Geheime Daten auf dem Druckpapier?

Diplominformatiker der TU Dresden entwickeln Verfahren gegen Druckerüberwachung

Mitteilung: Technische Universität Dresden

Sie sind winzig klein, mit bloßem Auge kaum sichtbar und trotzdem auf fast allen Ausdrucken von Farblaserdruckern vorhanden: winzig gelbe Punkte – sogenannte Trackingpunkte - bilden einen digitalen Fingerabdruck, der in keinem Handbuch erwähnt wird und doch Informationen enthält, die ein Erkennen der druckenden Person ermöglicht. Das Muster der Punkte variiert je nach Hersteller und verrät zum Beispiel die eindeutige Seriennummer des Druckers, den Druckertyp oder das Druckdatum mit der Uhrzeit.

Timo Richter und Stephan Escher von der Professur Datenschutz und Datensicherheit der TU Dresden haben die Punkte genauer analysiert. Im Rahmen einer Diplomarbeit fanden sie heraus, wie der Fingerabdruck von jedermann gelesen werden kann. In einem Experiment wurden 1286 Seiten von 141 Druckern 18 verschiedener Hersteller untersucht. Dabei entdeckten sie über die im Jahr 2005 vom Deutschen Forschungsinstitut für Künstliche Intelligenz gefundenen Codierungsmuster diverse weitere. Während damals die Mustererkennung über manuelle Bildvergleiche erfolgte, können die Dresdner Informatiker die Muster automatisch digital finden und größtenteils auch dekodieren, welche Informationen der Drucker im Ausdruck hinterlassen hat.

Warum unsere Ausdrucke seit über 15 Jahren mit gelben Punkten gekennzeichnet werden, bleibt unklar: Betroffene Drucker-Hersteller gaben auf Anfrage weder Auskunft über den Grund der Tracking-Punkte noch zum Auftraggeber. Zum einen können die Punkte genutzt werden, um Verbrechen aufzuklären: Beispielsweise wenn vertrauliche Dokumente beim Teilen in falsche Hände geraten, bei der Aufklärung von Versicherungsbetrug, Zeugnisfälschungen oder vielleicht auch zusätzlich zum Wasserzeichen, um unerlaubte Gelddrucke zu verhindern.

Dass die Druckeridentifikationscodes nicht nur zur Verbrechungsbekämpfung eingesetzt werden, zeigt der Fall der jungen Whistleblowerin Reality Leigh Winner, welche vom US-Geheimdienst über Trackingpunkte entdeckt und inhaftiert wurde. Winner soll seit 2016 auf die Hackeraffäre zwischen Russland und den USA bezogene, nachrichtendienstliche Informationen an die Nachrichtenwebseite „The Intercept“ weitergeleitet haben. Überführt wurde sie durch die Trackingpunkte auf den Ausdrucken. Druckeridentifikationscodes können also ebenso dazu dienen, Menschen zu überwachen.

„Wir finden es wichtig, dass die Menschen über die vorhandenen Codes und die damit mögliche Überwachung aufgeklärt werden“, so Escher. „Die neue EU-DSGVO regelt den Umgang mit digitalen Daten. Den wenigsten ist bewusst, dass sie auch mit analogen Geräten überwacht werden können.“

„Jeder Mensch sollte sich frei äußern können – dazu gehört auch das Aufdecken von Missständen.“ Richter hat deshalb in seiner Diplomarbeit ein Verfahren entwickelt, welches die Codes so weit zerstört, dass eine Rückführung auf die druckende Person nicht mehr möglich ist. Dabei werden die Muster auf dem Druckerpapier analysiert und mittels seiner App in den freien Feldern weitere Punkte ergänzt, so dass das ursprüngliche Codewort nicht mehr erkenn- und entschlüsselbar ist.

Mit der App „Deda“ kann jeder sein Druckerpapier auf Tracking-Punkte prüfen und diese anonymisieren. Sie steht kostenlos unter https://dfd.inf.tu-dresden.de/ zur Verfügung.

Seine Ergebnisse stellte Richter auf der sehr renommierten Internationalen ACM Information Hiding and Multimedia Security 2018 vor, die vom 21.-22. Juni in Innsbruck stattfand. Sie ist die wohl wichtigste Veranstaltung im Bereich der Multimediasicherheit und zieht Forscher und Interessenten aus der ganzen Welt an.

PM v. 27.6.2018
Katrin Presberger
Pressestelle
Technische Universität Dresden
Quelle:
www.tu-dresden.de
www.idw-online.de