG nachfragen, ob es die Schlüssel sichern soll. Dies ist sehr ratsam. Wenn du deinen privaten Schlüssel verlierst, kannst du keine an dich verschlüsselten Dateien oder Texte mehr entschlüsseln. Deshalb ist es sinnvoll, ab und zu die Schlüsseldateien auf externe Datenträger z.B. Disketten oder CD-ROMs zu sichern und gut aufzuheben.

Verschlüsseln und Signieren von Mails, Texten und Dateien:

Nachdem du dein Schlüsselpaar erstellt hast, deinen öffentlichen Schlüssel an deine Freunde weitergegeben hast und die öffentlichen Schlüssel deiner Freunde importiert hast, ist das schwierigste überstanden.
Zum Testen und Herumspielen genügt es auch, wenn du bisher lediglich dein eigenes Schlüsselpaar erstellt hast.

1. Verschlüsseln von Mails und Texten

Wenn du einen kurzen Beispieltext geschrieben hast, kannst du ihn markieren und mit der rechten Maustaste oder über das Menü in die Zwischenablage kopieren. PGP/GPG bietet nun eine Möglichkeit, den Inhalt der Zwischenablage zu verschlüsseln. Anschließend kannst du den Text wieder einfügen. Der Text ist nun unleserlich geworden.

Hierzu gibt es die Funktion „Zwischenablage verschlüsseln“ bzw. „Encrypt clipboard“. Diese findest du unter:

- PGP-Windows in der Startleiste rechts, wenn du auf das Schloss klickst
- GPG-Windows in der Startleiste rechts, wenn du auf das Windows-Privacy-Tray-Symbol klickst
- PGP-Macintosh, wenn du PGP öffnest
- GPG-Macintosh, wenn du GPG Tools öffnest, gibt es einen Button „verschlüsseln“ und dann „Zwischenablage verwenden“.
- GPG-Linux, wenn du GPG gestartet hast, unten rechts in der KDE-Leiste auf das Symbol klicken

Anschließend musst du eine oder mehrere EmpfängerInnen auswählen. Zum Testen kannst du an dieser Stelle dich selber auswählen. Den nun verschlüsselten Text kannst du aus der Zwischenablage wieder in das Textbearbeitungsprogramm oder das E-Mail-Formular einfügen (ganz normal mit rechter Maustaste oder über das Menü).
Der verschlüsselte Text sieht dann z.B. so aus:

```
óóBEGIN PGP MESSAGEóó
Version: PGP 8.0
qANQR1DBwU4DAClA4VKxE6oQCADQzMjVvVi78VswnHaGz3iJyMdzi4ijHeAm/czN
ch1q21PenrcGOOFupO5at3dEfZK8n55zQqE27Jd0q8GuGpotD5uArrRCxuP97NHC
w0uBx076KEynJyhCzG/xCQJ6FeM1u5kr2ayY8qW0RLKyNGVrGuL65IFbRLTCUDtw
FaqC0CG73TQFj2jeLmr9yoG/voZfFKn1IaewdBeap9dZn/tZQjt6UqpnvuDExEFs
McXrF600Ky44zHgyogaJtjkE7DvtjhPhVGGdxi/4pGUJw6yuRRuDf4ZHRKmcTvSR
a4UPz8XERjwtWeBVgO5f5L3NKJcNkLRGxNlyqDtk6Qfn0ihTCACivgpgWT3XVP0W
WptqZn17Cpaz056arTLFCJg82z+SZlZAaRIlaNwPE+pCmh7q/Dt1xlHazl0KMzs+
qpKFeL4mOrCfkxboXwdEQoN29CwEbuknyL7su5zxuRGBZT49mnI/hr+teiu8RK06
hZ9x4SPaffFolY6TdlYVVPobWLMwBgATMg8mITj9kMwtMjt+y/QhcSILiQLGB8p4
vvvbkGjAU65hOtVL4X0Fc9OscDo5TMgiRWO7LwgNX67TMvF/UPL7kEj4Cj0C6jez
XZYSoELbmRuG2w2qTT7owlsWsLpV5jXUSzEwHwbSpI+OB1QBi0Ac6GD2eL6yF+p5
ysMmzlJY0joBnroK0oFiE0bgLlwvQqZtMoZKN/23ULPszSANQWvuqGKH/v70WC1D
óóEND PGP MESSAGEóó-
```

Diesen Textblock könntest du nun als E-Mail absenden und fertig.

2. Entschlüsseln von Mails und Texten

Wenn du die Nachricht mit deinem eigenen Schlüssel verschlüsselt hast, kannst du sie nun wieder entschlüsseln. Einfach den verschlüsselten Text in die Zwischenablage kopieren und das selbe wie eben machen, nur statt auf „verschlüsseln“ jetzt auf „entschlüsseln“ klicken! Du wirst nun nach deinem Passwort gefragt. Anschließend kannst du den jetzt entschlüsselten Text wieder in ein Textbearbeitungsprogramm oder das E-Mail-Formular einfügen und ihn dir durchlesen.

**Es können
E-Mails,
einfache Texte
oder komplette Dateien
ver- und entschlüsselt
werden.
Die
verschlüsselten Daten
können nur
von den
(in PGP/GPG ausgewählten)
EmpfängerInnen
wieder
entschlüsselt werden.**

3. Ver- und Entschlüsseln von Dateien
Das Ver- und Entschlüsseln von Dateien ist sogar noch einfacher als bei Texten!

Bei PGP:
Einfach die entsprechende Datei mit der rechten Maustaste (beim Mac mit ctrl+Maustaste) anklicken und dann sollte ein Untermenü „PGP“ erscheinen. Hier „Verschlüsseln“ bzw. „Entschlüsseln“ auswählen.

Bei GPG unter Windows:
Den „File-Manager“ über das GPG-Symbol laden. Dort Dateien hineinziehen und dann auf „Verschlüsseln“ bzw. „Entschlüsseln“ klicken.

Bei GPG unter Macintosh:
Statt auf den Button Zwischenablage zu klicken einfach eine Datei auswählen. Geht also fast genauso wie das Ver-/Entschlüsseln von der Zwischenablage

Bei GPG unter Linux:
Hier wird der GNU Privacy Assistent benötigt, der allerdings nicht bei allen Linux-Distributionen vorinstalliert ist. Alternativ können auch Dateien über die Kommandozeile (shell) verschlüsselt werden. Die Befehle stehen auf der GPG-Homepage.

Beim Verschlüsseln einer Datei musst du wie beim Verschlüsseln eines Textes einen oder mehrere EmpfängerInnen auswählen. Das Programm erstellt eine Kopie der Orginaldatei, die verschlüsselt ist. Diese verschlüsselte Datei erscheint nun im gleichen Ordner wie die ursprüngliche Datei. Sie hat den gleichen Namen, aber ein anderes Symbol und eine andere Endung (.pgp). Du kannst nun diese verschlüsselte Datei einfach an eine Mail anhängen.
Wenn du eine verschlüsselte Datei geschickt bekommst, musst du diese zuerst auf deinem Computer speichern. Nach dem Entschlüsseln erscheint die entschlüsselte Datei in dem gleichen Ordner wie die verschlüsselte. Du kannst sie nun ganz normal öffnen.

Achtung! Wenn du eine E-Mail mit angehängten Dateien verschickst, musst du den Nachrichtentext (den „Body“) sowie jede anzuhängende Datei einzeln verschlüsseln. Falls du mehrere Dateien verschickst, bietet es sich an, diese zuvor (mit z.B. winzip) zu komprimieren und den gepackten Ordner komplett zu verschlüsseln und an die Mail anzuhängen.

4. Signieren und Überprüfen
Zusätzlich zum Verschlüsseln gibt es auch die Möglichkeit, einen Text oder eine Datei zu unterschreiben bzw. zu signieren. Dazu wählst du den oder die EmpfängerIn aus und bestätigst anschließend mit deinem Passwort, dass von dir ist. Der oder die EmpfängerIn kann dann überprüfen, ob die Nachricht wirklich von dir stammt.
Wenn du eine E-Mail bekommst, überprüft der auf deinem Computer gespeicherte, öffentliche Schlüssel des oder der AbsenderIn, ob die Nachricht wirklich von ihm oder ihr kommt.
Sowohl der Menüeintrag „Signieren“ bzw. „Sign“ als auch der Eintrag „Überprüfen“ bzw. „Verify“ findet sich in PGP/GPG ungefähr an der selben Stelle wie „Verschlüsseln“ bzw. „Entschlüsseln“.

Das Ver- und Entschlüsseln von Dateien ist ähnlich einfach wie das von Texten. Dateien und Texte lassen sich signieren, um die Echtheit des Absenders zu garantieren.

E-Mail-Programme:

Für manche E-Mail-Programme gibt es spezielle PGP- oder GPG-Erweiterungen. Nach deren Installation erscheint im Programm ein Menüeintrag oder ein Schloss-Symbol. Wenn du diesen Eintrag bzw. das Symbol auswählst, öffnet sich automatisch das PGP/GPG-Programm und du brauchst nur noch den Schlüssel des Empfängers anzugeben. Der Vorteil ist mehr Komfort, der Nachteil ist, dass du selber nicht mehr direkt den Text und die Anlagen verschlüsselst und theoretisch was falsch machen kannst, ohne es zu merken. Deshalb solltest du das auf jeden Fall erst einmal mit „unwichtigen“ Daten testen (auch mit Dateianlagen).

Problemzone Festplatte

Stell dir vor die Bullen machen bei dir eine Hausdurchsuchung, weil du beim Plakatieren erwischt oder auf einer Demo verhaftet wirst, oder einfach in einer politischen Gruppe aktiv bist. In vielen Fällen werden bei Hausdurchsuchungen auch persönliche Gegenstände z.B. Computer beschlagnahmt. Deshalb solltest du dir sehr genau überlegen, was du auf deiner Festplatte speicherst und wie du deinen PC vor unbefugtem Zugriff von Schnüfflern schützen kannst. Denn erstens dienen Hausdurchsuchungen der Ausspionierung von politisch Aktiven und linken Strukturen und zweitens wird oft aufgrund konkreter Ermittlungsverfahren versucht, Linken irgend etwas anzuhängen. Und da kommt es reichlich ungelegen, wenn man Druckvorlagen für Demoflyer oder Diskussionstexte für deine Gruppe auf deinem Computer findet...

Windows-Passwort/Login

Die meisten modernen Computer sind bereits mit einem so genannten Login-Passwort geschützt. Das verhindert, dass jemand einfach so einen Computer einschalten und auf dessen Daten zugreifen kann. Windows- und andere Login-Passwörter hindern Ermittler oder sonstige Einbrecher jedoch nicht daran, die Verkleidung deines Computers abzunehmen und deine Festplatte in einen anderen Rechner einzubauen, um spätestens dort auf sämtliche Daten zugreifen zu können. Und genau das wird nach einer Hausdurchsuchung passieren. Diese Art von „Schutz“ hilft also höchstens gegen lästige Mitbewohner oder neugierige Arbeitskollegen, ist aber sonst total sinnlos.

Verschlüsselung der Festplatte

Wenn du sensible Dateien vor Schnüfflern schützen möchtest, kannst du diese wie beschrieben mit PGP/GPG verschlüsseln. Die Datei wird dann eben nicht per E-Mail verschickt, sondern lagert verschlüsselt auf deiner eigenen Festplatte.
Du musst bei dieser Variante allerdings jede zu schützende Datei einzeln verschlüsseln und einzeln entschlüsseln, wenn du sie brauchst.
In den meisten Fällen ist es deshalb wesentlich praktischer, gleich eine ganze Festplattenpartition zu verschlüsseln. Bei dieser Variante der Verschlüsselung wird einfach eine Festplatten-Datei irgendwo auf der Festplatte angelegt, die z.B. 20 GB groß ist (oder 10 GB, oder 2 GB, je nachdem wie groß du sie haben möchstest und wie viel Platz insgesamt auf der Festplatte zur Verfügung steht) . Dieser Teil der Festplatte ist durch ein Passwort gesichert. Wenn du die Datei öffnest erscheint sie automatisch als Laufwerk auf deinem Computer (z.B. als Laufwerk „E“ im Windows-Explorer oder Arbeitsplatz). Im Gegensatz zur E-Mail-Verschlüsselung gibt es also keinen privaten/öffentlichen Schlüssel. Der ist deshalb gar nicht nötig, da die Datei ja nicht zur Verschickung an jemand anderes gedacht ist.

Im Grunde ist das ganz einfach: Du installierst ein entsprechendes Programm, erstellst über das Programm eine Festplattenpartition und schon kannst du dort Dateien speichern. Mehr gibt es eigentlich nicht zu erklären, da sich die Einrichtung bei den meisten Programmen beinahe von selbst erklärt; du musst dir nur überlegen wie groß der verschlüsselte Teil der Festplatte sein soll und dir ein gutes Passwort ausdenken.
Je nach Betriebssystem bieten sich folgende Programme an:
Für Windows:
- Vollversion von PGP (kostet ca. 100 Euro) http://www.pgp.com
- TrueCrypt (kostenlos) http://www.truecrypt.org
Für Macintosh:
- Vollversion von PGP (kostet ca. 100 Euro) http://www.pgp.com
- FileVault oder Festplattendienstprogramm (im Betriebssystem bereits eingebaut).
Für Linux:
- In gängigen Linux-Distributionen ist die Verschlüsselung von Festplatten bereits integriert.

Ein Windows-Passwort schützt zwar das System, nicht aber die Festplatte. Sie kann ausgebaut und in einem anderen Gerät gelesen werden. Die Verschlüsselung von Teilen der Festplatte ist eine sichere Lösung.

Dateien dauerhaft löschen

Wer mit dem Computer arbeitet, legt zwangsläufig Dateien an. Diese sind entweder selber erstellt worden (in dem Moment wo man etwas speichert) oder werden von diversen Programmen oder vom Betriebssystem temporär (vorübergehend) angelegt. Wenn man Dateien löscht, wandern sie zunächst einmal in den Papierkorb und bleiben weiterhin auf der Festplatte.
Wenn die Staatsanwaltschaft im „Papierkorb" deines Computers wühlt und sich ebenso einfach sämtliche gelöschte Texte der letzten paar Monate zugänglich machen kann, dann ist das sicherlich nicht so toll. Aber auch ein häufig gelehrter Papierkorb garantiert nicht dafür, dass die Dateien auch wirklich für immer verschwunden sind.

Auch aus dem Papierkorb gelöschte Dateien lassen sich mit bestimmten Programmen wiederherstellen. Manchmal ist das auch erwünscht, wenn z.B. aus Versehen etwas gelöscht wurde. Das liegt daran, dass beim Löschen nicht der eigentliche Dateiinhalt überschrieben wird, sondern nur der Eintrag, wo sich die Datei befindet wird aus dem Dateisystem entfernt. Der Dateiinhalt wird erst überschrieben, wenn der nun freigegebene Speicherplatz durch neue Dateien belegt wird. Wann eine Datei also wirklich überschrieben wurde (und damit nicht wiederherstellbar ist), lässt sich nur schwer nachvollziehen.
Aus diesem Grund gibt es Programme, mit denen sich Dateien dauerhaft löschen lassen. Die Dateien werden dabei nicht nur entfernt, sondern der Platz, wo sie auf der Festplatte lagerten, wird mehrfach überschrieben.

Auch gelöschte Daten lassen sich wiederherstellen. Um sie dauerhaft zu löschen, müssen sie „überschrieben" werden. Das Säubern der Festplatte verhindert, dass Spuren von vergangenen Arbeitsprozessen rekonstruiert werden können.

Am einfachsten geht das mit PGP/GPG:

Windows:
- PGP: Datei mit der rechten Maustaste anklicken und auf PGP/sicher löschen klicken.
- GPG: Win Pravacy Tray-Symbol anklicken und File-Manager öffnen. Dateien ins Fenster ziehen und auf File/Wipe klicken.

Macintosh:
- PGP: Datei mit der rechten Maustaste bzw. CTR-Mausklick anklicken und auf PGP/wipe clicken.
- Mac OS X: Datei in den Papierkorb ziehen. Im Finder das Menü „Finder/Papierkorb sicher entleeren" auswählen.

Linux:
- http://wipe.sourceforge.net installieren.

Festplatte säubern

Bei dem eben beschriebenen Verfahren des dauerhaften Löschens von Dateien ging es nur um selbst angelegte Dateien, die anschließend manuell entfernt werden sollen.
Dateien, die das System vorübergehend erzeugt (z.B. Druckaufträge etc.), werden automatisch wieder gelöscht. Aber auch sie lassen sich wiederherstellen. Um auch dies zu verhindern, kann die gesamte Festplatte gesäubert werden. Es gibt spezielle Programme, mit denen sich der gesamte freie Speicherplatz auf der Festplatte überschreiben lässt. Unter anderem PGP/GPG bietet solch eine Funktion an. Der freie Speicher sollte mit mehreren Durchgängen überschrieben werden, da sonst Magnetisierungsspuren von überschriebenen Dateien auf der Festplatte bleiben, die mit hohem technischen Aufwand gelesen werden können. Nicht alle Versionen von PGP und GPG bieten diese Funktion an.
In GPG kann z.B. mit dem File Manager mit „Wipe Free Space" der freie Festplattenplatz gesäubert werden. Bei PGP sucht man die Funktion „Freien Speicherplatz löschen" und kann anschließend das zu säubernde Laufwerk und die Anzahl der Durchgänge auswählen. Das Überschreiben selbst dauert einige Minuten und sollte hin und wieder durchgeführt werden. Auch der Speicherplatz auf Disketten und USB-Sticks kann auf diese Weise gesäubert werden, so dass sich nicht mehr rekonstrieren lässt, welche Daten sich auf den Medien befanden.

Problemzone Passwörter

Heutzutage müssen wir uns eine ganze Latte von Passwörtern merken: Für Online-Banking, zum Mailen, auf Arbeit, für den PC zu Hause etc. Viele Leute haben nur ein oder zwei Passwörter, die sie für alles verwenden. Das ist jedoch nicht sonderlich intelligent. Der Webmaster eines Chat-Forums sollte doch nicht mit deinem Passwort auf dein Online-Konto zugreifen können und der Administrator bei dir auf Arbeit sollte auch nach Möglichkeit deine E-Mails nicht lesen können.

Außerdem ist es sinnlos, einerseits z.B. eine Festplatte zu verschlüsseln und andererseits ein unsicheres Passwort zu verwenden oder das knackbare Windows-Anmeldepasswort gleichzeitig für verschlüsselte Dateien zu benutzen.
Die ganzen bisher aufgezählten Sicherheitstechniken machen nur Sinn, wenn sich die verwendeten Passwörter nicht sofort knacken lassen.
Zum Thema Passwörter gibt es grundsätzlich zwei Dinge zu sagen:

1. Nimm unterschiedliche Passwörter für unterschiedliche Dinge oder du kannst dir die Passwörter auch gleich schenken!

2. Verwende sichere Passwörter!

Stellt sich nun die Frage, was ein Passwort „sicher“ macht. Hierzu muss man sich in die Situation von Schnüfflern rein versetzen. Wer Passwörter knacken will arbeitet in der Regel mit entsprechenden Programmen, die z.B. alle Wörter aus dem Duden ausprobieren; eine andere Möglichkeit ist, Wörter oder Wortkombinationen auszuprobieren, von denen man denkt, dass sie für dich einfach zu merken sind: also Geburtsdatum, Adresse, Telefonnummer, Name vom Haustier usw.
Eine letzte Möglichkeit Passwörter zu knacken ist, einfach alle Möglichkeiten durchzutesten, die es überhaupt geben kann (natürlich automatisiert). Ein entsprechendes Programm kann einfach alle Möglichkeiten testen, bis es das Passwort durch Ausprobieren herausgefunden hat. Deshalb ist ein Passwort, was z.B. nur aus 4 Zeichen besteht sicherlich in wenigen Minuten knackbar. Je länger ein Passwort ist, desto länger ist auch die Zeit, die benötigt wird, um alle Möglichkeiten auszuprobieren. Heutzutage wird davon ausgegangen, dass z.B. ein Passwort mit 10 Zeichen Länge in einigen Jahren geknackt werden kann. Bei 11 Zeichen werden bereits einige hundert Jahre benötigt, bei 12 Zeichen einige tausend Jahre. Allerdings ist es schwer, solche Aussagen mit Sicherheit zu treffen. Die Dauer hängt letztlich vom Aufwand ab, der betrieben wird und von der Geschwindigkeit der Computer, die das Passwort knacken sollen. Außerdem sind das rein rechnerische Angaben, Zufallstreffer sind natürlich immer möglich.

Trotzdem sollte man beim Erstellen eines „sicheren“ Passwortes folgendes beachten:

- Es darf nicht im Duden vorkommen
- Ein Passwort sollte nicht schon für andere Dinge verwendet werden
- Sollte nicht erratbar sein (z.B. Geburtsdatum)
- Ein Passwort muss eine bestimmte Mindestlänge haben (min. 12 Zeichen)
- Es sollte aus verschiedenen Zeichen bestehen (Zahlen, Buchstaben und sonstige Zeichen) – allerdings muss man beachten, dass es deutsche Sonderzeichen auf ausländischen Tastaturen nicht gibt, was ein Problem sein kann, wenn man seine Mails im Urlaub abrufen will.

Ein Tipp hierzu: Passwörter lassen sich einfacher merken, wenn bestimmte Dinge kombiniert werden. Z.B. Geburtsdatum verdrehen und mit Telefonnummer und jedem zweiten Buchstaben des Namen vermischen oder so etwas.

**Ein Passwort
macht nur Sinn,
wenn es
sicher ist:
Um so länger
und unerratbarer,
desto besser.
Ein Passwort
für alles
ist so sicher
wie ein
Wohnungsschlüssel
für die
ganze Straße.**

Netzwerke und Internetanschluss

Bei den meisten Betriebssystemen und Anwendungen werden früher oder später Sicherheitslücken bekannt. Oft entstehen Sicherheitslücken auch durch die fehlerhafte Konfiguration des Computers. Diese Lücken können genutzt werden, um entweder direkten Zugriff auf einen Computer und dessen Daten zu erlangen oder um einfach nur Schaden durch Datenverlust anzurichten. Deshalb ist es unverzichtbar, den Computer mit entsprechender Software vor solchen Angriffen zu schützen. Auch regelmäßige Updates des Betriebssystems sollten durchgeführt werden.
Inwiefern man sich gegen Überwachungsmöglichkeiten schützen kann, die Repressionsorgane durch neue Programme wie den schon erwähnten „Kommissar Trojaner" erhalten, lässt sich nicht genau sagen. Aber ganz von solchen gezielten Angriffen auf einzelne Computer abgesehen, gibt ein wahllos mit dem Internet kommunizierender Rechner allerhand Informationen über nicht legal erworbene Software raus, was auch zu strafrechtlichen Konsequenzen führen kann.

Wenn man ein Funknetzwerk nicht sichert, ist das so wie wenn man ein Kabel vom Computer bis auf die Straße verlegt. Zumindest beim Datenverkehr ins Internet gilt: Vertrauen ist gut, Kontrolle ist besser!

Firewall

Normalerweise kann jedes Programm von alleine ins Internet gehen und persönliche Daten übermitteln. Außerdem können Hacker von außerhalb versuchen, über Sicherheitslücken auf den Computer zuzugreifen. Dies ist besonders in DSL-Zeiten gefährlich, wo man mit seinem Computer praktisch immer online ist, auch wenn man nicht surft und häufig sogar ohne sich selber noch einwählen zu müssen.

So genannte Firewalls kontrollieren den Netzverkehr ins Internet und aus dem Internet. Die Kommunikation *nach außen* erfolgt an eine bestimmte Netzwerkadresse (z.B. 200.10.8.5) und je nach Netzwerkdienst (http, E-Mail, ...) an einen bestimmten Port (z.B. Port 80), wenn man eine Internetseite aufruft. So ein Zugriff lässt sich bei manchen Firewalls für jedes Programm einzeln erlauben oder verbieten (beim erstmaligen Zugriff fragt die Firewall den Benutzer). Dadurch kann verhindert werden, dass Computer unbemerkt Daten versenden. Aber nicht alle Firewalls bieten diesen Schutz nach außen.

Wichtiger ist der Schutz der Kommunikation *von außen*: Wenn ein Computer aus dem Internet auf einen bestimmten Dienst deines Computers zugreifen möchte, wird die Firewall dies im Normalfall verhindern oder nachfragen. So kann verhindert werden, dass jemand aus dem Internet z.B. auf deine Dateien zugreift.

Neben einer Firewall-Software, die auf dem Computer installiert wird gibt es auch Firewall-Hardware. Z.B. haben viele Router eine integrierte Firewall. Dies bietet zusätzlichen Schutz. Weiteren Schutz bietet es, nichts zu aktivieren, was man im Netz nicht braucht (z.B. Dateifreigabe, falls nicht benötigt).

Funk-Netzwerke

Neuerdings werden immer häufiger WLAN-Funknetze eingesetzt. Hier ist die Gefahr von Sicherheitslücken besonders groß. Ein offenes WLAN-Netz ist praktisch so wie wenn man ein Netzwerkkabel vom Computer bis auf die Straße verlegt und jedeR sich einstöpseln kann! Ist ein WLAN-Netzwerk nicht richtig abgesichert, können Hacker somit ohne große Mühe direkt in das Netzwerk eindringen und ggf. Zugriff auf den Computer und persönliche Daten erlangen.

Deshalb muss für das WLAN zu Hause unbedingt ein verschlüsselter Zugang mit Kennwort aktiviert werden (WEP oder besser WPA). Wer sich nicht sicher ist wie das funktioniert sollte im Zweifelsfall lieber auf Funknetze verzichten.

Wer unterwegs z.B. im Internetcafe WLAN nutzt sollte sich zumindest der Risiken bewußt sein. Manche Firewalls verhindern auch in einem offenen WLAN-Netz, dass fremde Rechner auf den eigenen Computer zugreifen können.

Keine Panik, aber trotzdem dran denken...

Das Anliegen dieser Broschüre war nicht, in irgendeiner Weise Paranoia vor dem Überwachungsstaat zu verbreiten und moderne Technik zu verdammen. Wir wollen natürlich nicht, dass die Linken keine Computer mehr benutzen – das wäre Unsinn. Auch für die politische Arbeit ist moderne Technik ein sinnvolles und inzwischen auch fast unverzichtbares Hilfsmittel geworden, das vieles wesentlich einfacher macht. Nur sollte man einige Sicherheitsstandards beachten, die in der konkreten Anwendung viel unkomplizierter sind als es sich zu Anfang anhört. So kann mit wenig Aufwand ein recht hoher Schutz gegen staatliche Überwachung erzielt werden.
Aber genau bei diesen Sicherheitsstandards scheint die Linke in letzter Zeit etwas gepennt zu haben. War bei dem Aufkommen der Mobiltelefone noch eine gewisse Skepsis gegenüber ihren potenziellen Nebenwirkungen verbreitet, wird mit Computern und Internetkommunikation inzwischen schon fast fahrlässig umgegangen. Grade vor dem Hintergrund von dauernden Erweiterungen der Befugnisse der Repressionsorgane halten wir das für sehr bedenklich und eine Außereinandersetzung der Linken mit dieser Problematik für überfällig. Diese Broschüre soll dazu ein Beitrag sein.
Von den geforderten Sicherheitsstandards im Umgang mit Computertechnik einmal ganz abgesehen, gibt es natürlich immer Themen, die man lieber komplett offline klären sollte. Dass sind dann solche Sachen, die auch an Kneipentischen nichts zu suchen haben. Aus den Erläuterungen dieser Broschüre ist hoffentlich auch ersichtlich geworden, dass kein Schutz so richtig 100-prozentig sicher ist. Wir warnen also ausdrücklich davor, strafrechtlich all zu relevante Sachen oder Informationen, die besonders geeignet scheinen, die Linke zu kriminalisieren, überhaupt der Computertechnik zugänglich zu machen!

Hauptziel dieser Broschüre ist es, ein Bewußtstein und Verständnis für Computersicherheit zu schaffen, auch für Leute mit geringen Computerkenntnissen. Genauere Infos zur Installation bestimmter Programme gibt es auf unserer Homepage bzw. haben auch die meisten Leute jemanden im Freundeskreis, der bei solchen Fragen weiterhelfen kann.

Impressum:
internationale KommunistInnen Berlin, kontakt@interkomm.tk, Stand Februar 2007
V.i.S.d.P.: Petra Schmitt, Krossener Str. 10, 10247 Berlin, Auflage: 2.000 Exemplare
Die Broschüre zum Download sowie etwaige Ergänzungen und weiterführende Informationen gibt es auf unserer Homepage

www.interkomm.tk

Anregungen oder Kritik zu der Broschüre nehmen wir natürlich auch gerne entgegen.

Weitere nützliche Links

zum Thema Computersicherheit und Antirepression:

www.raw.at/compsec/compsec.htm
(sehr ausführliches Handbuch zu Computersicherheit)

www.rote-hilfe.de
(allgemeine Infos zu Antirepression, einiges zu Computersicherheit)

www.helmbold.de/pgp
(Installationsanleitung und Tipps für den Umgang mit PGP)

Moderne Technik sinnvoll einsetzen, ohne fahrlässig zu handeln: Computertechnik kann nie 100% sicher sein, strafrechtlich relevante Dinge haben am Computer nichts zu suchen.