TLfDI

Thüringer Landesbeauftragter
für den **Datenschutz** und die **Informationsfreiheit**

Digitale Selbstverteidigung

Sehr geehrte Damen und Herren,

diese Hinweise sollen Ihnen Mittel zur „digitalen Selbstverteidigung“ an die Hand geben. Nach kurzen Hinweisen auf die Gefahrenlage werden Sie mit Tipps versorgt, wie Sie Ihren digitalen Schutz erhöhen können. Mit weiterführenden Links können Sie sich tiefgreifender informieren. Der TLfDI wünscht erkenntnisreiche Lektüre und Erfolg beim Aufbau Ihrer geschützten Daten-Privatsphäre.

Tino Melzer, TLfDI

Bei Fragen allgemein zum Datenschutz wenden Sie sich bitte an den TLfDI, natürlich auch bei Fragen und Anregungen zu dieser Broschüre, die im Mai 2026 in der 12. Auflage aktualisiert wurde. Gefahren im Internet sind leider nicht unmittelbar wahrnehmbar, aber gleichwohl allgegenwärtig. Hat man die Gefahren erkannt, gilt es, sich davor zu schützen – los geht’s!

Der TLfDI wünscht Ihnen viel Spaß und viele Erkenntnisse beim Lesen.

Inhalt

1. Allgemeine Hinweise

Datenvermeidung ist das Mittel der Wahl, um seine Privatsphäre zu schützen; idealerweise bis hin zur absoluten Anonymität.
Welche Maßnahmen von Ihnen ergriffen werden können, zeigen wir Ihnen jetzt:

Datenvermeidung allgemein

Grundsätzlich gilt die Regel: Was man im Internet nicht von sich preisgibt, kann dieses auch nicht wissen.

Was können Sie tun?

Prüfen Sie genau, welche Angaben wirklich benötigt werden (also welche Pflichtangaben sind) und welche Angaben nur optional sind. Auch bei sozialen Netzwerken müssen Sie zur Nutzung des Netzwerkes nicht alle nachgefragten Angaben eingeben.
Passen Sie außerdem auf, welche Bilder und Videos Sie ins Netz stellen. Sind Gesichter auf den Bildern zu sehen, die von anderen

wiedererkannt werden können, so können diese Gesichter auch unter Umständen von Wiedererkennungsalgorithmen echten Personen oder Personenprofilen zugeordnet werden (siehe z.B. https://www.edpb.europa.eu/news/national-news/2022/french-sa-fines-clearview-ai-eur-20-million_de). Auch können so (bei ausreichend hoher Bildauflösung) unter Umständen biometrische Merkmale Ihrer Person extrahiert werden. Eine spannende Anekdote ist z.B. bei https://www.ccc.de/de/updates/2014/ursel nachzulesen.

Was können Sie außerdem tun?

Wo es erlaubt ist, nutzen Sie zur Anmeldung ein Pseudonym. Um Ihre Passwörter zu schützen, nehmen Sie bei sehr selten verwendeten Zugängen „Einmalpasswörter". Denken Sie sich einfach für den einmaligen Gebrauch ein sehr komplexes Passwort aus und verwenden Sie es. Ein komplexes Passwort sollte aus mindesten 8 unterschiedlichen Zeichen bestehen – besser sind 12 Zeichen. Nähere Informationen dazu finden Sie unter Umsetzungshinweise zum Baustein: ORP.4. Identitäts- und Berechtigungsmanagement (bund.de), hier u.a. unter ORP.4.M23 und ORP.4.M22. Bei der nächsten Anmeldung lassen Sie Ihr Passwort dann einfach zurücksetzen. Auf den meisten Webseiten funktioniert das so, indem Sie den Link „Passwort vergessen" klicken und den dortigen Anweisungen folgen. Da heutzutage an sehr vielen Plattformen Passwörter genutzt werden, empfiehlt sich der Einsatz eines Passwort-Safes wie z.B. KeePass oder 1Password. Achten Sie vor allem darauf,

dass für den Fall, dass die Passwörter auch in der Cloud des Passwort-Safe-Anbieters gespeichert werden, der Anbieter keinen Zugriff auf die Passwörter besitzt. Hierzu muss die Dokumentation des Anbieters aussagefähig sein.

Die Browserchronik

Die Datensammlung beginnt bereits im Browser Ihres internetfähigen Gerätes, und zwar in der Chronik bzw. der Verlaufsanzeige Ihres Browsers. Der Browser ist das Programm, mit dem Sie Internetseiten aufrufen. In der Chronik bzw. Verlaufsanzeige werden alle besuchten Webseiten und angewählten Weblinks gespeichert. Daher weiß der Browser noch nach Wochen, welche Links Sie beim letzten Besuch angesehen haben. Diese Information kann auch von Webseiten, die Sie besuchen, abgefragt werden.

Was können Sie tun?

Für die Chronik des Browsers kann man in den Browsereinstellungen selbst festlegen, ob man diese übernehmen möchte oder nicht, oder ob diese Daten von Zeit zu Zeit gelöscht werden. Wie, erfahren Sie bspw. auf https://www.datenschutz.de/datenspuren-im-internet-vermeiden/ für PCs und für mobile Geräte auf https://support.google.com/chrome/answer/95589?hl=de. Wählen Sie unter „Gesamten Verlauf löschen“ Ihr Gerät aus.

Cookies

Eine weitere Methode zum Nachverfolgen Ihres Weges durch das Internet ist der Einsatz von Cookies. Dies sind kleine Textdateien, die manche Websites beim Aufrufen der Website auf Ihrem Gerät speichern. Die Textdateien tragen meistens eine eindeutige Identifikationsnummer, über die der Rechner später wiedererkannt werden kann und eine zusätzliche Information über die besuchte Website. Gesetzte Cookies können aber auch websiteübergreifend ausgewertet werden und zur Profilbildung beitragen – Cookies sind also auch kleine Verräter bzw. Spione.

Was können Sie tun?

Viele Websites fragen beim ersten Besuch nach der Einwilligung zum Speichern von Cookies. Nutzen Sie das Cookie-Banner und informieren Sie sich über die Daten, die die Website über ihren Besuch speichern wird, sodass Sie eine informierte Entscheidung treffen können.
Im Browser kann man in den Browsereinstellungen ebenfalls das Speicherverhalten von Cookies aufgerufener Websites einstellen, z.B. ob Cookies in jedem Fall automatisch gespeichert werden, nur auf Nachfrage oder überhaupt nicht. Sinnvoll erscheint auch die Einstellung, die nach dem Beenden des Browsers alle genutzten Cookies löscht. Denn spätestens, wenn man online etwas kaufen möchte, wird man während der Sitzung nicht umhinkommen, Cookies des Online-Shops zuzulassen, damit die Bestellung erfolgreich erfolgen

kann. Wie man im Browser Cookies zulassen bzw. verbieten kann, erfahren Sie https://www.datenschutz.de/datenspuren-im-internet-vermeiden/ (gleicher Link wie oben), für Mozilla Firefox: https://support.mozilla.org/de/kb/cookies-erlauben-und-ablehnen, Google Chrome: https://support.google.com/accounts/answer/61416?hl=de, Apple Safari: https://support.apple.com/de-de/guide/safari/ibrw850f6c51/16.1/mac/13.0, Microsoft Edge: https://support.microsoft.com/de-de/microsoft-edge/cookies-in-microsoft-edge-l%C3%B6schen-63947406-40ac-c3b8-57b9-2a946a29ae09

Surfen im „Privatmodus“

Um nicht ständig die Chronik und die gespeicherten Cookies von Hand löschen zu müssen, bieten moderne Browser einen „Privatmodus“, der dafür sorgt, dass solche Datenspuren nur während der aktuellen Sitzung auslesbar sind. Nach dem Beenden des Browsers werden Cookies und Chronik automatisch gelöscht.

Was können Sie tun?

Der Privatmodus wird in jedem Browser unterschiedlich aktiviert: auf dem Rechner kann er bspw.

- in Firefox im „Menü“ (oben rechts – Symbol: drei Balken) unter „Neues privates Fenster“ aktiviert werden,
- im Safari auf dem Mac befolge folgende Anleitung:

https://support.apple.com/de-de/guide/safari/ibrw1069/mac,

- bei Google Chrome im „Menü“ (oben rechts – Symbol: drei Balken) unter „Neues Inkognitofenster“ aktiviert werden.
- im Edge im „Menü“ (oben rechts – Symbol: drei Punkte) unter „Neues InPrivate-Fenster“ aktiviert werden.

Verschlüsselungsmöglichkeiten von Websites

Die meisten Websites bieten heute schon eine verschlüsselte Datenübermittlung an. Dies bedeutet, die Verbindung vom Webserver zu Ihrem Endgerät ist so gesichert, dass kein Unbefugter die Daten zur Kenntnis nehmen kann.

Was können Sie tun?

Achten Sie darauf, ob beim Browser in der Adressleiste „https:// ...“ oder ein Schlosssymbol ( ) erscheint. Ist dies nicht der Fall, geben Sie einfach vor der Angabe www. „https://“ in der Adresszeile ein. Aus http://www.tlfdi.de wird so z.B. https://www.tlfdi.de.
Funktioniert dies nicht, unterstützt die Webseite keine Verschlüsselung. In diesem Falle sollten Sie sich überlegen, ob Sie tatsächlich personenbezogene Daten auf der Webseite eingeben wollen, da die Datenübermittlung ansonsten unverschlüsselt erfolgt.

Sichere Kurznachrichten und Chats

Kurznachrichtendienste und Chats werden heute häufig schon verschlüsselt übertragen. Dadurch können z.B. „Angreifer“ oder „Mithörer“ die Daten auf dem Datenweg nicht einfach mitlesen. Ist eine Schadsoftware, wie z.B. ein Trojaner, auf Ihrem Gerät installiert, welche z.B. die Tastatureingabe oder die Bildschirmanzeige ausliest, nützt allerdings Verschlüsselung gar nichts. Auch Betreiber der Kurznachrichtendienste könnten die Inhalte evtl. mitlesen und daraus wieder Informationen für Profile extrahieren.

Was können Sie tun?

Verwenden Sie verschlüsselte Kurznachrichten mit einer sogenannten Ende-zu-Ende Verschlüsselung. Ein einfaches Browser-Plugin oder eine entsprechende App kann dann zur verschlüsselten Unterhaltung mit Ende-zu-Ende Verschlüsselung genutzt werden und der Betreiber oder Personen mit krimineller Energie können nicht mehr mitlesen. Den Link beispielsweise zum Programm CryptoCat finden Sie hier: https://de.wikipedia.org/wiki/Cryptocat. CryptoCat ist eine Browsererweiterung oder eine App für Smartphones, die eine Ende-zu-Ende verschlüsselte Kommunikation ermöglicht. Alle großen Anbieter von Messenger-Apps wie iMessage, WhatsApp,

© gena96 – Fotolia

Threema oder Signal nutzen mittlerweile Ende-zu-Ende Verschlüsselung. Bei Telegram muss gezielt die Funktion „geheimer Chat“ genutzt werden. Die Verschlüsselung betrifft aber nur Inhalte der Nachrichten. Andere App-Bestandteile, wie die Kontakte oder der Status sind dem Anbieter der App meist im Klartext bekannt. Aber wie gesagt, wenn Sie Schadsoftware auf Ihrem Gerät haben, welche die Tastatureingaben und Bildschirminhalte mitliest, hilft auch die beste Verschlüsselung nicht. Deshalb ist es wichtig, dass Sie neben der Ende-zu-Ende Verschlüsselung stets die Sicherheitsupdates des Antivirenprogramms, des Betriebssystems und anderer Programme installiert haben (siehe hierzu „Absicherung des PCs“).

Suchmaschinen

Die Betreiber von Suchmaschinen versuchen, möglichst viele Informationen über ihre Nutzer zu erfahren. Auch durch die Auswertung der von Ihnen eingegebenen Suchbegriffe kann viel über Sie herausgefunden werden.

Was können Sie tun?

Es gibt datenschutzfreundliche Suchmaschinen, welche die IP-Adressen der Nutzer anonymisieren oder gar nicht erst speichern (derzeit z.B. https://www.metager.de, https://duckduckgo.com oder https://www.startpage.com).

Anonymes Browsen

Nicht nur beim Suchen im Internet erfolgt möglicherweise durch Suchmaschinen eine Profilbildung. Auch durch das Setzen von Cookies beim Aufrufen von Websites, welche manchmal auch Werbebanner beinhalten oder sogenannte Social-Plug-Ins nutzen, kann eine Profilbildung erfolgen. Deswegen müssen Sie, wenn Sie Ihre Identität verschleiern wollen, weitere Maßnahmen treffen.

Was können Sie tun?

Sie können das Tor-Netzwerk nutzen. Auf einer sehr grundlegenden Ebene versucht das Tor-Netzwerk eine anonyme Internetkommunikation zu erzeugen. Dazu werden Mechanismen des Internets so verändert, dass eine Nachverfolgung der Daten sehr erschwert wird. Hintergrundinformationen zum Netzwerk finden sich unter https://de.wikipedia.org/wiki/Tor_%28Netzwerk%29. Unter diesem Link finden Sie ebenfalls die Schwachpunkte des Netzwerkes und die Beschreibung erster Versuche, die Anonymisierungsfunktionen zu umgehen (Abschnitt „Kritik und Schwachstellen“).

Was können Sie außerdem tun?

Man kann außerdem einen Proxy-Server nutzen, welcher als Mittelsmann (oder besser Mittelsmaschine) die Webseitenanfrage in Ihrem Auftrag übernimmt und die Webseiteninhalte dann an Ihr Gerät weiterleitet.

Damit wird Ihre Internetadresse vor dem Webseitenbetreiber verborgen, es sei denn, Sie haben entsprechende Cookies zugelassen. Es gibt auch noch weitere Mechanismen, welche die Anonymisierung von Proxyservern umgehen könnten. Trotzdem lohnt sich die Nutzung eines Proxy-Servers, wenn man seine Datenspuren so gering wie möglich halten möchte. Im Internet gibt es frei zugängliche Proxy-Server. Um diese zu nutzen, müssen Sie einige Systemeinstellungen ihres Betriebssystems anpassen.
Geben Sie dazu unter Windows in der Suche „Proxyeinstellungen ändern" ein und konfigurieren Sie unter den Verbindungseinstellungen den von Ihnen gewünschten Proxy. Für macOS folgen Sie: https://support.apple.com/de-de/guide/mac-help/mchlp2591/mac, für Android-Smartphones https://support.google.com/nexus/answer/2819519?hl=de und wählen Sie unter „Erweiterte WLAN-Einstellungen" den Punkt „Proxy-Einstellungen konfigurieren". Für iOS-Smartphones benutzen Sie https://support.apple.com/de-de/HT202693. Die Anonymität von Proxy-Servern kann allerdings durch Cookies oder JavaScript recht einfach umgangen werden. Nähere Informationen dazu finden Sie auf der Webseite der TU-Dresden: https://anon.inf.tu-dresden.de/help/jap_help/de/help/otherServices.html. Noch weitergehende Werkzeuge zum anonymen Surfen werden ebenfalls von der TU-Dresden zur Verfügung gestellt – https://anon.inf.tu-dresden.de/help/jap_help/de/help/about.html. Durch die Nutzung des Tor-Netzwerkes oder von Proxy-Servern in Verbindung mit dem privaten Surf-Modus

des Browsers (inkl. sehr restriktiver Cookie-Einstellungen) kann aber bereits eine ganz gute Anonymisierung erreicht werden.

Kinder- und Jugendschutz

Auch im Internet muss der Kinder- und Jugendschutz eingehalten werden. Deshalb sollten auch Eltern sich regelmäßig über die Gefahren informieren, denen ihre Kinder im Internet evtl. ausgesetzt sein können. Diese Gefahren können sich zum einen aus dem Besuch von z.B. nicht jugendfreien Webseiten ergeben oder, indem die Kinder oder Jugendlichen aktiv von Fremden kontaktiert werden – z.B. über Chats- und Nachrichten-Apps. Neben den bekannten Kommunikationsdiensten wie Facebook-Messenger, WhatsApp oder Threema gibt es auch zahlreiche Onlinespiele, die eine Chatfunktion beinhalten. Auch gibt es – speziell für Kinder – Nachrichten und Apps, welche kindgerecht gestaltet sind.

Diese kindgerechten Apps mit Chatfunktion ziehen leider auch Pädophile an. Diese versuchen dann, mit falscher Identität über Geschenke oder Versprechungen, die Kinder- und Jugendlichen zu sexuellen Handlungen zu überreden.

Was können Sie tun?

Sprechen Sie mit ihren Kindern. Wenn jemand Kontakt sucht, oder Dinge wie Spiele-Gegenstände oder Spiele-Währung gegen Fotos oder Videos eintauschen will, so sollte das Kind vorsichtig sein. Kennt ihr Kind das digitale Gegenüber als echte Person, so ist die Gefahr des Missbrauchs geringer. Weitere Informationen finden Sie auf den Seiten der Polizei (z.B. https://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/aktion-kinder-sicher-im-netz/ in den Abschnitten Addbörsen und Chaträume).

Was können Sie außerdem tun?

Nutzen Sie sichere Seiten für Ihre Kinder. Webseiten wie Frag-Finn (https://www.fragfinn.de/) oder SWR-Kindernetz (https://www.kindernetz.de/) bieten erhöhte Sicherheit, indem nur ausgewählte, kindgerechten Inhalte angeboten werden. Problematischer wird es bei Jugendlichen, da diese oft zum Ziel haben, unbekannte Personen kennenzulernen und dies meist außerhalb des elterlichen Kontrollbereichs geschieht. Zunehmend nutzen die Jugendlichen auch Apps zum Kennenlernen – Apps zu diesem Zweck gibt es viele, daher kann an dieser Stelle nicht auf jede einzelne App

eingegangen werden. Und auch hier gilt: diese Portale werden ebenso genutzt, um die Leichtgläubigkeit und Unbedachtheit der Jugendlichen auszunutzen.

Was können Sie außerdem tun?

Sensibilisieren Sie ihre Kinder. Nicht jeder, der vorgibt ein Jugendlicher oder eine Jugendliche zu sein, ist dies auch tatsächlich. Es kann vorkommen, dass Fake-Profile zum Anlocken der Jugendlichen genutzt werden. Auch hier hilft der Link der Polizei zur besseren Information weiter (https://www.polizei-praevention.de/themen-und-tipps/basisschutz-empfehlungen/soziale-netzwerke-und-chats, diesmal die Abschnitte Sexting, AddBörsen und Chaträume). Außerdem sind Partnerbörsen auch nicht immer das, was sie zu sein scheinen (siehe Link https://www.heise.de/newsticker/meldung/Verdacht-auf-Abzocke-bei-Dating-Plattform-Lovoo-2821077.html und https://www.watchlist-internet.at/news/tinder-bots-betruegen-mit-scheinbarer-verifizierung/).

Soziale Netzwerke

Soziale Netzwerke dienen vor allem der Kommunikation und der Selbstdarstellung (Profil)der Nutzer. Häufig werden diese Netzwerke privat genutzt und damit auch persönliche Daten ausgetauscht bzw. gespeichert. Auch stellen Nutzer oft personenbezogene Daten von anderen Nutzern ein. Dadurch bekommt der Betreiber dieser

Netzwerke natürlich automatisch einen Eindruck über diese Personen, wie z.B. ihre Interessen, ihren Freundeskreis aber auch ihre Probleme oder ihre die finanzielle Kaufkraft. Neben Facebook, Instagram, X (ehemals Twitter) und SnapChat ist TikTok die wohl erfolgreichste „Newcomer-Plattform" der letzten Jahre. Hier wird nicht mehr über Text oder Bilder miteinander kommuniziert, sondern über Kurzvideos.
Datenschutz auf sozialen Netzwerken ist also immer zweigeteilt: einmal muss man entscheiden, welche Daten man überhaupt von sich oder anderen eingibt (diese kennt dann der Betreiber) und welche Daten andere Nutzer des Netzwerkes zu Gesicht bekommen können. Anders als bei Messengern kann der Dienstanbieter grundsätzlich alle Inhalte des sozialen Netzwerkes lesen und räumt sich meist auch umfangreiche Rechte auf diese Inhalte ein. Allerdings kann der Zugriff anderer Nutzer auf eigene Inhalte gut gesteuert werden und diese Möglichkeiten sollten auch sehr gewissenhaft konfiguriert werden (siehe weiter hinten im Text).
Soziale Netzwerke aber auch Online-Partnerbörsen werden gerne auch zum sogenannten „Scamming" genutzt. Dabei wird mit dem Opfer, meist Singles, Kontakt aufgenommen und sehr langsam eine emotionale Verbindung aufgebaut. Die vermeintlichen Kontakte sind häufig angeblich Ärzte, Rechtsanwälte oder Generäle mit interessantem Lebenslauf und viel Geld. Diese meiden allerdings ein konkretes Treffen und geraten nach einer Weile plötzlich in Not und benötigen dringend finanzielle Hilfe. Das ist alles Schwindel!

Was können Sie tun?

Für den ersten Fall, überlegen Sie genau, welche Daten Sie ihrem Profil anvertrauen da dies dann auch der Betreiber kennt. Und prüfen Sie, ob diese Daten für den Zweck, für welches das Profil genutzt werden soll auch wirklich notwendig sind. Der zweite Fall, die Sichtbarkeit nach außen, ist meist eine Frage der Einstellungen. Hierzu gibt es im Internet für jeden Dienst gute Anleitungen (suchen Sie einfach nach dem Stichpunkt „Privatsphäre"). Für Facebook finden Sie z.B. die Anleitungen https://www.facebook.com/about/basics, für X/Twitter https://support.twitter.com/articles/334631, für Instagram https://help.instagram.com/448523408565555, für WhatsApp https://www.whatsapp.com/faq/de/android/23225461 und für TikTok unter https://support.tiktok.com/de/account-and-privacy (Sprache lässt sich ganz unter auf der Website einstellen).

Was können Sie außerdem tun?

Beachten Sie zum Thema „Scamming" außerdem die Hinweise zu korrektem Verhalten unter https://www.polizei-beratung.de/themen-und-tipps/betrug/scamming/. Übrigens, Scamming- Opfer sind sowohl Frauen, aber auch Männer.
Vermeiden Sie prinzipiell zu viel Ihrer persönlichen Daten auf sozialen Plattformen preiszugeben – so werden Sie gar nicht erst als mögliche Zielperson erkannt.

Schutz vor digitalem Identitätsdiebstahl

Digitaler Identitätsdiebstahl hat viele Gesichter. Allen gemeinsam ist, Kriminelle geben sich im Internet als eine andere Person aus. Dies kann schwerwiegende Folgen haben – von finanziellen Schäden über Rufschädigung bis zu strafrechtlichen Konsequenzen. Deshalb sollten Sie es Cyberkriminellen so schwer wie möglich machen.

„Mögliche Indizien für einen Identitätsmissbrauch sind etwa:

- Sie erhalten Zahlungsaufforderungen für Bestellungen, die Sie nicht getätigt haben.
- Das Einloggen bei einem Internetdienst, dem E-Mail-Anbieter oder bei einem sozialen Netzwerk ist trotz vermeintlich korrektem Passwort nicht möglich.
- In Ihrem Namen werden Beiträge im Internet veröffentlicht, E-Mails versendet oder Profile in sozialen Netzwerken erstellt.
- Sie erhalten von Ihrem Dienstleister eine Benachrichtigung, dass ein neues Gerät für den Dienst registriert wurde oder Sie den Dienst von einem ungewöhnlichen Ort genutzt haben, ohne dass dies tatsächlich der Fall ist."

Was können Sie tun?

Datenlecks prüfen: Nutzen Sie kostenlose Dienste wie den Identity Leak Checker des Hasso-Plattner-Instituts oder den Identity Leak Checker des BSI, um zu erfahren, ob Ihre E-Mail-Adresse in bekannten Datenlecks aufgetaucht ist.

Ausweisdaten schützen: Versenden Sie niemals leichtfertig Kopien Ihres Personalausweises.

Bei Anlage eines neuen Nutzer-Accounts:

- Nutzen Sie starke Passwörter und einen Passwort-Manager.
- Verwenden Sie für jeden Dienst ein eigenes Passwort.
- Aktivieren Sie Mehr-Faktor-Authentisierung, wo möglich.
- Nutzen Sie unterschiedliche Nutzernamen auf unterschiedlichen Plattformen. So wird die Bildung eines Gesamtprofil über Sie erschwert.

Quellen:

- https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Cyber-Sicherheitslage/Methoden-der-Cyber-Kriminalitaet/Identitaetsdiebstahl/Schutzmassnahmen/schutzmassnahmen_node.html
- https://www.polizei-beratung.de/themen-und-tipps/gefahren-im-internet/identitaetsdiebstahl/
- https://datenschutz.hessen.de/datenschutz/internet-und-medien/umgang-mit-identitaetsdiebstahl

Passkeys – ein guter Passwort-Ersatz

Passwörter sind heutzutage problematisch. Für jede Plattform benötigt man (idealerweise) ein anderes Passwort. Diese Passwörter müssen unterschiedlich komplex sein und sich all diese Passwörter zu merken,

ist nur sehr schwer möglich. Daher ist die Nutzung von Passwort-Safes heutzutage verbreitet und kann auch empfohlen werden. Geraten die Passwörter dennoch in falsche Hände, reagiert man aber oft zu spät.

Was können Sie tun?

Mit Passwörtern kann man sich durch „Wissen“ bei einer Plattform anmelden. Passkeys ersetzen dies durch „Besitz“. Sie sind kleine Geräte, die man per USB oder NFC mit PC, Tablet oder Smartphone koppeln kann. Hier ist der Faktor „Besitz“ das Sicherheitsmerkmal. Diese Geräte übernehmen – vereinfacht gesagt – die Passwort-Generierung und nur das eine Gerät, welches man in Besitz hat, kann das richtige Passwort generieren. Dafür wurde durch Verschlüsselungstechnologie und abgesicherte Hardware gesorgt. Wem also Passwörter zu umständlich sind, der kann auf Passkeys umsteigen. Aber Vorsicht: im Vorfeld muss man recherchieren, ob die Plattform, an der man sich anmelden möchte, Passkeys auch unterstützt. Weitere Informationen findet man unter https://www.bsi.bund.de/dok/1107470 .

Daten in der Cloud

Viele Bürger nutzen heutzutage Cloud Services: zum Speichern von E-Mails, Fotos oder Dokumente aber auch als Webdienste, die herkömmliche Software zum Schreiben von Text, Erzeugen von Bildern und Filmen oder sogar zum Anfertigen der Steuererklärung

ersetzen. Cloud Nutzung birgt aber auch Risiken: was passiert, wenn der Cloud-Dienst plötzlich nicht mehr erreichbar oder verfügbar ist? Was passiert mit meinen Daten in dieser Cloud noch? Wie sicher ist die Cloud gegenüber Fremdangreifern? Bei der Entscheidung, eine Cloud zu nutzen, sollten diese Punkte alle eine Rolle spielen.

Was können Sie tun?

Recherchieren Sie vor allem, wie vertrauenswürdig und zuverlässig der Dienst ist. Unabhängige Erfahrungsberichte helfen dort weiter. Auch ein Blick in die Datenschutzerklärung ist hilfreich, insbesondere welche Verarbeitungszwecke dort beschrieben sind und welche anderen Empfänger Ihrer Daten dort genannt werden. Auch sollten ähnliche Dienste miteinander verglichen werden. Recherchieren Sie außerdem, wo die Server des Cloud-Anbieters stehen. Ideal sind europäische Server. Haben Sie außerdem einen Plan B: im einfachsten Fall eine lokale Kopie der Daten in der Cloud, die in regelmäßigen Abständen aktualisiert wird. Ein paar ergänzende Tipps findet man außerdem hier: https://www.bsi.bund.de/DE/Themen/Verbraucherinnen-und-Verbraucher/Informationen-und-Empfehlungen/Cloud-Computing-Sicherheitstipps/Cloud-Risiken-und-Sicherheitstipps/cloud-risiken-und-sicherheitstipps_node.html.

2. Spezielle Tipps zu PCs

Zusätzlich zu den genannten Tipps kann man auf dem PC bzw. dem Laptop noch ein paar weitere Maßnahmen zur Datenvermeidung treffen:

Browserkennung verschleiern

Beim Aufruf sendet der verwendete Browser neben der Adressangabe (URL) auch seine Browserkennung. Dies ist teilweise notwendig, um speziell auf diesen Browser angepasste Versionen der Webseiten anzuzeigen. Außerdem werden Informationen, wie z.B. das genutzte Betriebssystem, übertragen. Angreifer könnten wegen dieser Information gezielt Schwachstellen in Browsern und Betriebssystemen ausnutzen.

Was können Sie tun?

Um diese Information etwas zu verschleiern, können Sie bspw. den User Agent Switcher (https://addons.mozilla.org/de/firefox/addon/user-agent-switcher-revived/) für Firefox installieren

oder für Chrome (https://chrome.google.com/webstore/detail/user-agent-switcher-for-c/djflhoibgkdhkhhcedjiklpkjnoahfmg).
Mit diesem Agenten können Sie nach außen die verwendeten Browser-Version „x“ schnell in einen anderen Browser, beispielsweise den Internet Explorer Version „y“ umwandeln, obwohl Sie tatsächlich immer noch mit Firefox oder Chrome surfen. Welche Browserversion Sie dabei senden wollen, können Sie bequem über einen Menüpunkt dieses Agenten steuern.
Für Microsoft Edge benötigen Sie kein Plugin, sondern können in den mitgelieferten Entwickler-Tools die nötigen Einstellungen vornehmen. Dazu muss im Menü (drei Punkte rechts Oben) unter „weitere Tools“ → „Entwicklungstools“ ausgewählt werden. Dann im neuen Unterfenster wieder im Menü (drei Punkte rechts oben) „weitere Tools“ → „Netzwerkbedingungen“ im Bereich „Benutzer-Agent“ den Haken entfernen, dass immer der Standard genutzt werden soll, und aus der Liste darunter einen anderen Browser auswählen (Details siehe https://windowsunited.de/anleitung-microsoft-edge-chromium-user-agent-umschalten/). Für Google Chrome ist das Vorgehen identisch.
Für Apples Safari Browser auf einem Mac muss über „Einstellungen“ → „Erweitert“ das Entwicklermenü eingeblendet werden (Häkchen ganz unter in den erweiterten Einstellungen). Danach kann über das Menü „Entwickler“ → „User-Agent“ ein beliebiger anderer Browser vorgegeben werden.

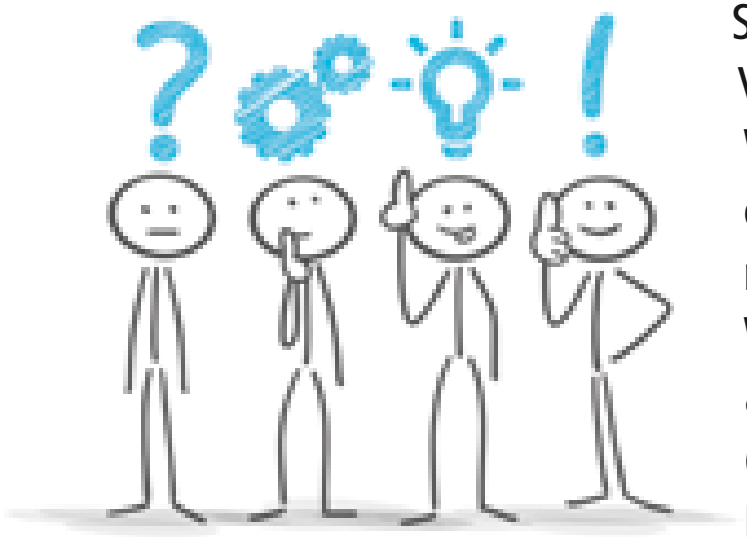
Zusätzliche Verschlüsselungsmöglichkeiten am PC

Es gibt allerdings noch weitere Kommunikationsarten, die durch eine Verschlüsselung geschützt werden können. Das Senden und Empfangen von E-Mails wäre solch ein Fall. Hier kann durch (auch frei erhältliche) Zusatzprogramme die Verschlüsselungsmöglichkeit nachgerüstet werden. Solche Programme können in der Regel die komplette E-Mail verschlüsseln oder nur Dateien, die dann an E-Mails angehangen werden können. Sie sollten darauf achten, dass Sie zur Verschlüsselung Programme verwenden, die Ende-zu-Ende verschlüsseln, d.h. das tatsächlich nur Absender und Empfänger den Inhalt einer Nachricht lesen können.

Was können Sie tun?

Wenn Sie beispielsweise über das Programm PGP, GnuPG oder GPG4Win verfügen, können Sie damit verschlüsselte Nachrichten senden und empfangen, die Ende-zu-Ende verschlüsselt sind. Ende-zu-Ende Verschlüsselung bedeutet, dass nur der Nachrichten-empfänger und Sie die Nachricht im Klartext lesen können. Alle weiteren, bei der Übertragung der Nachricht Beteiligten, sehen nur verschlüsselten Text und besitzen nicht die Möglichkeit, die Nachricht zu entschlüsseln. Diese Funktion sehen die Verschlüsselungsmöglichkeiten der gängigen freien E-Mail-Dienste nicht vor. Weitere Informationen zu PGP erhalten Sie unter

https://www.datenschutzzentrum.de/artikel/1177-Daten-verschluesselt-uebertragen-aber-wie.html#extended, zu GPG4Win https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Informationen-und-Empfehlungen/Freie-Software/E-Mail-Verschluesselung/GPG4Win/gpg4win_node.html und zu GnuPG unter https://www.bsi.bund.de/dok/11486410.
Die Nutzung dieser Programme erfordert meist etwas Erfahrung und Eingewöhnung. Lassen Sie sich aber dadurch nicht abschrecken, sondern trauen Sie sich! Das alles ist kein Hexenwerk. Wie unter „Sichere Kurznachrichten und Chats“ schon erwähnt, kann installierte Schadsoftware auch hier sämtliche Verschlüsselung unwirksam machen.



© *Matthias Enter – Fotolia*

Wer seine Daten auch auf der eigenen Festplatte verschlüsseln möchte, kann dazu bei speziellen Windows-Versionen (Windows Pro & Enterprise) Encrypting File System (EFS) und BitLocker nutzen und bei Linux LUKS).

Was können Sie außerdem tun?

Zum einen kann die oben erwähnte Software zur E-Mail Verschlüsselung auch zur Verschlüsselung von einzelnen Dateien und Ordnern auf dem Rechner genutzt werden. Auch sollte man

vom Betriebssystem bereitgestellte Verschlüsselungsmechanismen nutzen, falls diese vorhanden sind (z.B. für Windows BitLocker und EFS, für Linux LUKS). Zusätzlich zu den von Betriebssystemen bereitgestellten Verschlüsselungswerkzeugen können auch quelloffene Hilfsprogramme wie VeraCrypt oder dm-crypt genutzt werden, um verschlüsselte Datenbereiche auf sonst unverschlüsselten Dateisystemen zu erzeugen (siehe https://www.bsi.bund.de/DE/Themen/Unternehmen-und-Organisationen/Standards-und-Zertifizierung/IT-Grundschutz/it-grundschutz_node.html, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/IT-GS-Kompendium_Einzel_PDFs_2022/07_SYS_IT_Systeme/SYS_2_1_Allgemeiner_Client_Edition_2022.pdf?__blob=publicationFile&v=3).

Absicherung des PCs

Um zu verhindern, dass Schadsoftware auf Ihren PC gelangt, sollten Sie unbedingt folgende zusätzliche Maßnahmen ergreifen:

Was können Sie tun?

Benutzen Sie immer aktuelle Antiviren-Programme und Firewalls. IT-Fachzeitschriften bieten Ihnen – auch online – in der Regel eine Übersicht bekannter Antiviren-Programme, die meist kostenlos zur Verfügung stehen. Dies ist auch deshalb notwendig, da es noch keinen effektiven Schutz vor Viren auf Smartphones gibt (siehe

Daten verschlüsseln) und evtl. infizierte Smartphone an den PC angeschlossen werden könnten. Ebenso sollten Sie darauf achten, immer die neusten Sicherheitsupdates vom Antiviren-Programm, vom Betriebssystem, vom Browser und den weiteren installierten Programmen durchgeführt zu haben. Mit ClamAV ist seit 7 Jahren ein Open-Source Virenscanner verfügbar, der seit 2022 auch in der Version 1.0 nun das Entwicklungsstadium verlassen hat. Der Virenscanner ist sowohl für Windows als auch für Linux und Mac verfügbar (siehe https://www.clamav.net/).

Was können Sie außerdem tun?

Auch von E-Mail-Anhängen oder von in E-Mails enthaltenen Links kann Gefahr ausgehen. Werden hier beispielsweise unerwartete Lieferungen angekündigt oder sind Rechnungen und Mahnungen enthalten, obwohl Sie diese nicht erwarten, so ist das Risiko groß, dass Schadsoftware enthalten ist oder durch Klicken auf einen Link auf den PC dann geladen wird. Aktivieren Sie die Links bzw. Anhänge nicht.

Was können Sie außerdem tun?

Standardmäßig hat Ihr PC in der Regel nur ein Benutzer-Konto. Dieses ist auch mit vollen Administrationsrechten ausgestattet. Sie sollten ein zusätzliches Nutzerkonto ohne Administratorrechte einrichten und dieses während der täglichen Arbeit nutzen. Ein Administrator-Nutzer

kann Systemeinstellungen ändern, Programme installieren und hat sehr weitreichenden Zugriff auf Systemdateien. Daher kann eine Software, in dem Moment, in dem Sie mit Administrationsrechten am Rechner angemeldet sind, im Hintergrund Schadsoftware ohne Ihr Wissen tief im System installieren. Die Software besitzt bei der Installation immer die Rechte des angemeldeten Nutzers. Wird diese Software durch einen Nicht-Administrator ausgeführt, so ist auch ihr Schadenspotential auf die Rechte dieses Nutzers beschränkt. Wie Sie unter Windows einen Nutzer ohne Administratorrechte anlegen, erfahren Sie unter https://support.microsoft.com/en-us/windows/add-or-remove-accounts-on- your-pc-104dc19f-6430-4b49-6a2b-e4dbd1dcdf32. Wie dies unter macOS funktioniert, erfahren Sie unter https://support.apple.com/de-de/guide/mac-help/mchl3e281fc9/mac. Die notwendigen Einstellungen finden Sie in der Regel unter der Hilfe Ihres Betriebssystems (Stichwort: Benutzerverwaltung / Benutzerkonto). Sollten an Ihrem Rechner weitere Personen arbeiten, so richten Sie für Diese weitere eigene Nutzerkonten ohne Administratorrechte ein. So kann das Risiko der Ausbreitung von Schadsoftware verringert werden.

Windows 10 / Windows 11

Windows 11 ist das derzeit aktuelle Betriebssystem von Microsoft und löst Windows 10 ab. Windows 10 ist durch Microsoft um zahlreiche Dienste, wie einen Sprachassistenten, eine Cloud-Anbindung oder eine Standortermittlung erweitert worden, um auch den heutigen

Standards der mobilen Betriebssysteme zu entsprechen. Ursprünglich gab es hier wenig manuelle Einstellmöglichkeiten zu diesen Datenströmen, welche aber mittlerweile besser konfigurierbar sind.

Was können Sie tun?

Lesen Sie die Bestimmungen zum Datenschutz (https://privacy.microsoft.com/en-us/privacystatement) sorgfältig durch. Dort werden die erhobenen Daten und ihr Verwendungszweck beschrieben. Wie Sie einige grundlegende Einstellungen in den Windows Versionen Windows 11/10 Home und Windows 11/10 Pro verändern können, finden Sie z.B. bei https://support.microsoft.com/de-de/windows/%C3%A4ndern-der-datenschutzeinstellungen-in-windows-55466b7b-14de-c230-3ece-6b75557c5227 zusammengefasst. Für die datenschutzgerechte Konfiguration von Windows 10 Enterprise hat das Bayerische Landesamt für Datenschutzaufsicht (BayLDA) einen ausführlichen Report der dazu notwendigen Gruppenrichtlinien unter https://www.lda.bayern.de/media/windows_10_report.pdf veröffentlicht (Kap. 1.1, 2.1, 3.1), welcher mittlerweile schon älter ist, sowie der Dokumentation von Microsoft selber unter https://learn.microsoft.com/en-us/windows/privacy/manage-connections-from-windows-operating-system-components-to-microsoft-services.

Daten sicher löschen

Auch die Datenlöschung gehört zur digitalen Selbstverteidigung. Sollten Sie Ihren alten PC verschrotten oder verkaufen, so können andere, Ihnen unbekannte Personen relativ einfach auf diese Daten zugreifen. Dies gilt auch für ausgemusterte mobile Datenträger wie z.B. CDs, DVDs, USB-Speichersticks, SD-Karten und externe USB-Festplatten.

Was können Sie tun?

Für gebrannte CDs und DVDs gibt es besondere Schredder, die die Datenträger zerkleinern. Haben Sie so etwas nicht, können Sie die CDs und DVDs auch auf der Datenseite mit Sandpapier zerkratzen und die Scheibe dann in möglichst viele kleine Teile zerbrechen. Dann können die Daten nur noch mit Spezialausrüstung gelesen werden. Daten auf USB- Sticks und mobilen Festplatten sind schwerer zu löschen. Auf keinen Fall reichen normale Löschbefehle des Betriebssystems oder das Verschieben in den Papierkorb aus, die Daten auch tatsächlich unwiederbringlich zu löschen. In beiden Fällen können die Daten recht einfach durch Software wiederhergestellt werden. Das Formatieren der Datenträger hilft auch nur bedingt, da häufig einfach neue Verwaltungsinformationen über die alten geschrieben werden und die tatsächlichen Daten noch vorhanden sind. Um softwareseitig diese Laufwerke zu löschen, ist Zusatzsoftware wie z.B. „Active@ KillDisk“, „DiskWipe“ oder „BleachBit“ notwendig – um ein paar

kostenlose Tools zu nennen. Hier gibt allerdings auch der Entwickler keine endgültige Garantie, ob die Daten tatsächlich nicht mehr wiederherstellbar sind. Gerade bei der neuen Generation von Festplatten, sog. Solid-State- Drives (SSDs) kann der PC evtl. nicht auf alle physikalisch vorhandenen Datenbereiche zugreifen, sodass es dort erst recht keine Garantie für eine endgültige Löschung gibt. Daher sollten Sie im Zweifel die Datenträger immer physisch zerstören (Durchbohren, Verbiegen, Zerschmettern, Schreddern). Wägen Sie den Geldgewinn durch Weiterverkauf gegen den potentiellen Schaden gut ab. Wollen Sie den gesamten Inhalt des PCs oder Laptop vor dem Weiterverkauf löschen, können Sie dies nicht im normalen Betrieb tun. Daher muss das Löschen ein separates Betriebssystem übernehmen. Auf den Seiten des Bundesministeriums für Sicherheit in der Informationstechnik (BSI) finden sich Hinweise (https://www.bsi.bund.de/dok/6599236) zur Nutzung von Software, welche jeweils von einem separaten Datenträger (z.B. USB-Stick) ausgeführt werden müssen. Unter diesem Link finden Sie auch weitere nützliche Hintergrundinformationen zum Löschen. Moderne Betriebssysteme wie Windows 10 und 11 bieten auch die Option an, das System sicher zurückzusetzen. Die notwendigen Schritte finden in der Regel unter der Hilfe Ihres Betriebssystems (Stichwort: Wiederherstellung). Wichtig ist, dass während des Zurücksetzens nicht die Option der „schnellen Datenlöschung“gewählt wird, sondern der „vollständigen Datenlöschung“. Aber auch hier gilt: im Zweifel lieber den Datenträger vernichten und auf den Erlös verzichten.

3. Spezielle Tipps zum Smartphone

Zugang zum Smartphone sichern

Damit Ihr Smartphone oder Tablet nicht ohne Ihre Zustimmung von anderen genutzt werden kann und auch im Falle eines Diebstahls oder Verlusts geschützt ist, sollten Sie möglichst den Zugriff auf Ihr Gerät absichern.

Was können Sie tun?

Smartphones bieten in der Regel unterschiedliche Funktionen zur Zugriffskontrolle an. Nutzen Sie diese! Jedes Gerät kann durch eine PIN oder ein Passwort geschützt werden. Häufig sind auch Wischgesten oder biometrische Erkennungen möglich. Bei der Zugriffssteuerung mit PIN sollten Sie mindestens 8 Ziffern verwenden. Ein Passwort aus Buchstaben und Zahlen ist aber noch sicherer. Die Freigabe per Muster oder biometrischen Merkmalen (Fingerabdruck, Gesichtserkennung oder Augenscan) sind zwar bequem, aber haben oft Schwachstellen. Alternativ sind auch biometrische Merkmale (Gesicht, Fingerabdruck) zur Freischaltung üblich, was von der Sicherheit ungefähr eine 4-5-stelligem Code entspricht (Ausnahmen

gelten hier für Personen des öffentlichen Lebens, bei welchen leicht Fälschungen der Merkmale anzufertigen sind). Mittlerweile sind diese Merkmale in besonders gesicherten Speicherbereichen der Smartphones abgelegt, sodass diese nicht einfach ausgelesen werden können und als sicher gespeichert gelten können. Zusätzlich muss aber immer noch eine PIN oder ein Passwort eingerichtet werden. Wie dies auf Geräten von Apple funktioniert, finden Sie unter https://support.apple.com/de-de/HT204060. Die Anleitungen für das aktuelle Android-Betriebssystem (ab Version 10) finden Sie bei https://support.google.com/android/answer/9079129?hl=de. Bitte beachten Sie, dass die Einstellungsmöglichkeiten bei Android-Geräten durch den Hersteller variieren können.

Smartphones und Schadsoftware

Sie kennen sicher Virenscanner für PCs.
Auch für Smartphones gibt es heutzutage Software, die vorgibt, Dateien auf Viren untersuchen oder das Smartphone vor Schadsoftware schützen zu können. Durch die spezielle Architektur der App-Ausführung kann allerdings kein dem PC vergleichbarer Schutz hergestellt werden (siehe https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Lageberichte/Lagebericht2017.pdf?__blob=publicationFile&v=3, Seite 16 ff.), sodass die Wirksamkeit dieser Virenscanner-Apps bezweifelt werden muss und nur für definierte Bereiche anwendbar ist.
Das komplette Smartphone kann durch die Software nicht überprüft

werden. Dennoch gibt es Software, die durch Regelwerke spezielle Prüfungen durchführen kann, eventuelle Bedrohungen identifizieren kann und in zugänglichen Bereichen (z.B. dem Browser) nach Viren und Bedrohungen sucht. Oft wird die Schadsoftware allerdings bereits mit einer App aus dem App-Store ausgeliefert. Hierzu kann keine wirksame Gegenmaßnahme empfohlen werden.

Was können Sie tun?

Installieren Sie daher nur Apps, die Sie wirklich benötigen und von App-Stores, die Sie kennen. Lesen Sie die Bewertungen in den App-Stores und prüfen Sie, ob es sich tatsächlich um den echten Anbieter handelt. Installieren Sie Apps als Einzeldateien (sog. APK-Files), wie sie manchmal als Download angeboten werden, nur, wenn Sie genau wissen was Sie tun und die Quelle vertrauenswürdig ist.
Diese Dateien werden durch niemanden kontrolliert und können auch modifiziert sein, d. h. einen Schadcode enthalten.
Hilfreich ist auch, die Fachliteratur zu lesen und dort kritisch eingeschätzte Apps oder nicht mehr benötigte Apps wieder zu deinstallieren. Wenn Sie Apps zur Verbesserung der Sicherheit Ihres Smartphones suchen, finden Sie eine Übersicht hier: https://www.av-test.org/de/antivirus/mobilgeraete/ und auf https://mobilsicher.de/hashtag/virenscanner.

Daten verschlüsseln

Heutzutage werden die Daten auf dem Smartphone meist automatisch verschlüsselt und erst bei der Nutzung wieder entschlüsselt. Unter „Sichere Kurznachrichten und Chats“ wurde bereits auf die Verschlüsselungsmöglichkeit in Chats und Messenger hingewiesen, womit Sie Ihre Kommunikation schützen können. Wenn Sie Daten durch Apps in die jeweilige Cloud speichern, können diese auch verschlüsselt werden.

Was können Sie tun?

Nutzen Sie Programme wie „BoxCryptor“ oder „OpenPGP Keychain“ um Daten, die in der Cloud gespeichert werden sollen zu verschlüsseln. Leider ist auf dem Gebiet der mobilen Apps noch viel Arbeit zu tun, die meisten Apps sind im Cloudbereich nicht einschätzbar und können nicht bedenkenlos empfohlen werden. Lesen Sie sich die Kommentare und die Beschreibungen vor dem Gebrauch gut durch. Wollen

© kotoyamagami – Fotolia

Sie E-Mails verschlüsseln, gibt es zu diesem Zweck Apps wie z.B. „Symantec Mobile Encryption for IOS“. Apple hat seit iOS Version 16.2 die Möglichkeit geschaffen, Daten in der iCloud automatisch so zu verschlüsseln, dass auch Apple diese nicht mehr entschlüsseln kann (siehe https://support.apple.com/en-us/HT202303).
Diese Feature muss aber manuell aktiviert werden (siehe https://support.apple.com/de-de/HT212520).

Spezielle Datenspuren beim Smartphone vermeiden

Smartphones besitzen einige Sensoren, die ein PC üblicherweise nicht hat (Bewegungsmesser, Standortlokalisierung). Über diese Sensoren und der Fähigkeit der drahtlosen Vernetzung können Bewegungsprofile erstellt werden. Daher bedarf es noch einiger Maßnahmen zur Datenvermeidung, die speziell für Smartphones gelten:

Was können Sie tun?

Aktivieren Sie Standortlokalisierung, Bluetooth und WLAN nur bei Bedarf. Hier kann sonst durch die direkte Standortmessung bei GPS bzw. die Kennung des Smartphones in Netzwerken ein Bewegungsprofil angelegt werden. Dies gilt auch dann, wenn das Smartphone nicht in einem WLAN angemeldet oder per Bluetooth mit einem anderen Gerät verbunden ist.

Sind Bluetooth oder WLAN aktiv, suchen diese im Hintergrund ständig nach neuen Netzwerken, in welche Sie sich evtl. einklinken können. Auch dieser Vorgang hinterlässt Datenspuren. So kann der Weg einer Person durch ein Kaufhaus z.B. nur aufgrund der „durchlaufenen" WLANs oder Bluetooth-Netze rekonstruiert werden.

Was können Sie außerdem tun?

Bei einigen (auch moderneren) Android Versionen „lauschen" manche Programme und Dienste auch nach Abschalten des WLANs weiterhin nach Netzwerkkennungen. Um diese Funktion zu deaktivieren, müssen Sie z.B. unter „Einstellungen" → „WLAN" → Symbol: drei Punkte (meistens in der rechten oberen Bildschirmecke) → „Erweitert" → „Suche immer erlauben" bzw. „Scannen immer verfügbar" deaktivieren.

Was können Sie außerdem tun?

Prüfen Sie, welche Daten von einer App überhaupt angefordert werden und ob diese zum Betrieb der App notwendig sind. Diese Informationen finden Sie z.B. bei Android-Smartphones vor der Installation im Google Play Store unter „App-Info“ → „App-Berechtigungen“ → „Weitere Informationen“. Dort gibt es auch Kurzbeschreibungen, was die einzelnen Berechtigungen bedeuten, da die verwendeten Begriffe nicht immer für sich sprechen. Unter iOS (Apple-Geräte) ist die Herangehensweise eine andere. Nach der Installation besitzt die App keine speziellen Rechte und darf gerade mal das Internet nutzen oder lokal Daten speichern. Sowohl bei aktuellen Android-Geräten, als auch bei iOS- Smartphones werden spezielle Rechte, wie der Zugriff auf das Adressbuch oder die Standortlokalisation, beim ersten Gebrauch abgefragt. Hier sieht man also, welche Nutzeraktion dazu führt, dass die Daten benötigt werden und muss nach der Situation entscheiden, ob dies in diesem Fall sinnvoll erscheint. Prüfen Sie auch die Datenschutzerklärungen des App-Anbieters. Hier sind häufig Erklärungen zu finden, warum bestimmte Daten notwendig sind. Die Datenschutzerklärungen sind häufig nur im App-Store selber zu finden und selten Bestandteil der App. Sollten Ihnen Berechtigungen merkwürdig erscheinen, z.B. wenn eine Taschenlampen-App SMS versenden können will oder das Adressbuch benötigt, recherchieren Sie im App-Store nach alternativen Apps, die eine ähnliche Funktion „ohne Nebenwirkungen“ bieten.

Ebenso kann der Datentransfer von Apps im Hintergrund eingeschränkt werden. Wenn Apps nicht im Vordergrund sind (d.h. auf dem Bildschirm offen), können sie im Hintergrund dennoch Aktivitäten entfalten und so z.B. Standortdaten weitersammeln. Manchmal macht dies Sinn, häufig aber nicht. Um diese Aktivitäten im Hintergrund zu blockieren, gibt es sowohl für Android-Systeme Möglichkeiten (siehe https://www.kuketz-blog.de/hintergrundaktivitaet-von-android-apps-einschraenken-digitaler-schutzschild-teil10/) also auch für iOS (siehe https://communities.apple.com/de/thread/251444315).

Daten sicher Löschen

Daten auf einem Smartphone sicher zu löschen ist schwierig. Einige Daten sind auf der SIM- Karte des Smartphones gespeichert und verschwinden, nachdem die Karte entfernt wurde. Speziell auf Smartphones sind das allerdings sehr wenige Daten. Kontakte, E-Mails, Kurznachrichten und Bilder liegen im Speicher des Gerätes selbst und können von dort auch nur mit den Systemaufrufen des Geräts gelöscht werden – im Zweifel sind die Daten also wiederherstellbar. Auch wenn dies einem Löschen nicht gleichkommt, kann man aber die Verschlüsselung der Daten nutzen, um unerlaubten Zugang zu verhindern.

Was können Sie tun?

Aktivieren Sie die Verschlüsselung auf dem Gerät. Dadurch werden alle Daten verschlüsselt und ein Auslesen bringt zwar Daten hervor,

diese sind aber nicht ohne weiteres interpretierbar. Wie dies für Android-Geräte funktioniert finden Sie unter https://support.google.com/nexus/answer/2844831?hl=de und die Anleitung für iPhones finden Sie bei https://www.apple.com/de/business/docs/iOS_Security_Guide.pdf. Bevor Sie Ihr Gerät weiterverkaufen, löschen Sie manuell alle Bilder, Nachrichten, E-Mails usw. und deinstallieren Sie danach alle Apps (Anleitung für Android: https://support.google.com/googleplay/answer/2521768?hl=de und für Apple-Geräte: https://support.apple.com/de-de/HT201274). Im letzten Schritt setzten Sie das Smartphone auf die Werkseinstellungen zurück (Anleitung für Android: https://support.google.com/android-one/answer/6088915?hl=de, Apple-Geräte sind nach dem Löschen aller Daten schon zurückgesetzt). Auch hier gilt im Zweifel: eine physikalische Zerstörung löscht am besten. Beachten Sie jedoch, dass vorher der Akku des Gerätes entfernt werden muss. Wird der Akku bei der Zerstörung beschädigt, kann ein Brand oder gar eine Explosion entstehen.

4. Spezielle Tipps zu Smartwatches und Fitnesstrackern

Tragbare Technikartikel (Wearables), wie Smartwatches oder Fitnesstracker, sind im Trend. Fitnesstracker messen die Bewegung und oft auch den Puls des Trägers während Smartwatches, neben der Zeitanzeige, Zusatzfunktionen wie Erinnerungen und Benachrichtigungen anzeigen, aber mitunter auch den Puls und die Aktivität (Sitzen, Gehen, Laufen, Fahren) des Trägers messen können. Auch werden dabei häufig GPS-Koordinaten aufgezeichnet. Smartwatches gibt es mittlerweile, ähnlich wie Smartphones, von vielen Herstellern. Die Software basiert aber vor allen Dingen auf Android, „Wear OS“ genannt, oder auf einer Apple Lösung, „WatchOS“ genannt oder anderen Eigenentwicklungen (Fitbit OS, Garmin OS). In den allermeisten Fällen kommunizieren diese Geräte über Bluetooth oder WLAN mit Ihrem Smartphone, um die gesammelten Daten abzuspeichern oder empfangene Nachrichten anzuzeigen. Welche Smartwatch dabei mit welchem Smartphone-System kompatibel ist, entnehmen Sie bitte im Zweifel

der Beschreibung der Smartwatch. Zurzeit gilt, dass WatchOS ein iPhone mit iOS zur Kommunikation benötigt, während Wear OS mit Smartphones aus allen Welten genutzt werden kann. Besitzer einer Xiaomi, Fitbit oder Garmin Smartwatch können „mit beiden Welten“ kommunizieren.

© Helmut Spoonwood – Fotolia

Was geschieht mit den von der Smartwatch aufgenommenen Daten zur Aktivität und zum Puls?In der Regel sind die Daten nicht nur auf der Smartwatch gespeichert, sondern auch auf dem mit der Uhr gekoppelten Smartphone, um den Erfüllungsgrad von Trainingsprogrammen zu überwachen bzw. um dem Nutzer Tagesprofile zu seiner Aktivität anzuzeigen. Es gibt allerdings bereits Apps, welche die Gesundheitsdaten in deren Cloud speichern, z.B. Google Fit für Smartwatches mit Wear OS. Vorsicht: Einige Android- Smartwatches können bereits die Daten auch ohne das Smartphone direkt über WLAN in die Cloud laden. Die Gefahren sind bei der Nutzung von Gesundheits-Apps folgende: zum einen kann der Nutzer unbewusst oder ungewollt Daten an Google und Drittanbieter von Apps freigeben und zum anderen können die Daten auf dem Smartphone oder der Smartwatch durch Dritte eingesehen werden. Laut Spiegel (Ausgabe 50/2015, Seite 15) geben einige Gesundheits-Apps die vertraulichen Daten an bis zu 14 verschiedene Netzadressen weiter, im Durchschnitt sind es fünf. Apple gibt an, seit einiger Zeit keinen Zugriff auf Gesundheitsdaten (auch in der Cloud) mehr zu haben, sondern nur das Teilen von Daten mit anderen Nutzern zu erlauben (siehe https://support.apple.com/de-de/HT212629) und dann Dritten Zugriff auf die Daten zu erlauben, wenn der Nutzer explizit diese zu Forschungszwecken freigibt – aber nur in den USA (https://support.apple.com/de-de/HT213359).

Was können Sie gegen ungewolltes Hochladen der Daten tun?

Hier hilft vor allen Dingen, sich vor der Nutzung einer Gesundheits-App ausreichend zu informieren. Für das iPhone gibt es eine Schnittstelle, „HealthKit“ genannt, welche die Daten zentral auf dem iPhone speichert. Die Steuerung der Datenzugriffe geschieht durch die App „Health“. Durch eine weitere Schnittstelle, „ResearchKit“ genannt, können die Daten auch an Apple übermittelt werden. Die Dokumentation zu ResearchKit finden Sie für Standardnutzer https://www.apple.com/de/researchkit/ und für tiefgreifendere Informationen für Entwickler https://support.apple.com/de-de/guide/iphone/iph5ede58c3d/ios In jedem Fall kann der Nutzer pro App entscheiden, welche Daten von welcher App einsehbar sind (https://www.apple.com/de/ios/health/). Die Datenverarbeitung auf Android Smartphones ist meist App-basiert und nutzt nicht unbedingt, wie unter iOS auf iPhones, eine gemeinsame Basis zur Datenverwaltung. Hier muss der Nutzer pro Hersteller und eingesetzter App selbst recherchieren, was mit den aufgenommenen Daten passiert, wo diese gespeichert sind und an wen diese Daten eventuell übertragen werden. Apps (auf der Smartwatch oder dem Smartphone), welche Google Fit benutzen, können über die Einstellung von Google-Fit (https://support.google.com/accounts/answer/6098255?hl=de) die Erlaubnis zum Zugriff auf die Daten gewährt oder entzogen werden. In jedem Fall landen die Fitnessdaten auf Ihrem Google-Fit Konto

in der Cloud. (Zitat aus der Hilfe zu den Einstellungen: „Sobald sie [Anm. d. Red.: die App] die Erlaubnis hat, kann eine mit Google Fit verbundene App von jedem Gerät aus auf Informationen in Ihrem Google Fit-Konto zugreifen.“) In diesem Fall können Sie also nichts gegen das Hochladen der Daten tun.

Was können Sie gegen unberechtigten Zugriff auf die Smartwatch tun?

Schützen Sie Ihre Smartwatch vor unberechtigtem Zugriff. Auf der Smartwatch ist dies ähnlich einfach wie bei Smartphones: für Android gibt es Apps, die diese Funktion übernehmen (siehe App „Showear“), die Apple Watch fragt bereits bei der Inbetriebnahme, ob eine 4-stellige Pin zum Sperren genutzt werden soll. Nutzen Sie diese Option. Wird die Apple Watch vom Handgelenk entfernt, sperrt sie sich automatisch. Auch WearOS bietet die Möglichkeit, eine PIN festzulegen (siehe https://support.google.com/wearos/answer/9248353?hl=de&co=GENIE.Platform%3DAndroid) und auch Geräte von Garmin (siehe https://support.garmin.com/de-DE/?faq=oV4SrjEVTv457Qe4slSge5) und Fitbit (siehe https://help.fitbit.com/articles/de/Help_article/2250.htm) unterstützen das Feature.

5. Spezielle Tipps zum Smart-Home

Smarte Geräte im Haushalt erfreuen sich immer größerer Beliebtheit. Neben Smartphones, Tablets und herkömmlicher PCs sind auch diese Geräte voll vernetzte Rechner. Getarnt als Haushaltsgeräte, Glühbirnen, Lautsprecher usw. werden diese Geräte aber häufig nicht als Computer wahrgenommen und die Gefahren dieser Geräte für die eigene Privatsphäre somit unterschätzt.

Smart-Home Steuerung

Bereits seit einiger Zeit sind Steuerungen von Licht, Heizung, Schlössern, Rollos, Steckdosen, Staubsaugerroboter usw. Stand der Technik. Meist können diese Geräte in einer Hersteller-App genutzt werden oder (besser) in ein einheitliches Framework eingebunden werden. Häufig geschieht dies über WLAN und die Geräte können dadurch auch direkt aus dem Internet angesprochen werden.
Nur wenige sind ausschließlich lokal über Bluetooth oder ZigBee ansprechbar. Fast immer gibt es für Geräte im Haus oder der Wohnung eine zentrale Steuereinheit, welche wiederum über das Internet ansprechbar ist. Nutzern ist selten bewusst, dass die Apps dabei über einen zentralen Server mit den Geräten kommunizieren.

Diese Architektur bietet einige Angriffspunkte, welche von Nutzern beachtet werden sollte (siehe https://tarnkappe.info/artikel/datenschutz/google-nest-gehackt-wenn-hacker-das-eigene-zuhause-uebernehmen-37612.html, https://nvd.nist.gov/vuln/detail/CVE-2018-6692).

Was können Sie tun?

Achten Sie darauf, dass alle Geräte regelmäßig Firmware-Updates bekommen und spielen Sie diese ein. Überlegen Sie, ein Gerät auch wieder zu entfernen, wenn der Hersteller keine Softwareaktualisierung mehr anbietet. Wenn möglich, achten Sie darauf, dass die Steuerung auch lokal funktioniert (d.h. auch ohne Internetverbindung in das Haus oder die Wohnung). Hilfreich ist hier der neue Standard für Haus-Automation mit dem Namen „Matter“ (siehe https://en.wikipedia.org/wiki/Matter_(standard)). Dieser erlaubt es, Geräte rein lokal über ein oder mehrere Admin-Geräte zu steuern (siehe https://www.consumerreports.org/smart-home/matter-smart-home-standard-faq-a9475777045/), so dass kein Zugang der Geräte ins Internet mehr nötig ist. Wer will, kann die Geräte damit für Internetzugriffe komplett sperren – dadurch sind diese aber auch „außer Haus“ nicht mehr ansprechbar. Neben Matter gibt es noch weitere Protokolle, welche auch ausschließlich lokale Nutzung zulassen (ZigBee). Hier muss jeder Nutzer aber nach wie vor im Vorfeld Informationen zum Betrieb von Steuerungs- Hub und vernetzten Geräten einholen.

Smarte Kameras

Zur Überwachung von Wohnräumen oder als Ersatz von Türspionen werden vermehrt auch „smarte Kameras" eingesetzt. Die Preise für solche Geräte sind stark gefallen, was auch zur zunehmenden Verbreitung von Kameras im privatem Umfeld beiträgt. Sowohl für Betroffene (gefilmte) als auch für Betreiber sei an dieser Stelle kurz gesagt, dass die Überwachung von öffentlichem Raum fast nie zulässig ist (siehe https://www.datenschutzkonferenz-online.de/media/oh/20200903_oh_v%C3%BC_dsk.pdf, Kap. 5.2 und 5.6). Aber auch bei der Überwachung des eigenen Grundstücks sind zahlreiche rechtliche Rahmenbedingungen zu beachten (siehe Link vorher). Der Fokus liegt hier aber nicht zu sehr auf der Rechtsproblematik. Vielmehr ist zu beachten, dass sehr viele Haus-Kameras, die per WLAN oder LAN an das Internet angeschlossen sind, die Aufnahmen über einen zentralen Server auf das Smartphone liefern. Dies ermöglicht es Angreifern, auf die Videodatenströme zuzugreifen. Ein Beispiel vom Dezember 2022 kann man hier nachlesen: https://www.heise.de/news/Eufys-Kameras-funken-ungefragt-in-die-Cloud-und-sind-per-Web-zugaenglich-7358310.html. Anstelle des gefühlten Sicherheitsgewinnes haben Nutzer durch den Einsatz von Kameras genau das Gegenteil erreicht. Und Einzelfälle sind das nicht (siehe https://www.heise.de/security/meldung/Der-Hacker-im-Schlafzimmer-Amazons-Ring-Kameras-werden-massenhaft-gehackt-4617254.html).

Was können Sie tun?

Überlegen Sie sich genau, ob ein smarte Kamera tatsächlich nützlich ist. Was wollen Sie damit detektieren und ist das realistisch und sinnvoll (oft sind Gesichter aus der Aufnahmeposition nämlich gar nicht erkennbar oder die Lichtverhältnisse machen Aufnahmen unbrauchbar)? Prüfen Sie, ob Kameras lokal Bilddatenströme liefern (z.B. indem Sie das WLAN vom Internet trennen – dann sollte die Kamera dennoch funktionieren). Leider ist dies dann kein Beweis, dass die Kamera NUR lokal Bilddaten abliefert (siehe den Fall Eufy vom Dez. 2022). Falls Ihnen das möglich ist, sperren Sie der Kamera den Zugang zum Internet. Spielen Sie die neueste Firmware auf (geht meist über eine App) und sichern Sie den Zugriff auf die Kamera möglichst mit 2-Faktor-Authentifizierung. Verwenden Sie Kameras nur an Orten, an denen es unschädlich ist, wenn Dritte Zugriff auf die Videodaten erlangen. Im Zweifel verzichten Sie lieber auf den Einsatz von Überwachungskameras.

Sprachassistenten

Sprachassistenten wie Alexa, Siri, Hello-Google und Cortana finden sich in allen neuen Smartphones, in smarten Lautsprechern oder Terminals sowie zunehmend in Haushaltsgeräten wieder. Den Assistenten ist gemeinsam, dass ein Kommandowort erkannt wird und danach das gesprochene Kommando verstanden und ausgeführt werden muss. Die Erkennung des Kommandowortes

passiert noch auf dem Gerät, Dazu muss das Mikrofon dauerhaft aktiv sein. Aber die Spracherkennung und Sinn-Interpretation wird auf Servern der Hersteller durchgeführt. Nur Apple verlagert einige der Funktionen nun auf Nutzergeräte. Bei der Kommandoerkennung und -interpretation werden Audioaufnahmen an Server der Hersteller geschickt, um die Funktion sicherzustellen. So landen sehr viele Sprachaufnahmen auf Servern der Hersteller. Natürlich sind dies nicht nur Sprachkommandos. Es kann fälschlicherweise ein Kommandowort erkannt werden oder durch Radio, Fernsehen usw. wird das Kommandowort gesagt. Weiterhin können auch Hintergrundgeräusche mit übertragen werden: kurz – es ist durch den Nutzer schwer zu steuern, was genau an die Hersteller von Sprachassistenten an Daten geschickt werden. Bereits 2021 hat die EDSA (ein europäisches Steuerungsgremium der Datenschutzaufsichtsbehörden) daher Empfehlungen an die Hersteller gegeben, wie die Systeme idealerweise designt werden sollen (siehe https://edpb.europa.eu/system/files/2022-02/edpb_guidelines_202102_on_vva_v2.0_adopted_de.pdf). Für den Nutzer sind dabei nur sehr wenige Hinweise dabei, aber diese werden nun kurz zusammengefasst.

Was können Sie tun?

Stellen Sie sicher, dass Ihr Smart-Speaker seine Aktivität (passives Lauschen auf das Kommandowort) optisch signalisiert. Kaufen Sie Smart-Speaker, welche den Sprachassistenten (oder das Mikrofon) per Schalter oder Menü deaktivieren kann. Achten Sie darauf, dass ein

Sprachassistent auch ohne registrierten Nutzerzugang funktionieren kann. Prüfen Sie regelmäßig, welche Audio-Aufnahmen bereits vorhanden sind und durch den Hersteller verarbeitet wurden. Bei Amazon Echo-Geräten kann das beispielsweise in der Alexa-App durchgeführt werden (unter Einstellungen – Datenschutz – „Ihre Alexa-Daten verwalten - Sprachaufnahmen-Verlauf überprüfen). Es ist auch sinnvoll, die Daten möglichst kurz speichern zu lassen (Option „Sprachaufnahmen automatisch löschen“). Ob Daten bei Amazon dann tatsächlich gelöscht werden, kann man als Anwender nicht überprüfen. Einmal erfasste Aufnahme werden meist zur Qualitätsverbesserung und Profilbildung länger verarbeitet.

So nützlich Sprachassistenten im Haushalt sein könnten, die Menge an akustischen Informationen, die unbeabsichtigt aufgenommen und an den Hersteller übertragen werden, übersteigen unter Umständen die Menge an praktischen Funktionen. Die Nutzung eines unscheinbaren Mikrofons zu Hause sollte daher wohl überlegt sein. Seien Sie sich auch bewusst, dass Gäste und Kinder sich in Zimmern mit Sprachassistenten nicht so achtsam verhalten könnten. Informieren Sie ihre Besucher über die smarten Mikrofone und bieten Sie an, sie ggf. während des Besuchs zu deaktivieren.

6. Text- und Bildgeneratoren

Seit Anfang 2023 sind Textgenerator und Bildgeneratoren in der breiten Masse der Bevölkerung angekommen. Diese neuartigen Dienste können Aufgabestellungen verstehen und selbstständig umsetzen (z.B. „Schreibe einen Aufsatz über das Leben von Goethe“ oder „Zeichne ein Bild einer Katze im Stil des Expressionismus“). Für einige Alltagsaufgaben im Büro oder auch in der Schule sind diese Werkzeuge zweifelsohne sehr nützlich. Auch für kreative Arbeit können so sehr schnell erste Ergebnisse produziert werden. Allerdings haben Text- und Bildgeneratoren zwei Probleme: 1. können die Generatoren Inhalte völlig frei erfinden und 2. benötigen die Generatoren momentan noch so viel Rechenleistung, dass die Dienste bei großen Anbietern in Rechenzentren laufen. Es gibt nur sehr wenige Anwendungen (für Interessierte), welche tatsächlich auf eigenen Rechnern lauffähig sind. Damit werden alle Anfragetexte und auch die Antworttexte oder –bilder auf diesen Servern in Rechenzentren gespeichert. Die Unterhaltungen sind also nicht privat und nur in der

eigenen App sichtbar. Beispiele solcher Generatoren sind ChatGPT, Google Bard, Meta AI (nutzt Llama), Microsoft Copilot, Dall-E, Canva, Adobe Firefly, stability.ai Stable Assistant und viele mehr.

Was können Sie tun?

Für das erste Problem (Inhalte können frei erfunden sein) hilft im Moment nur der gesunde Menschenverstand. Prüfen Sie Aussagen durch Belege aus zuverlässigen Quellen. Wenn Bildinhalte im Internet auftauchen, denken Sie an die Möglichkeit, dass diese frei erfunden/ generiert sind. Die Technik ist mittlerweile so gut, dass Plagiate oder frei erfundene Inhalte auf den ersten Blick oder auch bei intensiver Prüfung gar nicht mehr als frei generierte Inhalte erkennbar sind. Beim zweiten Problemfeld gilt: erzähle dem Server nichts, was man nicht auch seinem Bürgermeister erzählen würde. Krankengeschichten, eigene Ängste, Geldsorgen usw. sollten keinem Chatbot / Generator mitgeteilt werden. Zurzeit ist auch den Datenschutz-Aufsichtsbehörden unklar, was bei verschiedenen Diensten mit den generierten Daten oder den Nutzer-Eingaben eigentlich geschieht und wie lange diese gespeichert werden.

Fortsetzung folgt.

Impressum

Die verallgemeinernden Personenbezeichnungen in diesem Bericht gelten aus Gründen der Lesefreundlichkeit der Texte jeweils in der männlichen und weiblichen Form.

12. Auflage, Aktualisierung 05/2026

Titelbild: © ls_pictures – Fotolia

Herausgeber: Thüringer Landesbeauftragter für den Datenschutz
und die Informationsfreiheit
Häßlerstraße 8, 99096 Erfurt
Postfach 900455, 99107 Erfurt
Telefon: 0361-573112900
E-Mail: poststelle@datenschutz.thueringen.de
Internet: www.tlfdi.de

Druck: DRUCKEREI WITTNEBERT
Inh. Ulrich Janzen e. K.
Magdeburger Allee 79, 99086 Erfurt
Telefon: 0361-7467190, Telefax: 0361-7467191
E-Mail: Wittnebert@t-online.de