Vorwort

Foto: Svetlana Fitz

Liebe Kolleginnen und Kollegen,

manchmal glaube ich, wir haben den Schuss nicht gehört. Auch nach Edward Snowdens Enthüllungen und zahlreichen Datenskandalen bei Facebook nutzen wir in unserem beruflichen Alltag immer noch unsichere Dienste und füttern Datenkraken mit Informationen. Der gläserne Journalist sollte eigentlich ein Albtraum sein, aus dem man so schnell wie möglich erwachen möchte. Dennoch lassen wir wie selbstverständlich Google an unserer Internetrecherche teilhaben, nutzen das gleiche unsichere Passwort für mehrere Accounts und verschicken E-Mails meist unverschlüsselt.

Klar, einen hundertprozentigen Schutz gibt es nicht und niemand soll in Paranoia verfallen. Dennoch zählt die lahme Ausrede, man habe nichts zu verbergen schon lange nicht mehr. Der Mensch ist nun einmal ein Gewohnheitstier, dem es schwer fällt, Eigenarten abzulegen und neue Wege zu beschreiten. „Der härteste Gegner ist nach wie vor die eigene Bequemlichkeit“, bringt es Matthias Eberl im Interview auf den Punkt.

Mit dem vorliegenden Dossier möchten wir Lust machen, die Komfortzone zu verlassen. Wir zeigen erste Schritte hin zu mehr Datensicherheit auf, was unsere Arbeit ebenso sehr schützt wie die Informationsquellen.

Jens Brehl

INHALTSVERZEICHNIS

Datenlecks stopfen S. 1 – 3
Interview mit Multimedia-Journalist Matthias Eberl S. 3 – 4
Betriebssystem Linux Mint S. 5 – 6
Sichere Passwörter vergeben S. 6 – 7
Buchrezension: „NSA – Nationales Sicherheitsamt” S. 8

Verschlüsselung

Datenlecks stopfen

Jede große Reise beginnt mit dem ersten Schritt – in diesem abgedroschenen Sprichwort steckt viel Wahrheit. Wer von jetzt auf gleich alles verschlüsseln und seine komplette Kommunikation und seine Daten absichern will, läuft Gefahr, bald frustriert das Handtuch zu werfen. Daher ist es eine kluge und vor allem nachhaltige Strategie, sein Vorhaben Schritt für Schritt anzugehen.

Schritt 1: Updates, Datendiät Suchen ohne Google

Im Grunde sollte es jedem Computernutzer in Fleisch und Blut übergangen sein, regelmäßig die Updates des Betriebssystems und der verwendeten Software zu installieren, um Sicherheitslücken zu schließen. Dennoch siegt hin und wieder der innere Schlendrian.

Der Großteil der Datenspur, die wir täglich hinter uns her ziehen, ist unnötig. Man muss in sozialen Netzwerken nicht ständig posten, wo man sich befindet und was man gerade macht. Wer Kundenkarten nutzt, bekommt oft einen kleinen Rabatt, zahlt aber mit seinen vollständigen Daten, was er wann zu welchem Preis kauft. Statt EC- oder Kreditkarte kann man auch zu Bargeld greifen und muss das Smartphone wirklich dabei sein, wenn man einen Informanten trifft? Wie wäre es mit Datendiät?

Für seine Internetrecherchen muss man nicht zwangsläufig Google verwenden und dem dahinter stehenden Konzern Alphabet verraten, für welche Themen man sich gerade interessiert. Die Suchmaschinen Startpage (www.startpage.com) und Duckduckgo (www.duckduckgo.com) speichern keine Nutzerdaten und ermöglichen so das anonyme Suchen nach Informationen.

Schritt 2: Mittels Messenger und E-Mails sicher kommunizieren

Der Messenger WhatsApp ist äußerst beliebt, allerdings ist er auf vielen Ebenen problematisch. Facebook erhebt mit seinem Dienst Metadaten – sprich wer wen kennt, wann und von wo man jemandem schreibt – und verknüpft die gewonnenen Informationen mit denen aus seinem sozialen Netzwerk. Der auf Datensicherheit spezialisierte Journalist Matthias Eberl weist zudem auf die als unsicher geltende Verschlüsselung und den möglichen Zugriff amerikanischer Ermittlungsbehörden hin. Wer sich zudem neu bei dem Dienst anmeldet, lädt sämtliche Kontaktdaten seines Adressbuchs hoch. „Wir können es nicht verantworten, dass Namen von hunderten Journalisten, deren Kontakte und womöglich Informanten bei Facebook landen“, sagt Eberl mit Nachdruck. Spätestens seit die DSGVO in Kraft getreten ist, sei WhatsApp für Firmen und auch Journalisten nicht mehr nutzbar.

Sichere Alternativen sind die Messenger Signal (www.signal.org/de/) und Threema (www.threema.ch/de). Sie sind ebenso leicht zu installieren und zu bedienen. Man kann damit sogar verschlüsselt telefonieren – sie sind demnach auch gute Werkzeuge, um mit Informanten zu kommunizieren.

Es hat Gründe, warum nur wenige Leute ihre E-Mails verschlüsseln: Das Einrichten ist aufwendig und unterscheidet sich je nach Betriebssystem und E-Mail-Programm. Die Funktionsweise ist aber immer gleich. Beim Einrichten der Verschlüsselung werden ein privater und öffentlicher Schlüssel erzeugt. Das sind zwei Textdaten mit einem Wirrwarr an Zahlen und Buchstaben. Der öffentliche Schlüssel wird verteilt, indem man ihn entweder per noch unverschlüsselter E-Mail verschickt, oder zum Download auf seiner Internetseite bereit hält. Stellt man sich eine E-Mail als einen Tresor vor, der nur vom Empfänger geöffnet werden soll, schließt der Versender mit dem öffentlichen Schlüssel des Empfängers ab. Nur dieser hat mit seinem privaten Schlüssel und einem zusätzlichen Passwort Zugang. Wer den Tresor, sprich die Nachricht, unterwegs abfängt, kann nichts damit anfangen.

Wer E-Mails sicher verschlüsseln möchte, muss beim Einrichten ein paar technische Hürden überwinden. Daher sind entsprechende Workshops und der Rat von erfahrenen Kollegen essentiell. Hilfe gibt es auch bei Reporter ohne Grenzen (siehe Infokasten).

Schritt 3: Orientierung im Darknet

Jetzt wird es schmuddelig und kriminell. Wir alle wissen ja, dass das Darknet – der „dunkle Teil des Internets“ – voller Pornographie, digitaler Raubkopien, Waffen- und Drogenhändlern ist. Ja, das alles kann man dort recht leicht finden. Allerdings können wir uns dort frei und vor allem anonym bewegen. Perfekt für eine Internetrecherche, von der vorerst niemand erfahren soll – wichtig für Journalisten und besonders für Menschen, die in totalitären Staaten leben. Mithilfe des Darknets lassen sich nämlich auch Internetsperren umgehen.
Der Weg ins Darknet verläuft über das Projekt Tor und dem Herunterladen des entsprechenden Tor Browsers (www.torproject.org/de/download/), den es für Windows, macOS X, iOS, Linux und Android gibt. Wer dahinter eine kryptische Software vermutet liegt falsch, denn der Tor Browser basiert auf Firefox, der bereits perfekt für das anonyme Netzwerk und allgemein in Sachen Datenschutz angepasst ist. Allerdings ist er deutlich langsamer, weil er meine Route über mehrere Stationen oft in unterschiedlichen Ländern umlenkt. So bleibt die ursprüngliche IP-Adresse verborgen.

Schritt 4: Daten sicher teilen

Im redaktionellen Arbeitsalltag ist es wichtig, einfach und schnell Daten zu teilen. Besonders, wenn die am gemeinsamen Projekt arbeitenden Kollegen von unterschiedlichen Orten aus tätig sind. Daher ist Dropbox als so genannter „Cloud-Dienst“ beliebt. Er ist leicht zu bedienen und in der Basisversion kostenfrei. Allerdings ist laut Eberl unklar, ob der US-amerikanische Betreiber hochgeladene Daten einsehen kann und inwieweit Ermittlungsbehörden Zugriff haben.

Wer sich bei Dropbox einloggt, verknüpft seine E-Mail-Adresse mit seiner IP-Adresse. „Das sind wahnsinnig wertvolle Daten für die Werbeindustrie. Somit ist erkennbar, wer den Rechner gerade benutzt und welche Internetseiten er aufruft. Der komplette Browserverlauf kann somit einer bestimmten Person zugeordnet werden – besonders, wenn der Dropbox-Client stets im Hintergrund läuft“, warnt Eberl. Ein Datengau für jede Recherche. Hier zeigt sich die Tracking-Problematik der Werbeindustrie: Kaum einer weiß, welche Unternehmen letztendlich Zugriff auf die Daten haben, wo diese landen und wozu sie letztendlich heute oder in (naher) Zukunft verwendet werden.

Eine deutlich bessere Alternative sind eigene Speicherlösungen wie Nextcloud (www.nextcloud.com), die im Grunde ebenso leicht wie Dropbox zu bedienen sind, aber die Daten auf dem eigenen Server ablegen – dies ist in der Regel der Hoster, wo auch die Internetseite liegt. Oft sind hier noch etliche Gigabyte Platz frei. Es gibt ebenfalls Apps, um Nextcloud per Smartphone oder Tablet mobil zu nutzen.

Schritt 5: Königsdisziplin sicheres Betriebssystem

Windows und macOS X „funken“ so genannte Telemetriedaten nach Hause zu Microsoft oder Apple. Sie sollen dazu dienen, Absturzursachen zu ermitteln und Software zu verbessern. Allerdings ist kaum herauszufinden, welche Daten abfließen, ob sie anonym gespeichert und wofür sie genau verwendet werden.

Wer auch bei seinem Betriebssystem Datenlecks schließen will, kommt an Linux nicht vorbei. Hiervon gibt es zahlreiche Varianten, was Einsteigern den Überblick erschwert. Wer von Windows umsteigt,

Hilfe im Internet

Die gemeinnützige Organisation Reporter ohne Grenzen bietet ab Anfang Juli mit dem digitalen Helpdesk ausführliche Informationen und Online-Schulungen zu Verschlüsselung, Anonymisierung und mehr.

https://helpdesk.rsf.org/

Auf der Suche nach sicheren Alternativen für beliebte Programme?

Auf www.prism-break.org wird man für jedes Betriebssystem fündig.

(Jens Brehl)

ist mit Linux Mint in der Cinnemon Edition gut beraten (siehe Seite 5).

Wer absolut keine Datenspuren hinterlassen möchte, startet das freie Betriebssystem Tails (https://tails.boum.org/index.de.html) – eine Linux-Variante, die auf hohe Datensicherheit ausgelegt ist – direkt vom USB-Stick. Cookies, Browserverläufe oder gar untergejubelte Schadprogramme landen nicht auf der Festplatte und sind nach einem Neustart verschwunden. Sollen Daten wie Textdokumente erhalten bleiben, legt man einen Datencontainer an. Dieser ist automatisch verschlüsselt und mit einem Passwort geschützt. Wie man einen bootfähigen USB-Stick mit Tails erstellt, erfährt man im Infokasten des Artikels „Den Daten-Spionen einen Schritt voraus“ auf Seite 5. Das Prinzip ist das gleiche.

„Wie man heute noch Facebook nutzen kann, ist mir unbegreiflich“

Multimedia-Journalist Matthias Eberl über die Sinnhaftigkeit verschlüsselter Kommunikation und die vermeintliche Sicherheit von Betriebssystemen

Journalisten stecken in der Regel viel Herzblut in die Recherche. Weniger Aufmerksamkeit schenken sie meist den Fragen rund um die Datensicherheit – sprich, wie sich die gewonnenen Informationen vor unbefugten Zugriffen schützen lassen. Dabei ist es nicht zwingend nötig, zum IT-Nerd zu mutieren und jede E-Mail zu verschlüsseln. Der Multimedia-Journalist Matthias Eberl, der sich auf Informanten- und Datenschutz spezialisiert hat, zeigt im Interview auf, wie ein guter Anfang gemacht werden kann.

Absolut sicher? Datenschutz ist auch Informantenschutz. *Foto: Jens Brehl*

Jens Brehl: Was versäumen Journalisten und Redaktionen am häufigsten, um ihre Daten zu sichern?

Passwortsicherheit ist ein riesiges und vernachlässigtes Thema. Viele nutzen aus Bequemlichkeit das gleiche Passwort für unterschiedliche Accounts und Dienste. Anfang des Jahres tauchte im Internet mit Collection #1 eine riesige Liste von Logindaten, E-Mail-Adressen und Passwörtern auf. Die Informationen stammen unter anderem aus Datenlecks von beliebten Anbietern wie Dropbox und schlecht gesicherten Internetforen. Wenn das gleiche Passwort Zugang zu verschiedenen Accounts gibt, ist dem Missbrauch Tür und Tor geöffnet (siehe Artikel „‚geheim‘ ist wahrlich kein Geheimnis“ auf Seite 6). Ein weiterer Dauerklassiker ist die mangelhafte Datensicherung, sprich das fehlende regelmäßige Backup.

Zu sicheren Passwörtern und regelmäßigen Datensicherungen raten IT-Experten seit Jahrzehnten. Erschreckend, dass man dafür weiterhin ein Bewusstsein schaffen muss.

Der härteste Gegner ist nach wie vor die eigene Bequemlichkeit.

Warum sollte sich beispielsweise ein Lokaljournalist, der weder zum Themenkomplex Geheimdienste noch investigativ recherchiert, Gedanken um Datensicherheit machen und beispielsweise seine E-Mails verschlüsseln?

Auch der Lokaljournalist kann irgendwann an den Punkt gelangen, an dem ein Informant ihm sicher Daten zukommen lassen können muss, so dass beide geschützt sind. Zunächst gilt es das Risiko zu bewerten: Wie wichtig sind die Daten? Wie wahrscheinlich ist ein unbefugter Zugriff? Wer hat ein Interesse an den Daten, welche Ressourcen stehen ihm zur Verfügung und würde er illegale Methoden einsetzen? Welcher Aufwand ist gerechtfertigt, um die Daten zu schützen? Welche technischen Lösungen setze ich ein?

Wer nicht gerade technikaffin oder gar Informatiker ist, stößt schnell an seine Grenzen. Daher ist es auch eine Aufgabe von Journalistenverbänden und Organisationen allge-

„Leser müssen Nachrichten filterfrei konsumieren können“: Matthias Eberl (rechts) beim DJV-Workshop zu Informantenschutz und Verschlüsselung. *Foto: Jens Brehl*

mein sowie in konkreten Fällen zu beraten, welche technischen Mittel wie beispielsweise E-Mail-Verschlüsselung eingesetzt werden können. Schließlich haben freie Journalisten und kleinere Verlage anders als Der Spiegel, Süddeutsche Zeitung und Die Zeit oft keine eigenen Experten.

Facebook hangelt sich seit Jahren von einem Datenskandal zum nächsten. Jüngst wurde bekannt, dass der Konzern Beobachtungslisten von Kritikern führt, welche sich wiederum durch technische Möglichkeiten leicht überwachen lassen (https://blog.wdr.de/digitalistan/facebook-methoden-wie-beim-nachrichtendienst/). Medien berichten zwar, aber zementieren durch das Nutzen von Facebook und seinen Diensten wie WhatsApp oder Instagram weiterhin deren wirtschaftliche Basis. Das passt doch nicht zusammen.

Wie man nach zehn Jahren Skandalgeschichte und den andauernden Lügen von Mark Zuckerberg Facebook noch nutzen kann, ist mir unbegreiflich. Jeder einzelne Journalist muss seine Verantwortung allerdings mit sich ausmachen, wie es auch die Medienunternehmen tun müssen.

Ein Hauptargument ist, man gehe dorthin, wo man seine Leser findet. Dann schluckt man halt auch mal eine Kröte, um sein eigenes Geschäftsmodell zu sichern.

Natürlich gehört es zum journalistischen Auftrag, die Mediennutzer zu erreichen. Ein Teil der Leser wird jedoch immer sensibler und möchte der Werbeindustrie nicht mehr alle Daten verfügbar machen – was ja einem kompletten Ausverkauf des Privatlebens gleich kommt. Bislang kenne ich keinen Verlag, der in Sachen Facebook ein Ausstiegskonzept hat. Dabei ist es ungemein wichtig, dass Leser Nachrichten filterfrei konsumieren können.

Natürlich gibt es auch Angst, weniger Aufmerksamkeit zu bekommen oder Wichtiges zu verpassen. Vor allem Freiberufler brauchen Mut, um auf Facebook und dessen Dienste zu verzichten. Ich verstehe jeden, der argumentiert, er könne sich diesen Schritt nicht leisten. Allerdings kann jeder zumindest darauf hinweisen, dass WhatsApp in Sachen Datenschutz problematisch ist und als Kommunikationsmöglichkeit einen sicheren Messenger wie Signal anbieten. Journalisten sind schließlich keine reinen Unternehmer, sondern haben auch eine gesellschaftliche Verantwortung und eine Vorbildfunktion.

Windows und macOS X senden sogenannte Telemetriedaten über mein Nutzungsverhalten und eingesetzte Programme an Microsoft bzw. Apple. Was für Daten werden erfasst und kann man die Betriebssysteme sicher einstellen?

Bei Microsoft Office wird unheimlich viel erhoben, wie Absturz- aber auch Nutzungsdaten. Bleibt zu hoffen, dass die Informationen nur dem Verbessern der Produkte dienen und anonym verwendet werden. Allerdings bleibt die Unsicherheit, welche Daten insgesamt von den Betriebssystemen erhoben werden, und ob beispielsweise amerikanische Sicherheitsbehörden Zugriff haben. Generell stellt Windows im Zuge der DSGVO viele Unternehmen – und damit auch freiberufliche Journalisten – vor große Probleme.

Selbst mir ist es zu mühsam, juristisch und technisch zu durchschauen, welche Daten abfließen und was damit gemacht wird – ob bei Microsoft oder Apple. Unter dem Strich ist es dann einfacher, ein sicheres Betriebssytem wie Linux zu verwenden. Der Umstieg ist zwar mühsam, aber die Datensicherheit wird deutlich erhöht (siehe Artikel „Daten-Spionen einen Schritt voraus“ auf Seite 5).

Warum setzt sich bei Journalisten und Medienunternehmen das sichere Betriebssystem Linux nicht durch?

Man muss alte Gewohnheiten brechen und sich mit einem neuen Betriebssystem beschäftigen. Der Umstieg fällt mitunter schwer. Oftmals ist man auch von bestimmten Programmen – oder im Falle von Apple – sogar von der Hardware abhängig. Wer viel Grafik bearbeitet und Filme schneidet, ist bei macOS X und Windows deutlich besser aufgehoben. Für Journalisten, die hauptsächlich schreiben, bietet Linux wiederum viele Vorteile.

Zur Person

Matthias Eberl arbeitet als freier Multimedia-Journalist in München. Edward Snowdens Enthüllungen über die NSA waren für ihn der Startschuss, sich auf das Thema Datensicherheit zu spezialisieren. Er hat sich zum Datenschutzbeauftragten weiterbilden lassen, gibt Kurse zu Informantenschutz und Verschlüsselung und berät darüber hinaus Unternehmen. Privat wie beruflich ist er bestrebt, so wenig Datenspuren wie möglich zu hinterlassen. www.rufposten.de

Den Daten-Spionen einen Schritt voraus

Mehr Datensicherheit mit dem freien Betriebssystem Linux Mint

Im Sommer 2017 wagte ich einen großen Schritt: Mitten im laufenden Betrieb meines Medienbüros stieg ich von Windows 7 auf das freie Betriebssystem Linux Mint (https://www.linuxmint.com/) um. In höchstens zwei Arbeitstagen wollte ich den Wechsel komplett abgeschlossen haben. Ein ehrgeiziges Ziel, welches mich bei Erfolg mit einer erhöhten Datensicherheit belohnen würde. Rückblickend frage ich mich, was mich zuvor so lange davon abgehalten hat.

So langsam kam mein Windows 7-Laptop in die Jahre und oft gab es Probleme mit den Updates. Entweder dauerte es Stunden, bis sie heruntergeladen wurden oder sie ließen sich gar nicht installieren. Selbst das neue Aufspielen des Betriebssystems sorgte nur kurze Zeit für Ruhe. Ein neuer Laptop musste her. Doch ich scheute den Neukauf, da neue Geräte ausschließlich mit Windows 10 ausgeliefert werden und Konkurrent Apple für mich keine Alternative ist. Den Wechsel auf das neue Windows wollte ich daher so lange wie möglich hinauszögern. Als Journalist liegen die Gründe auf der Hand: Meine Daten müssen sicher bei mir verwahrt sein.

In die Tiefen der Systemeinstellungen

Windows 10 „funkt“ ständig Daten über eingesetzte Programme, mein Nutzungsverhalten und mehr nach Hause zu Microsoft. Viel mehr, als es bei den vorherigen Windows-Versionen. Herauszufinden was genau wann übertragen wird, ist fast schon eine Wissenschaft. Ein für einen Konzern (zumindest teilweise) gläserner Journalist müsste für jeden Kollegen ein Albtraum sein – ist es meist aber nicht. Zu oft machen wir uns zu wenig Gedanken, kennen keine Alternativen oder scheuen den Aufwand diese einzusetzen.

Viele „Spionage“-Dienste von Windows 10 lassen sich schon während der Installation abschalten. Allerdings ist es mitunter nötig, tiefer in die Systemeinstellungen einzusteigen, um so weit wie möglich die ungewollten Datenübertragungen zu verhindern.

Linux Mint verschafft dem Nutzer das Gefühl, wieder Herrscher über die eigenen Daten zu sein.
Foto: Jens Brehl

Ist dies geschafft, muss man letztendlich Microsoft vertrauen, dass die Privatsphäre wie gewünscht gewahrt bleibt. Mein Vertrauen reicht dafür nicht aus. Zurück bliebe ein mulmiges Gefühl. Nicht zuletzt können durch Updates und neue Funktionen weitere „Spionage“-Dienste hinzukommen.

Hilfe aus dem Hacker-Universum

Es gibt nicht „das“ Linux, sondern viele unterschiedliche Distributionen wie Arch, Debian, Ubuntu, Fedora, Suse und etliche mehr. Da der Quellcode offen ist, können Entwickler das System an verschiedene Bedürfnisse anpassen und erweitern. So nützlich die Vielfalt auch ist, kann sie im ersten Moment verwirren.

In meiner Heimatstadt Fulda stieß ich auf Magrathea Laboratories (https://mag.lab.sh/), einen so genannten Hackerspace. Hier treffen sich keine Kriminellen, die Daten aus fremden Systemen kopieren und meistbietend verkaufen. Vielmehr ist es ein offener Treffpunkt und Lernort für alle an Technik interessierten Menschen. Nachdem ich beim Plaudern mein Windows-Dilemma schilderte, zeigte mir jemand seinen Laptop, auf dem Linux Mint lief.

Auf den ersten Blick sieht die Benutzeroberfläche Windows recht ähnlich. Links unten in der Taskleiste klicke ich auf „Menü“ und erhalte eine Ansicht der installierten Programme und diversen Einstellungsmenüs, die ich jeweils mit einem Mausklick öffne. Alles ist übersichtlich und intuitiv bedienbar. Libre (Office-Anwendungen), Firefox (Browser), Thunderbird (E-Mail-Client), PDF-Betrachter, own cloud (freie Cloud-Anwendung), GIMP (Bildbearbeitung), VLC Media Player und mehr liefert Mint mit. Neue Programme lassen sich via „App Store“ mit wenigen Mausklicks installieren. Das für mich geeignete System war also gefunden; ich brauchte nur noch den passenden Laptop.

Die Mitglieder des Hackerspace nutzen fast ausschließlich Lenovo ThinkPads, da diese bestens mit Linux laufen und so entschied auch ich mich für diesen Hersteller. Johannes und Martin halfen mir durch die Installation, die ähnlich wie Windows mittels eines Assistenten vollzogen wird.

Ab in den Arbeitsalltag

Nun kam die Stunde der Wahrheit. Die Hardware ist ein Problem, weshalb sich Linux als Desktop-Betriebssystem kaum durchsetzt. Damit Drucker, Scanner und Co. funktionieren, sind so genannte „Treiber“ nötig. Die meisten liefert der Linux Kernel mit, der durch Updates beständig erweitert wird. Allerdings kann es sein, dass es vor allem bei neuen Geräten (noch) keine Treiber für Linux gibt oder man diese aufwendig nachinstallieren muss. Mitunter muss man dann die Ebene der Benutzeroberfläche verlassen und im Terminal Kommandozeilen tippen.

Meinen Scanner und Netzwerkdrucker erkannte Linux Mint sofort. Via externer Festplatte waren meine sämtlichen Daten in wenigen Minuten übertragen. Bereits unter Windows hatte ich Firefox genutzt und importierte einfach meine Lesezeichen. Die E-Mail-Konten waren in Thunderbird ebenso schnell eingerichtet, wie die Verschlüsselung mittels des Plugins Enigmail. Bei Libre-Office sind einzelne Funktionen in anderen Menüs untergebracht, aber die Eingewöhnungszeit ist kurz. Natürlich kann Libre sämtliche Microsoft Office Formate öffnen und auch in diesen abspeichern. Meine Kunden erhalten wie gewohnt Texte in .docx. Auch wenn die Redakteure im Dokument Änderungswünsche markieren und Kommentare einfügen, bleiben diese wie meine auch beim mehrmaligen Überarbeiten unter unterschiedlichen Betriebssystemen erhalten.

Ein Wermutstropfen sind Programme von Adobe, da diese nur mit etwas Bastelei unter Linux funktionieren. Das freie Grafikprogramm GIMP kann professionelle Software wie Photoshop nicht völlig ersetzen. So dient mir mein Windows 7-Laptop nur noch für das Nutzen von Photoshop und Acrobat, da ich bislang noch nicht die Muse hatte, die Programme unter Linux Mint mittels des Programms „Wine“ zum Laufen zu bringen. Wer mit Bilddateien im Raw-Format arbeitet, ist unter Linux mit dem kostenfreien Darktable gut bedient.

Unterm Strich habe ich mir den Wechsel viel aufregender vorgestellt. Schon nach wenigen Wochen hatte ich mich vollständig an Linux Mint gewöhnt. Seitdem bin ich wieder Herrscher über meine Daten und fühle mich in Sachen Informantenschutz und Datensicherheit deutlich wohler.

Jens Brehl

Im Netz:

Wer Linux Mint ausprobieren möchte, muss es nicht gleich installieren. Man kann es als Live-System direkt vom USB-Stick booten. Wie das genau funktioniert erklärt das Video: https://www.youtube.com/watch?v=umDgpEDZz8o.

„geheim“ ist wahrlich kein Geheimnis

Mit KeePassX sichere Passwörter erstellen und verwalten

Kaum zu glauben, aber wahr: Zeichenfolgen wie 123456, qwertz, der eigene Vorname oder geheim sind immer noch beliebte Passwörter. Eines haben sie gemeinsam: Sie sind leicht zu knacken und daher alles andere als sicher. Aber wie sieht es denn nun aus, das sichere Passwort? Und wie merkt man sich jedes einzelne für jeden Account, vom Mailpostfach bis hin zu Twitter, Facebook und Co.?

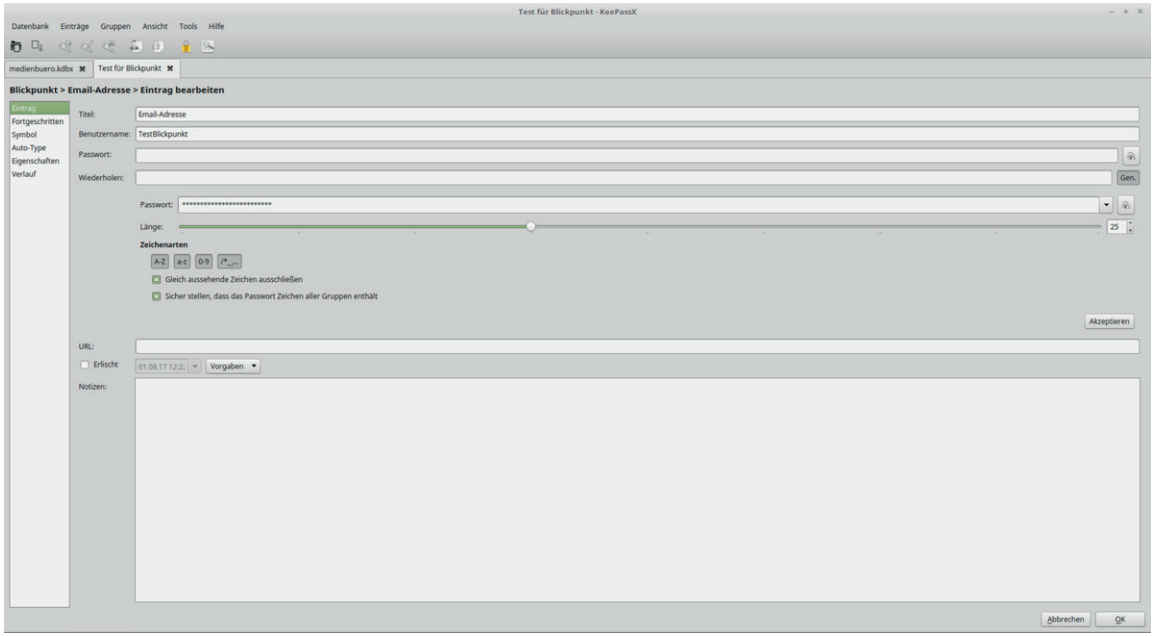
Schritt 1: Das sichere Passwort

Ein wirklich sicheres Passwort besteht aus mindestens 12 Zeichen und enthält Zahlen, Sonderzeichen und Buchstaben in großer wie kleiner Schreibweise – aber keine Wörter, die im Wörterbuch stehen. Mu.7Uti2TKue1B! ist bestens geeignet. Wie man sich ein solches Ungetüm merkt? Hinter der Zeichenfolge steckt der Satz: Morgens um Punkt 7 Uhr trinke ich 2 Tassen Kaffee und esse 1 Brötchen! Die Zeichenfolge besteht aus dem jeweils ersten Buchstaben der einzelnen Worte, aus „Punkt“ wird „.“ und Zahlen werden als Ziffern genutzt. Wie immer gilt: Jedes Passwort nur einmal vergeben!

Wer sich nicht jedes Mal einen solchen Satz überlegen möchte, kann sichere Passwörter auch automatisch generieren lassen. Zahlreiche Internetseiten bieten hier ihre Dienste an, diese sind aber in der Regel nicht vonnöten. Schließlich müssen Passwörter ja auch noch sicher aufbewahrt werden.

Schritt 2: Sichere Passwörter sicher aufbewahren

Man muss sich keinen physischen Safe anschaffen, wenn man einen auf seinem Computer installieren kann. Die Programme nennt man Passwortmanager oder auch Passwortsafes. Zu empfehlen ist KeePassX, denn die kostenfreie Software ist für alle Betriebssysteme verfügbar und dank App hat man auch unterwegs via Smartphone Zugriff auf seine Passwörter. Alle Daten ver-



Mit KeePassX ist ein sicheres Passwort schnell generiert und als Eintrag gespeichert. *Screenshot: Jens Brehl*

bleiben beim Nutzer und werden bei keinem Dienstleister gespeichert.

Um eine neue Datenbank am Computer anzulegen, vergibt man zunächst ein Master-Passwort – und da dieses später den Zugriff auf die Datenbank schützt, muss es unbedingt ein sicheres und leicht zu merkendes sein.

Danach zeigt der Bildschirm ein leeres Verzeichnis. In der neuen Datenbank sind natürlich noch keine Passwörter in Form von Einträgen gespeichert. Es ist sinnvoll, zunächst im Reiter „Datenbank“ auf „Datenbankeinstellungen“ zu gehen und im ersten Feld einen Namen für die Datenbank zu vergeben. Als Nächstes klickt man ebenfalls im Reiter „Datenbank“ auf „Datenbank speichern“ und bestimmt einen Speicherort. Dort erscheint nun eine Datei mit der Endung .kdbx. Dies ist die angelegte verschlüsselte Datenbank, die sich nur mithilfe des zu Beginn gewählten Master-Passworts öffnen lässt. Geht es verloren, ist ein Zugriff nicht mehr möglich!

Jetzt gilt es, die zahlreichen Passwörter in die Datenbank einzupflegen. Dafür klickt man den entsprechenden Button mit dem Schlüsselsymbol und grünem Pfeil. Hier bitte einen Namen (Titel) vergeben und folgende Daten eintragen: Benutzername, Passwort (muss zur Sicherheit wiederholt werden), eine URL, sprich Internetadresse, unter der das Passwort gegebenenfalls genutzt wird, um sich einzuloggen und auf Wunsch Notizen.

Mit einem Klick auf den Button „Gen.“ kreiert KeePassX ein sicheres Passwort nach den eingestellten Vorgaben. Dazu sollte man unbedingt alle Zeichenarten aktivieren, da das Nutzen von Sonderzeichen extra zugeschaltet werden muss. Im Feld Passwort erscheinen nun Sternchen. Wer das Augensymbol rechts daneben anwählt, kann sich das Passwort im Klartext anzeigen lassen. Soll es für den Eintrag genutzt werden, auf „Akzeptieren“ und dann auf „OK“ klicken. Das erste Passwort ist hinterlegt.

Automatische Übertragung

Bevor man sich in eines seiner Konten einloggt, startet man KeePassX, gibt das Master-Passwort der Datenbank ein und wählt den erforderlichen Eintrag aus. Benutzername und Passwort muss man nicht mühsam abtippen: über einen Rechtsklick auf den Eintrag kann man sie nacheinander in die Zwischenablage kopieren. Die Zwischenablage wird nach einigen Sekunden automatisch gelöscht – siehe unter Tools Einstellungen Sicherheit. Alternativ lässt sich auch „Auto Type“ ausführen (Rechtsklick auf den Eintrag und „Auto-Type ausführen“ wählen oder das Tastenkürzel „Strg“ + „V“ KeePassX unter Windows und Linux nutzen), um Benutzername und Passwort automatisch im zuletzt geöffneten Fenster eintragen.

Für Android-Smartphones ist die App Keepass2AndroidOffline erhältlich. Einfach die Datenbankdatei auf das Smartphone kopieren; mittels App und Datenbankpasswort hat man dann auch unterwegs stets Zugriff auf alle Passwörter. Zudem ist es direkt in der App möglich, neue Einträge zu speichern. Allerdings ist es dann ratsam, die geänderte Datenbankdatei auch auf seinen Computer zu kopieren.

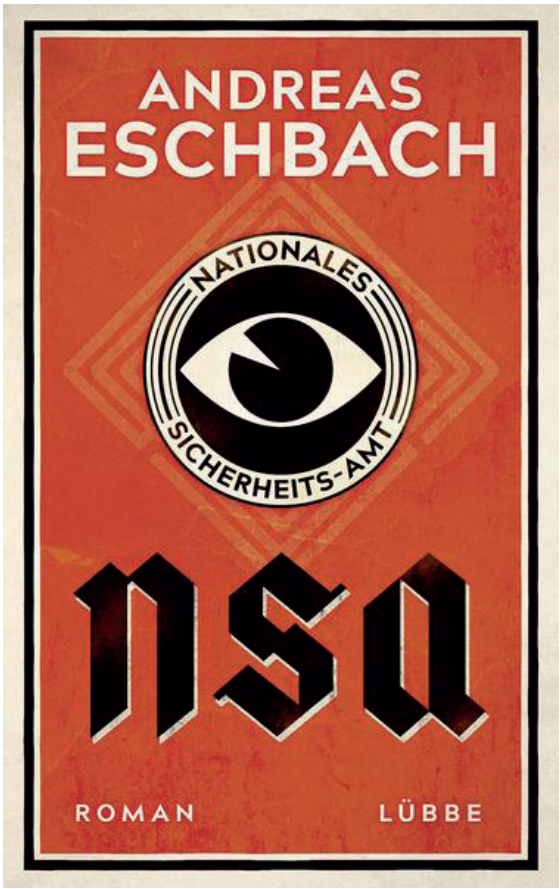
Fazit: Sichere Passwörter zu erstellen und ebenso sicher aufzubewahren, ist kein Hexenwerk. Das Einzige, was einen davon abhalten kann, ist die pure Faulheit. Wer möchte schon seine private Korrespondenz bei Facebook, nicht öffentlichen Telefonnummern oder bei Dropbox gespeicherte Fotos frei im Internet finden? Eben dies ist im Januar 2019 Robert Habeck, dem Bundesvorsitzenden der Grünen, nebst weiteren Politikern aber auch Schauspielern und anderen Personen des öffentlichen Lebens passiert. Unsichere und mehrfach für unterschiedliche Dienste genutzte Passwörter erleichtern nur den Datendiebstahl.

Jens Brehl

Dachbodenleiter + Campingtoilette = Judenversteck?

Rezension: Andreas Eschbachs Fiktion von der Überwachungsbehörde „NSA – Nationales Sicherheitsamt“

Was wäre, wenn es im Dritten Reich bereits Computer, Internet, E-Mails, soziale Medien und Mobiltelefone gegeben hätte? In seinem Roman „NSA – Nationales Sicherheitsamt“ entwirft Andreas Eschbach genau dieses Szenario. Immer enger überwacht das Regime seine Bürger. Bargeld ist abgeschafft, jeder Kauf wird elektronisch erfasst. Wer zu viele Lebensmittel oder gar eine Dachbodenleiter und eine Campingtoilette erworben hat, versteckt wahrscheinlich Juden oder andere Feinde des Staates. Doch die Nazi-Regierung will noch viel mehr, als „nur“ alles über seine Bürger wissen.



Helene Bodenkamp arbeitet als Programmiererin im Nationalen Sicherheitsamt. Sie ist talentiert, aber naiv. Sie spürt den politischen Wandel und fragt sich, wohin ihre jüdische Schulfreundin verschwunden ist. Dennoch erfüllt sie ihre Pflicht. Sie hackt sich nicht nur in amerikanische Computer ein, um die dortige Rüstungsproduktion zu sabotieren, sondern schreibt Programme, die dem Staat alles über seine Bürger verraten. Kein Wunder: Privater Datenspeicher ist verboten, alles wird in zentralen Datensilos – in der Realität würde es „Cloud“ heißen – erfasst.

Eschbach verquickt wahre geschichtlichen Ereignisse und reale Personen mit seiner Fiktion. Anne Franks Versteck fliegt auf, da ihre Helfer zu viele Lebensmittel einkaufen. Ihr Tagebuch wird verbrannt. Die Geschwister Scholl sind wenige Tage, nachdem sie das erste Flugblatt der Weißen Rose in Umlauf gebracht haben, verhaftet. Ihre Mobiltelefone haben sie durch Metadaten und Standortbestimmung verraten. Als die Programmiererin Helene Bodenkamp immer mehr Zweifel an der Richtigkeit ihres Tuns kommen, wendet sie die Technik gegen das Regime. Gleichzeitig nimmt die staatliche Überwachung weiter zu. Ein erster Prototyp der künstlichen Intelligenz wertet Datenströme automatisch aus und meldet ungewöhnliches Verhalten. Doch dies ist nur die Spitze des Eisbergs.

Trotz zahlreicher Skandale gehen viele Menschen sorglos mit ihren Daten um. Getreu dem Motto: Ich habe ja nichts zu verbergen. Das Thema digitale Überwachung ist meist nicht greifbar. Das fiktionale Szenario in Eschbachs „NSA – Nationales Sicherheitsamt“ lässt seine Leser an vielen Stellen nach Luft schnappen und vielleicht sogar das eigene Verhalten hinterfragen, denn: Selbst „harmlose“ Daten verraten kombiniert viel über einzelne Menschen.

Der Roman weist allerdings auch Längen auf, da die Lebensgeschichten der beiden Hauptprotagonisten extrem ausführlich geraten sind. Gerade im ersten Drittel nehmen langatmige Passagen viel Raum ein. Zudem möchte die Sympathie nicht so recht auf Helene Bodenkamp, die Heldin des Buchs, überspringen. Zum Ende hin erscheint so manche Wendung zudem arg konstruiert. Der Ausgang der Geschichte ist allerdings ein echter Paukenschlag.

Jens Brehl

IMPRESSUM:

Herausgeber: *Deutscher Journalisten-Verband, Landesverband Hessen e. V. | Rheinbahnstraße 3 | 65185 Wiesbaden*
V.i.S.d.P.: *Knud Zilian*
Redaktion: *Andreas Lang (ala)*