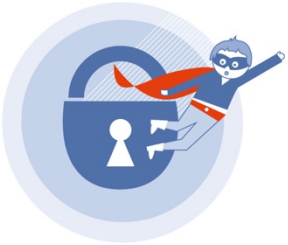
Jhcon
Datenschutzberatung



Ausgabe 4/2022

Liebe Leserin, lieber Leser,

„Welche Folgen kann das für den Datenschutz haben?“ Das sollten Sie sich weitaus häufiger fragen, als dies vermutlich heute geschieht. So kann selbst ein defekter USB-Stick noch Daten preisgeben, obwohl Sie glauben, er sei nur noch etwas für die Mülltonne.

Auch das Nachverfolgen der Online-Aktivitäten mittels Cookies und anderer Tracking-Verfahren kann weitaus mehr ermöglichen als personalisierte Internetwerbung. Daher erklärt diese Ausgabe die häufig übersehenen Risiken durch Online-Tracking ebenso wie den richtigen Umgang mit defekten Speichermedien wie z. B. USB-Sticks, externe Festplatten, Speicherkarten.

Jörg Hagen, Datenschutzbeauftragter

Nicht einfach wegwerfen: Defekte mobile Datenträger

Erkennt der Computer den USB-Stick oder die externe Festplatte nicht mehr oder ist gar das Stick-Gehäuse defekt, landet das beliebte Speichermedium schnell im Müll. Doch oftmals sind die gespeicherten Daten noch lesbar – ein unterschätztes Datenrisiko!

Der Sturz vom Schreibtisch

Manche Berichte von Dienstleistern, die sich auf Datenrettung spezialisiert haben, klingen abenteuerlich, sind aber wahr: „Der Hund hat meinen USB-Stick gefressen! – Ein Hund erlebte eine metallische Überraschung, als er einen USB-Stick mit seinem Lieblingskauspielzeug verwechselte – mit dem Ergebnis, dass der USB-Stick unlesbar wurde“.

Doch es müssen nicht die Haustiere sein, die zu scheinbar defekten USB-Sticks beitragen. Es kann bereits ein Sturz des Speichersticks vom Schreibtisch auf einen harten Boden reichen, wenn es kein besonders stabiles Modell ist.

Ganz gleich, welche Ursache es hat: Viele kennen das Problem, dass sie einen USB-Stick, eine externe Festplatte oder eine Speicherkarte an den Rechner anstecken und der Rechner das Medium nicht mehr erkennt und anzeigt. Was tun? Ab in den Müll? Lieber nicht!

Von Datenrettern und Datendieben

Tatsächlich lassen sich viele defekte Speichermedien noch auslesen, die Daten darauf retten. Sowohl für Privatpersonen als auch für Unternehmen gibt es Datenrettungslösungen, die die verloren geglaubten Daten in vielen Fällen wieder zum Vorschein bringen. Je nach Problem mit dem Speichermedium nennen Datenretter durchaus Erfolgsraten von 90 Prozent.

Leider können aber nicht nur seriöse Datenretter die Inhalte von defekten Datenträgern wiederherstellen, das können auch Datendiebe. Ob der USB-Stick einen Elektronikfehler hat, es einen Wasser- oder

Brandschaden gab, der Stick abgebrochen ist oder die Firmware des Speichermediums nicht mehr funktioniert: In vielen Fällen gelangen sowohl Datenretter als auch Datendiebe noch an die Daten.

Datendieben ist kaum etwas zu teuer

Die professionelle Datenrettung ist kostspielig. Je nach betroffenen Daten aber wird man als Privatperson oder Unternehmen bereit sein, den Service zu beauftragen. Datendiebe jedoch verdienen so viel an gestohlenen Daten, dass sie den Aufwand nicht scheuen, wenn ein spannend erscheinender Datenträger einer Firma im Müll zu finden ist.

In aller Regel übersteigt der Wert der Daten den Geldbetrag, den die Anschaffung des Datenträgers gekostet hat, um ein Vielfaches. Deshalb sind auch defekte Speichermedien ein beliebtes Diebesgut.

Defekte Datenträger müssen zerstört werden

Sind also die Daten auf einem defekten Stick, einer defekten Festplatte oder einer defekten Speicherkarte noch als Kopie oder Backup anderweitig verfügbar und macht somit eine Datenrettung keinen Sinn, werfen Sie trotzdem den mobilen Datenträger nicht in den Müll.

Aus gutem Grund sollten Sie Dokumente und Datenträger mit zu schützenden Daten datenschutzgerecht entsorgen. Im Unternehmen regelt dies meist eine entsprechende Richtlinie. Halten Sie es privat ebenso, dass Sie wichtige Dokumente und Speichermedien nicht einfach wegwerfen, wenn sie Sie nicht mehr benötigen oder sie kaputt aussehen.

Defekte Speichermedien müssen noch einer sicheren Entsorgung zugeführt werden, also so zerstört werden, dass selbst Datenretter und damit auch Datendiebe keine Chance mehr haben. Ein schlichter Hammer oder Bohrer hat da schon so manch guten Dienst geleistet.

Was Online-Tracking alles verraten kann

Nicht nur die Werbewirtschaft nutzt Tracking-Verfahren, um die Online-Aktivitäten von Nutzenden nachzuverfolgen. Online-Tracking macht weitaus mehr möglich als personalisierte Online-Werbung: einen genauen Blick auf die persönlichen Einstellungen.

Ist Online-Tracking wirklich so schlimm?

Eine Trendstudie des BVDW (Bundesverband Digitale Wirtschaft) untersuchte die Akzeptanz für Werbung im Internet. Demnach sind sich drei Viertel der Befragten (71 Prozent) bewusst, dass Werbung ein unverzichtbares Finanzierungsmittel der digitalen Angebote im Internet ist. Gleichzeitig empfindet mehr als die Hälfte der Befragten (58 Prozent) Werbung als grundsätzlich störend.

Jeder zweite Internetnutzende (52 Prozent) gibt an, Cookies in den eigenen Browser-Einstellungen zu löschen, so eine Umfrage des Digitalverbands Bitkom. Doch so manchem erscheint die Sorge wegen Online-Tracking übertrieben. Immerhin ist dann die Online-Werbung, die angezeigt wird, passender zu den persönlichen Interessen und aktuellen Internetsuchen. Aber Internetwerbung ist nicht alles, wofür sich die Analysen der Online-Aktivitäten nutzen lassen.

Persönliche Eigenschaften könnten transparent werden

Tatsächlich geht es bei Online-Tracking um mehr als möglichst erfolgversprechende Online-Werbung. So zeigt der Datenschutzbericht „Risiken im Zusammenhang mit dem Tracking- und Targeting-Ökosystem im digitalen Werbemarkt“ der Internationalen Arbeitsgruppe zum Datenschutz in der Technologie weitere Risiken auf, die das Tracking im Internet mit sich bringen kann.

Die Datenschützer berichten, dass sich das Tracking mittlerweile über digitale Werbung hinaus nutzen lässt, etwa um Meinungsbildungsprozesse zu manipulieren. Das ist möglich, weil Online-Tracking es erlaubt, eine Sammlung persönlicher Eigenschaften und Interessen zu einer Person anzulegen. Dies könnte nicht nur die Werbewirtschaft, sondern auch ein Interessenverband oder eine Partei für sich nutzen.

Sammlungen persönlicher Eigenschaften kann man sich selbst ansehen:

- Google Ads Setting (Einstellungen für personalisierte Werbung) beispielsweise verrät Nutzenden mit Google-Konto, was bereits alles über die Person bekannt ist.
- Auch bei Facebook zum Beispiel kann man sich die „Ad Preferences“ (Interessenbasierte Online-Werbung verwalten) ansehen, um dann festzustellen, dass sogar die Nähe zu einer politischen Partei dort hinterlegt sein kann.

Hohe Diskriminierungs- und Manipulationsrisiken

Die Datenschützer warnen vor den häufig übersehenen Risiken durch Online-Tracking: Das vertiefte Wissen über einzelne Nutzerinnen und Nutzer, insbesondere über die emotionale Verfassung, könne genutzt werden, um persönliche Vorurteile und Schwächen zu identifizieren. Es erlaubt Dritten, diese auszunutzen, um individuelles Verhalten zu beeinflussen oder sogar zu kontrollieren.

Der Datenschutzbericht nennt konkrete Beispiele: So beeinflusste Facebook im Jahr 2012 den Newsfeed von 1,9 Millionen seiner Nutzerinnen und Nutzer in den USA, um sie zum Wählen zu bewegen. Facebook behauptet, dass es den Anteil der Wählerinnen und Wähler innerhalb dieser Gruppe um drei Prozentpunkte erhöhen konnte. Die Datenschützer machen klar: Würden Facebook oder andere soziale Netzwerke eine solche Manipulation hypothetisch nur bei Nutzerinnen und Nutzern eines bestimmten politischen Spektrums anwenden, könnte das einen entscheidenden Einfluss auf den Ausgang von Wahlen haben.

Es gibt also sehr gute Gründe, sich über den Schutz vor heimlichem Online-Tracking genau zu informieren! Lesen Sie deshalb genau die Online-Hilfe zu Ihrem Browser, damit Sie alle verfügbaren Einstellungen kennen und einsetzen, die sich gegen ungewolltes Tracking richten.

Impressum

Redaktion:
Dipl. - Ing. Jörg Hagen
Betriebl. Datenschutzbeauftragter

Anschrift:
Jhcon Datenschutzberatung
Königstraße 50 A
D - 30175 Hannover
Telefon: 0511 51543831
E - Mail: info@jhcon.de