Dienstag, 06. August 2019, 15:00 Uhr
~11 Minuten Lesezeit

Die Zwangsbeglücker

Microsoft-Produkte sind allgegenwärtig — das ist gefährlich für Datensicherheit und Privatsphäre im Netz.

von Wolfgang Romey
Foto: Preechar Bowonkitwanchai/Shutterstock.com

Privathaushalte, Vereine, Kirchen, gemeinnützige Organisationen, Parteien, Betriebe und Unternehmen, Krankenhäuser, die öffentlichen Verwaltungen, Ministerien, der gesamte Bildungsbereich, alle nutzen intensiv Microsoft-Produkte. Ausgenommen sind nur die Bereiche, in denen leistungsfähige und sichere Datenverarbeitungssysteme eingesetzt werden müssen: die Rechenzentren der Banken und Versicherungen, die Hochschulrechenzentren, die Rechenzentren der öffentlichen Verwaltung und so weiter. Dort wird oftmals das Freie Betriebssystem GNU/Linux (1) eingesetzt. Das ist auch gut nachvollziehbar, denn die

Rechenzentren müssen ja ohne Ausfälle fehlerfrei arbeiten.

Dann kam WannaCry

Die EDV-Landschaft ist also weitestgehend einheitlich. Was ist daran so schlimm? Was daran so schlimm ist, konnte man im Mai 2017 beobachten, als der WannaCry (https://de.wikipedia.org/wiki/WannaCry)-Virus zuschlug. Die Zuganzeige der Bahn funktionierte nicht, Krankenhäuser mussten auf Notbetrieb umstellen, in China konnte man an etwa 20.000 Tankstellen nur noch bar bezahlen, um nur einige Folgen zu nennen.

Entscheidend dafür war zweierlei: Auf allen betroffenen Computern lief eine Version des Betriebssystems Windows von Microsoft, die nicht auf den letzten Stand gebracht worden war. Für die sehr weit verbreiteten Versionen XP und 8.1 bot Microsoft schon seit einiger Zeit keine Sicherheitsupdates an, die die Rechner hätten schützen können.

Lag also Fahrlässigkeit vor, weil die betroffenen Rechner nicht auf den letzten Stand gebracht worden waren? Keineswegs. Es ist nicht einfach, ein großes Rechnernetzwerk auf dem aktuellen Software-Stand zu halten. Das ist personalintensiv, man kann nicht sicher sein, dass das Updaten erfolgreich sein wird, oftmals funktioniert danach vorhandene Hardware, beispielsweise der Drucker, nicht mehr. Also belässt man es lieber beim bestehenden Zustand und handelt sich unter Umständen massive Sicherheitsprobleme ein — nicht ohne Grund heißt es: „Never change a running system!“

> ***Sicherheitsprobleme entstehen, weil der Quellcode des***

> ***Betriebssystems Windows geheim ist.***

Nur die Institutionen, denen der Quellcode des Programms zugänglich gemacht worden war, konnten ihn überprüfen. Dazu gehört auch die NSA, die die für WannaCry aufgedeckte Sicherheitslücke gefunden, aber nicht veröffentlicht hat, da man sie für Angriffszwecke nutzen wollte. Allerdings war damit die Büchse der Pandora offen, aus der WannaCry entwich und von Kriminellen genutzt wurde.

Das war aber nicht die letzte Sicherheitslücke, die gefunden wurde: Am 15. Mai 2019 wurde auf Golem.de gemeldet: „*Eine **Sicherheitslücke in Windows** (https://www.golem.de/news/microsoft-warnt-eine-sicherheitsluecke-wie-wanna-cry-1905-141264.html) ermöglicht das Ausführen von Schadcode aus der Ferne. Eine Schadsoftware könnte sich wie WannaCry selbstständig weiterverbreiten. Microsoft stellt sogar für Windows XP Patches bereit.*“

Wie kann es sein, dass in einer 2001 eingeführten Software immer noch Sicherheitslücken entdeckt werden? Das liegt unter anderem daran, dass Software zu den komplexesten technischen Produkten gehört, die es gibt. Wichtiger ist aber, dass Microsoft den Quelltext der Software nicht veröffentlicht und damit die Fehlersuche drastisch erschwert. Wäre der Quelltext offen einsehbar, wäre die Sicherheitslücke vermutlich entdeckt und geschlossen worden. — Wie das beim freien Betriebssystem GNU/Linux Praxis ist.

> ***Grundsätzlich hat eine einheitliche IT-Landschaft den Nachteil, dass sie für Virenprogrammierer und alle anderen, die den Nutzern übel wollen, hoch attraktiv ist, also beispielsweise um die Zugangsdaten zu Bankkonten auszuspähen.***

Gelingt ein Angriff, gelingt er gleich bei vielen Millionen Nutzern.

GNU/Linux ist aus zwei Gründen nicht so attraktiv:

- Es ist (noch) zu wenig verbreitet, als das sich ein Angriff lohnen würde;
- Es gibt mehr als 200 Distributionen (2), die GNU/Linux als Betriebssystem nutzen. Die Sicherheitseinstellungen sind zudem drastisch restriktiver als bei einem Windowssystem.

Die Gefahr, Sicherheitslücken flächendeckend ausgesetzt zu sein, ist nur einer der Gründe, von unfreien Betriebssystemen wie Windows und Mac OS zu einem Betriebssystem zu wechseln, bei dem der Quellcode offen liegt und deshalb Fehler und Sicherheitslücken gefunden und behoben werden können und der verbesserte Programm-Code ohne Lizenzprobleme verteilt werden kann, weil die Lizenz, unter der GNU/Linux entwickelt wird, dies explizit erlaubt.

Wir schenken Ihnen Windows 10

Microsoft hat in der Vorbereitung auf Windows 10, die aktuelle Version seines Betriebssystems, sein Geschäftsmodell geändert. Man will zukünftig, wie von Google und Facebook vorgemacht, sein großes Geld mit den Daten der Nutzer verdienen. Die Version 10 des Betriebssystems Windows ist deshalb den meisten Nutzern aufgedrängt worden, bei neuen Rechnern ist Windows 10 in den meisten Fällen vorinstalliert. Nach der Installation ist Windows 10 mit Funktionen ausgestattet, die die Daten der Nutzer umfassend erfassen und an Microsoft liefern. Mitschnitt der Sprache oder Erfassung der Tastatureingaben ist nur ein kleiner Teil davon.

> ***Mit Windows 10 holt man sich also ein umfassendes Ausforschungssystem ins Haus.***

Deshalb hat das Bundesamt für Sicherheit in der

Informationstechnik (BSI) eine **Empfehlungen für Privatanwender** (https://www.bsi-fuer-buerger.de/SharedDocs/Downloads/DE/BSIFB/Publikationen/BSI_CS_019.pdf?__blob=publicationFile&v=4) zur sicheren Nutzung von Geräten unter Microsoft Windows 10 herausgegeben. Skandalös ist, dass das BSI aus Steuergeldern eine Version von Windows 10 (**Bundesclient** (https://www.heise.de/ix/meldung/Bund-will-Windows-10-ueber-Bundesclient-sicher-nutzen-koennen-3907088.html)) erstellen lassen will, die den sicheren Einsatz von Windows 10 in der öffentlichen Verwaltung ermöglichen soll. Diese Kosten kommen zu den aus Steuergeldern finanzierten Lizenzen hinzu.

In den Niederlanden ist eine Datenschutz-Folgenabschätzung durchgeführt worden mit dem Ergebnis, dass es hohe **Datenschutz-Risiken bei Microsoft** (https://www.privacycompany.de/datenschutz-folgenabschatzung-zeigt-risiken-bei-microsoft-office-proplus-enterprise/) Office ProPlus Enterprise gibt, das etwa 300.000 Mal in niederländischen Behörde eingesetzt wird.

Hessens Datenschutzbeauftragter Michael Ronellenfitsch warnt, dass die mit dem Büropaket in der Cloud gespeicherten Daten in den USA abgegriffen werden könnten und kommt zum Ergebnis: ***„Einsatz von Microsoft Office 365 an Schulen ist unzulässig"*** (https://www.heise.de/newsticker/meldung/Datenschuetzer-Einsatz-von-Microsoft-Office-365-an-Schulen-ist-unzulaessig-4466156.html). Das wird aber vermutlich wenig Folgen haben, weil fast alle, der Bildungsminister, die Bildungsadministration, die Eltern und die Schüler, den Einsatz für unumgänglich halten. Wen stört da schon die Rechtslage? Zumal es die Software **umsonst** (https://www.microsoft.com/de-de/education/products/office) gibt. Ich frage mich, ob die Rechtswidrigkeit nicht für alle öffentlichen Einrichtungen gilt, die Office 365 einsetzen.

Weitere Nachteile und Gefahren

Wichtig ist auch, dass man bei den Microsoft-Programmen in der Regel nur die Lizenz zur Nutzung der Programme erwirbt. Man ist damit Microsoft bei den Kosten für ein Upgrade ausgeliefert, Microsoft ist völlig frei in der Preisgestaltung. Da die neuen Versionen der Programme oftmals mit den alten Versionen nicht mehr ohne Probleme zusammen arbeiten, ist man als Nutzer gezwungen, die Lizenz für die Nutzung der neuen Version zu erwerben.

In den letzten Tagen ist deutlich geworden, dass es gefährlich ist, wenn man die Programme nicht besitzt. So hat Microsoft angekündigt, dass es die **Server für Bücher** (https://www.wired.com/story/microsoft-ebook-apocalypse-drm/) abschalten wird, für die die Nutzer auch nur eine Nutzungslizenz erworben haben. Die gesamte Büchersammlung ist damit erst einmal weg. Zwar wird Microsoft die Kosten für den Erwerb der Lizenzen erstatten, für Texte mit Anmerkungen gibt es sogar 25 US-Dollar mehr, ein mit Anmerkungen versehener Text kann aber für den Nutzer wesentlich mehr wert sein.

> ***Sichtbar geworden ist in den letzten Tagen auch, dass sich Microsoft an der Sanktionspolitik der US-amerikanischen Administration beteiligt.***

GitHub, ein Angebot für die Entwicklung und Verwaltung von Software, das vor einiger Zeit von Microsoft übernommen wurde, **verweigert seit kurzem Nutzern den Zugang auf der Grundlage ihrer Nationalität** (https://medium.com/@hamed/github-blocked-my-account-and-they-think-im-developing-nuclear-weapons-e7e1fe62cb74): Der Zugang zu GitHub ist für Nutzer aus dem Iran, Syrien, der Krim, Kuba und Nordkorea blockiert, sie haben also keinen Zugang mehr zu ihrer Software. Das Perfide daran ist, dass dies ohne Vorankündigung geschehen ist.

Für die öffentliche Hand entstehen durch die zu zahlenden Lizenzkosten wiederkehrende Ausgaben in Millionenhöhe. Nicht ohne Grund ist Bill Gates Milliardär geworden. Statt diese Mittel für die Pflege und Weiterentwicklung beispielsweise der öffentlichen IT-Infrastruktur zu verwenden, werden Nutzungsrechte erworben, die noch nicht einmal die Möglichkeit der Einsichtnahme in den Programmcode beinhalten. Diese Lizenzkosten entstehen für jeden, der Microsoft-Produkte (legal) nutzt und sich wegen des nicht frei verfügbaren Programmcodes abhängig von Microsoft macht.

Die Abhängigkeit geht aber noch weiter: Das Programmpaket MS-Office verwendet für die Speicherung der erzeugten Daten wie Texte, Tabellen oder Präsentationen Datei-Formate, deren **Dokumentation** (https://fsfe.org/activities/os/msooxml.en.html#compatibility-and-interoperability) sehr komplex ist. Sie umfasst etwa 6.000 Seiten, die Dokumentation des freien OpenDocument-Standards, die beispielsweise die Bürosoftware LibreOffice verwendet, kommt dagegen mit 1.000 Seiten aus. Der Umfang der Dokumentation hat zur Folge, dass nur Microsoft in der Lage ist, Software zu erstellen, die das Datei-Format vollständig umsetzen. Glücklicherweise ist es gelungen, die Microsoft-Formate so weit zu entschlüsseln, dass Programme wie **LibreOffice** (https://de.libreoffice.org/) oder OpenOffice die Dateien weitgehend darstellen und bearbeiten können.

Bildungssystem

Besonders fatal ist die Verwendung von Microsoft-Software im Bildungsbereich. Vom Elementarbereich über die weiterführenden Schulen (Jahrgangsstufen 5 bis 13), den berufsbildenden Bereich, die Hochschulen und Einrichtungen der Weiterbildung: überall wird Microsoft-Software eingesetzt mit äußerst wenigen Ausnahmen in

den Bereichen, wo es um informatorische Bildung geht wie beispielsweise an Universitäten.

Selbstverständlich setzen auch die Verwaltungen dieser Einrichtungen sowie die Lehrer und Dozenten auf ihren Rechnern Microsoft-Software ein. Alle Personen in den jeweiligen Einrichtungen finden es deshalb selbstverständlich, dass in den Bildungsveranstaltungen diese Software eingesetzt wird.

> ***Für Microsoft sind dabei vor allem die Kinder und jungen Erwachsenen wichtig. Wie eine Einstiegsdroge werden deshalb das Betriebssystem Windows und die Office-Programme billig oder gar umsonst angeboten.***

Auch das Lehrpersonal erhält verbilligte Versionen der Lizenzen für die Programme. Microsoft weiß, wenn es gelingt, kleine Kinder zu Microsoft-Anwendern zu machen, ist das Monopol auf längere Zeit gesichert. Auch von der Bildungsadministration und den Eltern geht starker Druck aus: Die Kinder sollen auf die Tätigkeit in der Wirtschaft vorbereitet werden; früher war mal von Bildung die Rede. Durch die teilweise drastisch erniedrigten Preise für die Lizenzen entzieht sich Microsoft auch dem Vorwurf, die Gleichartigkeit der Lebensverhältnisse zu gefährden, weil Schülerinnen und Schüler aus armen Elternhäusern sich die Software nicht leisten können. Dass spätestens beim Verlassen des Bildungssystems wesentlich höhere Lizenzkosten fällig werden, wird ignoriert.

> ***Würde Freie Software verwendet, könnte diese auch in Zeiten von beispielsweise Arbeitslosigkeit ohne Probleme weiter verwendet und auf dem aktuellen Stand gehalten werden.***

Dass Freie Software auch auf alten Rechnern, die preiswert zu kaufen sind, ohne Probleme läuft, ist ein weiterer Aspekt.

Was das Lehrpersonal, ihre Vorgesetzten und die Bildungsadministration ignorieren, sind die Datenschutzprobleme, die mit dem Einsatz von Microsoft-Software verbunden sind. So hat das **Bundesamt für Sicherheit in der Informationstechnik (BSI) darauf hingewiesen** (https://www.heise.de/meldung/BSI-untersucht-Sicherheitseigenschaften-von-Windows-10-4227139.html), dass über Windows 10 und Office 365 *„eine Fülle von Telemetrie-Daten an Microsoft übermittelt“* würden. Deren Inhalte seien *„trotz wiederholter Anfragen bei Microsoft nicht abschließend geklärt“*. Es ist deshalb davon auszugehen, dass schon von sehr jungen Schülern Daten aus ihrer Bildungsbiografie gesammelt und weiter gegeben werden.

Besonders perfide ist, dass Microsoft versucht, die Nutzer auch im Bildungsbereich zur Nutzung der „Cloud“ zu bewegen. Die Nutzer verlieren so die Hoheit über ihre Rechner, weil sie weder kontrollieren können, was die Software, die sie nutzen, macht, sowie die Hoheit über ihre Daten, da sie auf in den USA stehenden Servern gespeichert und damit der USA-Justiz unterstellt sind. Auf die Tatsache, dass das rechtswidrig ist, wurde schon hingewiesen.

> ***Es ist aber noch ein inhaltlicher Aspekt zu behandeln: Mit Microsoft-Software kann informationstechnische Bildung — wenn überhaupt — nur sehr eingeschränkt stattfinden.***

Die Lernenden lernen „Word“ und nicht „Textverarbeitung“, „Excel“ und nicht „Tabellenkalkulation“, „PowerPoint“ und nicht „Präsentationen erstellen“ — dass sie dann auch „Googlen“ statt „im Internet suchen“ ist die traurige Konsequenz einer derartigen Bindung an bestimmte Programme. Sie erfahren nichts über Lizenzen oder die **Eigenschaften von Software** (https://www.rubikon.news/artikel/warum-wir-freie-software-brauchen). Da der Quelltext der Programme nicht zur Verfügung steht und folgerichtig auch nicht verändert werden kann und darf,

können die Lernenden auch nicht die Software, die sie nutzen, analysieren und gegebenenfalls verändern. In einem Informatik-Leistungskurs oder bei Hochschul- oder Weiterbildungsveranstaltungen wäre das durchaus denkbar.

Sicherheitsaspekte werden nicht behandelt, weil dann vielleicht Fragen zur benutzten Software entstehen könnten.

Was tun?

Da fast alle mit der Situation zufrieden sind, ist es schwer, etwas daran zu ändern. Was vielleicht machbar wäre, ist für die Nutzung von Freier Software unter Windows zu werben; also beispielsweise LibreOffice statt Microsoft-Office. In seinen Arbeitszusammenhängen könnte man für den Umstieg auf Freie Software argumentieren.

Insbesondere sollte man aber überall da, wo man es mit politisch denkenden Menschen zu tun hat, sie darauf hinweisen, dass sie mit ihrer IT-Praxis die Ausforschung und Überwachung der Bürger fördern und damit andere und sich selbst und die Organisationen, in denen sie unter Umständen tätig sind, gefährden. Warum nicht beispielsweise vom Verlag oder der Online-Publikation, bei der man veröffentlicht, fordern, dass auch odt-Dateien (1) angenommen werden?

> ***Dabei ist eine verantwortungsvolle IT-Praxis möglich, alle Werkzeuge stehen zur Verfügung, es ist nur ein wenig Einarbeitung (und unter Umständen Unterstützung) nötig:***

Statt Windows GNU/Linux, statt Microsoft-Office Libreoffice, statt der Microsoft-Cloud Nextcloud. Sicher surfen geht mit Firefox, anonym surfen mit dem TOR-Browser, E-Mail-Verschlüsselung ist

nicht so schwer, wie behauptet wird.

Ist mehr nötig, kann man zu **Tails** (https://tails.boum.org/index.de.html) greifen, die Software die von Edward Snowden und Glenn Greenwald, der ja inzwischen in Brasilien verfolgt wird, benutzt wurde, um der NSA nicht in die Fänge zu geraten.

Quellen und Anmerkungen

(1) **GNU/Linux** (https://www.gnu.org/gnu/linux-and-gnu.html) ist die korrekte Bezeichnung für das Freie Betriebssystem, das meist verkürzt als Linux bezeichnet wird.
(2) Eine Distribution ist die Zusammenstellung von Software, zu der immer als zentraler Bestandteil der sogenannte Kernel gehört. Eine Distribution ist immer auf bestimmte Einsatzzwecke abgestimmt und umfasst in der Regel mindestens Software für alle gängigen Aufgaben.
(3) odt ist das Textformat des **OpenDocumentFormats** (https://de.wikipedia.org/wiki/OpenDocument)

Dieser Artikel erschien bereits auf www.rubikon.news.

Wolfgang Romey arbeitete nach dem Studium der Theoretischen Elektrotechnik als Lehrer für Mathematik,

Elektrotechnik und Digitaltechnik im Berufsbildenden Bereich, später als Lehrerausbilder im Vorbereitungsdienst, dem Referendariat. Dann folgte ein Wechsel in die Bezirksregierung Düsseldorf als Dezernent für Lehrerausbildung und später auch -fortbildung. Er verfügt über etwa 20 Jahre Erfahrung darin, angehende Lehrerinnen und Lehrer auf die Bildungsarbeit mit Digitalen Medien vorzubereiten und deren Urteilskraft in diesem Feld zur Entfaltung zu verhelfen. Die kritische Auseinandersetzung mit den dramatischen Folgen der Digitaltechnik, die ihm extrem unterentwickelt scheint, ist bis heute sein Thema.