Stand: 11.1.2019

Empfehlungen des LfDI Rheinland-Pfalz für die Nutzung von Online- und Social Media-Diensten

Aktuelle Vorfälle, bei denen Personen des öffentlichen Lebens Opfer einer unbefugten Veröffentlichung persönlicher Daten waren, haben einmal mehr die Verwundbarkeit digitaler Kommunikation vor Augen geführt. Gerade bei der Bereitstellung und Verarbeitung durch Dritte werden Daten in teils schwer steuerbarer Weise übermittelt und gespeichert, was es den Betroffenen erschwert, den Überblick und die effektive Verfügungsmacht zu behalten.

Im Fall der Veröffentlichung persönlicher Daten von Personen des öffentlichen Lebens lässt die Art der Daten den Schluss zu, dass diese jedenfalls zum Teil elektronischen Adressbüchern, Social-Media-Accounts und Cloud-Diensten entstammen, für welche ein unbefugter Zugriff aufgrund kompromittierter Zugänge möglich war.

Soweit die Verfügungsmacht des Einzelnen reicht, sollten für ein Mindestmaß an Datenschutz und Datensicherheit daher die nachfolgenden Empfehlungen berücksichtigt werden.

Sorgfalt bei Auswahl der Anbieter von Diensten

Bei der Nutzung elektronischer Dienste sollte für die Speicherung und Verarbeitung persönlicher Daten nicht unreflektiert auf Seriosität und Altruismus des Anbieters vertraut werden. Zurückliegende Fälle zeigen, dass Datenbestände häufig unkontrolliert für Zugriffe Dritter geöffnet werden (z.B. Facebook/Cambridge Analytica).

- Insbesondere dort, wo Dienste kostenlos angeboten werden und das Geschäftsmodell auf der Sammlung und Auswertung von Daten von Nutzerinnen und Nutzern basiert, sollte daher datenmäßig Zurückhaltung geübt und jeweils geprüft werden, welche Daten dem Anbieter anvertraut werden. Ein sinnvolles Kriterium ist hierbei, ob der Anbieter europäischen Datenschutzregelungen unterliegt.
- Für die Nutzung von Speicher- und Kommunikationsdiensten sollte daher auf deutsche oder europäische Anbieter zurückgegriffen werden. So gewährleistet eine Reihe deutscher E-Mail-Anbieter im Rahmen einer Initiative durch die Verschlüsselung der Mail-Kommunikation zwischen den beteiligten Providern ein hinreichendes Maß an Vertraulichkeit bei der Übermittlung (https://www.e-mail-made-in-germany.de/index.html). Das Projekt „DE-Mail“ bietet darüber hinaus die Möglichkeit einer rechtssicheren Kommunikation (https://de-mail.info/).
- Für verschiedene Arten oder Bereiche der Kommunikation (privat, amts- oder funktionsbezogen) sollte überlegt werden, verschiedene E-Mail-Konten oder Kommunikationswege zu nutzen. Dies gilt auch für die Nutzung von Cloud-Diensten für die Ablage von Dokumenten, Fotos, Kontaktdaten etc.
- Anstelle gängiger Messenger-Dienste wie WhatsApp oder dem Facebook-Messenger sollte für sensible Nachrichten auf datenschutzfreundliche Alternativen wie Threema, SIMSme,

Wire, Hoccer oder Chiffry zurückgegriffen werden (https://www.youngdata.de/whatsapp-skype-co/whatsapp/).

- Google als Suchmaschine speichert die Suchanfragen und führt diese mit den Daten aus anderen Google-Diensten (z.B. GMail, Maps, Übersetzer, Youtube, Play-Store, Kalender, Fotos usw.) zusammen und ermöglicht damit die Bildung von Nutzungs-, Bewegungs-, und Verhaltensprofilen. Um zu vermeiden oder zu erschweren, dass solche Profile für die eigene Person gebildet werden, sollte auf Suchmaschinen wie Startpage (https://www.startpage.com/) oder Unbubble (https://www.unbubble.eu/) zurückgegriffen werden.

Verschlüsselung

Verschlüsselung bietet Schutz vor unbefugter Kenntnisnahme und schützt damit auch bei unbefugten Datenzugriffen oder Datenverlust. Auch ohne tiefergehende IT-Kenntnisse bestehen hier einfach nutzbare Möglichkeiten.

- Bei der Auswahl von Anbietern und Diensten sollte darauf geachtet werden, inwieweit diese eine Verschlüsselung der Kommunikationswege (s.o.) sowie eine verschlüsselte Speicherung von Zugangsdaten (Passworte) und Inhaltsdaten (Dokumente, Fotos, Kontaktdaten etc.) vorsehen.
- Bei der Anmeldung bei Online-Diensten, sollte darauf geachtet werden, dass die Zugangsdaten verschlüsselt übermittelt werden (erkennbar an der Angabe“ https“ sowie eines geschlossenen Schloss-Symbols in der Adresszeile des Browsers).
- Soweit die Möglichkeit besteht, sollten auch sonstige Zugriffe im Rahmen der Nutzung von Online-Diensten HTTPS-verschlüsselt erfolgen.
- Online-Dienste, die eine Anmeldung erfordern (z.B. E-Mail, Social Media, Messenger) sollten, soweit auf sie über öffentlichen WLAN-Netze zugegriffen wird, über eine verschlüsselte (VPN-)Verbindung genutzt werden. Hier stehen für verschiedene Plattformen (PC, Tablet, Smartphone) nutzbare Lösungen zur Verfügung (https://www.heise.de/download/specials/Anonym-surfen-mit-VPN-Die-besten-VPN-Anbieter-im-Vergleich-3798036).
- Bei der Ablage persönlicher Dokumente auf Cloud-Speichern sollte eine Verschlüsselung vorgesehen werden. Hier stehen einfach handhabbare Lösungen, z.B. über gängige Programme zur Komprimierung von Daten (ZIP), zur Verfügung (vgl. https://www.datenschutz.rlp.de/de/themenfelder-themen/cloud-speicher-sicher-nutzen/)

Schutz von Online-Zugängen und Zugangsdaten

Bei vielen Online- und Social-Media-Diensten ist die Nutzung an Zugangsdaten gebunden (E-Mail-Adresse oder Nutzer-ID, Passwort, PIN etc.). Für deren Schutz sollten die folgenden Empfehlungen berücksichtigt werden:

- Passworte sind die häufigste, zugleich aber auch schwächste Form der Absicherung eines Online-Zugangs. Daher sollten möglichst starke, nicht erratbare Passworte verwendet werden (vgl. https://www.passwortcheck.ch/passwortcheck/passwortcheck und https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Passwoerter/passwoerter_node.html)

- Wo angeboten oder unterstützt, sollte die Möglichkeit genutzt werden, für eine erfolgreiche Anmeldung neben einem Passwort auf eine zweite Information, z.B. einen per SMS zugeschickten Code, zurückzugreifen (2-Faktor-Authentifizierung). Für eine Reihe von Social Media-Plattformen wird dies angeboten (https://t3n.de/news/zwei-faktor-authentifizierung-google-facebook-dropbox-paypal-twitter-531483/)
- Für verschiedene Dienste sollten auch verschiedene Passworte verwendet werden, damit im Fall der Kompromittierung der Zugangsdaten eines Dienstes nicht auch die Sicherheit der anderen Zugänge betroffen ist. Dies gilt insbesondere dann, wenn die E-Mail-Adresse und das dort verwendete Passwort für eine Registrierung bei anderen Online-Diensten verwendet werden. Für die Verwaltung der Passworte kann auf sogenannte „Passwort-Manager“ zurückgegriffen werden, die eine verschlüsselte Speicherung von Zugangsdaten erlauben (siehe https://www.heise.de/tipps-tricks/Passwortmanager-So-verwalten-Sie-Ihre-Passwoerter-3934582.html). Da das dabei genutzte Master-Passwort den Charakter eines Generalschlüssels hat, sollte auf dessen Gestaltung und Verwendung besondere Sorgfalt verwendet werden.
- Passworte veralten im Lauf der Zeit bzw. werden unsicher. Daher sollte in bestimmten Abständen ein Wechsel des Passworts vorgenommen werden.
- In bestimmten Zusammenhängen, etwa, wenn Dienste oder Social Media –Kanäle im Namen des Nutzers/der Nutzerin von anderen Personen betrieben werden, kann unklar sein, an wen und zu welchem Zweck Zugangsdaten weitergeben wurden oder wer Kenntnis von Ihnen hat. Häufig ist auch nicht zu beeinflussen, ob und wo weitergegebene Passworte gespeichert werden. Auch dies sollte Anlass sein, Passworte regelmäßig zu wechseln.
- Die Applikationen von Online- und Social-Media-Diensten bieten häufig die (Komfort-) Funktion, dauerhaft angemeldet zu bleiben, um eine wiederholte Eingabe der Zugangsdaten zu vermeiden. Die hat zur Konsequenz, dass jeder, der Zugriff auf das Endgerät hat, potentiell auf die Daten des jeweiligen Dienstes zugreifen kann. Wo nicht erforderlich, sollte diese Funktion daher deaktiviert werden.

Zurückhaltung und Bedacht bei der Nutzung sozialer Medien

Welche Daten Online-Diensten und -Plattformen anvertraut werden, sollte mit Bedacht und Überlegung entschieden werden. Dies gilt insbesondere dort, wo soziale Netzwerke betroffen sind.

- In welchem Umfang dort wechselseitige Zugriffsmöglichkeiten bestehen, welche Daten geteilt oder im Rahmen der Nutzung weitergeben werden, sollte in bestimmten Abständen überprüft und hinterfragt werden.
- Für die Online-Diensten und -Plattformen anvertrauten Daten sollte in bestimmten Abständen überprüft werden, ob die Daten gelöscht werden können/sollten. Dies gilt insbesondere auch für in der Vergangenheit liegende, aktuell nicht mehr relevante Kommunikationsvorgänge (z.B. Chatverläufe). Häufig gibt es eine Funktion, die z.B. Chats nach einem einstellbaren Zeitraum automatisch löscht.
- Soweit die Möglichkeit genutzt wird, Sicherungskopien auf Cloud-Speichern abzulegen (z.B. für Kontaktdaten, Fotos, Dokumente, Chats usw.) sollte darauf geachtet werden, dass diese verschlüsselt werden. Alternativ sollten solche Sicherungskopien verschlüsselt auf dem eigenen PC abgelegt werden.

- Von der Möglichkeit, Adressbücher bzw. Kontaktdaten mit dem Online- oder Social Media-Dienst pauschal zu „synchronisieren“ sollte Abstand genommen werden. Stattdessen sollten ggf. notwendige Kontaktdaten dort gezielt und orientiert an der gewünscht zu adressierenden Zielgruppe (z.B. private Kontakte, funktionsbezogene Kontakte) eingegeben werden.
- Orientierung am Handlungsrahmen des LfDI zur Nutzung sozialer Medien durch Behörden des Landes Rheinland-Pfalz (https://www.datenschutz.rlp.de/de/themenfelder-themen/handlungsrahmen-soziale-netzwerke/)
- Um zu klären, über welche Daten Online- und Social Media-Dienste in Bezug auf die eigene Person verfügen, kann der datenschutzrechtliche Auskunftsanspruch nach Art. 15 DS-GVO geltend gemacht werden. Im Rahmen des Rechts auf Datenübertragbarkeit nach Art. 20 DS-GVO besteht zudem die Möglichkeit, die bereitgestellten Daten zu erhalten.
  Für einige Dienste kann letzteres über folgende Links beantragt werden:

  WhatsApp: https://faq.whatsapp.com/general/26000110
  Facebook: https://www.facebook.com/help/1701730696756992/?helpref=hc_fnav
  Twitter: https://help.twitter.com/de/managing-your-account/accessing-your-twitter-data

Schutz vor Phishing und Schadsoftware

- Schadsoftware und Phishing-Attacken gehören mittlerweile zum „digitalen Grundrauschen“ im Internet. Bei der Auswahl eines Anbieters (z.B. E-Mail-Provider) sollte daher darauf geachtet werden dass dieser diensteseitig bereits einen angemessenen Schutz vor Schadsoftware bietet (Virenschutz, SPAM-Filter).
- Eine Infektion mit Schadsoftware kann bereits durch das Öffnen eines Dateianhangs oder das Anklicken eines Links erfolgen. Wenn für angebotene oder zugesandte Nachrichten und Inhalte kein plausibler Zusammenhang erkennbar und/oder der Absender nicht bekannt ist, sollten entsprechende Anhänge nicht geöffnet werden.
- Für die Software der jeweils genutzten Geräte (PC, Tablet, Smartphone) werden im Lauf der Zeit erfahrungsgemäß Schwachstellen oder Sicherheitslücken offenbar. Daher sollte diese stets auf einem aktuellen Stand gehalten werden. Entsprechende Aktualisierungen sollten daher zeitnah installiert werden. Darüber hinaus sollte auf einen ausreichenden Schutz vor Schadsoftware geachtet werden; hier stehen für alle Plattformen geeignete Softwarelösungen zur Verfügung.

In seinem Internet-Angebot hält der Landesbeauftragte weitere Informationen zum Selbstdatenschutz und zur Vermeidung von Datenspuren im Internet bereit:

https://www.datenschutz.rlp.de/de/themenfelder-themen/selbstdatenschutz/