PIRATEN PARTEI

Wie mache ich meinen Computer abhörsicher?

Ein paar Tipps zum sauberen Umgang mit gespeicherten Daten und zur sicheren Kommunikation über den Rechner.

Vorratsdatenspeicherung, Online-Durchsuchungen, Laptop-Kontrolle am Flughafen. Nicht nur muss man seinen Computer heute vor Viren und Spionagesoftware zwielichtiger Geschäftemacher schützen, sondern auch vor unberechtigtem Zugriff durch den Staat. Ohne Rücksicht auf die Grundrechte sind die Gesetzgeber auf allen Ebenen dabei aus dem freien Bürger einen gläsernen Gefolgsmann zu machen. In diesem kurzen Info-Blatt wollen wir, die Piratenpartei Deutschland, ein paar Tipps geben, wie sie sich sowohl privater als auch staatlicher Spionage entziehen können.

Sicherheitsrisiko Mensch

Viele Risiken am Computer lassen sich bereits mit Hilfe von Programmen in den Griff kriegen. Von Anti-Viren-Software und Firewalls haben Sie bestimmt schon gehört und selbige auch bereits auf Ihrem Rechner installiert. Doch trotz aller Sicherheitssoftware bleibt immer ein großes Risiko bestehen: der Benutzer. Nicht selten haben Angreifer einen großen Wissensvorsprung vor den meisten Anwendern. Aus diesem Grund hier erst einmal drei wichtige Verhaltensregeln am Computer.

Verwenden Sie sichere Passwörter! Selbst das stabilste Schloss ist nutzlos, wenn es sich mit einem Schraubenzieher öffnen lässt. Das selbe ist es, wenn man einfache Passwörter benutzt, die sich zum Beispiel in einem Wörterbuch finden oder die ein nahe stehender leicht erraten kann, etwa den Namen des Ehepartners. Verwenden sie statt dessen möglichst lange Passwörter, die sowohl Groß- und Kleinbuchstaben, als auch Zahlen und Sonderzeichen enthalten. Gut zu merken sind z.B. Fußballergebnisse („Bayern schlägt 1860 mit 3:2!“ oder „Bayern-Hertha=4:1“).

Seien Sie misstrauisch! Begegnen Sie Aussagen gerade im Internet sehr wachsam. Die Chance zufällig beim Surfen ein Auto zu gewinnen ist gleich Null und wenn ihre Bank Sie auffordert ihre Daten auf einer Webseite einzugeben oder jemand den Sie nicht kennen Ihnen eine schmachtende Liebesmail schreibt, sollten Sie lieber zwei mal hinschauen.

Seien Sie vorsichtig in fremden Netzen! Sich mal schnell in den nächsten WLAN-Hotspot einklinken ist je nach Sicherungen unterschiedlich schwer. Aber einmal drin, kann jeder den eigenen Datenverkehr mithören. Achten Sie bei sensiblem Datenaustausch auf Verschlüsselung (beim Surfen z.B. erkennbar am Kürzel „http**s**://...“)

Abhörsicher E-Mailen

Wenn Sie eine E-Mail schreiben, wird diese völlig offen wie eine Postkarte durch das Netz gesendet. Jeder der an irgendeiner Stelle den Datenverkehr mithören kann (z.B. Ihr Provider), kann somit auch Ihre E-Mail lesen, ohne dass Sie etwas davon mitbekommen. Abhilfe schafft das verschlüsseln der Mail.

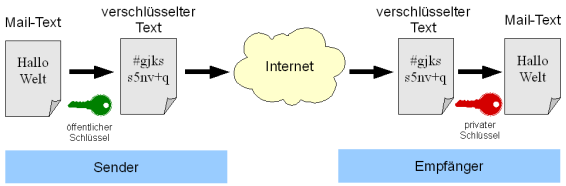
E-Mail-Verschlüsselung funktioniert nur sinnvoll mit einem Programm zum Empfang und zum Versenden von E-Mails, einem sog. E-Mail-Client.

Weit verbreitet ist z.B. *MS Outlook,* aber wir empfehlen freie Software wie den *Mozilla Thunderbird*[1].

Zum verschlüsseln der E-Mails verwenden Sie am besten das Programm *GnuPG*[2], es gibt aber natürlich noch andere (aber häufig auch kostenpflichtige) Software.

Um *GnuPG* und *Thunderbird* zu verbinden, gibt es das Plugin *Enigmail*[3]. Über dieses können Sie alle nötigen Funktionen von *GnuPG* steuern.

Um nun sicher mailen zu können, müssen Sie ein Schlüsselpaar erstellen. Der öffentliche Schlüssel dient zur Verschlüsselung der Mails, die an Sie geschrieben werden. Sie müssen ihn Ihrem Kommunikationspartner mitteilen. Zu diesem Zweck können Sie ihren öffentlichen Schlüssel z.B. per Mail verschicken oder auf einen Schlüsselserver hochladen. Der private Schlüssel dient zur Entschlüsselung ihrer Mails. Ihn müssen Sie auf jeden Fall geheim halten.



Anonym Surfen

Viele Anwender denken, dass Sie im Internet anonym sind. Doch dies ist nicht der Fall. Jedes mal wenn Sie im Internet kommunizieren, sei es Chatten, Surfen oder Mailen, tun Sie dies mittels einer sog. IP-Adresse (so etwas ähnliches wie eine Telefonnummer) und diese ist dank der Vorratsdatenspeicherung 6 Monate Ihrem Internetanschluss zuweisbar. Damit sie also im Netz anonym sind, müssen sie Ihre IP-Adresse verschleiern. Dazu gibt es mehrere Möglichkeiten. Zwei seien hier vorgestellt.

Proxy-Server sind Rechner im Netz, die für Sie eine Anfrage an einen Server stellen und Ihnen die Antwort übermitteln. Sie sind quasi Agenten, die für Sie eine Anfrage stellen. Zur Verwendung muss man nur die IP-Adresse des Proxy-Servers (Listen mit mit Proxy-Adressen finden sich im Netz) im Browser einstellen.

Proxy-Kaskaden sind eine Erweiterung dieses Prinzips. Ein einzelner Proxy-Server könnte ihre Anonymität aufheben, in dem er ihre Anfragen mitprotokolliert (ähnlich wie bei der Vorratsdatenspeicherung). Aus diesem Grund werden bei Proxy-Kaskaden mehrere Proxy-Server hintereinander gestellt und der Verkehr zudem verschlüsselt. Auf diese Weise kann Ihre Anonymität nur aufgehoben werden, wenn alle Proxy-Betreiber in der Kaskade zusammenarbeiten. Die zwei bekanntesten Systeme mit Proxy-Kaskaden sind *Tor*[4] und *JonDonym*[5].

Sensible Daten verschlüsseln

Der Computer ist für viele Leute heutzutage ein unverzichtbares Werkzeug. Häufig befinden sich private Fotos oder Geschäftsgeheimnisse auf dem Computer, die vor unrechtmäßigem Zugriff geschützt werden müssen. In einigen Ländern üblich (und vielleicht auch bald in der EU Alltag) ist z.B. die Laptop-Kontrolle am Flughafen. Hier müssten sie private oder geheime Daten entweder zu Hause lassen oder vom Zoll durchleuchten lassen. Beides keine guten Alternativen. Abhilfe schafft da das verschlüsseln der Daten, z.B. mit der freien Software *Truecrypt*[6]. Damit ist nicht nur das verschlüsseln von einzelnen Dateien, sondern sogar ganzen Festplatten möglich. Und durch die Möglichkeit ihre verschlüsselten Laufwerke in einer anderen verschlüsselten Datei zu verstecken, können Sie auf diese Weise ihre Daten sogar dann geheim halten, wenn Sie gezwungen werden Ihren Schlüssel preiszugeben (z.B. bei der Laptop-Kontrolle am Flughafen). Aber denken Sie dran: Auch hier steht und fällt alles mit dem Passwort!

Weitere Fragen?

Leider reicht der Raum in dieser Broschüre nicht für eine umfassende Erklärung aller Möglichkeiten sich gegen Überwachung und Spionage zu wehren aus. Aber natürlich hilft die Piratenpartei gerne bei Fragen weiter. Ihr Ansprechpartner ist:

1 http://www.mozilla-europe.org/de/products/thunderbird/
2 http://www.gnupg.org/index.de.html
3 http://enigmail.mozdev.org/
4 http://www.torproject.org
5 https://www.jondos.de/
6 http://www.truecrypt.org/

Impressum: Piratenpartei Deutschland – Bezirksverband Oberbayern, Postfach 440534, 80754 München; ViSdP: Andreas Popp, Wackerstr. 33, 85051 Ingolstadt