Bundesministerium
Inneres

Bundesamt für Verfassungsschutz
und Terrorismusbekämpfung

Internet, Social Media und Big Data

Handlungsempfehlungen für die private Internetnutzung von Mitarbeiterinnen und Mitarbeitern

Impressum

Medieninhaber, Verleger und Herausgeber:
Bundesministerium für Inneres
Bundesamt für Verfassungsschutz und Terrorismusbekämpfung
Herrengasse 7, 1010 Wien
bvt.gv.at
Autor: Cyber Security Center - Bereich Prävention
Druck: Digitalprintcenter des BMI

Überarbeitete Neuauflage
Wien, Juli 2020

Rückmeldungen: Ihre Überlegungen zu vorliegender Publikation übermitteln Sie bitte an csc@bvt.gv.at.

Cyber Security .BVT
Dieses Projekt wird durch den Fonds für die Innere Sicherheit kofinanziert.

Vorwort

Philipp Blauensteiner

Das Internet beherrscht in zunehmendem Maße alle Lebensbereiche, gleich ob in einem dienstlichen oder privaten Kontext. Mitarbeiterinnen und Mitarbeiter in verschiedenen Organisationen, Unternehmen oder Behörden haben dabei neben ihrer dienstlichen Identität zur gleichen Zeit auch eine private Identität.

Obwohl eine unserer zentralen Empfehlungen dahingeht, dienstliche und private Aktivitäten stets strikt zu trennen, ist es nachvollziehbar, dass es durch das Nebeneinander dieser beiden Identitäten immer wieder zu gewissen Überschneidungen kommen kann. Genauso wie dienstliche Themen ins Privatleben überschwappen können, können auch private Aktivitäten Einflüsse auf dienstliche Interessen haben.

Die vorliegende Ausgabe der CSC-Schriftenreihe soll diesem Umstand gerecht werden. Die Zielsetzung ist, den Mitarbeiterinnen und Mitarbeitern Grundlagen zu vermitteln und eine Reihe von Handlungsempfehlungen an die Hand zu geben, um sich verantwortungsbewusst und sicher durch das Internet im Allgemeinen und durch soziale Medien im Speziellen zu bewegen. Das vorliegende Dokument wird durch Informationen und Handlungsempfehlungen zu dem medial omnipräsenten Thema Big Data abgerundet.

Einige Themen finden dabei in mehreren Abschnitten Erwähnung. Dies ist beabsichtigt und soll die Möglichkeit bieten, die jeweiligen Überlegungen aus mehreren Blickwinkeln zu betrachten.

Philipp Blauensteiner
Leiter des Cyber Security Centers

Inhalt

1 Internet

1.1 Was ist das Internet?

> "The Internet is becoming the town square for the global village of tomorrow." (Bill Gates)

Wenn mehrere Personen über „das Internet" sprechen, kann es leicht sein, dass sie völlig unterschiedliche Vorstellungen darüber haben, worum genau es eigentlich geht. Im tagtäglichen Sprachgebrauch werden in diesem Zusammenhang oftmals verschiedene Begriffe vermischt, am häufigsten wohl Internet und World Wide Web.

Internet

Das Internet ist eine Infrastruktur. Das Internet ist ein weltumspannender Zusammenschluss vieler einzelner Computernetzwerke. Es ist gleichsam die physische Basis, auf der alle jene Internet-Dienste aufbauen, die wir kennen und nutzen (z. B. World Wide Web, E-Mail).

World Wide Web

Das World Wide Web ist ein Dienst. Das World Wide Web erlaubt es seinen Nutzerinnen und Nutzern, den Inhalt von Websites aufzurufen und auf ihren jeweiligen Rechnern anzuzeigen. Das Programm, das zur Nutzung dieses Dienstes benötigt wird, ist der Browser (z. B. Mozilla Firefox, Google Chrome).

Das World Wide Web (WWW) wiederum gliedert sich in mehrere Bereiche.

- **Visible Web/Clear Web**: Das sogenannte Visible Web/Clear Web ist jener (kleine) Teil des World Wide Web, der indiziert, d. h. über Suchmaschinen auffindbar, ist. Er ist für jedermann leicht nutzbar und beinhaltet unter anderem alle öffentlichen Webangebote.
- **Deep Web**: Das sogenannte Deep Web ist der weitaus größte Teil des World Wide Web (je nach Quelle bis zu 90% des WWW). Es beinhaltet alle Webangebote, die nur einem eingeschränkten Personenkreis zur Verfügung stehen. Dies umfasst unter

anderem Bereiche mit unternehmensinternen Daten, sowie kostenpflichtige Webangebote (z. B. Streamingdienste), private Foren oder personenbezogene Dienste (z. B. Online-Speicher). Die Inhalte des Deep Web sind nicht indiziert und können daher über Suchmaschinen nicht gefunden werden.

- **Darknet**: Das sogenannte Darknet ist derjenige, von Medien teilweise stark mystifizierte Teil des World Wide Web, der nur unter Verwendung bestimmter Technologien bzw. Werkzeuge (z. B. TOR) erreichbar ist. Beim Darknet handelt es sich nicht per se um etwas „Böses“ oder Verbotenes. Es gibt viele vollkommen legitime Anwendungsszenarien, die die Nutzung des Darknets rechtfertigen. Aufgrund der technischen Möglichkeiten zur Verschleierung der eigenen Identität, haben sich im Darknet jedoch auch viele grenzwertige und kriminelle Angebote angesiedelt.

1.2 Grundsätze

Um das Internet und seine Dienste optimal nutzen zu können, muss großes Augenmerk auf das eigene Verhalten gelegt werden. Begriffe wie Sicherheit, Datenschutz, Privatsphäre oder Netiquette dürfen keine leeren Phrasen sein, sondern müssen tagtäglich gelebt werden. Ein Abweichen von den entsprechenden Regeln und Empfehlungen gereicht Nutzerinnen und Nutzern auf die eine oder andere Art immer zum Nachteil.

Die folgenden Überlegungen befassen sich mit ganz allgemein gehaltenen Grundsätzen und Leitlinien für die Nutzung des Internets. In den folgenden Abschnitten wird dann auf einige spezielle Themen noch detaillierter eingegangen. Dieser Abschnitt dient hingegen primär als Überblick.

Verhalten Sie sich im Internet stets so, wie Sie sich auch im realen Leben verhalten würden.

Das Internet verleitet viele Nutzerinnen und Nutzer, vor allem aufgrund seiner vermeintlichen Anonymität, zu einem von diesem Grundsatz abweichenden Verhalten. Im Folgenden sind einige plakative Beispiele zusammengestellt:

- Würden Sie in der realen Welt private Details aus Ihrem Leben einer riesigen Menschenmenge verraten?

- Würden Sie in der realen Welt Details Ihrer beruflichen Tätigkeit oder vertrauliche Informationen über Ihren Dienstgeber veröffentlichen?
- Würden Sie in der realen Welt bei einer Meinungsverschiedenheit sofort aggressives oder beleidigendes Verhalten zeigen?
- Würden Sie in der realen Welt Ihre Kreditkartendaten jedem beliebigen Unbekannten zur Verfügung stellen?

Machen Sie sich den Wert Ihrer persönlichen Daten bewusst und schützen Sie diese entsprechend.

Ihre persönlichen Daten stellen einen erheblichen Wert dar, nicht nur ideell, sondern auch monetär. Auch im Internet gibt es nichts umsonst. Jeder Dienst, der kostenlos angeboten wird, finanziert sich durch alternative Quellen. In der Mehrzahl der Fälle erfolgt dies durch Werbung oder durch die Nutzung und/oder den Weiterverkauf Ihrer persönlichen Daten.

Es ist technisch möglich, dass im Hintergrund Daten aus mehreren verschiedenen Quellen (z. B. Nutzung von Suchmaschinen, Besuch von Websites, Verwendung von Kundenkarten, Selbstdarstellung in sozialen Medien, Verwendung von Sprachassistenten und digitalen Fitnessgeräten) aufgezeichnet, gesammelt und miteinander verknüpft werden. So bildet sich mit der Zeit ein hochdetailliertes Abbild jedes einzelnen Benutzers. Diese Informationen können leicht auch zu Ihrem Nachteil verwendet werden.

Trennen Sie stets dienstliche und private Aktivitäten im Internet.

Wie einleitend dargestellt, haben Mitarbeiterinnen und Mitarbeiter neben einer privaten Identität zur gleichen Zeit auch eine dienstliche Identität. Überschneidungen und gegenseitige Beeinflussungen dieser zwei Lebensbereiche sollten so weit wie möglich vermieden werden. Insbesondere sollte das Folgende beachtet werden:

- Verwenden Sie niemals Ihre dienstliche E-Mail-Adresse, um sich privat für einen Dienst im Internet zu registrieren.
- Verwenden Sie Kennwörter für dienstliche Accounts niemals auch für private Accounts.

Ein zentraler Bestandteil der Nutzung von Berufsplattformen wie „XING“ oder „LinkedIn“ ist es, dort die eigenen Qualifikationen, Erfahrungen, Leistungen und Alleinstellungsmerkmale bestmöglich darzustellen. Dabei darf nie vergessen werden, dass durch entsprechende Angaben Interessen des eigenen Unternehmens verletzt werden können. Wird beispielsweise angegeben, dass man hohe Kompetenz im Bereich einer bestimmten Hard- oder Software hat, kann daraus geschlossen werden, dass genau diese Hard- oder Software im jeweiligen Unternehmen eingesetzt wird.

In diesem Zusammenhang ist es daher auch wichtig, diesbezügliche interne Richtlinien oder im Arbeitsvertrag festgehaltene Regelungen unbedingt einzuhalten. Wägen Sie daher Ihren Wunsch nach Selbstdarstellung im Internet und etwaige Sicherheitsinteressen Ihres Arbeitgebers gewissenhaft gegeneinander ab.

Vergessen Sie nie, dass das Internet kein rechtsfreier Raum ist und beachten Sie stets entsprechende Gesetze und Vorschriften.

In einigen Bereichen des Internets hat sich bei vielen Menschen im Lauf der Zeit ein allzu sorgloser Umgang mit Recht und Gesetz entwickelt. Insbesondere, aber keineswegs ausschließlich im Zusammenhang mit dem Urheberrecht, fehlt vielen Menschen jegliches Unrechtsbewusstsein bei Verstößen gegen geltendes Recht.

Grund für dieses Verhalten ist die vermeintliche Anonymität im Netz. Dies ist allerdings ein Trugschluss. Jede Aktivität im Internet hinterlässt mehr oder weniger eindeutige Spuren. In den meisten Fällen ist es möglich, die Identität des Nutzers oder der Nutzerin zu ermitteln.

1.3 Empfehlungen zum Verhalten

Regelungen für das persönliche Verhalten von Individuen im Internet lassen sich unter dem Begriff Netiquette zusammenfassen. Der Begriff setzt sich aus den Worten "Net" (Internet) und "Etiquette" (Benehmen) zusammen.

Netiquette hat per se keine Rechtskraft. Es gibt keine Gesetze, die Menschen zur Einhaltung von Netiquette verpflichten. Vielmehr handelt es sich dabei um eine lose Zusammenstellung von Verhaltensregeln und -empfehlungen, die den Umgang zwischen Nutzerinnen und Nutzern des Internets fair und angenehm für alle gestalten sollen.

Es muss allerdings beachtet werden, dass viele Anbieter von Diensten im Internet die Einhaltung einer von ihnen in Art und Umfang definierten Netiquette als Geschäftsbedingung definieren und ein Zuwiderhandeln zu privatrechtlichen Implikationen (z. B. dem Ausschluss vom jeweiligen Angebot) führen kann.

Gängige Empfehlungen, vor allem im Zusammenhang mit Kommunikation in sozialen Medien, Foren oder Chatrooms, sind unter anderem:

- Es ist stets ein respektvoller und angemessener Umgang mit dem jeweiligen Gegenüber einzuhalten. Unhöflichkeiten, Beleidigungen und Beschimpfungen sind jedenfalls zu vermeiden.
- Gängige Konventionen sollen stets berücksichtigt werden. So gilt beispielsweise das fortgesetzte Schreiben in fetter Schrift oder in Großbuchstaben als unhöfliches Schreien und sollte daher vermieden werden.
- Vertrauliche Informationen oder Informationen, die eine andere Person bloßstellen könnten, dürfen nicht geteilt werden.
- Extreme oder extremistische Äußerungen (z. B. rassistischer Natur) sind zu unterlassen. In solchen Fällen kann leicht auch die Grenze zu strafrechtlichem Verhalten (z. B. Verhetzung) überschritten werden.
- Geltendes Recht des eigenen, aber auch des Landes des Anbieters des Dienstes ist unbedingt einzuhalten.

2 Social Media

> "Don't say anything online that you wouldn't want plastered on a billboard with your face on it." (Erin Bury)

Soziale Medien können grob als die Summe von Diensten des Internets definiert werden, die das Erstellen und Teilen von durch Nutzerinnen und Nutzern selbst erstellten Daten ermöglichen. Charakteristisch an sozialen Medien ist damit, dass sich eine zuvor im Wesentlichen unidirektionale Kommunikation zu Interaktion wandelt. Die Informationen, die in sozialen Medien geteilt werden, werden von den Nutzerinnen und Nutzern selbst erstellt und veröffentlicht.

Eine zentrale Voraussetzung für eine Teilnahme an sozialen Medien ist in der Regel die Bereitschaft, persönliche Daten einer eingeschränkten oder auch uneingeschränkten Öffentlichkeit preiszugeben. Wie der Erfolg und die Verbreitung von sozialen Medien deutlich zeigen, ist diese Bereitschaft in großem Umfang vorhanden. Oft bleibt dabei das Bewusstsein um den Wert persönlicher Daten und der Privatsphäre auf der Strecke. Private Informationen von einzelnen Individuen waren noch nie leichter und in größerem Umfang allgemein verfügbar als heute.

2.1 Grundsätze

Die folgenden Überlegungen befassen sich mit ganz allgemein gehaltenen Grundsätzen und Leitlinien für die Nutzung von sozialen Medien.

Veröffentlichen Sie nichts, das Sie nicht auch in der realen Welt persönlich vertreten würden.

Die vermeintliche Anonymität verleitet in bestimmten Situationen dazu, Kommentare abzugeben, zu denen man sich in der realen Welt nicht bekennen würde. Wenn man der Meinung ist, dass für einen bestimmten Kommentar Anonymität unbedingt erforderlich sei, sollte in der Regel auf eine Veröffentlichung verzichtet werden.

Doppelt hält besser. Überlegen Sie vor dem Verfassen eines Kommentars, ob Sie diesen tatsächlich veröffentlichen möchten und überlegen Sie vor dem Absenden des Kommentars, ob Sie diesen tatsächlich so absenden wollen.

Vergessen Sie niemals, dass das Internet niemals vergisst.

Auch wenn da und dort die allgemeinen Geschäftsbedingungen mancher Diensteanbieter den Nutzerinnen und Nutzern anderes versprechen, ist es in der Realität doch so, dass eine Information, die einmal im Internet geteilt wurde, dort wohl für alle Zeiten verfügbar und abrufbar sein wird.

Es ist daher von ganz zentraler Bedeutung, dass sich Nutzerinnen und Nutzer bei jeder Information, die sie teilen möchten, vor einer Veröffentlichung genau überlegen, ob sie wollen, dass diese Information heute, aber auch in vielen Jahren für jedermann verfügbar sein soll.

2.2 Überlegungen zur Privatsphäre

Datenschutz und die Nutzung sozialer Medien sind nahezu ein Widerspruch in sich. Der Erfolg von sozialen Medien begründet sich zu einem guten Teil dadurch, dass er Menschen die Möglichkeit der Selbstdarstellung bietet. Entscheidet man sich trotzdem zur Nutzung einer Plattform, sollten folgende Punkte beachtet werden:

- **Allgemeine Geschäftsbedingungen und Datenschutzerklärung**: Es erscheint sinnvoll, vor dem Anlegen eines Accounts sowohl die allgemeinen Geschäftsbedingungen (AGB) des jeweiligen Anbieters, als auch dessen Datenschutzerklärung zumindest überblicksartig durchzugehen. Sie geben, wenn auch mitunter nicht ganz leicht auffindbar, Hinweise darauf, was mit den von Ihnen geteilten Informationen geschieht, wer diese erhält und welche Rechte zum Schutz dieser Daten Sie haben.
- **Benutzername**: Es ist sinnvoll, für jedes genutzte soziale Netzwerk eine andere E-Mail-Adresse als Benutzername zu verwenden. Abgesehen von generellen Sicherheitsüberlegungen, erschweren Sie dadurch eine Verknüpfung Ihrer Daten über Plattformgrenzen hinweg.
- **Pseudonym**: Überlegen Sie bereits im Vorfeld, zu welchem Zweck Sie das soziale Netz nutzen möchten und ob für diesen Anwendungszweck die Bekanntgabe Ihres

Klarnamens erforderlich ist. Ist dies nicht der Fall, empfiehlt sich die Nutzung eines Pseudonyms. Die Verwendung von Pseudonymen im Internet stellt grundsätzlich eine legitime Vorgangsweise dar. Beachten Sie aber, dass manche Anbieter in ihren AGB die Verwendung von Klarnamen explizit verlangen und Sie widrigenfalls gegen eben diese AGB verstoßen.

- **Privatsphäreneinstellungen**: Lernen Sie die Möglichkeiten der Privatsphäreneinstellungen kennen und nutzen Sie diese auch. Überlegen Sie, wer Ihre Texte und Ihre Bilder sehen soll und wer nicht. Überlegen Sie insbesondere, ob Sie die verbreitete Option „Freunde von Freunden" wirklich nutzen wollen. Bedenken Sie dabei, dass in diesem Fall Menschen Ihre Daten einsehen können, die Sie nicht kennen und zu denen Sie keinerlei Bezug haben (bei einer angenommenen Anzahl von 200 Freunden pro Nutzer, geben Sie mit dieser Option Ihre Daten für mehr als 40.000 Menschen frei).
- **Öffentlichkeit von Daten**: Betrachten Sie jedoch im Zweifelsfall alle einem sozialen Netzwerk zur Verfügung gestellten Daten – und zwar unabhängig von den von Ihnen getroffenen Einstellungen – als potentiell veröffentlicht. In der Vergangenheit ist es mehrfach vorgekommen, dass durch die Restrukturierung von Privatsphären-einstellungen, durch Datenleaks oder auch durch unautorisierte Weitergabe von Daten an (Werbe-)Partner die von Ihnen festgelegten Einstellungen zur Privatsphäre obsolet wurden.
- **Suchmaschinen**: Viele Plattformen bieten die Möglichkeit, die eigenen Inhalte nicht von Suchmaschinen erfassen zu lassen. Diese Option bietet den Vorteil, dass Daten zu Ihrer Person (in der jeweiligen Plattform) nicht über externe Suchmaschinen gefunden werden können.

2.3 Persönliche Informationen

Ist man sich darüber im Klaren, aus welchem Grund und zu welchem Zweck man eine Platt-form nutzen möchte, kann man von Fall zu Fall entscheiden, ob die Veröffentlichung von bestimmten Daten sinnvoll und notwendig ist. Beachten Sie dabei jedoch immer folgende Punkte:

- **Blick in die Zukunft**: Fragen Sie sich vorab, ob Sie wirklich wollen, dass die Allgemeinheit bzw. der festgelegte Empfängerkreis die jeweiligen Informationen erhält und überlegen Sie vor allem, ob Sie das auch in Zukunft noch wollen. Einmal im Netz ist die Information in der Praxis nicht mehr aus dem Netz zu entfernen.

- **Rechte Dritter**: Stellen Sie des Weiteren vorab sicher, dass Sie mit der Veröffentlichung weder implizit noch explizit Rechte Dritter verletzen. Insbesondere im Zusammenhang mit Bildern ist zu bedenken, dass nicht jedes selbst gemachte Bild automatisch frei von Rechten Dritter (z. B. abgebildete Dritte) ist. Fragen Sie zur Sicherheit bei den Betroffenen nach, ob Sie ein Bild veröffentlichen dürfen, dass diese zeigt.
- **Interessen Dritter**: Stellen Sie vorab sicher, dass Sie mit der Veröffentlichung weder implizit noch explizit legitime Interessen Dritter verletzen (z. B. interne Informationen über den Arbeitgeber).
- **Schutz vor Kriminellen**: Bedenken Sie stets, dass Informationen, die Sie während einer oder über eine Abwesenheit (z. B. Urlaubsreise) teilen, unter Umständen auch von Kriminellen gelesen werden können. Einbrecherbanden recherchieren vor einer etwaigen Tat vermehrt in sozialen Medien, ob und wie lange ein Haus oder eine Wohnung leer steht.
- **Recruiting**: Es ist heute gängige Praxis, dass Recruiter im Zuge eines beruflichen Aufnahmeverfahrens die Profilseiten der Kandidaten in ihre Bewertungen miteinbeziehen. Erscheinen Kommentare oder Bilder (z. B. Alkoholkonsum) nicht opportun, kann das ein Ausscheiden Ihrer Bewerbung bedeuten, ohne dass Ihnen der Grund dafür je bewusst sein wird.
- **Nennung des Arbeitgebers**: Falls Ihr Profil Inhalte zeigt, die den Interessen oder Werten Ihres Arbeitsgebers zuwiderlaufen könnten (z. B. Alkoholkonsum, aufreizende Bilder) und Sie diese aus welchen Gründen immer, trotzdem veröffentlichen wollen, erscheint es empfehlenswert, zumindest auf die Nennung des Arbeitgebers in Ihrem Profil zu verzichten.

2.4 Empfehlungen zum Verhalten

Abschließend sind noch einige zusätzliche Empfehlungen, insbesondere zum richtigen Umgang mit Freunden bzw. Followern und zum Verhalten in möglichen Konfliktsituationen zusammengefasst.

Freunde und Follower

Es ist nicht empfehlenswert, Freundschaftsanfragen (oder Ähnliches) von Personen anzunehmen, die Ihnen nicht persönlich bekannt sind. Wird ein Nutzer oder eine Nutzerin in die

eigene Freundes- oder Follower-Liste aufgenommen, gelten für diese Person (je nach getroffenen Einstellungen) erweiterte Zugriffsrechte auf Ihre Daten.

Auch ist große Vorsicht geboten, wenn Bekanntschaften aus sozialen Medien Sie um Geld oder Gefälligkeiten ersuchen.

Konfliktsituationen

Ergeben sich im Zuge der Nutzung von sozialen Medien Konfliktsituationen, so sollte diesen so umsichtig wie möglich begegnet werden. Dabei ist zu bedenken, dass eine schriftliche Auseinandersetzung (insbesondere, wenn sie spontan und ohne Pause zur Selbstreflexion geführt wird) in aller Regel den Konflikt eher verstärkt, als dass sie eine Lösung herbeiführt. Lassen Sie sich keinesfalls zu Beleidigungen oder Beschimpfungen des Gegenübers hinreißen, auch wenn Sie sich im Recht fühlen.

Insbesondere in Foren existieren darüber hinaus Menschen, deren Ziel es ist, durch Provokation Aufmerksamkeit zu erlangen. Glauben Sie, ein solches Verhalten zu erkennen, gilt der Grundsatz „Don't feed the troll". Reagiert man auf deren Provokationen, haben diese Menschen ihr Ziel erreicht. Ignoriert man sie hingegen, hat man gute Chancen, dass die Provokation von selbst aufhört.

3 Big Data

> “If you are not paying for it, you're not the customer; you're the product being sold.” (blue_beetle)

Dieses Zitat zirkuliert seit Jahren in immer wieder abgewandelter Form im Internet. Basierend auf den Nachforschungen der Website „Quote Investor“ wurde es erstmals am 26. August 2010 in einem Kommentar auf der Website „MetaFilter“ veröffentlicht. Es beschreibt pointiert die Tatsache, dass es auch im Internet nichts umsonst gibt. Wird ein Dienst kostenlos angeboten, bezahlt der vermeintliche Kunde die Dienstleistung mit der bewussten oder unbewussten Zurverfügungstellung von persönlichen Daten. Das Sammeln, Speichern und Auswerten dieser Daten ist ein wesentlicher Teilaspekt von Big Data.

3.1 Big Data und Konsequenzen

Big Data ist als Schlagwort in den Medien omnipräsent. Wie auch bei vielen anderen populären Begriffen, ist die Bandbreite von Themen, die diesem Begriff zugeordnet werden, vergleichsweise groß. Im engeren Sinn beschreibt der Begriff lediglich ganz allgemein all jene Datenbestände, die zu groß sind, um manuell bearbeitet werden zu können. Im Lauf der Zeit hat sich, vor allem durch die Berichterstattung von Massenmedien, um diesen Begriff jedoch eine ganze Reihe von Themen angesiedelt.

Der gläserne Mensch

Dabei steht zumeist das Konzept des sogenannten gläsernen Menschen im Zentrum der Überlegungen. Demzufolge generiert der moderne Mensch permanent Daten, sei es beispielsweise durch die Nutzung von Suchmaschinen, die Verwendung von Kundenkarten, die Selbstdarstellung in sozialen Medien, den Besuch von Websites oder die Verwendung von Sprachassistenten und digitalen Fitnessgeräten. Werden diese Daten im Hintergrund aufgezeichnet, gesammelt und miteinander verknüpft, so bildet sich mit der Zeit ein hochdetailliertes Abbild jedes und jeder Einzelnen, dessen Aufbau, Pflege und Weiterverkauf an Dritte ein hochprofitabler Wirtschaftszweig geworden ist.

Die Website der Initiative „Klicksafe“ der Europäischen Union[1] beschreibt die sich daraus ergebenden Konsequenzen wie folgt:

> „Menschen werden also aufgrund ihrer durch Big Data vorhergesagten Neigungen beurteilt – und nicht aufgrund ihres tatsächlichen Verhaltens. […] Die Verhaltensvorhersagen durch Big Data gefährden also insbesondere unsere Handlungs- und Entscheidungsfreiheit als Subjekt. Darüber hinaus ist es problematisch, dass aus unseren Datenspuren und Dateneingaben ein digitales Ich geformt wird, dessen genaue Gestalt wir selbst gar nicht kennen können. Dieses „Digitale Double“ ist mit unserer eigenen Person nicht identisch – aber es ist das, was Wirtschaftsunternehmen und Sicherheitsbehörden von uns kennen.“

Vom Wissen und Handeln

In der einschlägigen Fachliteratur zum Thema Datenschutz wird oft vom sogenannten „Privacy Paradoxon“ gesprochen. Dieser Begriff beschreibt das zwiespältige Verhalten vieler Menschen in Bezug auf den Schutz ihrer persönlichen Daten.

Einerseits ist bei vielen Bürgerinnen und Bürgern eine stark ausgeprägte Sensibilität im Bereich des Datenschutzes vorhanden, solange es sich um tendenziell abstrakte Betrachtungen oder um geografisch weit entfernte Anwendungen handelt. So führte beispielsweise die Einführung des obligatorischen Anfertigens von Fotos bei der Einreise in die USA zu enormer medialer Aufmerksamkeit und weltweiter Empörung, die bis zu Boykottaufrufen gegen die USA reichte. Die Tatsache, dass jeder und jede Reisende bei der Immigration fotografiert wird, löste bei sehr vielen Menschen massive Datenschutzbedenken aus. Das Wissen um Datenschutz und der Wunsch nach Schutz der Privatsphäre ist also in weiten Teilen der Bevölkerung durchaus vorhanden.

Auf der anderen Seite haben aber weite Teile der Bevölkerung – möglicherweise auch genau diejenigen, bei denen im oben angeführten Beispiel das Herstellen eines einzigen Fotos zu größten Bedenken geführt hat – überhaupt kein Problem damit, tagtäglich ihr intimstes Privatleben in Bild und Ton auf sozialen Medien einer Weltöffentlichkeit darzulegen oder durch die permanente Nutzung von Pulsuhren und Schrittzählern Gesundheitsdaten mit

[1] https://www.klicksafe.de/themen/medienethik/privatsphaere-und-big-data/kontrolle-ueber-die-eigene-identitaet/

den jeweiligen Herstellern und dahinterliegenden unbekannten Dritten zu teilen. Das bedeutet letztlich, dass in weiten Teilen der Bevölkerung zwar das Wissen um die Bedeutung von Datenschutz vorhanden ist, dies jedoch in vielen Fällen nicht zu einem reflektierten Umgang mit den eigenen Daten führt.

3.2 Technische Grundlagen

Im Folgenden soll der Teilaspekt von Big Data betrachtet werden, der sich mit dem Sammeln, Speichern und Auswerten von Daten bei der Nutzung von Diensten des Internets beschäftigt.

Datenspeicherung beim Websurfing

Jeder Aufruf einer Website im Internet führt zur Speicherung einer Reihe von Daten:

- Name und IP-Adresse des zugreifenden Geräts
- Betriebssystemname und -version
- Browsername und -version, sowie etwaige installierte Plug-ins
- URL der aufgerufenen Website
- URL der zuletzt aufgerufenen Website (Referrer)
- Zeitstempel

Diese Daten werden aufgezeichnet und können entsprechend der Datenschutzbestimmungen des Betreibers verwendet werden. Es besteht im Normalfall keine Möglichkeit, diese Datenspeicherung zu unterbinden.

Cookies

Cookies tauchen in der medialen Berichterstattung regelmäßig auf und werden dabei oft in stark mystifizierter und reißerischer Art und Weise dargestellt. Bei Cookies handelt es sich allerdings keineswegs um etwas per se „Böses“, sie sind vielmehr für eine effiziente Nutzung des Internets unerlässlich. Allerdings können Cookies selbstverständlich auch für fragwürdige Praktiken missbraucht werden, was leider auch passiert. Cookies sind allerdings keine lauffähigen Programme und können daher auch keine Schadsoftware im herkömmlichen Sinn beinhalten.

Cookies sind, wenn sie in legitimer Art und Weise verwendet werden, wichtige Hilfsmittel für eine komfortable Nutzung des World Wide Web. Die Darstellung einer beliebigen Website im Browser ist mitunter von bestimmten Nutzerdaten (beispielsweise Standort und Spracheinstellung des aufrufenden Geräts, persönliche Seiteneinstellungen) abhängig. Diese werden in der Regel beim ersten Besuch der Seite abgefragt und dann in Cookies gespeichert. Wird die Seite zu einem späteren Zeitpunkt neuerlich besucht, werden beim Aufruf der Seite die Informationen aus dem Cookie ausgelesen und die Website präsentiert sich sofort in der gewünschten Art und Weise.

Cookies können wie einleitend beschrieben jedoch auch für mitunter fragwürdige Zwecke missbraucht werden. So ist es beispielsweise möglich, das Surfverhalten eines Nutzers oder einer Nutzerin durch Auswertung von vorhandenen Cookies einzusehen.

- **Unbedingt erforderliche Cookies**: Diese Cookies werden für die ordnungsgemäße Funktion der Website benötigt (z. B. für die Darstellung des Warenkorbs beim Online-Shopping)
- **Funktionale Cookies**: Dabei handelt es sich um die oben erwähnten funktionalen Elemente, wie Standort oder Sprachauswahl.
- **Performance Cookies**: In solchen Cookies werden Informationen zum Nutzerverhalten (z. B. Aufruf von Unterseiten, Suchbegriffe, die zum Besuch der Seite geführt haben, Ladezeiten) gespeichert.
- **Werbecookies**: Diese Cookies speichern Nutzerinformationen, die zum Erstellen personalisierter Werbung genutzt werden.

Die „E-Privacy-Richtlinie“ der Europäischen Union verpflichtet die Betreiber von Websites, eine Einverständniserklärung zur Nutzung von Cookies einzuholen. Dies macht sich bei den meisten Websites durch das Erscheinen eines entsprechenden Anfragefensters beim ersten Besuch einer Website bemerkbar. Hier ist Vorsicht angebracht: Mit dem offensichtlichen Zustimmen-Button stimmt man der Nutzung aller Arten von Cookies zu. Möchte man hier differenzieren, muss man meist in einen Unterbereich des Abfragefensters einsteigen, wo die oben dargestellten Cookie-Typen einzeln freigegeben oder blockiert werden können.

3.3 Digitale Selbstverteidigung

Ein interessantes Konzept, die Hoheit über die eigenen Daten zu behalten oder wiederzuerlangen, ist die digitale Selbstverteidigung. Der Begriff beinhaltet alle Maßnahmen und

Handlungen, die Nutzerinnen und Nutzer des Internets setzen können, um die Menge an persönlichen Daten im Internet so klein wie möglich zu halten.

Grundlage für eine erfolgreiche Anwendung von digitaler Selbstverteidigung ist jedoch, sich unter anderem mit folgenden Fragen auseinanderzusetzen:

- Warum sind meine persönlichen Daten überhaupt schützenswert?
- Wie, wo und durch wen werden persönliche Daten gesammelt?
- Zu welchem Zweck werden meine persönlichen Daten genutzt?
- Wer aller erhält die von mir gesammelten persönlichen Daten?
- Was sind mögliche Konsequenzen einer missbräuchlichen Nutzung?

Ist ein Bewusstsein zu diesen Fragen geschaffen, können Nutzerinnen und Nutzer gezielt Maßnahmen setzen. Es ist empfehlenswert, dem Umgang mit persönlichen Daten größtes Augenmerk zu schenken.

Die folgenden Handlungsempfehlungen sollen dabei helfen, die Menge an digitalen Spuren bei der Nutzung von Diensten im Internet so klein wie möglich zu halten.

Rechtliches

Am Anfang jeglicher Nutzung von Diensten im Internet sollte eine zumindest überblicksartige Auseinandersetzung mit den rechtlichen Rahmenbedingungen der jeweiligen Nutzung stehen.

- Beachten Sie bei der Nutzung von Diensten im Internet stets die allgemeinen Geschäftsbedingungen (AGB) des Anbieters und vor allem dessen Datenschutzerklärung.
- Nehmen Sie sich für den Anmeldevorgang ausreichend Zeit und übergehen Sie Rechtstexte nicht einfach ungelesen. Schon ein einzelnes übersehenes Häkchen kann Ihre rechtliche Position in Bezug auf Widerrufsrechte oder den Datenschutz massiv beeinträchtigen.
- Widersprechen Sie, wo immer möglich, der Nutzung Ihrer Daten zu Marketing- und Werbezwecken bzw. der Weitergabe Ihrer Daten an Dritte.

Cookies

Cookies befinden sich in einem Spannungsfeld zwischen Komfort und Datenschutz. Ein rigoroses Vorgehen hat einen positiven Einfluss auf den Datenschutz, schränkt jedoch die Funktionalität vieler Dienste teils erheblich ein.

- Der erste Schritt zum richtigen Umgang mit Cookies ist ein Verständnis für deren Funktion (vgl. technische Grundlagen).
- Können und wollen Sie auf einen Teil der Funktionalität von Diensten im Internet verzichten, können Sie die Nutzung von Cookies im Browser vollständig deaktivieren. Geht Ihnen diese Einschränkung zu weit, können Sie nur die Cookies von Drittanbietern (oder Werbeanbietern) im Browser deaktivieren. Diese haben in der Regel keinen Einfluss auf die Funktionalität.
- Behalten Sie einen Überblick darüber, welche Cookies auf Ihrem Rechner gespeichert sind. Sie können sich alle gespeicherten Cookies in Ihrem Browser anzeigen lassen. Ihr Browser bietet im Regelfall auch die Möglichkeit, vor dem Setzen jedes einzelnen Cookies Ihre Erlaubnis einzuholen. Dies kann eventuell zu einigem zusätzlichen Aufwand führen, gibt Ihnen aber immer einen vollständigen Überblick, was auf Ihrem Rechner geschieht.
- Löschen Sie Cookies, die Sie nicht benötigen oder nicht wünschen. Im Ihrem Browser besteht die Möglichkeit, einzelne oder alle Cookies wieder zu entfernen.

Beachten Sie aber, dass in modernen Browsern Cookies nur eine Möglichkeit unter vielen sind, Daten lokal zu speichern und sie zu identifizieren. Weitaus mehr Sicherheit als das Löschen bzw. Blockieren von Cookies, bietet die Verwendung des anonymen Modus Ihres Browsers (siehe unten).

Nutzung von Suchmaschinen

Viele bekannte Suchmaschinen speichern jeden von Ihnen eingegebenen Suchbegriff und nutzen diese Informationen, um Ihr hinterlegtes Profil aufzubauen und zu ergänzen.

- Informieren Sie sich in den allgemeinen Geschäftsbedingungen (AGB) der Suchmaschine und dessen Datenschutzerklärung, wie Ihre Suchanfragen verwertet werden.
- Sind Sie mit der Nutzung Ihrer Suchanfragen nicht einverstanden, sollten Sie darüber nachdenken, Ihre bevorzugte Suchmaschine zu wechseln.

Nutzung von E-Mail- und Clouddiensten

Viele kostenlose E-Mail- und Clouddienste nutzen die von Ihnen gesendeten und empfangenen Nachrichten, sowie die gespeicherten Daten, um Ihr hinterlegtes Profil aufzubauen und zu ergänzen.

- Informieren Sie sich in den allgemeinen Geschäftsbedingungen (AGB) des Anbieters und dessen Datenschutzerklärung, ob und wie Ihre E-Mails bzw. Daten verwertet werden.
- Sind Sie mit der Nutzung nicht einverstanden, sollten Sie in Erwägung ziehen, den angebotenen Dienst nicht zu verwenden.
- Verwenden Sie gegebenenfalls solche Anbieter nicht zum Versand oder zur Speicherung vertraulicher Informationen.

Nutzung von Instant Messengern

Instant Messenger wie z. B. „WhatsApp“ nutzen heutzutage zumeist eine „End-2-End-Verschlüsselung“ zum Schutz Ihrer Nachrichten. Allerdings übermitteln einige Instant Messenger laufend eine Kopie aller in Ihrem Gerät gespeicherten Kontaktdaten an den jeweiligen Betreiber.

- Beachten Sie, dass Sie mit der Nutzung eines Instant Messengers in der Regel bestätigen, dass Sie von allen gespeicherten Kontakten das Einverständnis haben, dass deren Kontaktdaten an den Betreiber weitergegeben werden. Insbesondere in einem dienstlichen Kontext können hier sehr schnell datenschutzrechtliche Aspekte schlagend werden.

3.4 Datenschutz im Browser

Im Zentrum des Sammelns Ihrer Daten steht vor allem der verwendete Browser. Die Standardeinstellungen vieler Browser erlauben in der Regel weitgehende diesbezügliche Möglichkeiten. Doch es bestehen in den meisten Fällen zahlreiche Möglichkeiten, das Sammeln von Daten einzuschränken. Im Folgenden ist eine Reihe von diesbezüglichen Handlungsempfehlungen zusammenfasst:

Allgemeines

- I**nstallieren Sie zeitnah alle verfügbaren Sicherheitsupdates für Ihren Browser**. Sicherheitslücken im Browser führen, neben generellen Sicherheitsproblemen, auch immer wieder zu teils massiven Problemen mit dem Schutz Ihrer persönlichen Daten.
- **Nutzen Sie Ihren Browser ohne Anmeldung**. Viele Browser bieten die Möglichkeit, sich permanent bei einem dahinterliegenden Dienst anzumelden. Dies wird in der Regel damit beworben, dass Sie Ihre Einstellungen und Lesezeichen komfortabel zwischen mehreren Geräten synchronisieren können. Gleichzeitig erleichtert diese Anmeldung dem Anbieter aber auch, alle im Zusammenhang mit der Browsernutzung von Ihnen generierten Nutzungsdaten Ihrem Profil zuzuordnen.
- **Speichern Sie keine Kennwörter im Browser**. Die meisten Browser bieten Ihnen an, verwendete Kennwörter direkt im Browser zu speichern, damit Sie diese bei einem neuerlichen Besuchen der Seite nicht nochmals eingeben müssen. Dies stellt je nach Anbieter mitunter ein erhebliches Sicherheitsrisiko dar. Insbesondere bei Rechnern, die von mehreren Personen genutzt werden (und ganz besonders bei der Nutzung von fremden Rechnern) sollte eine Speicherung unbedingt unterbleiben.
- **Behalten Sie den Browserverlauf im Auge**. Ihr Browser speichert die Adressen aller von Ihnen besuchten Webseiten ab und stellt Ihnen diese als Verlauf zur Verfügung. Das bedeutet, dass Ihr Browser jederzeit den vollständigen Überblick über Ihre Aktivitäten im World Wide Web hat. Wollen Sie dies nicht, sollte der Browserverlauf beim Schließen automatisch oder manuell gelöscht werden. Dies ins insbesondere dann relevant, wenn auch andere Personen Zugriff auf den Rechner haben.

Komfortfunktionen

- **Deaktivieren Sie die automatische Vervollständigung**. Viele Browser merken sich von Ihnen getätigte Eingaben und verwenden diese als Vorschläge für die künftige Nutzung derselben oder anderer Webseiten. Ist diese Funktion aktiviert, bedeutet dies, dass auch persönliche Daten im Browser gespeichert werden.
- **Deaktivieren Sie das schnelle Laden von Webseiten**. Was auf den ersten Blick sehr vorteilhaft erscheint, kann bei genauerer Betrachtung durchaus Nachteile mit sich bringen. Das schnelle Laden wird dadurch erreicht, dass Ihr Browser beim Öffnen einer beliebigen Webseite sofort und ungefragt im Hintergrund alle auf dieser Seite verlinkten weiteren Webseiten öffnet. Klicken Sie dann auf einen Link, kann die weitere Webseite ohne zusätzliche Ladezeiten sofort geöffnet werden. Dabei müssen Sie aber berücksichtigen, dass der Browser auch alle im Hintergrund geladenen Seiten so behandelt, als hätten Sie selbst diese geöffnet.

- **Deaktivieren Sie die Nutzung der Adresszeile für Suchanfragen**. Gibt man in die Adresszeile eines Browsers eine Adresse ein, wird diese bei manchen Browsern gleichzeitig als Suchanfrage interpretiert. Dies soll es ermöglichen, dass für unvollständige oder falsche Eingaben trotzdem sinnvolle Ergebnisse geliefert werden. Durch diese Vorgangsweise wird allerdings jede Adresseingabe gleichzeitig eine Suchanfrage, die Ihrem Profil zugerechnet wird.

Datenübermittlungen an Anbieter

- **Übermitteln Sie keine Absturzberichte**. Diese Funktionalität soll den Anbietern helfen, Fehler in deren Software zu erkennen. Um Fehler allerdings effektiv analysieren zu können, benötigt der Anbieter eine große Menge an zusätzlichen Informationen, deren Übermittlung Sie durch das Nutzen dieser Funktionalität zustimmen. Dazu können je nach Anbieter unter anderem auch vollständige Speicherabbilder oder Listen der auf dem Rechner installierten Software gehören.
- **Übermitteln Sie keine Nutzungsstatistiken**. Oft wünschen sich die Anbieter die Übermittlung von anonymisierten Nutzungsstatistiken. Es wird betont, dass keine personenbezogenen Daten übertragen werden. Das stimmt in der Regel zwar, es hat sich aber gezeigt, dass diese Daten durch Verknüpfung mit Datenbeständen aus anderen Quellen zu einem späteren Zeitpunkt sehr wohl eindeutig Ihnen zugeordnet werden können.

Anonymer Modus

Eine Möglichkeit, alle diese Maßnahmen zur Datenreduktion gleichzeitig zu nutzen, ist der anonyme Modus, den viele Browser anbieten. Wechselt man in diesen Modus, werden auf dem lokalen Rechner keine Daten zu Aktivitäten im Browser gespeichert. Schließt man den anonymen Modus, werden alle angeführten Nutzungsdaten wieder entfernt.

Ein verbreitetes Missverständnis im Zusammenhang mit dem anonymen Modus ist allerdings, dass viele glauben, dass man in diesem Modus gegenüber dem Internet an sich anonym bleibt. Dies ist ein Trugschluss. Der anonyme Modus bietet keinerlei Anonymität nach außen. Diese kann, wenn überhaupt, nur durch die Verwendung spezieller Werkzeuge (z. B. TOR) oder die Nutzung von Virtual Private Network-Lösungen (VPN) erreicht werden.

Bundesministerium für Inneres
Bundesamt für Verfassungsschutz und Terrorismusbekämpfung
Cyber Security Center – Bereich Prävention
Herrengasse 7, 1010 Wien
csc@bvt.gv.at
bvt.gv.at