Abstimmungen und Wahlen

Alle geheimen Personenwahlen und Abstimmungen sollten offline stattfinden, da geheime Wahlen online nicht allgemein nachprüfbar und technische Systeme grundsätzlich - wenn auch mit einigem Aufwand - manipulierbar sind. Ansonsten bietet sich die Software „Dudle“ beispielsweise für die Terminfindung an.

Mehr Informationen und Empfehlungen zur sicheren Kommunikation im Internet gibt’s auf:
www.prism-break.org

Unsere Landesarbeitsgemeinschaft ist offen für alle Mitglieder der LINKEN und natürlich auch für interessierte Nicht-Mitglieder. Wir treffen uns regelmäßig alle zwei Monate um über linke Netzpolitik im Besonderen und die digitale Welt im Allgemeinen zu diskutieren.

Als LAG Netzpolitik wollen wir künftig die Informationsarbeit ausbauen und Diskussionsveranstaltungen innerhalb und außerhalb unserer Partei organisieren. Wir stehen jederzeit für Fragen und Debatten zur Verfügung und freuen uns über Anregungen.

Wann und wo wir uns treffen, findest du regelmäßig auf unserer Website: netzpolitik.die-linke-berlin.de

Falls du Fragen hast oder konkrete Informationen zu unserer Arbeit suchst, kannst du dich natürlich auch per Mail an uns wenden:

DIE LINKE. Berlin / LAG Netzpolitik
Kleine Alexanderstr. 28
10178 Berlin
E-Mail: lag.netzpolitik@die-linke-berlin.de

netzpolitik.die-linke-berlin.de

(Sichere) Kommunikation im Internet

Was man wissen sollte.
Eine Handreichung der Landesarbeitsgemeinschaft Netzpolitik.

DIE LINKE.
LANDESVERBAND BERLIN

Es ist viel von Datenunsicherheit und Überwachung die Rede. Mit diesem Flyer wollen wir die wichtigsten Stichpunkte aufgreifen und allen Interessierten und vielleicht nicht so technik-affinen Menschen ein paar sinnvolle Alternativen und Hinweise mit auf den Weg geben.

Zuallererst muss aber festgehalten werden, dass es keine vollständig sicheren Kommunikationswege gibt und dass Menschen, deren Existenz davon abhängt, sich in jedem Fall tiefergehend mit Computersicherheit auseinandersetzen müssen! Auch muss man sich stets fragen, ob alle involvierten Kommunikationspartner tatsächlich vertrauenswürdig sind. Letztendlich bietet die klassische Überwachung (z.B. Wohnraumüberwachung) auch immer einen wirksamen Angriffspunkt ("Wenn das Eintippen des Passworts gefilmt wird, ist es egal, wie gut das genutzte Programm ist.").

Nichtsdestotrotz ist es sehr sinnvoll, bestimmte kleine Schritte zu gehen, um zumindest nicht in die größten Sicherheitslöcher zu fallen. Neben den üblichen Tipps (sichere Passwörter wählen, regelmäßig Updates installieren, ...) findet ihr nachfolgend praktische Entscheidungshilfen zu vielen Fragen:

Betriebssysteme

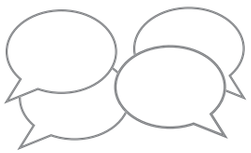
Die grundlegende Software jeden Geräts, egal ob Computer oder Telefon, ist das Betriebssystem. Freie und Open Source Betriebssysteme sind (wie bei anderer Software auch) als sicherer einzustufen, auch wenn dies kein Garant für absolute Sicherheit ist. Auf dem Computer sind also z.B. Ubuntu und Linuxmint ggü. Microsoft Windows und Apple OS X zu bevorzugen. Android-Telefone sind sinnvoll, weil hierbei die Software durch ein Open-Source-Programm (sog. custom ROMs) ausgetauscht werden kann.

Web-Browser

Firefox ist im Hinblick auf die Privatsphäre der zu empfehlende Browser. Das einfach zu bedienende Privacy-Badger-Plugin hilft, das sogenannte Tracking zu minimieren. Zum anonymen Surfen kann das so genannte Tor-Browser-Bundle verwendet werden.

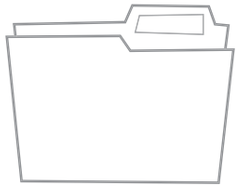
E-Mail

Grundsätzlich muss man davon ausgehen, dass alle E-Mails mitgelesen und gespeichert werden können. Abhilfe dagegen bietet nur eine sogenannte Ende-zu-Ende-Verschlüsselung wie mit dem Programm GnuPG/GPG4Win. Diese bedarf jedoch einer tiefergehenden Auseinandersetzung mit der Materie. Unabhängig davon bietet sich die Nutzung von E-Mail-Providern wie Posteo oder Mailbox.org an. Sie bieten standardmäßig bessere Einstellungen zum Schutz der Privatsphäre und verdienen kein Geld mit den Daten der Nutzerinnen. In jedem Fall ist es auch zu empfehlen, ein separates Programm zum Lesen der E-Mails zu verwenden (z.B. Thunderbird). E-Mails im Browser (z.B. bei web.de oder GMX) zu lesen und senden birgt größere Risiken für Privatsphäre und Sicherheit.



E-Mail-Verteiler

Für E-Mail-Verteiler bzw. Mailinglisten ist die Software „Mailman“ die bessere Alternative zu Angeboten der großen Konzerne wie Google. Der Mailman sollte auch auf einem vertrauenswürdigen Server laufen um unbefugten Zugriff zu verhindern und so konfiguriert werden, dass er keine Informationen an Außenstehende weitergibt.

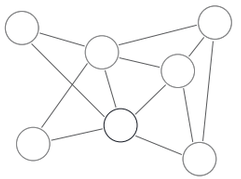


Datei-Austausch

Als sichere Alternative zum beliebten Dienst „Dropbox“ empfiehlt sich „Mega“ und (bedingt) „Teamdrive“. Soweit lokale Partei- oder Jugendstrukturen auch eigene Dateiaustauschdienste anbieten (wie Own-Cloud), sind diese zu bevorzugen.

Nachrichten auf dem Smartphone

Für sichere Kurzmitteilungen gibt es mehrere Alternativen: „Telegram“ (nur mit geheimer Chat-Funktion), TextSecure und Kontalk. Bei Mobilgeräten gilt es aber insbesondere zu beachten, dass oft andere Programme, die man installiert, die Sicherheit des gesamten Geräts gefährden können (selbst harmlos aussehende Spiele). Wer unter Android dieses Risiko minimieren möchte, kann den „F-Droid App-Store“ verwenden und sollte auf andere Apps weitgehend verzichten.



Soziale Netzwerke

Grundsätzlich sind die so genannten sozialen Netzwerke nicht als politische Plattform zu empfehlen und jegliche vertrauliche Kommunikation sollte besser über andere Kanäle stattfinden. Wer aus strategischen Gründen nicht auf die dort vorhandene Öffentlichkeit verzichten möchte, sollte sichergehen, dass dort angebotene Inhalte auch über andere Medien (Blog, Partei-Webseite...) verfügbar sind, um nicht den informativen Wert des "sozialen Netzwerks" unnötig zu steigern. Zudem sollten im Dialog in den sozialen Medien möglichst keine personenbezogenen Informationen ausgetauscht werden.