

Mozilla Thunderbird installieren und nutzen

German Privacy Foundation e.V.

27. Januar 2012

Inhaltsverzeichnis

1	Mozilla Thunderbird	1
1.1	Wörterbücher installieren	1
1.2	Spam-Filter aktivieren	2
1.3	Gesicherte Verbindungen zum Mail-Server	3
1.4	Sichere Konfiguration des E-Mail Client	5
1.5	Datenverluste vermeiden	5
1.6	X-Mailer Kennung modifizieren	6
1.7	Spam-Schutz	8

1 Mozilla Thunderbird

Informationen und Downloadmöglichkeiten für Mozilla Thunderbird stehen auf der deutschsprachigen Website des Projektes unter www.thunderbird-mail.de/ zur Verfügung. Linux Distributionen enthalten in der Regel Thunderbird. Mit der Paketverwaltung kann Thunderbird und die deutsche Lokalisierung komfortabel installiert und aktualisiert werden. Debian GNU/Linux bietet eine angepasste Version von Thunderbird unter dem Namen *Icedove*.

Nach dem ersten Start von Thunderbird führt ein Assistent durch die Schritte zur Einrichtung eines E-Mail Kontos. Nacheinander werden die E-Mail-Adresse sowie die Server für den Empfang und das Versenden von E-Mails abgefragt. Es können auch die Einstellungen eines bisher verwendeten Programms übernommen werden.

Danach sollte man sich einen Moment Zeit nehmen, um die folgenden erweiterten Features von Thunderbird zu konfigurieren.

1.1 Wörterbücher installieren

Nach der Installation einer lokalisierten Version von Thunderbird sind die Wörterbücher für die Standardsprache in der Regel bereits vorhanden. Für alle weiteren Sprachen können die nötigen Wörterbücher zusätzlich installiert werden. Diese stehen unter <http://www.thunderbird-mail.de/> zum Download

zur Verfügung.

Nach dem Download ist Thunderbird als Administrator zu starten. Der Menüpunkt *Extras* -> *Erweiterungen* öffnet den Dialog für die Verwaltung der Plug-Ins. Hier ist der Button *Installieren* zu wählen und in dem sich öffnenden Dateidialog sind die gespeicherten Wörterbücher auszuwählen. Die installierten Wörterbücher erscheinen nicht in der Liste der Plug-Ins.

Nutzer von OpenOffice.org können die Wörterbücher dieser Office-Suite verwenden und müssen sie nicht erneut herunterladen. Für die deutsche Rechtschreibprüfung sind die Dateien *de_DE.aff* und *de_DE.dic* aus dem Unterverzeichnis *share/dict/ooo* der OpenOffice.org Installation in das Unterverzeichnis *components/myspell* der Thunderbird Installation zu kopieren und in *de-DE.aff* sowie *de-DE.dic* umzubenennen.

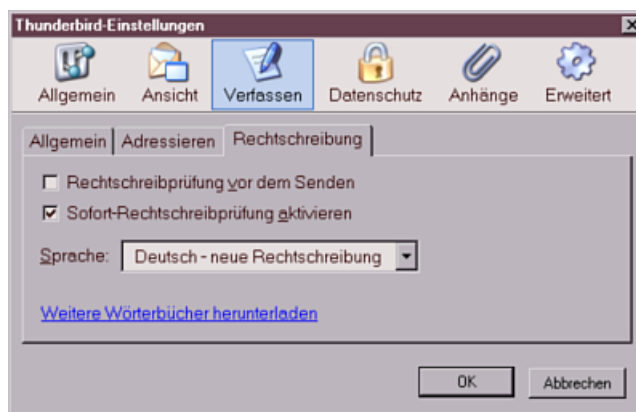


Abbildung 1: Sprache für Rechtschreibung wählen

Im Anschluss ist im Einstellungsdialog in der Sektion *Verfassen* die gewünschte Default-Sprache für das Schreiben von E-Mails auszuwählen und die von einer Textverarbeitung gewohnten Funktionen zur Rechtschreibprüfung stehen auch in Thunderbird zur Verfügung.

1.2 Spam-Filter aktivieren

Das Mozilla Team bezeichnet nicht erwünschte E-Mails (Spam) als Junk. Den integrierten lernfähigen Filter aktiviert man über den Menüpunkt *Extras* -> *Junk-Filter*.

Im Einstellungsdialog des Filters sollte man die beiden Optionen für das automatische Verschieben der Junk-Mails in einen speziellen Ordner aktivieren, am einfachsten in den Ordner *Junk* des entsprechenden Kontos. Außerdem sollte der lernfähige Filter aktiviert werden. Ich bin immer wieder von der guten Erkennungsrate beeindruckt.

1.3 Gesicherte Verbindungen zum Mail-Server

Die Grafik im Bild 2 zeigt den Weg einer E-Mail vom Sender zum Empfänger.

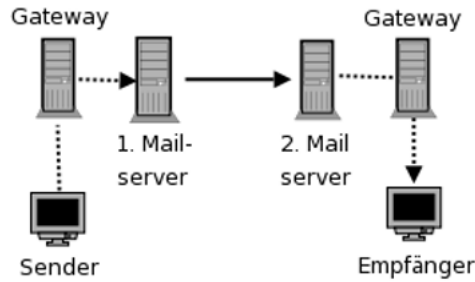


Abbildung 2: Der Weg einer E-Mail durch das Web

In der Regel sind die Rechner der Nutzer nicht direkt mit dem Internet verbunden. Der Zugang erfolgt über ein Gateway des Providers oder der Firma.

Der 1. Mailserver nimmt die Mail via SMTP entgegen und sendet sie an den 2. Mailserver. Hier liegt die Mail, bis der Empfänger sie mittels POP3 abrufen. Mit dem Abrufen kann die Mail auf dem Server gelöscht werden. Es ist auch möglich, die Mail auf dem Server zu lesen, z.B. über ein Webinterface oder mittels IMAP-Protokoll. Die Möglichkeit des weltweiten Zugriffs auf seine Mails erkaufte der Nutzer sich jedoch mit einer Einschränkung des Datenschutzes. (siehe <http://blog.kairaven.de/archives/1060-Unsichere-und-geschuetzte-E-Mail-Sphaeren.html>).

Die im Bild 2 gestrichelten dargestellten Verbindungen zu den Mailservern können mittels SSL bzw. TLS kryptografisch gesichert werden. Das hat nichts mit einer Verschlüsselung des Inhalts der E-Mail zu tun. Es wird nur die Datenübertragung zum Mailserver verschlüsselt und es wird sichergestellt, dass man wirklich mit dem gewünschten Server verbunden ist.



Abbildung 3: Konfiguration für das Abrufen von Nachrichten

Wie einfach es ist, ungesicherte Verbindungen zu belauschen, die Passwörter zu extrahieren und das Mail-Konto zu kompromittieren, wurde auf der re:publica 2008 demonstriert.

Bewusst oder unbewusst können auch Provider die sichere Übertragung deaktivieren und damit den Traffic mitlesen. Es wird einfach die Meldung des Mail-Servers 250-STARTTLS gefiltert und überschrieben. Scheinbar verfügen alle DSL-Provider über die Möglichkeit, dieses Feature bei Bedarf für einzelne Nutzer zu aktivieren. (<http://www.heise.de/security/news/meldung/116073>) Die Standard-Einstellung der meisten E-Mail Clients ist *“TLS verwenden wenn möglich”*. Diese Einstellung ist genau in dem Moment wirkungslos, wenn man es braucht weil der Traffic beschnüffelt werden soll.

Fast alle Mail-Server bieten Optionen zur verschlüsselten Kommunikation mit dem E-Mail Client. Diese Option ist in Thunderbird nach der Einrichtung eines neuen Kontos zu aktivieren. Die Einstellungen des POP3-Servers findet man in dem Dialog *Konten...* im Unterpunkt *Server-Einstellungen* des Kontos (Bild 3). In der Regel unterstützen POP3-Server die SSL-Verschlüsselung.

Ebenfalls im Dialog *Konten...* findet man die Einstellungen für die SMTP-Server (ganz unten). In der Liste der Server ist der zu modifizierende Server auszuwählen und auf den Button *Bearbeiten* zu klicken. In dem sich öffnenden Dialog kann eine Option zur verschlüsselten Versendung gewählt werden.

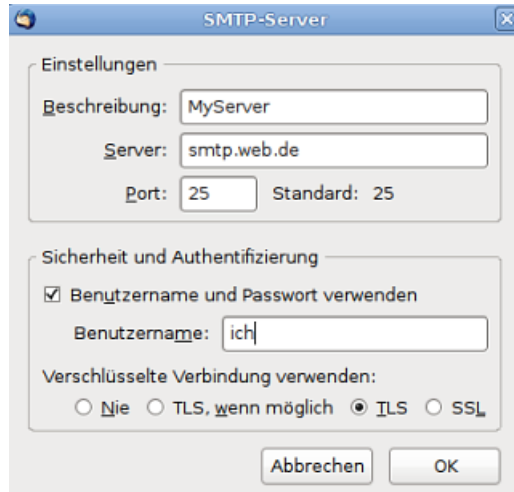


Abbildung 4: Konfiguration für den SMTP-Server

Viele SMTP-Server bieten neben TLS-Verschlüsselung für Port 25 auch auf den Ports 587 (submission, TLS) oder 465 (SMTP-SSL) verschlüsselte Verbindungen für das Senden von E-Mails. Diese Ports muss man bei der Verwendung von Anonymisierungsdiensten wie Tor oder JonDonym nutzen, da diese Dienste den Port 25 aus Gründen des Spam-Schutzes in der Regel sperren.

1.4 Sichere Konfiguration des E-Mail Client

Einige Hinweise für die sichere und unbeobachtete Nutzung des Mediums E-Mail mit Mozilla Thunderbird:

- Mit der Verwendung von HTML in E-Mails steht dem Absender ein ganzes Bestarium von Möglichkeiten zur Beobachtung des Nutzers zur Verfügung: HTML-Wanzen, Java Applets, JavaScript, Cookies usw. Am einfachsten deaktiviert man diese Features, wenn man nur die Anzeige von *Reinem Text* zulässt.



Abbildung 5: Ansichten als reien Text darstellen

Die Option findet man im Menüpunkt *Ansicht* -> *Nachrichtentext* (siehe Bild 5). Wer auf grafischen Schnick nicht ganz verzichten will, wählt die Option *Vereinfachtes HTML*. In diesem Fall werden nur HTML Tags für das Layout interpretiert, beispielsweise Fettdruck oder Tabellen.

- Die Option *Anhänge eingebunden anzeigen* im Menü *Ansicht* sollte man ebenfalls deaktivieren, um das gefährlicher Anhänge nicht schon beim Lesen einer E-Mail automatisch zu öffnen.
- Das Laden externer Grafiken ist zu blockieren. Häufig wird dieses Feature von Spammern zu Beobachtung des Nutzers eingesetzt. Die Option findet man im Dialog *Einstellungen* in der Sektion *Datenschutz* auf dem Reiter *Allgemein*.
- Gespeicherte Passwörter für den Zugriff auf SMTP-, POP- oder IMAP-Server sollten mit einem Masterpasswort vor Unbefugten geschützt werden (siehe Bild 6).

1.5 Datenverluste vermeiden

Die folgenden Hinweise wurden von den Mozilla-Entwicklern erarbeitet, um den Nutzer bestmöglich vor Datenverlusten zu schützen:

- Das Antiviren-Programm ist so einzustellen, dass es den Profildrner von Thunderbird NICHT(!) scannt. Die automatische Beseitigung von Viren kann zu Datenverlusten führen.

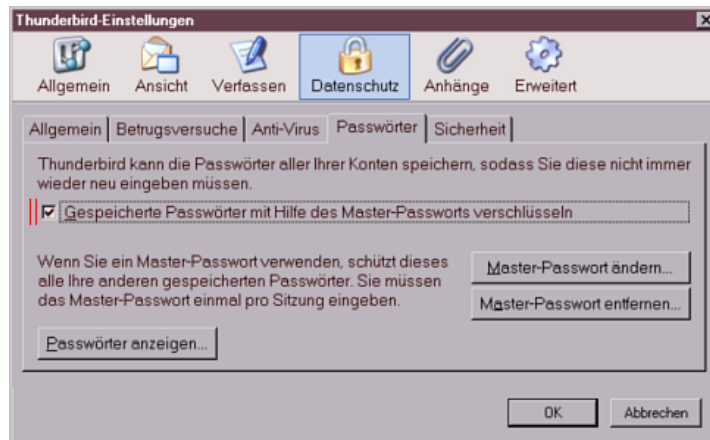


Abbildung 6: Masterpasswort festlegen

- Der Ordner *Posteingang* sollte so leer wie möglich gehalten werden. Gelesene E-Mails sollten auf themenspezifische Unterordner verteilt werden.
- Die Ordner sollten regelmäßig komprimiert werden. Hierzu ist mit der rechten Maustaste auf den Ordner zu klicken und der Punkt *Komprimieren* zu wählen. Während des Komprimierens sollten keine anderen Aktionen in Thunderbird ausgeführt werden.

Alternativ kann man in den Einstellungen von Thunderbird in der Sektion *Erweitert* auch eine automatische Komprimierung konfigurieren, sobald es lohnenswert ist (siehe Bild 7). Bei jedem Start prüft Thunderbird, ob die Ordner komprimiert werden können.

- Regelmäßig sollten Backups des gesamten Profils von Thunderbird angelegt werden. Unter WINDOWS sichert man *C:/Dokumente und Einstellungen/<NAME>/Anwendungsdaten/Thunderbird*, unter Linux ist *\$HOME/.thunderbird* zu sichern.

1.6 X-Mailer Kennung modifizieren

Wir haben gelesen, dass es kriminelle Elemente gibt, die via Internet ihre Software auf fremden Rechnern installieren möchten. In diesem Zusammenhang werden oft die Stichworte “Spambot” oder “Bundstrojaner” genannt.

Voraussetzung ist die Kenntnis der vom Opfer genutzten Software. Genau wie jeder Webbrowser sendet auch Thunderbird eine user Agent Kennung im Header jeder E-Mail, die Auskunft über die genutzte Programmversion und das Betriebssystem liefert. Das folgende (veraltete) Beispiel stammt aus der Mail eines Unbekannten:

```
...
User-Agent: Thunderbird 2.0.0.6 (X11/20070728)
```

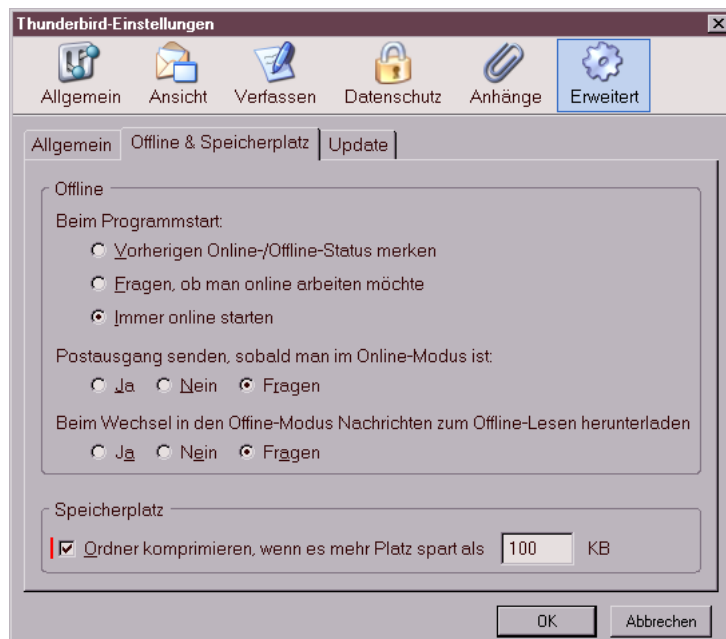


Abbildung 7: Ordner automatisch komprimieren

X-Enigmail-Version: 0.95.3

...

----- BEGIN PGP MESSAGE -----

Version: GnuPG v1.4.6 (GNU/Linux)

...

Aha, er nutzt also Thunderbird in der Version 2.0.0.6 unter Linux, hat die Enigmail-Erweiterung v.0.95.3 installiert und verwendet die GnuPG-Version 1.4.6. Das war damals eine typische Kombination für Ubuntu Edgy.

Die User-Agent-Kennung kann in den erweiterten Einstellungen modifiziert werden. Im Einstellungs-Dialog findet man in der Sektion *Erweitert* den Reiter *Allgemein*. Ein Klick auf den Button Konfiguration bearbeiten öffnet eine Liste aller Optionen.

Hier fügt man die neue String-Variable **general.useragent.override** als neuen Wert ein, indem man mit der rechten Maustaste auf einen freien Bereich klickt und im Kontext-Menü den Punkt *Neu - String* wählt.

Man kann auf eine beachtliche Auswahl an Kennungen für die Variable *general.useragent.override* zurückgreifen. Da jeder E-Mail Client einen typischen Aufbau des Headers verwendet, sollte man für einen plausiblen Fake nur Kennungen von Thunderbird Versionen verwenden. (Da auch Spam-Scanner diese Informationen analysieren, bleibt eine Mail mit einem Outlook-Fake eher im Junk hängen.)

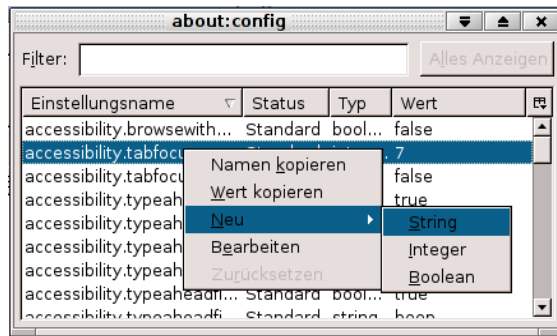


Abbildung 8: Neue Config-Variable anlegen

Mozilla/5.0 (Windows; U; Windows NT 6.0; en-US; rv:1.9.2.15)
 Gecko/20110303 Thunderbird/3.1.9

Mozilla/5.0 (X11; U; Linux i686; en-US; rv:1.9.2.21)
 Gecko/20110831 Thunderbird/3.1.13

Mozilla/5.0 (Windows; U; Windows NT 6.0; de; rv:1.9.2.15)
 Gecko/20110303 Lightning/1.0b2 Thunderbird/3.1.9

Mozilla/5.0 (Windows NT 6.0; rv:8.0) Gecko/20111105 Thunderbird/8.0

Mozilla/5.0 (Windows NT 6.1; WOW64; rv:9.0) Gecko/20111222
 Thunderbird/9.0.1

Mozilla/5.0 (Macintosh; Intel Mac OS X 10.7; rv:9.0)
 Gecko/20111222 Thunderbird/9.0.1

Wer die Erweiterung Enigmail für die Verschlüsselung nutzt, sollte dieser Erweiterung die Geschwätzigkeit abgewöhnen und die Ausgabe von Versionen im Header deaktivieren. Die Variable *extensions.enigmail.addHeaders* ist in den erweiterten Optionen auf *false* zu setzen!

Außerdem sind in den Einstellungen von Enigmail für GunPG folgende zusätzliche Optionen einzutragen, welche die Ausgabe der GnuPG-Version unterbinden:

```
--no-emit-version
```

Anderenfalls sieht ein Schnüffler an einer signierten oder verschlüsselten E-Mail, dass nicht MacOS genutzt wird, sondern evtl. Linux oder WINDOWS.

1.7 Spam-Schutz

Man muss nicht bei jeder Gelegenheit im Web seine richtige E-Mail Adresse angeben. Damit fängt man sich eine Menge Spam (Junk) ein.

Außerdem ist die E-Mail Adresse ein wichtiges Identitätsmerkmal. Datensammler verwenden sie als ein Hauptmerkmal für die Identifikation, um darauf aufbauend Profile zu erstellen. Stichproben im Internet-Traffic weisen einen hohen Anteil von Suchanfragen nach Informationen zu den Inhabern von E-Mail Adressen aus.

Um die eigene E-Mail Adresse nicht zu kompromittieren und trotzdem Angebote zu nutzen, welche die Angabe einer Mailadresse erfordern, kann man temporäre *Wegwerf-Adressen* nutzen.

Bei der Nutzung temporärer Mailadressen geht es nicht(!) um die Umgehung der Vorratsdatenspeicherung. Hinweise dafür findet man im Abschnitt "*E-Mail anonym nutzen*".

10min Mail-Adressen

Man kann auf den Webseiten der Anbieter mit einem Klick eine E-Mail Adresse anlegen, die für 10min...60min gültig ist. Bei Bedarf kann die Verfügbarkeit der E-Mail Adresse verlängert werden. Das reicht, um sich in einem Forum anzumelden oder einen Blog-Kommentar zu posten.

- www.10minutemail.com (10min gültig, verlängerbar)
- mail2null.nl (10min gültig, Session-Cookies müssen freigegeben werden)
- tempemail.co.za (30min gültig, Session-Cookies freigeben)
- rentmail.org (60min gültig, Session-Cookies freigeben, 5-15min Verzögerung bei der Zustellung, da der Server Greylisting nutzt, nicht unbedingt empfehlenswert)

Um eine 10minuten Adresse für die Anmeldung in einem Forum o.ä. zu nutzen, öffnet man als erstes eine der oben angegebenen Webseiten in einem neuen Browser-Tab. Session-Cookies sind für diese Website freizugeben, mit Javascript sind die Webseiten oft besser bedienbar. Nachdem man eine neue temporäre Mail-Adresse erstellt hat, überträgt man sie mit Copy & Paste in das Anmeldeformular und schickt das Formular ab. Dann wechselt man wieder zu dem Browser-Tab der temporären Mailadresse und wartet auf die eingehende Bestätigungsmail. In der Regel enthält diese Mail einen Link zur Verifikation. Auf den Link klicken - fertig.

AnonBox des CCC

Die AnonBox (<https://anonbox.net>) ist ein ähnliches Projekt wie 10minutemail. Auf der Webseite kann ein E-Mail Account für den Empfang von Nachrichten erstellt werden. Der Account ist bis 24:00 Uhr des folgenden Tages gültig und nicht verlängerbar. Eingehende Nachrichten werden nach dem Abrufe gelöscht. Sie können nur 1x gelesen werden!

Die AnonBox bietet als einziges Projekt HTTPS-Verschlüsselung.

6-12h Mail-Adressen

Einige Anbieter von Wegwerf-E-Mail-Adressen bieten einen sehr einfach nutzbaren Service, der keinerlei Anmeldung erfordert. E-Mail Adressen der Form *pittiplatsch@trash-mail.com* oder *pittiplatsch@emaildienst.de* kann man überall und ohne Vorbereitung angeben.

Liste einiger Anbieter (unvollständig):

- <http://www.sofort-mail.de>
- <http://www.trash-mail.com>
- <http://dodgit.com>
- <http://www.mailinator.com/>

In einem Webformular auf der Seite des Betreibers findet man alle eingegangenen Spam- und sonstigen Nachrichten für das gewählte Pseudonym. Für das Webinterface des Postfachs gibt es keinen Zugriffsschutz. Jeder, der das Pseudonym kennt, kann die Nachrichten lesen. Alle eingegangenen Nachrichten werden nach 6-12h meist automatisch gelöscht.

In der Regel speichern diese Anbieter die Informationen über eingehende E-Mails sowie Aufrufe des Webinterface und stellen die Informationen bei Bedarf den Behörden zur Verfügung. Es handelt sich dabei nicht Anonymisierungsdienste.

Firefox Addon Bloody Vikings

Das Firefox Addon Bloody Vikings vereinfacht die Nutzung von Wegwerfadressen. Nach der Installation von der Webseite kann ein bevorzugter Dienst für die Wegwerfadressen gewählt werden.

<https://addons.mozilla.org/de/firefox/addon/bloody-vikings>

In Zukunft kann man in jedem Anmeldeformular mit der rechten Maustaste auf das Eingabefeld der E-Mail Adresse klicken und aus dem Kontextmenü den Punkt *Bloody Vikings* wählen. Es wird in einem neuen Browser Tab die Webseite des Anbieters geöffnet und die temporäre E-Mail Adresse in das Formularfeld eingetragen. Nach dem Absenden des Anmeldeformular wechselt man in den neu geöffneten Browser Tab und wartet auf die Bestätigungsmail.

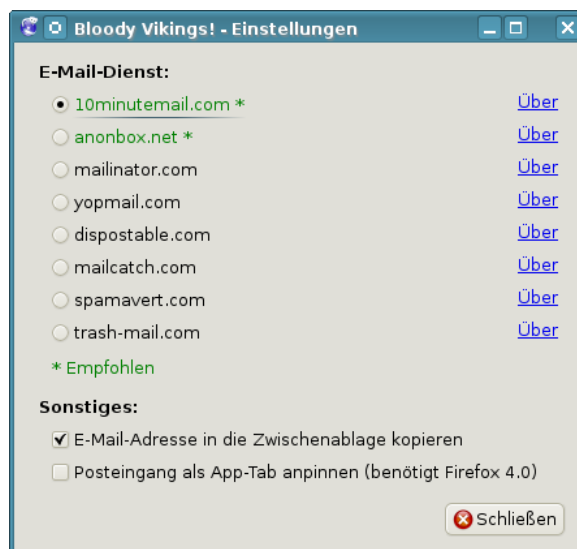


Abbildung 9: Bloody Vikings konfigurieren