DIGITALE SELBSTBESTIMMUNG

Hintergründe und Tipps zum Umgang mit Daten im Netz

Aus der Broschürenserie **GUTE ARBEIT!**
Gewerkschaft GPA – Abteilung Arbeit & Technik

gpa MEINE GEWERKSCHAFT

„You have to fight for your privacy, or you will lose it.“

Eric Schmidt (2013) CEO bei Google

„Metadata absolutely tells you everything about somebody's life, if you have enough metadata you don't really need content.“

Steward Baker (2013) Jurist bei der NSA

IMPRESSUM:
Herausgeber: Gewerkschaft GPA, 1030 Wien, Alfred-Dallinger-Platz 1
Redaktion: Clara Fritsch, Gewerkschaft GPA – Abteilung Arbeit & Technik
Layout: Christina Schier, Gewerkschaft GPA – Abteilung Organisierung und Marketing
Bilder/Fotos: iStock, Edgar Ketzer, Christian Voigt, Michael Mazohl
ÖGB ZVR-Nr.: 576439352

Stand: März 2022

GUTE ARBEIT!

AUTORiNNEN

© Edgar Ketzer

Mag.ª Clara Fritsch

ist Soziologin und arbeitet in der Abteilung Arbeit & Technik der Gewerkschaft GPA. Sie beschäftigt sich schwerpunktmäßig mit den Themen Kontrolle am Arbeitsplatz, Beschäftigten-Datenschutz sowie IKT-Systemen und berät zur Gestaltung von Betriebsvereinbarungen.

© Christian Voigt

Christian Voigt

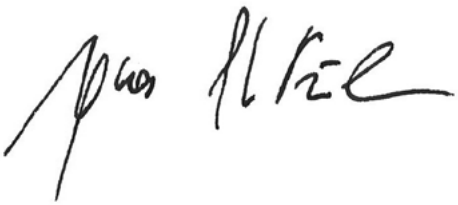
ist Soziologe und externer Referent für die Gewerkschaft GPA.

INHALT

VORWORT

Diese Broschüre bietet Hintergründe und Tipps für den selbstbestimmten und datensicheren Umgang mit internetbasierten, datenverarbeitenden Technologien und Plattformen. Zunehmend bestimmen Internetgiganten wie Google (Alphabet), Facebook (Meta), Amazon, Microsoft und Apple das Geschehen im Netz. Zugleich werden die von diesen Konzernen angebotenen Möglichkeiten auch wegen ihrer einfachen Zugänglichkeit und Vernetzungsvielfalt geschätzt. Digitalisierung und Internet bergen Risiken und Potenziale. Was es daher braucht, sind digitale Kompetenzen, um möglichst souverän mit Daten online – aber auch offline – zu agieren. Das Ziel ist es, Risiken klein zu halten und die Vorteile der Technologien selbstbestimmt zu nutzen.

Die vorliegende Broschüre der Gewerkschaft GPA fasst Erfahrungen aus Beratungen, Seminaren und Workshops zusammen. Sie wird nicht die Antwort auf alle Fragen liefern, allerdings Mittel und Wege zu mehr digitaler Selbstbestimmung im Alltag aufzeigen. Ob in der Betriebsratsarbeit oder im Privatleben: Diese Broschüre trägt dazu bei, die Risiken besser einschätzen und somit eindämmen zu können.



Agnes Streissler-Führer
Mitglied der Gewerkschaft GPA Bundesgeschäftsführung,
zuständig für Digitalisierung und Innovation

Beispiele

Wertvolle Tipps

Wichtige Hinweise

EINLEITUNG

Seit Jahrzehnten transformiert Digitalisierung die Kommunikationsgewohnheiten, Wirtschaftsformen und Arbeitswelten. Einzelpersonen und deren individueller Alltag ist ebenso von digitalen Technologien beeinflusst, wie Arbeitsverhältnisse und die Gesellschaft insgesamt. Um ein möglichst großes Maß an Selbstbestimmung zu erhalten, hilft es die Kontrolle über die eigenen Geräte und BenutzerInnen-Konten möglichst aktiv zu betreiben, Kommunikationskanäle sorgsam zu wählen, jene Software-Einstellungen zu treffen, die mehr Privatsphäre-Schutz versprechen oder sich bewusst für bestimmte Speicherorte zu entscheiden. „Datenminimierung" lautet die Maxime. Die regelmäßige Beschäftigung mit den Themen Datenschutz und Datensicherheit gehört zur Realität dazu und soll mit dieser Broschüre möglichst einfach bewerkstelligt werden – ohne, dass alle IT-ExpertInnen werden müssen.

Um die Risiken besser einschätzen zu können, hilft es, sich über die Eigenschaften der digitalen Welt Klarheit zu verschaffen, worum es im ersten Kapitel geht. Danach wird auf einzelne Bereiche eingegangen und konkrete Handlungsoptionen empfohlen.

Fünf „goldene Regeln" für digitale Selbstbestimmung

1. Zugang sichern.

Der gut abgesicherte Zugang zu den eigenen Geräte und Accounts ist eine Voraussetzung für gut gesicherte Daten und Privatsphäre.

2. Daten sparsam verwenden.

Datenminimierung heißt nicht, dass Plattformen und Dienste Tabu sind. Das Prinzip der Datensparsamkeit bedeutet, möglichst wenige Daten und nur tatsächlich erforderliche zu verwenden, sich zu überlegen was wo und wie gesagt, gepostet, geteilt, gespeichert, wird.

3. Alternativen nutzen.

Gewisse digitale Grundausstattung ist unumgänglich. Betriebssystem, Smartphone, Bordcomputer im Auto, Kameras im öffentlichen Raum etc. lassen sich kaum umgehen. Oft gibt es jedoch gute Alternativen. Das sind solche, die das auch können, was die Marktführer bieten, aber unter deutlich besseren Vorzeichen mit mehr Selbstbestimmung.

4. am Ball bleiben.

Aktuelle Empfehlungen von ExpertInnen für den Schutz der Privatsphäre und den Umgang mit Datensicherheit einholen und umsetzen, macht durchaus Sinn, da sich der Stand der Dinge sehr rasch ändert. Was gestern noch datenschutzfreundlich war, kann morgen – nachdem es vielleicht von einem Tech-Konzern gekauft wurde – schon ganz anders aussehen. Abonnements von Datenschutz-Organisationen und Abfrage im Netz helfen dabei.

5. Datenschutz klappt nur solidarisch.

Im Alleingang für digitale Selbstbestimmung zu sorgen, ist kaum möglich. Zwar können Einzelne für ihre Sicherheitseinstellungen, Zugangsschutz etc. sorgen, doch wenn jeder und jede bloß „ihr eigenes Süppchen kocht", ist das noch kein Garant für das Grundrecht auf Schutz der eigenen Daten – dazu braucht es auch kollektive Maßnahmen (z. B. Free Open Source Software, Gesetze).

DAS DIGITALE UND SEINE FUNKTIONSWEISE

Um informierte Einschätzungen treffen zu können, hilft es ein paar Grundprinzipien über das Digitale zu kennen.

Alles in Nuller und Einser übersetzt

Digital kommt vom englischen Wort „digits" für Ziffern. Während es deren zehn gibt, Null bis Neun, ist die digitale Welt aber aus nur zwei Ziffern gebaut: 0 und 1. Sie stehen für einen von zwei möglichen Zuständen, für keine elektrische Ladung (0) oder eine elektrische Ladung (1). Sie können als Signal, als Befehl verwendet werden. Null oder Eins, ja oder nein, EIN oder AUS, entweder/oder. Der Kern des Digitalen sind die Nullen und Einser als kleinste Bausteine der Information. Im Binärcode sind Informationen einfacher kopier- und speicherbar, schnell übertrag- und verknüpfbar. Es werden viele Operationen möglich, die in analoger Form nicht möglich wären.
In der analogen Welt sind Dinge nicht in ein einziges Codesystem zerstückelt. Im binären Code, der globalen Verkehrssprache der digitalen Welt, quasi der „lingua franca", schwirren nicht nur Zahlen, Texte, Bilder und Töne etc., per elektronischer Datenverarbeitung durch das world-wide-web. Im selben unablässigen Strom der Nullen und Einsen sind auch die Programmiersprachen enthalten, also die Befehle an Sensoren, an Hard- und Software. Das alles läuft in Sekundenschnelle, dank immer leistungsfähiger werdender Computer und Datenübertragungsmedien. Nullen und Einsen sind gegenwärtig in Glasfaserkabeln und als kabellose bits'n'bytes, in digitalen Stromzählern oder Klimasensoren, Smartphones und Laptops oder Großsystemen zur Steuerung von kommunaler bis hin zu globaler Infrastruktur.

Vervielfältigen leicht gemacht

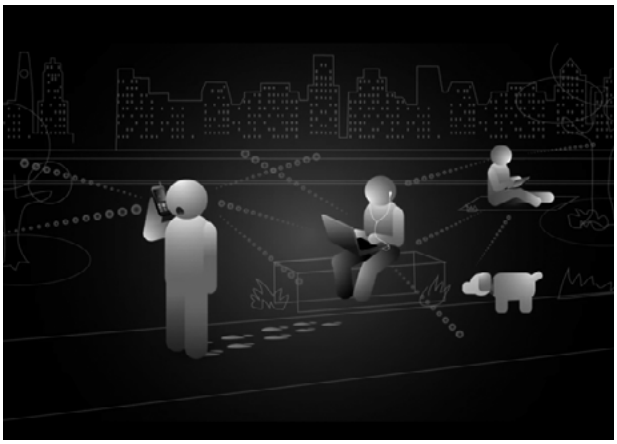
Schon seit einigen Jahren hat die Menge an in digitaler Form gespeicherten Informationen jene überholt, die sich im Laufe der Menschheitsgeschichte in Büchern, Gemälden oder Schallplatten angesammelt hat. Der Inhalt analoger Speichermedien wird oft digitalisiert. Dieser Vorgang, bei dem Information aus „alten" Speichermedien in den Binärcode übertragen werden, wird – vor allem im englischen Sprachraum – als „Digitalisierung" bezeichnet. Digitale Daten können im Gegensatz zu analog gespeicherten ohne großen Informationsverlust kopiert werden. Beim Kopieren eines gedruckten Buches, einer analogen Fotografie, einer Schallplattenaufnahme, gibt es unvermeidbar einen gewissen Informationsverlust. Das Kopieren von Nullen und Einsern schafft dagegen zwei idente Kopien im Binärcode. Original und Kopie sind weitgehend gleichwertig. Die gleichen Nuller und Einser, aus denen das E-Mail besteht, gibt es gleichzeitig vollkommen identisch im Gesendet- und im Posteingangsordner – sowie wie auf E-Mail-Servern von Providern und vermutlich Geheimdiensten.

Verknüpfen – fast – beliebig möglich

Im digitalisierten Zustand können Informationen ziemlich beliebig verknüpft werden. Über Hyperlinks

werden Daten und Informationen in neue Zusammenhänge gebracht. Websites werden miteinander verlinkt, Dateien verknüpft, Datenbanken verbunden.

Zu gewünschten Informationen werden Links per E-Mail verschickt. Ein online-Zeitungsartikel führt per klick weiter zu einem Mitgliedsformular. Das Fotoprotokoll eines Workshops verweist auf ein PDF-Dokument.



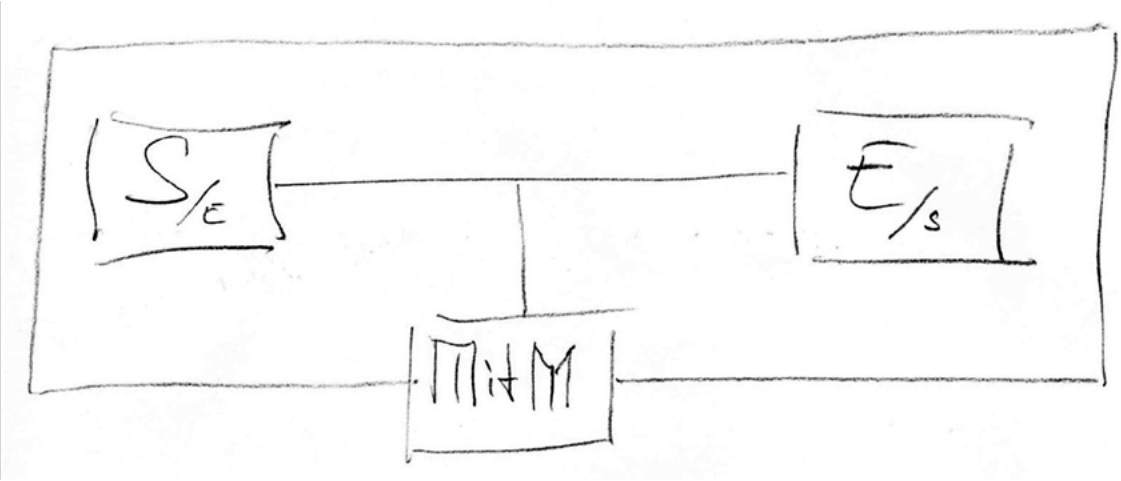
Das Online Spiel „Data Dealer" zeigt sehr anschaulich, wo Daten gespeichert werden und wie sie von anderen fremdbestimmt verwendet werden: www. datadealer.com

Die verlinkten Datenbestände und Programme überwinden die Grenzen der eigenen Geräte ebenso wie die von Firmen-Infrastrukturen und können zu externen Speicherorten bei externen Anbietern verknüpfen, zur sogenannten „Cloud". Bei all diesen Operationen werden bits'n'bytes übertragen.

Weil alles in die gleiche Struktur übersetzt ist, kann auch alles innerhalb dieser Struktur miteinander verknüpft werden

DATENÜBERTRAGUNG MIT ZWISCHENSTATIONEN

Der Transport einer analogen Ansichtskarte oder eines Briefs braucht Zwischenstationen – so auch der Transport, die Übermittlung von Daten. Im Unterschied zum analogen Postwesen fallen an den digitalen Knotenpunkten aller Wahrscheinlichkeit nach Kopien an, die bei AnbieterInnen, DienstleisterInnen, auf deren Rechnern, in Sicherungssystemen und Arbeitsspeichern abgelegt sind. Die Ansichtskarte geht zwar vom Briefkasten zum Postkasten durch mehrere Hände und kann unterwegs gelesen werden, sie bleibt aber ein Unikat, das von SenderIn zu EmpfängerIn weitergereicht wird. Beim E-Mail ist nicht klar, ob die Kopien auf



Schematische Darstellung von SenderIn – EmpfängerIn und Man-In-The-Middle. (by Christian Voigt)

Zwischenstationen, den Servern, erhalten bleiben oder gelöscht werden. Selbst wenn sie als gelöscht gelten, stellt sich die Frage, ob sie tatsächlich überall gelöscht wurden. Kopien fallen nicht nur im Zuge der Datenübertragung automatisch an, sie können von Dritten auch gezielt abgegriffen werden. Als Bezeichnung für diese Position von Dritten, die sich in die Datenübertragung einschalten, hat sich „Man in the Middle" oder kurz MitM etabliert.

„Man in the Middle" sind im digitalen Alltag immer existent. Das heißt noch nicht, dass sie Daten missbrauchen. Bei einer tatsächlichen Attacke aus der MitM-Position heraus nutzen AngreiferInnen aber diese Relaisstation in der Datenübertragung zum Beispiel dafür, dass sie mitlesen, Daten abgreifen und unberechtigter Weise auswerten. Beispielsweise wenn über Phishing-Mails und darin enthaltene Links, E-Mail-EmpfängerInnen in Täuschungsabsicht auf die Server und Websites der AngreiferInnen umgeleitet werden. Nach dem gleichen Prinzip werden Trojaner oder Malware untergejubelt, wenn EmpfängerInnen etwas herunterladen, das nicht von dem/der erwarteten AbsenderIn stammt. Im Fall von E-Mails, die absolut täuschungsecht, aber tatsächlich gefälscht sind, nennt sich diese Attacke dann E-Mail-Spoofing (z. B. „Sie haben ein neues Paket von der Post." mit einem nachgeahmten Logo der Österreichischen Post). Werden massenweise E-Mails – an mehr oder weniger zufällig abgegriffene Adressen – gesendet, spricht man von Spam (z. B. „Hilfe, ich bin in Moskau gestrandet und habe kein Geld mehr." von der Adresse einer Freundin).

Mit M-Attacken können allerdings auch eine viel öffentlichkeitswirksamere Richtung nehmen. Gelingt es AngreiferInnen, sich in die Steuerung eines Sensors für ein Zutrittssystem einzuschleichen, über den Smart-Meter des Energielieferanten oder über die Steuerung einer digitalen Werbefläche, können sie in damit verbundene weitere System eindringen oder diese – unbemerkt – übernehmen. Aufgrund des Umstands, dass in den Nullen und Einsen nicht nur Kommunikationsinhalte übertragen werden, sondern auch Metadaten oder ganze Programme, kann eine MitM-Attacke weitreichende Auswirkungen haben. Programme können umgeschrieben oder eigene Befehle eingespeist werden. Das infizierte Gerät kann nun Daten an unbekannte Dritte senden. Es kann als Spam-Verteiler dienen, für Attacken auf weitere Systeme missbraucht werden, das System lahmlegen, Erpressung zur Folge haben oder auch als Rechenleistung für das Mining von Kryptowährungen abgezweigt werden.

Möglicherweise informiert ein Gerät, dass es übernommen wurde. Das bezeichnet man als Ransomware, wenn nicht NutzerInnen selbst – aus guter Datenschutzpraxis heraus – die eigenen Dateien, Ordner und Laufwerke verschlüsselt haben, sondern unbekannte Dritte, die nun den Code zu den unlesbaren, weil verschlüsselten Daten haben. Den Schlüssel, mit dem der/die NutzerIn wieder an die eigenen Daten kommt, wollen die Cyberkriminellen in den meisten Fällen gegen Lösegeld herausrücken. Meist gelingt es nicht die eigenen Daten zu „befreien", ohne auf die Erpressung einzugehen.

Kann man „MAN IN THE MIDDLE" ATTACKEN vermeiden?
Es ist kaum zu vermeiden, dass digitale Kommunikation und Operationen über „Man in the Middle"-Positionen laufen. Was aber vermieden werden kann, sind erfolgreiche MitM-Attacken dort, wo strikte Regeln der Datenübertragung angewendet werden. Dort, wo die Integrität von Geräten und Programmen sicher ist, wo die Identität von SenderIn und EmpfängerIn überprüft wurde, wo die Daten verschlüsselt übertragen werden und alles in Backups gespeichert wird, ist die Wahrscheinlichkeit für schwerwiegende Folgen derartiger Attacken geringer.

Der überwiegende Großteil von Hacker-Attacken, Identitätsdiebstahl, Datenmissbrauch und allgemein Computerkriminalität läuft eigentlich gar nicht über „Man in the Middle"-Attacken. Häufiger wird auf die Schwachstelle Mensch gesetzt. Viele der berühmtesten Hacks funktionieren über „social engineering". Es meldet sich beispielsweise eine Vertrauen erweckende Stimme am Telefon als „Kollege aus der IT-Abteilung" oder „beauftragte Sicherheitsexpertin", verwickelt das vorher gezielt ausgesuchte Gegenüber in eine Gesprächssituation, bittet um die Überprüfung von ein paar Einstellungen oder erfragt unauffällig ein Passwort. Bekannt in dieser Hinsicht sind mittlerweile die Anrufe aus angeblichen Call-Centern von Microsoft.

Professionelles IT-Personal wird nie um ein Passwort fragen, genauso wenig wie Banken oder Online-Dienste Links ausschicken, um Benutzerdaten neu zu bestätigen. Bei solchen Anrufen und E-Mails sollten die Alarmglocken laut läuten und die Kommunikation beendet werden.

KONTROLLVERLUST

Ist die Kontrolle über Geräte und online-Zugänge einmal verloren, lässt sie sich nur schwer wiedererlangen. Daher sollte Vorsicht die Mutter der Porzellankiste und auch der Geräteverwaltung sein.

Digitale Datenübertragung läuft – wie andere Kommunikation auch – von SenderIn zu EmpfängerIn und zurück, wobei jeweils ein oder mehrere „Man in the Middle"-Stationen passiert werden. Auf diesem Weg begegnen den Nullern und Einsern mitunter Risiken, die es abzuschätzen gilt. Diese Risikofolgenabschätzung wird in IT-Kreisen threat modeling genannt. Dabei wird gefragt, welche Probleme auftreten könnten, wenn dies oder das genutzt wird, wenn die Wege der Datenübertragung diese oder jene Route nehmen, diese oder jene Inhalte transportieren. Es wird dabei analysiert, wie die gefundenen Risiken ausgeschalten oder minimiert werden können – beispielsweise indem die Nutzungseinstellungen geändert oder eine weniger risikoreiche Alternative genutzt wird.

Wenn jemand etwa eine Suchmaschine aufruft, um zu „Hautkrebs" zu recherchieren – welches potenzielle Risiko besteht für die Position MitM? Die Suchmaschine speichert vermutlich die Information und könnte sie als Datenhändler weiterverwenden. Die Wahl einer Privatsphäre respektierenden Suchmaschine wie startpage oder duckduckgo reduziert dieses Risiko.

Peter und Maria wollen sicher kommunizieren. Sie nutzen dazu E-Mail, Handy, WhatsApp, alles kunterbunt durcheinander. Was ist eigentlich das spezifische Risiko, das ihre Kommunikation unsicher macht? Haben sie den Verdacht, von jemand ausspioniert zu werden? Liest der Chef mit? Schreiben sie Dinge, die von Konzernen wie Google nicht ausgewertet werden sollen? Sind sie eigentlich ein heimliches Liebespaar, das nicht entdeckt werden möchte? Je nachdem wird die Analyse zu unterschiedlich vordringlichen Risiken und passenden Antworten kommen. Statt Gmail am Laptop nutzen Peter und Maria vielleicht besser den Signal Messenger auf ihren privaten Smartphones. Möglicherweise nutzen sie besser Datenschutz sensible E-Mail-Körbe von Posteo und statt Microsoft Outlook als E-Mail-Client in der Arbeit möglicherweise besser die Website von Posteo über den Tor Browser.

Einige Anbieter haben Software entwickelt, die zeigt, welche Player die Aktivitäten im Internet mitverfolgen. Eine solche App ist der „Privacy Badger".

Der „Privacy Badger" zeigt versteckte Drittanbieter, die Website-Aufrufe mitverfolgen.
(Screenshot by Christian Voigt)

METADATEN UND DEREN AUSWERTUNG

Ob bei digitaler Kommunikation, Navigation im Fahrzeug, Arbeit am Computer oder an der Produktionsmaschine: immerzu fallen sogenannte Metadaten an. Diese Metadaten sagen nichts darüber aus, was an Inhalten übertragen wird, jedoch jede Menge darüber wie wann an wen übertragen wird. Verbindungsdaten, wie Zeitstempel, Standortbestimmung geben Auskunft darüber wer wann wo und wie lange Datenspuren hinterlässt – beispielsweise bei der Arbeit. Die Daten sind ursprünglich nicht unbedingt personenbezogen, können aber indirekt Personen zugeordnet werden.

Was passiert eigentlich mit den METADATEN?
Daten, die im Internet oft nur als Nebenprodukt und ohne direkten Personenbezug entstehen, können zu Profilen verdichtet werden, die wiederum zur Bewertung von Personen dienen. Diese Profile sagen bisweilen mehr über eine Person aus, als diese eigentlich bereit wäre, über sich preiszugeben. Mitunter werden sie auf Basis intransparenter Parameter erstellt. In manchen Fällen würde sich die profilierte Person selbst nicht wiedererkennen.

Die Vorratsdatenspeicherung von Metadaten aus der Telekommunikation seitens des Staates Österreich ist 2014 vom österreichischen Verfassungsgerichtshof zu Fall gebracht worden, weil sie dem Grundrecht auf Datenschutz sowie dem Recht auf Privat- und Familienleben gemäß Artikel acht der Europäischen Menschenrechtskonvention widerspricht. Dennoch bestehen Geschäftsmodelle privater Unternehmen unter anderem im (Meta-)Daten sammeln, kaufen und verkaufen, Daten be- und auswerten, (Werbe-)Profile erstellen.

Bei Datenmaterial, das von Data-Profiling-Firmen herangezogen wird, ist nicht immer klar, wie es gesammelt wurde, welche Kriterien herangezogen und gewichtet wurden oder ob das Datenmaterial überhaupt berechtigt im Besitz der Unternehmen ist. Mit personenbezogenen Daten wird hochgerechnet, wie eine Person oder Personengruppe sich wahrscheinlich zukünftig verhalten wird und es wird eine Abstufung festgelegt, sogenanntes Scoring. Scoringwerte sind über Algorithmen errechnete Wahrscheinlichkeiten, die pro Person, Personengruppe oder pro Haushalt gesammelt werden. Wie die Algorithmen funktionieren, ob sie sinnvoll oder absurd sind, das lässt sich schwer nachvollziehen – in aller Regel handelt es sich nämlich um Geschäftsgeheimnisse.

Im Finanzbereich wird im Kreditscore die Hochrechnung ausgedrückt, ob Personen wahrscheinlich einen Kredit zurückzahlen werden können, also kreditwürdig sind – oder nicht.

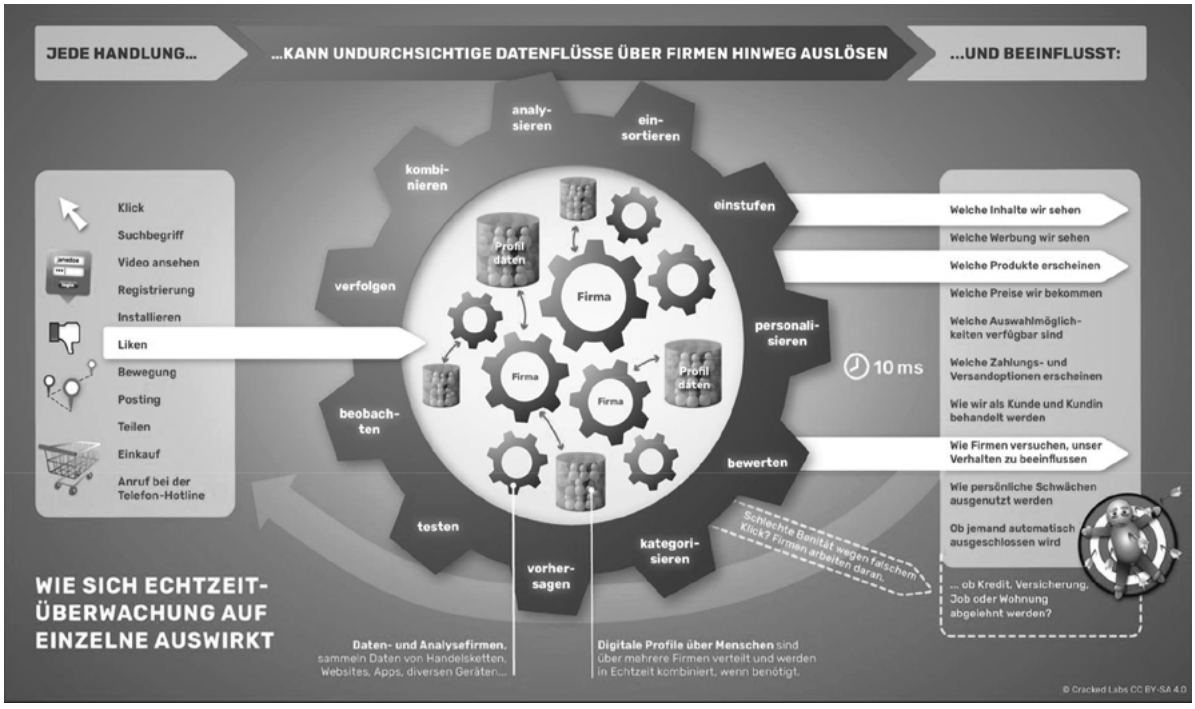
So ein Wahrscheinlichkeitsmodell kann laufend angepasst werden, weitere Daten integriert werden. Das Verarbeiten historischer Daten, um aktuelle zu interpretieren und daraus Schlüsse für die Zukunft zu ziehen, wird predictive analytics genannt. Nicht nur die vermutete Produktivität der ArbeitnehmerInnenschaft oder Kreditwürdigkeit wird auf diese Weise vorhersagend berechnet, auch die Höhe von Mieten in Abhängigkeit von der Kriminalitätsrate in der jeweiligen Wohngegend, das Zusammenpassen von Liebespaaren oder gar Straffälligkeit von einzelnen Menschen werden predictive analytics unterzogen.

Die Firma Workday bietet ein Produkt an, mit dem das Management laufende Prognosen hochgerechnet bekommt für die Wahrscheinlichkeit von Kündigungen seitens der ArbeitnehmerInnen. Der Europäische CEO erklärt im Interview: *„Unsere Software braucht 1,5 Jahre Datenhistorie der Firma, dann spuckt unser Algorithmus die Abwanderungswahrscheinlichkeit zu 93 Prozent richtig aus."* (https://www.business-punk.com/2016/06/workday-software/ [21.3.2022])

Die Europäische Datenschutzgrundverordnung (DSGVO) untersagt in Artikel 22, dass aufgrund rein maschineller Berechnungen schwerwiegende Entscheidungen über Personen getroffen werden. Sollte derartiges in Verwendung sein, müssen die Betroffenen jedenfalls über die zugrundeliegenden Logiken informiert werden und freiwillig einem solchen Profiling zugestimmt haben. Mitunter wird das als sogenanntes „Profilingverbot" bezeichnet, was nicht ganz richtig ist, da ja unter den Bedingungen der informierten Zustimmung und des menschlichen Einwirkens auf die Entscheidung Profiling juristisch betrachtet durchaus DSGVO-konform wäre.

Von der Zustimmung zu einem Profiling sollte nach Möglichkeit abgesehen werden, auch wenn Einzelne vielleicht scheinbar profitieren. Besonders im Arbeitszusammenhang oder bei der Gesundheit kann Profiling unangebrachte Nebenwirkungen haben. Zum Beispiel, dass Versicherungsverträge – zumindest für junge gesunde risikoarm lebende Menschen – günstiger werden, für alle anderen aber leider nicht.

Zahlreiche Unternehmen bauen aus Datenspuren im Netz elaborierte Werbe-Modelle auf deren Basis individuell adressiert, unterschiedlich bewertet und entschieden wird – Vieles davon unbemerkt, Einiges davon sichtbar (z. B., wenn Suchmaschinen und Social-Media-Plattformen personalisiert zugeschnittene Wahlwerbung anzeigen, wenn unterschiedlich Preise für ein und dasselbe Produkte angezeigt werden).



Schematische Darstellung der potenziellen Auswirkungen der Echtzeitüberwachung von Internet-Aktivitäten. CC BY-SA Cracked Labs, 2017

DIE ABSICHERUNG VON GERÄTEN

Die Voraussetzung für Datenschutz und Datensicherheit ist, dass die Kontrolle und Integrität der online verwendeten Geräte gewahrt ist. Das ist gleich bei der Inbetriebnahme eines Gerätes, bei der Anmeldung im Betriebssystem Thema. Dass nach wenigen Minuten der Inaktivität eines Gerätes eine erneute Anmeldung erforderlich wird, ist ein Vorteil für die Gerätesicherheit. „It's not a bug, it's a feature!", es sei also kein Fehler, sondern eine Funktion, würde die IT-SicherheitsexpertIn sagen. Mit einer rasch aktivierten Wiederanmeldung können Zugänge von (unbefugten) Dritten ausgeschlossen werden.

Die Zeit für die Aktivierung eines Bildschirmschoners auf eine halbe Stunde oder mehr zu stellen, ist kontraproduktiv. Die Empfehlung lautet gerade umgekehrt, diese Zeit auf zwei oder drei Minuten einzustellen. Zusätzlich sollte man mit einfachen Tastenkombinationen wie Windowstaste + L für „lock" Bildschirme und BenutzerInnen-Konten sperren, sobald eine Minute nicht am Gerät gearbeitet wird.

DIE BENUTZERINNEN-KONTEN UND IHRE VERWALTUNG

Tutorials im Netz sind ein effizienter Weg empfohlene Software und Einstellungen zu studieren. Für so gut wie alles sind auf Youtube Anleitungsvideos zu finden, die zeigen, wo bestimmte Einstellungen sich befinden und die gut erklären, warum an welcher Stelle dies oder das empfehlenswerte Schritte sind. Auch für BenutzerInnen-Verwaltungen in Windows, auf Android oder Apple Smartphones, für Linux oder Samsung lassen sich eine Menge hilfreicher Videos finden. (Nicht vergessen: bei Youtube einen Add-Blocker verwenden!)

Betriebssysteme auf PCs, Laptops und mobilen Geräten haben BenutzerInnen-Konten und diese werden wiederum in einer Benutzerverwaltung administriert. Konten können für alle NutzerInnen offenstehen, auf bestimmte Gruppen oder Abteilugen beschränkt oder nur den IT-Administratoren zugänglich sein. Sie können zur Anmeldung die Eingabe eines Passwortes bzw. Passsatzes verlangen, biometrische Daten wie den Fingerabdruck voraussetzen oder auch ohne eigenen Zugang funktionieren.

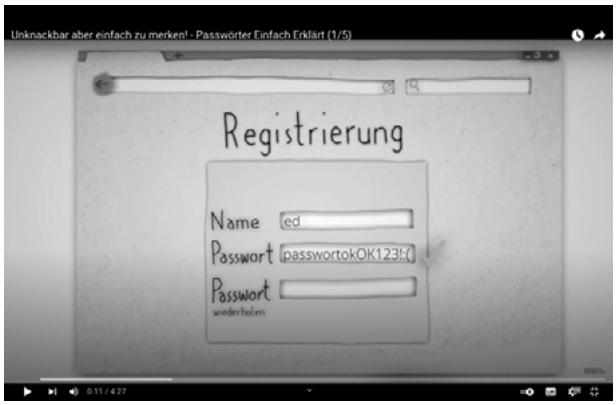
Für alle gemeinsam genutzten Geräte (innerhalb eines Netzwerks) gilt, dass mehrere Benutzerkonten mit unterschiedlichen Rechten angelegt sein sollten. Selbst dort, wo Geräte ausschließlich von einer Person allein genutzt werden, sollte das so gehandhabt werden. Für den täglichen Gebrauch wird nicht das Benutzerkonto mit Admin-Rechten benötigt, sondern ein eigenes für eben den alltäglichen Gebrauch. Wird mit diesem Konto etwas Problematisches heruntergeladen, fällt es Angreifern, Skripten oder Trojanern ungleich schwerer, etwas zu installieren und an Berechtigungen zu ändern, weil das Benutzerkonto das nicht zulässt. Für die Fälle, wo jemand anderer schnell Zugriff zum eigenen Gerät bekommen soll, sollten vorab Gästekonten eingerichtet sein. Eine Anmeldung ist dann jederzeit möglich, aber eben mit einem Gastkonto. Der schnelle Wechsel von Benutzerkonto zu Benutzerkonto lässt sich vorab üben, so dass er in der passenden Situation leicht von der Hand geht.

Pro Gerät sollte ein Benutzerkonto mit Administrationsrechten eingerichtet sein, um die alltägliche Nutzung von der Admin-Nutzung zu trennen. Außerdem kann noch ein Benutzerkonto für Gäste eingerichtet werden, um es Gästen zur Verfügung zu stellen.

DAS PASSWORT UND SEINE QUALITÄT

Wie werden Passwörter geprüft?
Wird ein Passsatz zur Anmeldung an einem Gerät eingegeben, wird er zu einem sogenannten „Hashwert" umgerechnet und mit dem gespeicherten Wert des Zugangssystems abgeglichen. Die Systeme, die Passwörter bzw. Passsätze abgleichen und bei Übereinstimmung eine Anmeldung zulassen, dürfen ihrerseits nie BenutzerInnen-Passwörter selbst speichern, sondern nur den Hashwert. Allfällig gehackte Datenbanken liefern AngreiferInnen dann keine Zugangsdaten.

Bei der Erstellung eines Passwortes gilt grundsätzlich je länger und komplexer desto sicherer. Die Verwendung von Groß- und Kleinbuchstaben in Kombination mit Ziffern und Sonderzeichen erhöht die Komplexität eines Passwortes. Seit geraumer Zeit wird empfohlen, statt einzelner Passwörter besser kurze Passsätze zu bilden. Sie sind einfacher merkbar und selbst ein kurzer Satz hat schnell die Länge von zwanzig Stellen. Sätze enthalten in der Regel Groß- und Kleinbuchstaben sowie Satz- oder Sonderzeichen, was ebenfalls ein Vorteil ist. Man könnte auf Sätze aus der persönlichen Umgebung zurückzugreifen (z. B. aus einem Buch, das im Betriebsratsbüro steht) oder mit einem Hobby zusammenhängen (Filmtitel, Reisedestinationen, Lied, Literaturzitat etc.).



Ein Erklär-Video zu Passwortqualität auf Youtube von Alexander Lehmann. https://www.youtube.com/watch?v=jtFc6B5lmIM

Zur sicheren Anmeldung an Geräten hilft hohe Passwortqualität. Ein ganzer Passsatz statt nur einem Wort ist empfehlenswert und diesen auch gegenüber Dritten nicht zu verraten. An diese Grundregel sollten NutzerInnen sich nicht nur im Arbeitsleben halten, sondern auch in Partnerschaften und Familien, bei sämtlichen genutzten Geräten. Ein Passwort kann auch per Zufallsgenerator erstellt werden, was eine hohe Sicherheit gewährleistet, dafür meist schwieriger auswendig zu merken ist.

Keinesfalls empfehlenswert ist das wiederholte Verwenden eines Passwortes bzw. -satzes für mehrere Accounts. Dort, wo Zugänge direkt kontrolliert werden, sollten niemals die Passwörter der BenutzerInnen gespeichert sein. Wird eine Datenbank mit Passwörtern gehackt, können sonst AngreiferInnen sehr schnell auf alle Plattformen mit den erbeuteten BenutzerInnen-Kontodaten zugreifen.

Passwörter können gestohlen werden, so genannte „Pwned" Passwords". Der Begriff stammt im Grunde vom Englischen „own", besitzen, „owned" besessen, und wird im übertragenen Sinne im Zusammenhang mit Passwort-Hacks als „erwischt" verwendet.

Ob eigene Benutzerkonten im Netz von einem Diebstahl betroffen sind, sollte regelmäßig nachgesehen werden; z. B. auf www.monitor.firefox.com oder www.haveibeenpwned.com .

Hat jemand zahlreiche Accounts und Zugänge zu verschiedensten online Plattformen und Netzwerken, so sind viele Zugangscodes, Passwörter und -sätze zu merken und regelmäßig zu ändern. Dazu bietet sich die Nutzung eines Passwort-Managers an. Das sind Programme, in denen eine große Anzahl an Zugängen sicher gespeichert werden können. Die Zugänge werden mit einem Master-Passwort verschlüsselt, das den Zugang zu allen anderen sichert und daher sehr stark sein sollte. Die eigentliche Liste, die Tresor-Datei, ist verschlüsselt und sollte an mindestens drei unabhängigen Speicherorten als Backup gesichert sein. Ein Passwort-Manager übernimmt die Verwaltung beliebig vieler Passsätze.

Anbieter für Software zum Passwort-Management gibt es viele mit unterschiedlichen Features (z. B. automatische Aktualisierung zwischen PCs, Laptops und Smartphones). Browser wie Firefox haben ebenso die Option, alle gespeicherten Passwörter im Browser mit einem Master-Passwort zu sichern. Sicherheitsschranken mit Master-Passwörtern werden zunehmend Standard in Browsern, Betriebssystemen, Smartphones und sollten genutzt werden.

Der Passwort-Manager „KeePass" sichert alle ihm anvertrauten Passwörter und -sätze in einer verschlüsselten Tresordatei. (Screenshot by Christian Voigt)

Biometrische Anmeldeverfahren (z. B. Fingerprint, Irisscan, Stimmerkennung, Handvenenscan etc.), werden mitunter als einfach zu verwendende Zugänge angepriesen, da die NutzerInnen sie immer mit dabei haben, sie nicht vergessen können und sie zugleich eindeutig zuordenbar sind. Sie sollten unbedingt nur in gut begründeten Fällen, bei hochvertraulichen Zugängen verwendet werden. Ein biometrisches Merkmal ist gänzlich einmalig, eben weil es nur einer einzigen Person zugeordnet werden kann, und bei Verlust oder Diebstahl kaum ersetzbar ist. Es wäre damit dieses einzigartige Erkennungsmerkmal bekannt gegeben und von einer Software bzw. einem Anbieter verarbeitet, was nicht im Sinne des Schutzes der Privatsphäre oder dem Schutz der Persönlichkeit ist.

SOFTWARE-UPDATES, OPEN SOURCE UND VIRENSCHUTZ

Software-Updates sind ein weiterer Aspekt zur Sicherheit von Geräten und Umgebungen. In aller Regel schließen Software-Updates Sicherheitslücken. Daher empfiehlt es sich, Updates besser früher als später zu installieren. Bei umfassenden, Wesentliches ändernden oder gänzlich neue Features implementierenden Updates (z. B. neue Generation einer Software oder neues Betriebssystem) macht es mehr Sinn, etwas zu warten und Erfahrungsberichte im Netz anzusehen.

Free Open Source Software (FOSS) ist nicht automatisch sicherer als proprietäre, geschlossene Software. Bei Software im Eigentum von gewinnorientierten Unternehmen kann es allerdings gefährlich werden auf Sicherheitslücken hinzuweisen, weil Gefängnisstrafen drohen. Der us-amerikanische Programmierer und radikale Vertreter von frei zugänglichem Wissen, Aaron Swartz, ist ein Beispiel dafür, dass Unternehmen ihr Eigentum rücksichtslos hüten.

Für Privatunternehmen kann es vorteilhafter sein, Lücken zu verheimlichen und/oder die AufdeckerInnen rechtlich zu belangen, als Sicherheitslücken aufzufinden und sie zu schließen. Die Öffentlichkeit erfährt nicht verlässlich von allfällig bestehenden Sicherheitsproblemen.

Bei Open Source Software ist es umgekehrt. Es ist legal und gewünscht, dass Software auf Missbrauchsmöglichkeiten getestet wird und gefundene Probleme veröffentlicht werden. Lücken sind also öffentlich bekannt und werden von der Community schnellstmöglich behoben. Das gilt zwar nicht bei jedem kleinen Softwareprojekt, aber jedenfalls bei populären und im besonderen Maße bei Software, deren Programmierer sich den Datenschutz „an die Fahnen heften".

Welche Alternativen gibt es?
Freie und/oder Open Source Software zu nutzen, kann von Vorteil sein. Beispielsweise kann als Betriebssystem Linux mit dem Libre Office die Funktionalität von Microsoft Office abdecken. Der Firefox Browser ist eine gute Alternative zu Google Chrome am Desktop und der Brave Browser die sicherere Alternative zu anderen Browsern auf mobilen Geräten. Der Signal Messenger ersetzt WhatsApp. Gimp kann statt Photoshop verwendet werden. Nextcloud empfiehlt sich statt OneDrive oder Dropbox, Jitsi an Stelle von Skype, CryptPad statt Google Docs, KeePass als Passwort-Manager, VeraCrypt als Verschlüsselungssoftware etc..

Es gibt zahlreiche Webseiten im Netz, die alle möglichen Programme/Apps in ihren „App-Stores" anbieten. Was auf der einen Seite praktisch wirkt, ist auf der anderen Seite mit Vorsicht zu genießen. Das Finanzierungsmodell dieser Seiten basiert oft auf Werbung, weswegen NutzerInnen ausspioniert werden, um das perfekt auf sie zugeschnittene Werbeprofil zu erstellen. So wird mitunter bei einem Download mehr heruntergeladen , als offensichtlich ist und eigentlich von den NutzerInnen erwartet und gewünscht wird. Außerdem sind diese Plattformen herunterladbarer Anwendungen ein lohnendes Angriffsziel, um die angebotene Software zu infizieren.

Programme/Apps sollte man bewusst auswählen und nicht voreilig installieren. Nach Möglichkeit sollte man auf Freie Open Source Software setzen.

Programme/Apps sind vorzugsweise von den Websites der Anbieter direkt herunterzuladen.

Im Idealfall wird vorab die Signatur der Softwarepakete überprüft. Das sind PGP-Signaturen (pretty good privacy), die das heruntergeladene Paket haben muss, andernfalls ist es gegenüber dem vom Hersteller gedachten Produkt verändert worden und etwas stimmt nicht.

Beim Download mit dem „Torbrowser" wird eine Signatur angegeben. (Screenshot by Christian Voigt)

Etwas Recherche im Netz, wie eine neue App bewertet wird, ist immer gut investierte Zeit. Bei Wikipedia und bei Datenschutz-NGOs (z. B. www.digitalegesellschaft.de) gibt es immer wieder aktuelle Informationen, von welcher Software abgeraten und welche empfohlen wird. Den Newsletter von Datenschutzorganisationen kann man getrost abonnieren, um über Empfehlungen und Warnungen auf dem Laufenden zu bleiben.

Software, die nicht mehr gebraucht wird, sollte wieder deinstalliert werden.

Bei der Installation von Apps für mobile Geräte sollte man sich auf die App-Stores verlassen können. Der App-Store von Apple hat diesbezüglich einen guten Ruf. Unter www.appcheck.mobilsicher.de sind Testberichte zu Android Apps zu finden.

Wird diese Vorsicht und Umsicht im Netz gelebt, braucht es eigentlich keinen Virenschutz. Versierte NutzerInnen betrachten Virenschutzprogramme bisweilen als offizielle Trojaner, die alles inspizieren dürfen und verzichten daher gerne darauf. Virenschutzprogramme können auch Geräte verlangsamen und bieten keine absolute Sicherheit gegen Viren, Trojaner, Malware etc., wenn man im Vertrauen auf sie sorglos agiert.

Für NutzerInnen, die sich aktiv um Datenschutz und Sicherheit bemühen, macht die Installation eines Virenschutzprogramms Sinn, solange sie nicht als Freibrief für sorglose Ignoranz missinterpretiert wird.

VERSCHLÜSSELUNG UND SICHERHEITSKOPIEN (BACKUPS)

„Die Cloud ist nichts anderes als anderer Leute Computer", lautet ein Spruch. In die Wolke, englisch „Cloud", transferieren lassen sich einzelne Dateien, Ordner oder auch ganze Laufwerke. Die „Cloud" dient nicht nur als Speicherort, es können über die Server externer Anbieter einzelne Programme und komplette Softwarepakete laufen. Cloud-Dienste werden von zahlreichen Unternehmen mit unterschiedlichsten Funktionen in verschiedensten Versionen angeboten. Typischerweise sind E-Mails oder Messenger-Dienste und deren Aufbewahrung und Verwaltung in der „Cloud" angesiedelt. Microsoft hat beispielsweise sein gesamtes riesiges Angebot in die Cloud verlagert. Es gibt Cloud-Anbieter zu allem, was online möglich ist – gratis oder als Abo, automatisch verschlüsselt oder nur auf Wunsch mit bestimmter Encryption-Software versehen, Speicherorte in aller Welt etc.. Der Vorteil von Daten auf fremden Servern liegt darin, dass sich Backups ablegen lassen, dass man von überall aus online darauf zugreifen kann, dass der Anbieter in der Regel die Verantwortung für die Wartung und Sicherheit übernimmt.

Ein Aspekt der digitalen Sicherheit sind Sicherungskopien.

Als sicher gespeichert gilt etwas nach der 3-2-1 Regel, wenn eine Datei in drei Kopien existiert, auf zwei verschiedenen Typen von Speichermedien, wobei mindestens eine Kopie außer Haus sein sollte. Diese Situation wäre z. B. gegeben, wenn eine Kopie auf der Festplatte des PCs oder Laptops liegt, eine auf einem externen Speichermedium (z. B. USB-Stick oder externe Speicherplatte) und eine in der Cloud (z. B. auf www.luckycloud.de). Die Kopien sollten entweder automatisch synchronisiert werden oder in regelmäßigen Abständen neu gespiegelt (kopiert) werden.

Verschlüsselung ist immer eine gute Idee, bei Dateien, Ordnern, Festplatten oder Festplatten-Partitionen (das sind Unterteilungen der Festplatte in unterschiedliche Bereiche). Verschlüsselung ganzer Festplatten oder Geräte ist wichtig, falls ein Gerät verloren geht oder gestohlen wird. Smartphones enthalten diese Option heute schon als Standard. Unabhängig von der Verschlüsselung der Geräte-Festplatte ist es unerlässlich, sensible Ordner und/oder Dateien eigens zu

verschlüsseln. Das ist umso wichtiger, wenn auch andere Personen Zugang zum Gerät haben.

Die Festplattenverschlüsselung ganzer Geräte hat die Achillesferse, dass die Verschlüsselung nur gegeben ist, wenn das Gerät ausgeschalten ist. Beim eingeschalteten PC, Laptop oder Smartphone ist die Festplatte notwendigerweise entschlüsselt, weil Betriebssystem und Programme sonst nicht laufen könnten. Geräte sollte man deshalb nicht permanent aktiviert lassen. Sie herunterzufahren ist eine weitere Schutzmaßnahme gegen ungewollten Zugriff.

Backups schützen gegen den Verlust der Daten, wenn der Zugriff auf ein Gerät nicht mehr gegeben ist. Opfer von Ransomware sind weniger erpressbar, wenn sie ihre Daten als Backups gesichert haben.

Zusammengefasste Tipps zur IT-Sicherheit

- Sicheres Passwort verwenden
- Bildschirmschoner aktivieren
- Geräte abdrehen, wenn sie außer Reichweite sind
- Virenschutz installieren
- Festplatte verschlüsseln
- Laufend Backups machen
- Sicherungskopien verschlüsseln
- Cloud-Dienste für verschlüsselte Backups nutzen
- Am Ball bleiben (z. B. per Newsletter)

SICHERE BROWSER UND IHRE EINSTELLUNGEN

Selbstbestimmtes Surfen beginnt bei der Auswahl und Anpassung der Browser, dem Blockieren der (versteckten) Datensammler, geht weiter bei der Nutzung von Social Media bis hin zur Wahl der Suchmaschine. Mit welchen Browser-Einstellungen und welchen Browsern im Netz gesurft wird, spielt eine wesentliche Rolle beim Schutz der Privatsphäre. Neben Googles Chrome, Microsoft Edge und Apples Safari gibt es Firefox als Alternative, die nicht einem Internetgiganten gehört.

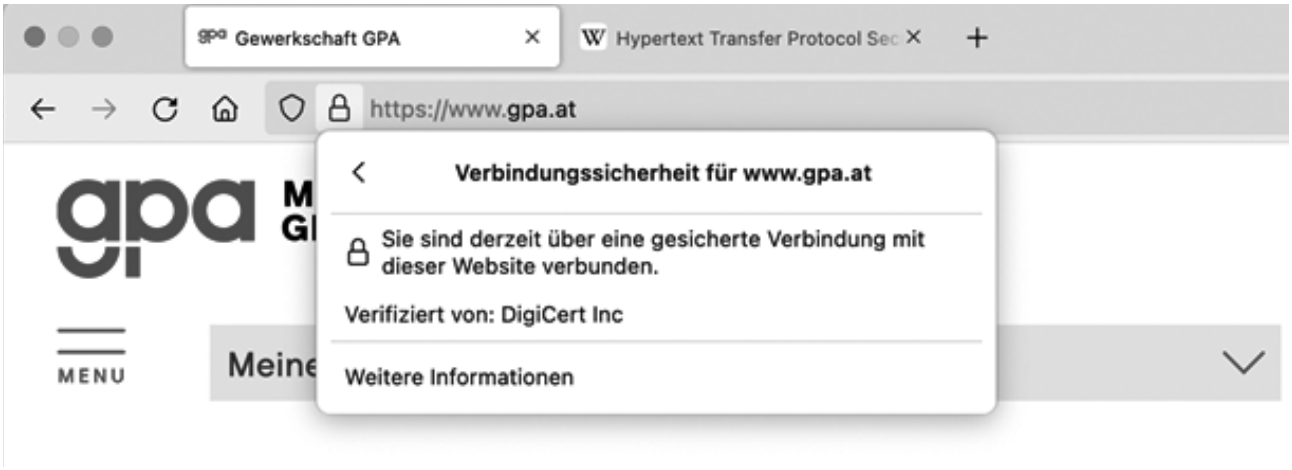
Ein Großteil der Internetaktivitäten mit mobilen Geräten läuft über Apps und die holt sich der/die NutzerIn in den Online-„Geschäften", den App-Stores, also einer Plattform, auf der die Apps heruntergeladen werden. Das gravierendste Problem stellt dabei die Online-Werbung von Google (alphabet), Amazon, Facebook (Instagram, Meta) auf ebendiesen Stores bzw. der jeweiligen zum Konzern gehörigen weiteren Plattform dar.

Drei Browser, die stabile Leistung erbringen, nicht fürs Datensammeln bekannt sind und keinem Internetgiganten gehören, seien hier explizit empfohlen: Mozilla Firefox, Tor und Brave.

Jede Empfehlung ist selbstverständlich nur eine Momentaufnahme. Es ist unklar, wie es mit der Mozilla Foundation und deren Firefox weitergeht. Es bleibt abzuwarten, wie sich Brave als Browser für Desktop Geräte entwickelt und finanziert. Daher gilt hier – wieder einmal – die Empfehlung, in regelmäßigen Abständen etwas Zeit in die Recherche zu aktuellen Entwicklungen zu investieren.

In letzter Zeit haben jedoch auch alle großen Anbieter die Datensicherheit vermehrt ausgebaut und binden zu diesem Zweck sinnvolle Features in ihre Browser ein. Allerdings basiert das Geschäftsmodell von Google, Amazon und Facebook stark auf Werbung, auf Anzeigen. Es besteht zwar ein Interesse, sich vor der Konkurrenz zu schützen und gegen Cyberkriminalität vorzugehen, doch werden die Konzerne nicht aufhören, personenbezogene Daten zu sammeln, zu aggregieren, zu detaillierten Personenprofilen zu bündeln und diese Informationen gewinnbringend zu nutzen.

Egal welcher Browser benutzt wird – und viele NutzerInnen verwenden mehrere parallel – man sollte die Einstellungen anpassen und durch Erweiterungen (oder Add-On's) so konfigurieren, dass sich Werbung, Tracker, Skripte und Cookies nicht beliebig „entfalten" können. Werbeblocker – im Internet-Jargon ist der englische Ausdruck Adblocker gebräuchlich – wie ublock-Origin und der Privacy Badger für die Abwehr unsichtbarer Tracker sind ein Muss. Für fortgeschrittene NutzerInnen bieten sich Add-On's wie NoScript zur Feinjustierung an, die pro Website differenzieren, wie mit Skripten umgegangen werden soll. Auf mobilen Geräten übernimmt der Brave Browser einige dieser Maßnahmen automatisch.



Das Symbol des Vorhängeschloss symbolisiert die sichere Verschlüsselung. (Screenshot by Christian Voigt)

Immer zu achten ist auf eine sichere Verbindung. Im Webadress-Feld eines Browsers ist zu sehen, ob die Verbindung zu einer Website per http oder über https aufgerufen wird. Das zusätzliche S steht für „secure" und bedeutet, dass erstens die Datenübertragung verschlüsselt und zweitens die Identität der Website von einer unabhängigen Zertifizierungsstelle validiert ist. Ohne das „s" würden eingegebene Daten als Klartext übertragen. Der Klick auf das Symbol führt zu weiteren Infos, wie beispielsweise die zertifizierende Stelle.

Parallel mehrere Browser installiert zu haben macht Sinn. Dann könnten Sicherheitseinstellungen in Abstufungen gesetzt werden, sodass ein eher offener Browser für Websites genutzt wird, denen begründet vertraut wird. Ein weiterer könnte dann restriktiver und speziell für Social Media Plattformen eingerichtet sein, sodass Werbung auf diesen Plattformen gezielt unterbunden wird. Der Torbrowser wiederum verschlüsselt die Datenpakete zu und von Servern extra noch einmal und nutzt das Tor-Netzwerk an Tor-Servern, um das Surfen zu anonymisieren. Allerdings kann das Tor-Netzwerk in manchen Betrieben blockiert sein.

SUCHMASCHINEN, SCHATTENPROFILE, LÖSCHRECHTE

Eingaben in Suchmaschinen enthalten potenziell eine schier unglaubliche Menge an (personenbezogenen) Informationen. In der Datenbank der Suchmaschine bleiben Suchhistorien mitunter jahrelang aufbewahrt – und ausgewertet. Alternative Suchmaschinen (z. B. StartPage, DuckDuckGo) sind dem gegenüber vorzuziehen, da sie keine Profile ihrer NutzerInnen erstellen.

Wer allerdings die großen Plattformen nicht nutzt, ist deshalb noch lange nicht unbekannt für diese Konzerne. Von Kontakten, die diese Plattformen nutzen, wird auch auf Personen rückgeschlossen, die sich von ihnen fernhalten – es werden sogenannte Schattenprofile angelegt. Diese werden aus Daten erstellt, die über den Umweg anderer NutzerInnen gewonnen werden (z. B. deren Adressbuch oder deren Standort). In den Schattenprofilen wird aufgrund vorhandener personenbezogener Daten auf Wohnort, Bildung, Kaufkraft etc. geschlossen.

E-Mails zwischen irgendeinem Anbieter (z. B. GMX) und Gmail-NutzerInnen werden dennoch von Google gespeichert. Google hat also logischerweise die E-Mails der einen wie der anderen, sowie Verbindungsdaten wann, von wo nach wohin wieviel gemailt wurde.

Online-Kommunikation und Kollaboration ist also dazu geeignet, großen Playern auch indirekt eine große Menge an personenbezogenen Daten zuzuspielen. So wird deutlich, dass Datenschutz nicht bloß eine individuell-persönliche Entscheidung ist, sondern alle

betrifft. Auch auf anderen Ebenen wird deutlich, dass es sich beim Datenschutz nicht um ein „Individualproblem" handelt. Die Instrumente, die zum Schutz der Privatsphäre zur Verfügung stehen, werden in der Regel nicht von einer Person entwickelt, sondern von einer Community und sie können auch nur hilfreich sein, wenn mehrere NutzerInnen sie anwenden. Ein einseitig verschlüsseltes E-Mail trägt wohl kaum zur Kommunikation bei. Es braucht also kollektives Handeln, um Daten und damit die Privatsphäre Einzelner zu schützen.

Im Umgang mit BenutzerInnenkonten im Netz (z. B. posten auf Facebook , shoppen bei Amazon etc.) würde es zum guten Ton gehören, für die jeweilige Anmeldungen eine eigene E-Mail-Adresse bereitzuhalten. Eine solche Ansammlung von E-Mail-Adressen, ein E-Mail-Korb, würde dann der Administration von Accounts dienen und man könnte unterscheiden zwischen privater, geschäftlicher, behördlicher, vereinsbezogener, etc. Kommunikation, um Schattenprofile zu vermeiden.

Gegenüber Plattformen, die nicht mehr genutzt werden, ebenso wie gegenüber Firmen, mit denen kein Geschäftsverhältnis mehr besteht, kann das Recht auf Löschung personenbezogener Daten in Anspruch genommen werden. Das Recht auf Auskunft kann gegenüber Plattformen und Firmen in Anspruch genommen werden, die eigentlich keine Daten über uns haben sollten, weil wir sie nicht nutzen. Jeder/jede NutzerIn, jeder/jede KonsumentIn, jeder/jede BürgerIn hat das Recht zu wissen, welche personenbezogenen Daten über sie selbst von einem Anbieter verarbeitet werden.

Auskunftsbegehren und Löschrechte
Gemäß Artikel 15 der Europäischen Datenschutz-Grundverordnung besteht ein Recht für Betroffene, von Datenverarbeitern, Firmen, Behörden kostenlose Auskunft über die bei den Verantwortlichen aktuell verarbeiteten Daten zu erhalten. Es muss beauskunftet werden, welche personenbezogenen Datenkategorien zu welchen Zwecken und von wem verarbeitet und allenfalls an welche Empfänger weitergeleitet werden. Nach Möglichkeit muss auch die Speicherdauer mitgeteilt werden.

Einfach selbst zu löschen sind Cookies, kleine Dateien, die von Webseiten in Browsern abgelegt werden. Das kann man in den Eigenschaften über die Cookie-Verwaltung pauschal für sämtliche Cookies machen (womit allerdings auch sämtliche Anmeldeinformationen, hinterlegte Passwörter, Suchverläufe etc. verloren gehen) oder jene einzeln von den Websites löschen, die man nicht braucht und möchte.

Zusammengefasste Tipps zum Internet-Surfen

- Browser bewusst auswählen (z. B. Firefox, Brave).
- Add-Blocker installieren (z. B. Privacy Badger).
- ausschließlich auf sicheren Seiten surfen (https).
- Suchmaschine bewusst auswählen (z. B. StartPage, DuckDuckGo).
- Einstellungen von Benutzerkonten nutzen und Informationssammlungen ausschalten (z. B. Cookies, Tracker).
- getrennte E-Mail-Adressen für getrennte Zwecke (z. B. privat, dienstlich, behördlich, shoppen).
- Recht auf Datenauskunft und Löschung nutzen.

SICHERE KOMMUNIKATION UND DEREN VERWALTUNG

Es sollte immer darauf geachtet werden, dass Daten verschlüsselt übertragen werden und die Quelle verlässlich ist. Bei E-Mails ist Verschlüsselung wünschenswert, aber nicht einfach. Sensible Daten sollten immer verschlüsselt gespeichert werden, dann sind die Inhalte auch in der Cloud oder bei Verlust sicher. Verschlüsselung von Kommunikation ist manchmal schwierig, manchmal unmöglich. SMS lassen sich beispielsweise technisch nicht verschlüsseln. Bei E-Mails ist Verschlüsselung möglich und wünschenswert, aber nicht einfach.

Eine Alternative zur Verschlüsselung
... bieten Messenger-Dienste an, die generell Nachrichten nur verschlüsselt zwischen SenderIn und EmpfängerIn verschicken (z. B. Signal oder WhatsApp) oder das e-mailen verschlüsselter Anhänge.

E-MAILS UND MESSENGER

Es gibt vertrauenswürdigere und weniger vertrauenswürdige E-Mail-Anbieter.

Empfehlenswert ist beispielsweise

- Posteo – www.posteo.de
- JP-Berlin – www.jpberlin.de
- Mailbox – www.mailbox.org

Die meisten dieser Anbieter haben ihre Server in Deutschland, unterliegen als voll der DSGVO und setzen ganz zentral auf Datenschutz. Optionen zur Verschlüsselung sind gegeben. Die Kosten sind ab einem Euro pro Monat für E-Mail, Kalender und Notizen gering.
Die meisten Messenger-Apps bieten Telefonie, Nachrichten, Videotelefonie, Gruppenchats, das Senden von Dateien. Messenger haben dem „guten alten" E-Mail daher den Rang abgelaufen.

Für vertrauensvolle sichere Kommunikation sind derzeit empfehlenswert:
Signal, der in den USA beheimatete, auf Open Source basierende, für Verschlüsselung und Datensparsamkeit bekannte Messenger (https://signal.org/de/).

Threema, der Schweizer Messenger bietet neben Verschlüsselung auch on-premise (also auf den firmeneigenen Servern laufend) und ohne hinterlegte Telefonnummern seine Dienste (https://threema.ch/de).

Um die Messenger zu nutzen, braucht es nur die Installation der jeweiligen App auf einem Smartphone und schon ist jedwede, über die App mögliche Kommunikation verschlüsselt. Bevorzugter Weise basieren die Messenger außerdem auf Open Source Software. Während WhatsApp, Facebook, Instagram, Gmail die Kontaktdaten aus den Adressbüchern der NutzerInnen ebenso speichert wie Metadaten, d. h. wer wann wie oft und wie lange mit wem kommuniziert, kommt Signal ohne das Speichern dieser Informationen aus.

Signal wird per App auf dem Smartphones installiert und bietet zusätzliche eine Desktop-App. (Screenshot by Christian Voigt)

Messenger-Dienste werden laufend auf den Markt gebracht. Die meisten haben allerdings entweder Werbung in ihr Geschäftsmodell integriert oder sind kostenpflichtig. Fast alle bieten mittlerweile verschlüsselte Kommunikationskanäle an.

DATEIEN UND ORDNER UND IHRE VERSCHLÜSSELUNG

Bei MS Office Programmen ebenso wie bei Libre Office und manchen anderen Anwendungen können Dateien mit einem Leseschutz abgespeichert werden. Leseschutz bedeutet, dass die Datei im nicht geöffneten Zustand verschlüsselt gespeichert ist und nur mit der Eingabe des richtigen Passworts geöffnet und bearbeitet werden kann. Leseschutz kann nicht nur für einzelne Dateien, sondern für Ordner vergeben werden. Ein Leseschutz ist empfehlenswert.

Damit mit Leseschutz versehene einzelne Dateien nicht zu einer Unmenge an verschlüsselten Dateien und einer Unmenge an Passwörtern führen, hilft ein Komprimierungsprogramm wie beispielsweise 7Zip oder WinRAR.

Der Leseschutz bedeutet natürlich nicht, dass mit der verschlüsselten Datei nicht doch etwas schief gehen kann (z. B. kann eine Datei verloren gehen, irrtümlich oder absichtlich gelöscht werden, kaputt gehen). Um einen Schaden durch Verluste hintanzuhalten, braucht es Backups.

Wann ist etwas sicher gelöscht?
Das Löschen von Dateien, verschieben in virtuelle Papierkörbe und ausleeren derselben, stellt kein sicheres Löschen dar. Damit wird im System lediglich der Speicherplatz dieser Dateien wieder als verfügbar markiert. Zum sicheren Löschen gibt es eigene Programme wie Eraser oder File Shredder, die diese nicht mehr benötigten Speicherorte mehrmals überschreiben.

Die datenschutzperspektivisch gesehen beste Verschlüsselung bieten derzeit

- VeraCrypt www.veracrypt.fr und/oder
- Pgp (pgp für pretty good privacy) auf www.openpgp.org

Beide Systeme genügen selbst militärischen Standards, sind Freie Open Source Software und das Betriebssystem ist übergreifend zwischen Windows, Linux und Apple nutzbar. Mit VeraCrypt können beliebig viele und unterschiedlich große virtuelle Tresore erstellt werden, in die Dateien verschoben werden können. Ein geschlossener Tresor ist nach heutigem Stand des Wissens auch für Geheimdienste nicht entschlüsselbar. VeraCrypt ist gegenüber pgp etwas einfacher für ungeübte NutzerInnen.

Zusammenfassende Tipps für die online Kommunikation

- vertrauenswürdige E-Mail-Anbieter bzw. Messenger nutzen (z. B. Signal, Posteo)
- Leseschutz für Dateien, Ordner und Laufwerke aktivieren
- Kommunikation verschlüsseln (z. B. VeraCrypt, PGP)
- Passwort-Manager für die unterschiedlichen Passsätze verwenden (z. B. KeePass)
- Nicht auf Backups vergessen

SPANNENDES RUND UM DAS THEMA

Der **Blog der Abteilung Arbeit & Technik** postet rund um das Thema Datenschutz im Arbeitsverhältnis.
https://arbeitundtechnik.gpa.at

Die **Abteilung für Konsumentenschutz der Arbeiterkammer Wien** hat immer aktuelle Informationen zum Datenschutz für KonsumentInnen:
https://wien.arbeiterkammer.at/beratung/konsumentenschutz/datenschutz/index.html

Der **ChaosComputerClub Berlin**, eine der ältesten NGOs im Datenschutz, betreibt ein wiki mit „Anleitungen zur digitalen Selbstverteidigung" – sehr empfehlenswert!
https://berlin.ccc.de/wiki/Digitale_Selbstverteidigung/Surfen

Die **österreichische NGO „epicenter.works"** hat ebenso hilfreiche Vorschläge zur „digitalen Selbstverteidigung" zusammengetragen:
https://epicenter.works/crypto

Die von Unterrichtsministerium und EU co-finanzierte **Organisation „Safer Internet"** stellt gut aufbereitete Materialien für Kinder, Jugendliche, PädagogInnen und SeniorInnen zur Internet-Nutzung bereit:
https://www.saferinternet.at/

NOYB steht für none of your business und dafür, dass unsere Daten sowie unsere Privatsphäre nicht das Geschäft anderer sein sollten. Die NGO ficht Musterprozesse gegen Internetkonzerne (z. B. Facebook) deren Ergebnisse mitunter die digitale Selbstbestimmung fördern:
www.noyb.eu/de

Cracked Labs ist ein unabhängiges Institut für kritische digitale Kultur, das wichtige Studien und Präsentation publiziert hat, darunter zu Überwachung und Kontrolle am Arbeitsplatz.
www.crackedlabs.org

Wer einfach am Ball bleiben möchte, schaut auf einer der folgenden websites vorbei oder abonniert sich deren Newsletter:

Digital Courage setzt sich seit 1987 in Deutschland für Grundrechte und Datenschutz ein und möchte Technik und Politik kritisch erkunden und menschenwürdig gestalten.
https://digitalcourage.de/

Netzpolitik ist seit vielen Jahren das zentrale deutschsprachige Medium für digitale Freiheitsrechte.
www.netzpoltik.org.

Chaos Computer Club ist wohl der weltweit älteste HackerInnen-Verein und behandelt in seinem Podcast Chaosradio alle Themen dieser Broschüre und darüber hinaus:
www.chaosradio.de/episoden

Der Netzpolitische Abend ist eine monatliche Veranstaltung mit Vorträgen und Diskussionen, die aufgezeichnet werden und für die gleichnamige Radio Orange Sendung aufbereitet werden.
www.o94.at/programm/sendereihen/der-netzpolitische-abend-at

Futurezone das vom ORF aufgebaute und später vom Kurier übernommene Medium versteht sich als Portal für sämtliche digitalen Themen und hat u.a. mit der Arbeiterkammer Medienkooperationen
www.futurezone.at

FM4 – der Journalist Erich Möchel ist versierter und langjähriger Experte zu Digitalisierungsthemen wie Überwachung, Datenschutz und Verschlüsselung beim ORF-Sender FM4.
www.fm4.orf.at/tags/erichmoechel

Der Online Standard hat eine Redaktion für den Schwerpunkt Web und dort einen Kanal für Netzpolitik:
www.derstandard.at/web/netzpolitik

ÜBERBLICK

ALTERNATIVE BROWSER

Mozilla Firefox
ist ein kostenloser, quelloffener Browser und lässt sich über unzählige Plugins, also Erweiterungen, anpassen und noch sicherer machen (z. B. Werbeblocker, Tracking-Schutz etc.).

Tor = The Onion Router
Bei diesem Browser läuft die Verbindung zu den Webseiten über mehrere Zwischenstationen, die zufällig ausgewählt werden und anonymisiert so das Surfen im Web, da die eigene IP-Adresse durch eine zufällig ausgewählte IP-Adresse aus dem Tor-Netzwerk ersetzt wird und nicht mehr erkennbar ist.

Brave
ist ein kostenloser, quelloffener Browser, der als App auf Smartphones genützt werden kann. Der Werbeblocker ist bereits integriert und unterbindet Tracking-Tools und Cookies.

BROWSER-ERWEITERUNGEN, SOG. ADD-ONS

uBlock Origin
ist eine kostenlos Browser-Erweiterung, deren Quelle öffentlich einsehbar und veränderbar (= „Open-Source“) ist. Blockiert und schützt damit vor ungewollter Werbung.

Privacy Badger
ist eine Browser-Erweiterung, die den/die NutzerIn vor ungewolltem Tracking schützt. Diese Plugin verhindert, dass man beim Surfen im Web websiteübergreifend verfolgt wird. Entwickelt wurde das Add-On von Electronic Frontier Foundation (EFF) einer internationalen NGO für digitale Rechte.

ALTERNATIVE SUCHMASCHINEN

StartPage
gehört zu den datenschutzfreundlichen Suchmaschinen. Die Suchanfragen werden an Google weitergeleitet und gibt deren Ergebnisse anonymisiert zurück. StartPage steht quasi als schützendes Schild zwischen dem/der UserIn und Google. Nach eigenen Angaben werden weder IP-Adressen noch Cookies gespeichert.

DuckDuckGo
betont den Schutz der Privatsphäre der NutzerInnen und speichert zwar die Suchbegriffe, aber nicht die IP-Adresse und setzt auch keine Cookies. DuckDuckGo zeigt allen NutzerInnen dasselbe Ergebnis, personalisiert also nicht.

DATEIEN VERSCHLÜSSELN

VeraCrypt
ist empfohlen zum Verschlüsseln der Daten auf Notebooks und externen Festplatten, VeraCrypt beruht auf quelloffenem Code. Was genau das Programm kann und wie man es installiert, ist beispielsweise hier erklärt: https://www.lehrerfreund.de/schule/1s/anleitung-veracrypt/4807

ALTERNATIVE MESSENGER-DIENSTE

Signal
ist eine sichere und kostenlose Alternative zu SMS, WhatsApp und Telegram. Die App kann Bilder, Dateien, Videos, Gespräche übermitteln und verschlüsselt diese ebenso wie die Metadaten der Kommunikation.

BROSCHÜREN DER GEWERKSCHAFT GPA ZUM THEMA

Die wunderbare Welt von Microsoft
und wie der Betriebsrat sie mitgestalten kann
Wien, Februar 2021, Broschüre der Gewerkschaft GPA

Arbeitswelt 4.1
Aspekte der Digitalisierung
Wien, Juni 2021, Broschüre der Gewerkschaft GPA

Sozial? Digital? Mit Potenzial?
Personalentwicklung aus Sicht des Betriebsrats
Wien, September 2021, Broschüre der Gewerkschaft GPA

Lost in Homeoffice?
Neue Rechtsgrundlage 2021 und aktuelle Gestaltungstipps
Wien, Mai 2021, Broschüre der Gewerkschaft GPA

JETZT MITGLIED WERDEN!

☐ Frau ☐ Herr ☐ Divers ☐.....

Familienname..... Vorname.....

Titel ..... Geburtsdatum

Straße/Haus-Nr. ..... PLZ/Wohnort .....

Telefonisch erreichbar ..... E-Mail .....

☐ Angestellte/r ☐ ArbeiterIn ☐ Lehrling/.....Lj. ☐ SchülerIn ☐ StudentIn
☐ Werkvertrag ☐ Zeitarbeitskraft ☐ Freier Dienstvertrag ☐ Zweitmitgliedschaft ☐ geringfügig beschäftigt

Derzeitige Tätigkeit ..... ☐ Ich war bereits Mitglied der Gewerkschaft von/bis .....

Beschäftigt bei Firma (bzw. Schule/Universität)..... Dienstort .....

Anschrift.....

Branche .....

Höhe des monatlichen Beitrages: **EUR** **BEITRITTSMONAT/-JAHR**

Der monatliche Mitgliedsbeitrag beträgt 1 % des Bruttogehalts bis zu einem Maximalbeitrag (siehe **www.gpa.at/mitgliedsbeitrag**), der jährlich angepasst wird. Der Mitgliedsbeitrag ist steuerlich absetzbar.

☐ Ich willige ein, dass ÖGB, ÖGB Verlag und/oder VÖGB mich telefonisch bzw. per elektronischer Post (§107 TKG) kontaktieren dürfen, um über Serviceleistungen, etwa Aktionen für Tickets, Bücher und Veranstaltungen zu informieren und sonstige Informationen zu übermitteln. Die Einwilligung kann jederzeit widerrufen werden.

Ich bezahle meinen Mitgliedsbeitrag durch: (Zutreffendes bitte ankreuzen)

☐ **BETRIEBSABZUG**

Ich erkläre, dass mein Gewerkschaftsbeitrag durch meinen Arbeitgeber von meinem Gehalt/Lohn/Lehrlingseinkommen abgezogen werden kann. Ich erteile deshalb meine Einwilligung, dass meine im Zusammenhang mit der Beitragseinhebung erforderlichen personenbezogenen Daten (angegebene Daten und Gewerkschaftszugehörigkeit, Beitragsdaten, KV-Zugehörigkeit, Eintritts-/und Austrittsdaten, Karenzzeiten, Präsenz-, Ausbildungs- und Zivildienstzeiten, Pensionierung und Adressänderungen) von meinem Arbeitgeber und von der Gewerkschaft verarbeitet werden dürfen, wobei ich diese Einwilligung zum Betriebsabzug jederzeit widerrufen kann.

☐ **SEPA LASTSCHRIFT-MANDAT** (Bankeinzug)

Ich ermächtige die Gewerkschaft GPA, die Zahlungen meines Mitgliedsbeitrages von meinem Konto mittels SEPA-Lastschrift einzuziehen. Zugleich weise ich mein Kreditinstitut an, die von der Gewerkschaft GPA auf mein Konto gezogene SEPA-Lastschriften einzulösen. Ich kann innerhalb von acht Wochen, beginnend mit dem Belastungsdatum, die Erstattung des belasteten Betrags verlangen. Es gelten dabei die mit meinem Kreditinstitut vereinbarten Bedingungen.

Der Einzug des Mitgliedsbeitrags erfolgt jeweils zum Monatsultimo.

☐ monatlich ☐ alle 2 Monate ☐ jedes Quartal ☐ 1/2 jährlich ☐ jährlich (Schüler-/StudentInnen, Zweitmitgliedschaft)

Wenn ich dem Betriebsabzug zugestimmt habe, diesen aber nicht mehr wünsche oder aus dem Betrieb ausscheide oder der Abzug des Mitgliedsbeitrages über den Betrieb nicht mehr möglich ist, ersuche ich die Zahlungsart ohne Rücksprache auf SEPA-Lastschrift von meinem bekannt gegebenen Konto umzustellen.

IBAN **BIC**

.....

Datum/Unterschrift

Ich bestätige, umseits stehende Datenschutzerklärung (auch abrufbar unter **www.oegb.at/datenschutz**) zur Kenntnis genommen zu haben.

.....

Datum/Unterschrift

1030 Wien, Alfred-Dallinger-Platz 1, Service-Hotline: +43 (0)5 0301,
E-Mail: service@gpa.at, ZVR 576439352, CID: AT48ZZZ00000006541

WerberIn-Mitgliedsnummer:.....

DATENSCHUTZINFORMATION (online unter: www.oegb.at/datenschutz)

Der Schutz Ihrer persönlichen Daten ist uns ein besonderes Anliegen. In dieser Datenschutzinformation informieren wir Sie über die wichtigsten Aspekte der Datenverarbeitung im Rahmen der Mitgliederverwaltung. Eine umfassende Information, wie der Österreichische Gewerkschaftsbund (ÖGB)/die Gewerkschaft GPA mit Ihren personenbezogenen Daten umgeht, finden Sie unter **www.oegb.at/datenschutz**

Verantwortlicher für die Verarbeitung Ihrer Daten ist der Österreichische Gewerkschaftsbund. Wir verarbeiten die umseits von Ihnen angegebenen Daten mit hoher Vertraulichkeit, nur für Zwecke der Mitgliederverwaltung der Gewerkschaft und für die Dauer Ihrer Mitgliedschaft bzw. solange noch Ansprüche aus der Mitgliedschaft bestehen können. Rechtliche Basis der Datenverarbeitung ist Ihre Mitgliedschaft im ÖGB/in der Gewerkschaft GPA; soweit Sie dem Betriebsabzug zugestimmt haben, Ihre Einwilligung zur Verarbeitung der dafür zusätzlich erforderlichen Daten. Die Datenverarbeitung erfolgt durch den ÖGB/die Gewerkschaft GPA selbst oder durch von diesem vertraglich beauftragte und kontrollierte Auftragsverarbeiter. Eine sonstige Weitergabe der Daten an Dritte erfolgt nicht oder nur mit Ihrer ausdrücklichen Zustimmung. Die Datenverarbeitung erfolgt ausschließlich im EU-Inland.

Ihnen stehen gegenüber dem ÖGB/der Gewerkschaft GPA in Bezug auf die Verarbeitung Ihrer personenbezogenen Daten die Rechte auf Auskunft, Berichtigung, Löschung und Einschränkung der Verarbeitung zu.

Gegen eine Ihrer Ansicht nach unzulässige Verarbeitung Ihrer Daten können Sie jederzeit eine Beschwerde an die österreichische Datenschutzbehörde (www.dsb.gv.at) als Aufsichtsstelle erheben.

Sie erreichen uns über folgende Kontaktdaten:

Gewerkschaft GPA
1030 Wien, Alfred-Dallinger-Platz 1
Tel.: +43 (0)5 0301
E-Mail: service@gpa.at

Österreichischer Gewerkschaftsbund
1020 Wien, Johann-Böhm-Platz 1
Tel.: +43 (0)1 534 44-0
E-Mail: oegb@oegb.at

Unseren Datenschutzbeauftragten erreichen Sie unter:
datenschutzbeauftragter@oegb.at

MITMACHEN – MITREDEN – MITBESTIMMEN

INTERESSENGEMEINSCHAFTEN DER GEWERKSCHAFT GPA bringen Menschen mit ähnlichen Berufsmerkmalen zusammen. Zum Austauschen von Erfahrungen und Wissen, zum Diskutieren von Problemen, zum Suchen kompetenter Lösungen, zum Durchsetzen gemeinsamer beruflicher Interessen.

Mit Ihrer persönlichen Eintragung in eine oder mehrere berufliche Interessengemeinschaften

- erhalten Sie mittels Newsletter (elektronisch oder brieflich) regelmäßig Informationen über Anliegen, Aktivitäten und Einladungen für Ihre Berufsgruppe;
- können Sie Ihre beruflichen Interessen auf direktem Weg in die Kollektivvertragsverhandlungen Ihres Branchenbereichs einbringen;
- erschließen Sie sich Mitwirkungsmöglichkeiten an Projekten, Bildungsveranstaltungen, Kampagnen, Internet-Foren und anderen für Ihre Berufsgruppe maßgeschneiderten Veranstaltungen, auch auf regionaler Ebene;
- nehmen Sie von der Interessengemeinschaft entwickelte berufsspezifische Dienstleistungen und Produkte in Anspruch (Fachberatung auf regionaler Ebene, Bücher, Broschüren und andere Materialien);
- beteiligen Sie sich an demokratischen Direktwahlen Ihrer beruflichen Vertretung auf Bundesebene sowie regionaler Ebene und nehmen dadurch Einfluss auf die gewerkschaftliche Meinungsbildung und Entscheidung.

Nähere Infos dazu unter: **www.gpa.at/interesse**

ICH MÖCHTE MICH IN FOLGENDE INTERESSENGEMEINSCHAFTEN EINTRAGEN:

☐ **IG PROFESSIONAL** ☐ **IG FLEX** ☐ **IG SOCIAL** ☐ **IG IT** ☐ **IG EXTERNAL**

Dieses Service ist für mich kostenlos und kann jederzeit von mir widerrufen werden.

☐ Frau ☐ Herr ☐ Divers ☐..... Titel.....

Familienname..... Vorname.....

Straße/Haus-Nr. ..... PLZ/Wohnort.....

Berufsbezeichnung..... Betrieb .....

Telefonisch erreichbar ..... E-Mail.....

.....
Datum/Unterschrift

gpa MEINE GEWERKSCHAFT

GEWERKSCHAFT GPA
IN GANZ ÖSTERREICH

SERVICE-HOTLINE:
+43 (0)5 0301

GEWERKSCHAFT GPA
Service-Center
1030 Wien, Alfred-Dallinger-Platz 1
Tel.: +43 (0)5 0301
Fax: +43 (0)5 0301-300
E-Mail: service@gpa.at

GPA Wien
1030 Wien, Alfred-Dallinger-Platz 1

GPA Niederösterreich
3100 St. Pölten, Gewerkschaftsplatz 1

GPA Burgenland
7000 Eisenstadt, Wiener Straße 7

GPA Steiermark
8020 Graz, Karl-Morre-Straße 32

GPA Kärnten
9020 Klagenfurt, Bahnhofstraße 44/4

GPA Oberösterreich
4020 Linz, Volksgartenstraße 40

GPA Salzburg
5020 Salzburg,
Markus-Sittikus-Straße 10

GPA Tirol
6020 Innsbruck,
Südtiroler Platz 14

GPA Vorarlberg
6900 Bregenz, Reutegasse 11

www.gpa.at

GUTE ARBEIT!

mitgliedwerden.gpa.at

gpa
MEINE GEWERKSCHAFT