Thüringer Allgemeine Erfurter Allgemeine vom 12.01.2019, Seite 3

Digitale Selbstverteidigung

So wie Sie Ihre Wohnung vor Einbrechern sichern, die Tür abschließen, vielleicht auch Gardinen aufhängen, so sollten Sie sich auch im Internet von Vorsicht leiten lassen

Von Kai Mudra

Erfurt. „Datenvermeidung ist das Mittel der Wahl, um seine Privatsphäre zu schützen, bis hin zu absoluter Anonymität." Das rät Lutz Hasse, Thüringens Landesbeauftragter für den Datenschutz, nachdem massenhaft persönliche Informationen über Politiker und Künstler veröffentlicht wurden. Seine Behörde hat einen Leitfaden mit Tipps für den täglichen sicheren Umgang mit Computern, Laptops, dem Tablet, aber auch dem Smartphone oder einem Fitnesstracker herausgegeben. Am Ende ist es aber immer Ihre Entscheidung, was Sie an Privatem preisgeben, um zu kommunizieren, sich darzustellen oder die zunehmenden Annehmlichkeiten der digitalen Welt zu nutzen.

Oberste Priorität: Datenvermeidung

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

- Prüfen Sie genau, welche Angaben beim Besuchen von Webseiten oder dem Nutzen von Leistungen im Internet wirklich nötigt und welche freiwillig sind.
- Überlegen Sie sich gut, welche Bilder Sie ins Netz stellen
- Wenn es erlaubt ist, nutzen Sie zur Anmeldung ein Pseudonym
- Nutzen Sie komplexe Passwörter mit mindestens acht unterschiedlichen Zeichen, bestehend aus Buchstaben in Groß- und Kleinschreibung, Zahlen und Sonderzeichen, aber keine Wörter
- Nutzen Sie, wenn möglich eine Zwei-Faktor-Authentisierung mit einem Passwort und einer zweiten Sicherheitsstufe, beispielsweise wenn Sie sich von einem fremden Gerät aus anmelden
- E-Mail-Anhänge nur öffnen, wenn Absender, Betreff und Mail-Text plausibel sind
- Achten Sie beim Nutzen von Bankverbindungen und Passwörtern darauf, dass die Webseite eine Verschlüsselung nutzt und der Link mit „https: //" beginnt
- Die Software des Betriebssystems der genutzten Computer und Mobilgeräte sollte regelmäßig über Updates des Hersteller aktualisiert werden
- Auch Antivirenprogramme sollten immer aktuell sein

Umgang mit einem Internet-Browser

Der Browser ist das Programm, mit dem Sie das Internet auf ihrem Computer oder Laptop, dem Smartphon oder dem Tablet aufrufen. Mit ihm beginnt bereits das Datensammeln. In seiner Chronik sind alle besuchten Internetseiten und Weblinks hinterlegt und können unter Umständen auch von anderen Webseiten abgerufen werden.

- Löschen Sie regelmäßig den Browserverlauf
- Gehen Sie vorsichtig mit Cookies um. Spätestens nach Beenden der Internetsitzung sollten im Browser alle genutzten Cookies gelöscht werden
- Aktivieren Sie dafür in den Browser-Einstellungen den „Privatmodus"
- Nutzen Sie Möglichkeiten, anonym im Internet zu surfen
- Das Verschicken von Nachrichten und Mails oder das Chatten im Internet ist mit einer Ende-zu Ende-Verschlüsselung am sichersten, wenn Ihr Gerät nicht von Schadprogrammen befallen ist. Entsprechende Krypto-Programme finden sich im Internet

Kinder und Jugendschutz

Eltern sollten sich regelmäßig über die Gefahren im Internet informieren, denen Kinder und Jugendliche ausgesetzt sind. Vor allem der Besuch nicht jugendfreier Internetseiten und das Nutzen von Chats und Nachrichten-Apps kann Risiken bergen. Die Gefahr eines möglichen Datenmissbrauchs steigt bei Jugendlichen. Sie entziehen sich bei der Internetnutzung zunehmend der elterlichen Kontrolle.

- Sensibilisieren Sie Ihre Kinder und die Jugendlichen für die Internet-Risiken
- Achten Sie darauf, dass Ihre Kinder als Gegenwert beispielsweise für Spiele oder andere Dinge kein Fotos oder Videos von sich eintauschen
- Die Gefahr eines Missbrauchs ist immer dann besonders hoch, wenn das Kind sein digitales Gegenüber nicht auch als Person kennt
- Achten Sie auf offizielle Anbieter, die für Kinder zertifizierte und geeignete Seiten im Internet betreiben

Verhalten in sozialen Medien

Soziale Netzwerke dienen der Kommunikation und Selbstdarstellung, beispielsweise über Profile. Persönliche Daten und die von anderen Nutzern werden eingestellt. So erhält auch der Betreiber Kenntnis über Interessen, den Freundeskreis oder die Kaufkraft. Jede Dateneingabe ist eine Gratwanderung.

- Überlegen Sie genau, welche Daten Sie Ihrem Profil anvertrauen
- Prüfen Sie ob die Daten für den Zweck des Profils erforderlich sind
- Prüfen Sie in den Einstellungen, welche dieser Daten Sie auch nach außen geben
- Prüfens Sie, welche Fotos Sie veröffentlichen. Software ist in der Lage, sie auf anderen Bildern zu finden oder von Ihnen biometrische Profile zu erstellen

Absicherung des Computers

Speziell für Computer gibt es noch einige weitere Möglichkeiten, um deren Sicherehit weiter zu erhöhen.

- Immer wenn das möglich ist, sollten Sie Daten verschlüsseln. Das betrifft ihre Festplatte, aber auch die Kommunikation mit dem Internet
- Sie sollten auf Ihrem PC ein zusätzliches Nutzerkonto ohne Administratorenrechte einrichten und diese für Ihre tägliche Arbeit nutzen. Damit können sie die Wirkung potenzieller Schadsoftware auf den PC einschränken
- Benutzen Sie keinesfalls Datenträger wie USB-Sticks oder Speicherkarten, die nicht Ihnen gehören. Auch mutmaßliche Werbegeschenke können Schadsoftware enthalten
- Löschen Sie Daten auf ihrem PC dauerhaft mittels Spezialsoftware. Das einfache Verschieben in den Papierkorb oder ein Formatieren des Datenträgers reicht zumeist nicht aus, um die Daten zu vernichten.
- Die beste Methode der Datenbeseitigung ist die physische Vernichtung des Datenträgers. CDs oder DVDs können mit Sandpapier bearbeitet und danach in kleine Stücke zerbrochen werden, damit diese unlesbar sind

Fortsetzung...

Der Umgang mit dem Smartphone

Smartphones werden zur mobile Kommunikation genutzt. Auf diesen Geräten sind zumeist zahlreiche persönliche Daten gespeichert.

So sind im Telefonbuch oft Hunderte Angaben zur Erreichbarkeit von Freunden, Bekannten und Verwandten, aber auch von Arbeitskollegen und wichtigen Servicestellen wie Ärzten oder Krankenkassen, vielleicht auch von Anwälten, Schuldnerberatern oder der Arbeitsagentur hinterlegt. Die kleinen mobilen Geräte kennen häufig die Passwörter oder Zugangsdaten zu sozialen Medien, vielleicht aber auch zum Bankkonto und sind in der Lage, bargeldlos zu bezahlen. Ein Verlust des Smartphones kann den Verlust all dieser Daten bedeuten oder schlimmer noch, den Missbrauch ermöglichen.

► Aktivieren Sie auf Ihrem Smartphone die Zugangskontrolle über ein Passwort, über eine PIN oder ein bestimmtes Muster auf dem Bildschirm. Bei biometrischen Daten wie Fingerabdruck oder Gesichtserkennung sollten Sie über die Datenvermeidung nachdenken

► Installieren Sie nur Apps, die Sie wirklich benötigen und dann von App-Stores, die sie kennen. Smartphones mit ihrer App-Struktur können nicht wie PC's mit einen Antivieren-Programm geschützt werden

► Prüfen sie genau, welche Daten eine App anfordert und ob diese zu deren Betrieb erforderlich sind

► Verschlüsseln Sie ihre Kommunikation über spezielle Apps um das Belauschen beispielsweise in W-Lan-Netzen zu erschweren

► Aktivieren Sie die Standortortung (GPS), sowie Bluetooth und W-Lan nur dann, wenn sie diese Funktion oder Verbindungen wirklich benötigen. Mit diesen Daten können ohne Ihr Wissen Bewegungsprofile erstellt werden. Bei Handys mit einem Android-Betriebssystem scannen manche Programme und Dienste trotz abgeschaltetem W-Lan weiter mögliche Verbindungen

► Weil das sichere Löschen von Daten auf einem Smartphone schwierig ist, kann das Verschlüsseln des Geräts verhindern, dass ihre persönlichen Daten von Unbefugten ausgelesen werden

Vorsicht bei Fitnesstrackern

Fitnesstracker, die Schritte zählen, Pulsschlag aufzeichnen, vielleicht auch die zurückgelegte Wegstrecke und das Schlafverhalten, sind im Trend. das gilt auch für sogenannte Smartwaches, die wie Uhren am Handgeleng getragen werden, Anrufe ankündigen und ebenfalls Gesundheitsdaten sammeln können. Beide Gerätegruppen kommunizieren zumeist mit Smartphones, bevorzugt vom selben Hersteller. So können die gesammelten Daten abgespeichert oder empfangene Nachrichten empfangen werden. Der Trend geht dahin, dass die Gesundheitsdaten in einer Cloud-Lösung also auch außerhalb des Smartphones auf einem Server hinterlegt werden. Laut Landesdatenschutzbeauftragten besteht bei Gesundheits-Apps die besondere Gefahr darin, dass unbewusst und ungewollt die Daten an Google, Apple oder Drittanbieter weiter geleitet werden.

► Informieren Sie sich vor der Installation einer Gesundheits-App genau über deren Aktivitäten

► Nutzen Sie bei Smartwaches ähnlich wie bei ihren Mobiltelefonen die Möglichkeiten den Zugang zu sichern

Weiterführende Links und Informationen zum Thema Datensicherheit im Internet aber auch für hilfreichen Programme und Apps finden Sie auf der Internetseite des Bundesamtes für Sicherheit in der Informationstechnik (BSI) und auf dem Internetauftritt des Thüringer Landesdatenschutzbeauftragten.

► www.bsi.bund.de
www.tlfi.de

Thüringer Allgemeine Erfurter Allgemeine vom 12.01.2019, Seite 3

Das Internet vergisst nichts: Gestohlene Daten noch immer verfügbar

Landesbeauftragter Hasse sieht kaum Möglichkeiten, das „Recht auf Vergessenwerden“ durchzusetzen.

Grüne denken über Ächtung illegal erlangter Informationen nach

Von Hanno Müller

Erfurt. Nach dem massenhaften Diebstahl persönlicher Daten von Politikern und Künstlern sind zwar der Täter gestellt und sein für die Verbreitung der gehackten Informationen genutzte Twitter-Account gesperrt. Nach Recherchen unserer Zeitung lassen sich gestohlene Dokumente wie Ausweiskopien, Brief- und Mailverkehr, Fotos sowie Adressbücher und E-Maillisten im Internet aber weiter aufrufen. Vermutet werden mehrere Gigabyte Datenmaterial, die der Hacker auf diversen Servern oder in dubiosen Foren bis zu sechs Mal gespiegelt hat. Wie oft sie dort bereits heruntergeladen und über andere Kanäle gespeichert oder weiterverbreitet wurden, ist unbekannt.

Das gilt auch für die vom Datenklau heimgesuchten Thüringer. Gehackt worden waren hierzulande Vertreter von CDU, Linke, SPD und Grünen. Besonders traf es die Linke. Zwar handelte es sich mehrheitlich „nur“ um die Veröffentlichung von Handy- und Festnetznummern sowie E-Mail-Adressen. Einige Thüringer hatte es allerdings deutlich härter getroffen. So stellte der Hacker etwa Adress- und E-Mailverzeichnisse von Karola Stange (Die Linke), eine Autorechnung von Christian Hirte (CDU) oder interne Fraktionsbriefe von Katrin Göring-Eckardt (Grüne) ins Netz.

Das Problem: Der Großteil der genannten Daten ist nach wie vor im Internet verfügbar. Das Gleiche gilt übrigens auch für die umfangreichen Datenkonvolute von Robert Habeck (Grüne) oder Extra3-Moderator Christian Ehring. Bei anderen wie Cem Özdemir (Grüne) spucken die Server dagegen inzwischen Fehlermeldungen aus.

Der Annahme „Das Internet vergisst nichts“ – einmal veröffentlicht, immer verfügbar – hielt Thüringens Landesdatenschützer Lutz Hasse gestern das „Recht auf Vergessenwerden“ nach Artikel 17 der europäischen Datenschutzgrundverordnung (DSGVO) entgegen. „Danach müssen Daten, die unrechtmäßig im Netz sind, gelöscht werden“, sagte Hasse. Formal sei Twitter in der Pflicht, die Empfänger abgerufener oder geteilter illegaler Daten zu informieren und zur Löschung aufzufordern. Er zweifele aber an, dass dies in der Realität tatsächlich funktioniert, sagte Hasse. „Insofern liest sich das Recht auf Vergessenwerden auf dem Papier zwar gut, in der Praxis ist es aber unheimlich schwer durchzusetzen“, so der Datenschützer. Privat heruntergeladene und verbreitete Daten könne niemand mehr nachvollziehen.

Betroffene Politiker setzen auf IT-Sicherheit

Christian Hirte, Beauftragter der Bundesregierung für die neuen Bundesländer, räumte gestern gegenüber unserer Zeitung ein, noch keine Schritte zur Löschung der veröffentlichten Daten unternommen zu haben. „Eine wirksame Löschung einmal im Internet veröffentlichter Daten ist schwierig, wenn nicht gar ausgeschlossen“, sagte Hirte. Zunächst müssten die Server ermittelt werden, auf welchen die Daten abgelegt sind. Im folgenden Schritt müsste der Serverbetreiber aufgefordert werden, die Daten zu entfernen. Nicht auszuschließen sei, dass die Daten mittlerweile auf Systemen gespeichert sind, die keine Verbindung zum Internet haben, so dass kein externer Zugriff möglich ist. Letztlich wäre ein immenser Aufwand nötig.

„Dass Daten von mir veröffentlicht wurden, ist unerfreulich. Lieber wäre es mir gewesen, eine alte Autorechnung nicht für jedermann zugänglich vorzufinden. Allerdings handelt es sich bei dem bisherigen Material nicht um hochsensible Information. Daher halte ich den Aufwand nicht für gerechtfertigt“, so Christian Hirte gestern.

Hoffnungen setzt der CDU-Politiker in Vorschläge des Bundesinnenministeriums zur Einführung von IT-Sicherheitskennzeichnungen oder zur Stärkung des bisherigen nationalen Cyberabwehrzentrums. Zudem müsse sich jeder im privaten Bereich fragen, wie sorgsam und sicher er mit Daten umgeht.

Aus dem Büro von Katrin Göring-Eckardt, hieß es gestern, wo es möglich sei, versuche man, illegal erlangte Daten im Netz löschen zu lassen. „Da sich diese aber massenhaft verbreiten und auch auf Servern im Ausland stehen, kommt man rechtlich und tatsächlich an Grenzen“, so Sprecher Wolf Albin. Die Grünen würden darüber nachdenken, die Verwendung illegal erlangter privater Daten zu ächten, um zumindest ihrer Verbreitung im Netz Grenzen zu setzen.

Was wenn die illegalen Dokumente dennoch aufgerufen werden? Für Datenschützer Hasse fällt dies unter Artikel 6 der DSGVO zur „Datenverarbeitung“. Demnach überwiegen hier die schutzwürdigen Interessen der Politiker und Künstler. „Jeder kann jetzt wissen, dass es sich um illegale Daten handelt und keine Rechtsgrundlage für die Nutzung besteht. Datenschutzrechtlich wäre eine Verarbeitung rechtswidrig. Wer es dennoch tut, bewegt sich in einer Grauzone“, so Hasse. Bei einer Anzeige könnten per richterlichem Beschluss Wohnungen durchsucht, Computer oder Handys beschlagnahmt oder Bußgelder erhoben werden.