


Linux im Alltag am 13.5. ab 10 Uhr



Von: [WD Zimmermann <wd.zimmermann@posteo.de>](mailto:wd.zimmermann@posteo.de)
An: [wolf-dieter zimmermann <wd.zimmermann@posteo.de>](mailto:wolf-dieter.zimmermann@posteo.de)
Datum: 22.04.23 13:39
Spam-Status: Spamassassin
Sicherheit: 
Anhänge: [OpenPGP_0xC42E25F77FF311A4.asc](#)

Not enough information to check signature validity.

[Show Details](#)

Liebe Freundinnen und Freunde Freier Software, gar von Linux.

Natürlich habe ich mich letztlich nicht beherrschen können und habe ChatGPT mit den Stichworten "Linux" und "Freiheit vor Viren" arbeiten lassen. Das Ergebnis:

/ZitatAnfang

Linux ist ein Betriebssystem, das von Natur aus aufgrund seiner Architektur und Sicherheitsmerkmale eine höhere Widerstandsfähigkeit gegen Viren und Malware aufweist als andere Betriebssysteme wie Windows oder MacOS.

Es gibt mehrere Gründe, warum Linux weniger anfällig für Viren ist:

Benutzerrechte: Unter Linux arbeiten Benutzer standardmäßig mit eingeschränkten Rechten. Selbst wenn ein Angreifer erfolgreich eine Schwachstelle im System ausnutzt, kann er nur auf die Ressourcen zugreifen, die für seinen Benutzerzugriff autorisiert sind. Dies erschwert das Eindringen von Viren in das System.

Geschlossene Ports: Linux-Systeme sind von Natur aus mit einer minimalen Anzahl von offenen Ports ausgestattet, wodurch potenzielle Angriffsvektoren minimiert werden. Jeder Dienst, der auf einem Linux-System ausgeführt wird, muss explizit konfiguriert und gestartet werden, um auf Netzwerkverbindungen zu lauschen.

Paketmanagement: Unter Linux werden Anwendungen in Form von Paketen installiert, die von offiziellen Quellen oder von vertrauenswürdigen Repositories bezogen werden. Dies bedeutet, dass jede Anwendung vor der Installation auf das System überprüft wird, um sicherzustellen, dass sie keine bösartigen Inhalte enthält.

Sicherheitsfokussierte Entwicklung: Linux ist ein Open-Source-Betriebssystem, das von einer breiten Community von Entwicklern gepflegt wird. Die Entwickler haben ein hohes Bewusstsein für Sicherheitsprobleme und arbeiten ständig daran, das System sicherer zu machen und Schwachstellen zu beheben.

Obwohl Linux nicht völlig immun gegen Viren und Malware ist, haben die oben genannten Faktoren dazu beigetragen, das System widerstandsfähiger zu machen. Es ist jedoch wichtig zu beachten, dass die Sicherheit eines Linux-Systems auch von den Handlungen des Benutzers abhängt, wie zum Beispiel dem Installieren von Anwendungen aus vertrauenswürdigen Quellen und dem Vermeiden von verdächtigen Links und Anhängen.

/ZitatEnde

Das hätte ich nicht schöner formulieren können! Ich hätte zusätzlich darauf hingewiesen, dass Freie Software eine wunderbare Ergänzung für Linux darstellt. Bei Freier Software stehen die Quellen in aller Regel bekanntlich offen im Internet.

Kritisch anmerken muss ich, dass diese Anfrage bei ChatGPT ein Vielfaches an Energie verbraten hat als wenn ich es einfach selbst formuliert hätte.

Interessant auch, dass in der beginnenden Diskussion zwei Forderungen zunehmend wichtig werden: Es sollen viele Anbieter werden, also keine Monopolbildung und eine öffentliche Kontrolle soll ebenfalls verstärkt werden. Kritisches Lesen bleibt allerdings für alle die Hauptdisziplin!

Ein Zweites: Letzthin habe ich mir ein ganzes Heft (c't Daten schützen) zum Thema Datensicherheit gekauft. Die Essenz fasse ich in die folgenden Tipps zusammen - damit könnt ihr euch schon mal das Geld sparen:

/ZitatAnfang

Online-Schurken haben es nicht nur auf DAX-Konzerne abgesehen, sondern auf jeden.

Jeder abgefischte Instagram- oder Netflix-Account bringt im Darknet zwar nur ein paar Dollar - aber Kleinvieh macht auch Mist.

Tipp 1: Immer mit aktuellen Versionen von Browser, Betriebssystem und Mailprogramm arbeiten. Ebenso das aktuellste Officepaket und pdf-Viewer.

Tipp 2: Immer die Textversion einer Mail einstellen, nicht die HTML-Version.

Tipp 3: Niemals einen Link in der Mail öffnen, beim scheinbaren Absender auf einem anderen Weg über Korrektheit vergewissern.

Tipp 4: An dich gerichtete Mails OHNE persönliche Ansprache immer misstrauen.

Tipp 5: Microsoft Office ist Angreifers Liebling, arbeite besser mit LibreOffice.

Tipp 6: Steuere Links besser über die Bookmarks im Browser, nicht aus der Mail an.

Tipp 7: Meide Abmelde-Links (Unsubscribe), filtere Spam in den Papierkorb, lösche sie möglichst schon vom Server.

Hinweis 1: Jeder Dienst hat sein eigenes Passwort

Hinweis 2: Lade niemals Dateien mit privaten Inhalten auf fremde Server. Denke daran: "There is no cloud. There are only other peoples computer".

Hinweis 3: Kein Backup, kein Mitleid.

/ZitatEnde

Es gab im Heft natürlich auch noch weitere Hinweise und Themen.

Anlass dieser E-Mail sind natürlich nicht nur die Inhalte, sondern die nächsten Termine.

Wie jedes Jahr findet auch diesmal wieder ein Termin in der VHS statt. Wie immer unter der Überschrift: "Linux im Alltag" - am 13.5., um 10 Uhr geht es los.

Für immer mehr Leute aus Mülheim ist das fast ein Pflichttermin, trifft man dort doch Interessierte, kann an Informationen und Workshops teilnehmen, sich schlau machen. Inzwischen sind mehr als 500 Rechner hier in Mülheim auf Linux umgestellt und machen dort selbstverständlich ihre Arbeit.

Das vollständige Programm kann unter <https://netzwerk-bildung.net/kurse-termine/lia/index.html> zur Kenntnis genommen werden, der Termin ist kostenfrei.

Wir hoffen auf regen Besuch, bieten wir doch nach dem Eingangsvortrag vier parallele Workshops an. Die sollten alle reichlich besucht werden.

Gerne kann auch im Kreis der Bekannten für den Termin geworben werden, sind doch aktuell viele Rechner unter anderen Systemen von Sicherheitslücken betroffen, die Viren gute Chancen für ein Eindringen eröffnen.

Außerdem sind wir am ersten Samstag im Mai (das ist heuer der 6.5) von 10.30 bis 13.30 Uhr im Medienzentrum anzutreffen. Auch dort findet

Beratung und Unterstützung bei Installation und Wartung eines höchst interessanten Systems statt. Aber das wisst ihr ja.

Bis denne!

--

Freundliche Grüße

Wolf-Dieter Zimmermann

E: wd.zimmermann@posteo.de

U: netzwerk-bildung.net

OpenPGP Key

This is an OpenPGP key, which can be used to sign or encrypt emails.

[Show key details ...](#) | [Import key](#)

End of signed message