TLfDI

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

Digitale Selbstverteidigung

Sehr geehrte Damen und Herren,
liebe Kinder, Jugendliche, Erwachsene, Eltern und Senioren,

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. Bei Fragen allgemein zum Datenschutz wenden Sie sich bitte an Ihren TLfDI, natürlich auch bei Fragen und Anregungen zu dieser Broschüre. 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!

Dr. Lutz Hasse, TLfDI

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 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 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.heise.de/tr/artikel/Face-Mit-dem-Gesicht-durch-die-Tuer-3888403.html). Auch können so (bei ausreichend hoher Bildauflösung) unter Umständen biometrische Merkmale Ihrer Person extrahiert werden. Eine nette Anekdote ist z.B. bei http://www.ccc.de/de/updates/2014/ursel nachzulesen.

Was können Sie außerdem tun?

Wo dies 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. Nähere Informationen dazu finden Sie auf https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKompendium/bausteine/ORP/ORP_4_Identit%C3%A4ts-_und_Berechtigungsmanagement.html unter ORP.4.A8 und ORP.4.A22.
Bei der nächsten Anmeldung lassen Sie Ihr Passwort dann einfach zurücksetzen. Auf den meisten Webseiten funktioniert dies, indem Sie den Link „Passwort vergessen" klicken und den dortigen Anweisungen folgen.

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 Browser-einstellungen selbst festlegen, ob man diese möchte oder nicht oder ob diese Daten von Zeit zu Zeit gelöscht werden. Wie, erfahren Sie bspw. auf https://www.datenschutz.rlp.de/de/themenfelder-themen/datenspuren-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 Webseiten beim Aufrufen der Webseite 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 Webseite. Gesetzte Cookies können aber auch von anderen Webseiten ausgewertet werden – Cookies sind also auch kleine Verräter bzw. Spione.

Was können Sie tun?

Im Browser kann man in den Browsereinstellungen ebenfalls das Speicherverhalten von Cookies aufgerufener Webseiten einstellen, z.B. ob Cookies in jedem Fall automatisch gespeichert werden, oder nur auf Nachfrage oder überhaupt nicht. Sinnvoll erscheint auch die Einstellung, die nach dem Beenden des Browsers, alle genutzten Cookies löscht. Denn spätestens wer online etwas kaufen möchte, wird 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.rlp.de/de/themenfelder-themen/datenspuren-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, Microsoft Internet Explorer: https://support.microsoft.com/de-de/help/17442/windows-internet-explorer-delete-manage-cookies, Microsoft Edge: https://support.microsoft.com/de-de/help/10607/microsoft-edge-view-delete-browser-history

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 „Privates Fenster“ aktiviert werden,
- im Internet Explorer unter „Einstellungen“

(oben rechts – Symbol: Zahnrad) im Unterpunkt „Sicherheit“→„InPrivate Browsen“ aktiviert werden,
- bei Google Chrome im „Menü“ (oben rechts – Symbol: drei Balken) unter „Neues Inkognitofenster“ aktiviert werden.

Verschlüsselungsmöglichkeiten von Webseiten

Die meisten Webseiten bieten heute schon eine verschlüsselte Datenübermittlung an. Dies bedeutet, die Verbindung vom Webseitenserver 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

© gena96 – Fotolia

Programm CryptoCat finden Sie hier: https://de.wikipedia.org/wiki/Cryptocat. Cpypto-Cat ist eine Browsererweiterung oder eine App für Smartphones, die eine Ende-zu-Ende verschlüsselte Kommunikation ermöglicht.
Aber wie gesagt, wenn Sie die Schadsoftware auf Ihrem Gerät haben, welche die Tastatureingaben und Bildschirminhalte mitliest, hilft auch dies 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, http://duckduckgo.com oder 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 Webseiten, 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“).

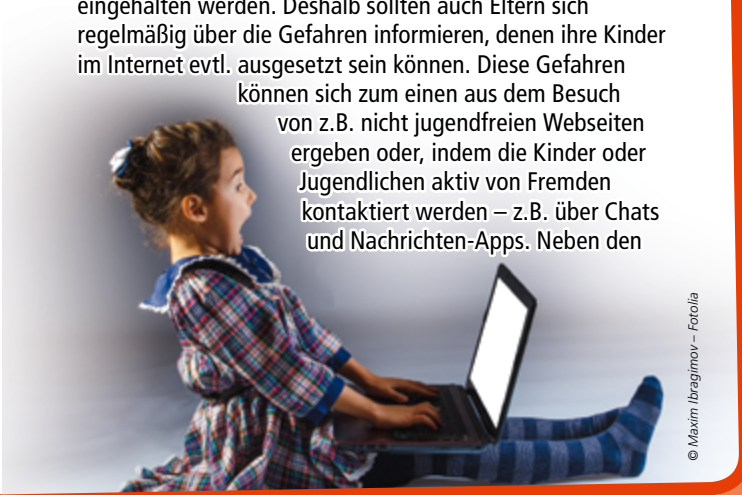
Was können Sie außerdem tun?

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 „Proxyserver konfigurieren" 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.

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 / Jugendlichen zu sexuellen Handlungen zu überreden.

Was können Sie tun?

Sensibilisieren Sie ihre Kinder. 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. http://www.polizei-praevention.de/themen-und-tipps/soziale-netzwerke-chats.html in den Abschnitten Addbörsen und Chaträume).

Was können Sie außerdem tun?

Nutzen Sie sichere Seiten für Ihre Kinder. Webseiten wie Frag-Finn (www.fragfinn.de) oder SWR-Kindernetz (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 missbraucht und die Leichtgläubigkeit und Unbedachtheit der Jugendlichen wird ausgenutzt.

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 (wieder http://www.polizei-praevention.de/themen-und-tipps/soziale-netzwerke-chats.html, diesmal die Abschnitte Sexting, AddBörsen und Chaträume). Außerdem sind Partnerbörsen auch nicht immer das, was sie zu sein scheinen (siehe Link http://www.heise.de/newsticker/meldung/Verdacht-auf-Abzocke-bei-Dating-Plattform-Lovoo-2821077.html und http://www.heise.de/ct/ausgabe/2015-22-Interne-Mails-bekraeftigen-Abzock-Verdacht-gegen-Dating-Plattform-Lovoo-2828167.html).

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. 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.
Soziale Netzwerke aber auch Online-Partnerbörsen werden gerne auch zum sog. „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. Dies 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 Twitter https://support.twitter.com/articles/334631, für Instagram https://help.instagram.com/116024195217477/ und für WhatsApp https://www.whatsapp.com/faq/de/android/23225461.

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.

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. Mit diesem Agenten können Sie nach außen den verwendeten Firefox Version x schnell in einen anderen Browser, beispielsweise den Internet Explorer Version y umwandeln, obwohl Sie tatsächlich immernoch mit Firefox Version x surfen. Welche Browserversion Sie dabei senden wollen, können Sie bequem über einen Menüpunkt dieses Agenten steuern. Für den Microsoft Internet-Explorer (ab Version 11) benötigen Sie keine zusätzliche Software. Hier müssen Sie im Menü (rechts oben – Symbol „Zahnrad“) die „F12 Entwicklertools“ auswählen und dann in dem neuen Fenster unter dem Punkt „Emulation“ → „Zeichenfolge des Benutzer-Agents“ von der Einstellung „Standard“ zum von Ihnen gewünschten Browser wechseln.

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. dass 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 Nachrichtenempfänger 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/Cyber-Sicherheit/Tools/Gpg4Win/gpg4win_node.html und zu GnuPG unter https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/Verschluesselung/EMail_Verschluesselung/In_der_Praxis/EMails_verschluesseln_in_der_Praxis_node.html.

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. Wer seine Daten auch auf der eigenen Festplatte verschlüsseln möchte, kann dazu bei speziellen Windows-Versionen (Windows Premium & 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/ITGrundschutz/ITGrundschutzKompendium/umsetzungshinweise/SYS/Umsetzungshinweise_zum_Baustein_SYS_2_1_Allgemeiner_Client.html, SYS2.1.M28).

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 – i. d. R. 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.

© Matthias Enter – Fotolia

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 bei http://windows.microsoft.com/de-de/windows/create-user-account#create-user-account=windows-7. Die notwendigen Einstellungen finden Sie in der Regel unter der Hilfe Ihres Betriebssystems (Stichwort: Benutzerverwaltung / Benuzterkonto). 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 10 ist das derzeit aktuelle Betriebssystem von Microsoft. Dieses Betriebssystem 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. Dabei fallen allerdings zahlreiche Datenströme an, die es in den vorhergehenden Versionen so noch nicht gab, siehe auch die Handreichung des TLfDI https://www.tlfdi.de/mam/tlfdi/themen/windows_10.pdf.

Was können Sie tun?

Lesen Sie die Bestimmungen zum Datenschutz (http://www.microsoft.com/de-de/privacystatement/default.aspx) sorgfältig durch. Dort werden die erhobenen Daten und ihr Verwendungszweck beschrieben. Wie Sie einige grundlegende Einstellungen in den Windows Versionen Windows 10 Home und Windows 10 Pro verändern können, finden Sie z.B. bei https://support.microsoft.com/de-de/help/4027945/windows-change-privacy-settings-in-windows-10 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).

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) findet sich (https://www.bsi-fuer-buerger.de/BSIFB/DE/Empfehlungen/RichtigLoeschen/richtigloeschen_node.html) die Empfehlung, dazu die ebenfalls kostenlosen Systeme DBAN oder PartedMagic zu nutzen, 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 8.1 und Windows 10 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 Zugangskontrolle an. Nutzen Sie diese. Entweder Sie verwenden z. B. ein sicheres Passwort (siehe Punkt „Datenvermeidung allgemein“), eine PIN oder Sie legen ein bestimmtes Muster fest, welches man auf dem Bildschirm zeichnen muss, um das Gerät nutzen zu können.
Wie dies auf Geräten von Apple funktioniert, finden Sie unter https://support.apple.com/de-de/HT204060. Die Anleitungen für das aktuelle Android-Betriebssystem (Version 6.0) finden Sie bei https://support.google.com/nexus/answer/2819522?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,

© kotoyamagami – Fotolia

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.

© dasdesign Fotolia

Was können Sie tun?

Installieren Sie daher nur Apps, die Sie wirklich benötigen und von App-Stores, die Sie kennen. Installieren Sie Apps als Einzeldateien (sog. APK-Files), wie sie manchmal als Download angeboten werden, nur, wenn Sie genau wissen was Sie tun. 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/.

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 Messengern 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 noch in einem experimentellen Stadium und können nicht bedenkenlos empfohlen werden.
Lesen Sie sich die Kommentare und die Beschreibungen vor dem Gebrauch gut durch.
Wollen Sie E-Mails verschlüsseln, gibt es zu diesem Zweck Apps wie z.B. „Symantec Mobile Encryption for IOS“.

Spezielle Datenspuren beim Smartphone vermeiden

Smartphones besitzen einige Sensoren, die ein PC üblicherweise nicht besitzt (Bewegungsmesser, GPS-Lokalisierung). 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 GPS, 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 „Weitere Informationen" → „Berechtigungen" → „Details ansehen". 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. Spezielle Rechte, wie der Zugriff auf das Adressbuch oder die Standortlokalisation, werden 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.

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.

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=en, 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 gibt es den Trend, zunehmend GPS-Koordinaten aufzuzeichnen. Smartwatches gibt es mittlerweile, ähnlich wie Smartphones, von vielen Herstellern. Die Software basiert aber vor allen Dingen auf Android, „Android Wear" genannt, oder auf einer Apple Lösung, „WatchOS" genannt oder der Eigenentwicklung von Pebble (Uhr). In den allermeisten Fällen kommunizieren diese Geräte über Bluetooth 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 und Android Wear ein Smartphone mit Android und einer speziellen App benötigen. Besitzer einer Pebble Smartwatch können „mit beiden Welten" kommunizieren. 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 Android Wear. 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 Gesundheitsapps folgende: zum einen kann der Nutzer unbewusst oder ungewollt Daten an Google, Apple 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 Gesundheitsapps die vertraulichen Daten an bis zu 14 verschiedene Netzadressen weiter. Der Schnitt lag bei 5.

Was können Sie gegen ungewolltes Hochladen der Daten tun?

Hier hilft vor allen Dingen, sich vor der Nutzung einer Gesundheitsapp 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 Dokumenation zu ResearchKit finden Sie für Standardnutzer http://www.apple.com/de/researchkit/ und für tiefgreifendere Informationen für Entwickler http://researchkit.org/. In jedem Fall kann der Nutzer pro App entscheiden, welche Daten von welcher App einsehbar sind (http://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

© Helmut Spoonwood – Fotolia

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 / das Smartphone tun?

Schützen Sie Ihr Smartphone vor unberechtigtem Zugriff wie in „Zugang zum Smartphone sichern“ beschrieben. Auf der Smartwatch ist dies ähnlich einfach: 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. Für die Pebble Smartwatch gibt es derzeit keine Möglichkeit, die Smartwatch zu sperren.

Fortsetzung folgt.

Impressum

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

7. Auflage

Titelbild: © ls_pictures – Fotolia

Herausgeber: Thüringer Landesbeauftragter für den Datenschutz
und die Informationsfreiheit
Häßlerstraße 8, 99096 Erfurt
Postfach 900455, 99107 Erfurt
Telefon: 0361-573112900, Telefax: 0361-573112904
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