

**Ausgeforscht: auch intime Details von Bundespolitikern im Handel**

Anmoderation

Anja Reschke :

Was treiben die Menschen im Internet? Nun, sie kaufen ein und gucken Pornos. Laut Netzstatistiken sind 30 Prozent der aufgerufenen Seiten pornografischen Inhalts. Wenn man sowas hört, fragt man sich natürlich, wer das wohl so ist im eigenen Umfeld. Nun, wir wissen jetzt, wer genau sowas guckt. Man gibt sich ja gerne dem Trugschluss hin, man wäre allein mit seinem Computer. Könnte da intime Dinge rein tippen, Informationen über Finanzen, Krankheiten, sexuelle Vorlieben rausziehen. Weiß ja keiner. Klar, Daten werden gespeichert, aber doch anonym. Und ja, es wird immer gewarnt, aber wer nimmt das so richtig ernst? Als allerdings unsere Kollegin mit einem Datensatz kam, den sie von einem Händler bekommen hatte, mit den Daten von drei Millionen Nutzern darauf, wurde uns ganz anders. Minutiös kann man da nachverfolgen mit Namen, wer wann welche Seite im Netz besucht hat. Auch die Namen vieler Politiker waren darunter, über die man so mehr erfahren kann, als ihnen lieb ist. Svea Eckert und Jasmin Klofta

Wir haben etwas von ihr, das nicht uns gehört. Etwas, das die Bundestagsabgeordnete Valerie Wilms beunruhigen wird. Es sind ihre Daten. Genauer gesagt: Alles, was sie im Internet getan hat. Es ist jede Suche, jede Reisebuchung, jeder einzelne Klick. Lückenlos gespeichert.

O-Ton

Valerie Wilms, Grüne

Bundestagsabgeordnete:

„Ist interessant, ja. Da kann man sehr gut entnehmen, wo ich meine Bankverbindung habe, wie oft ich in welche Zeitung reingucke, aha, da sind jetzt sogar noch, wo ich da noch für irgendwelche Parteitage was mache... Da ist auch sogar meine Krankenversicherung noch, das kommt ja alles. Ist schon ein Hammer, ist schon ein Hammer.“

Die unscheinbaren URLs speichern auch jede Suche, und offenbaren so, was Menschen gerade bewegt, etwa, für welche Krankheiten sie gerade Medikamente suchen.

O-Ton

Panorama: „Sie haben sich im August über das Medikament Tebonin informiert, das wird so bei Tinnitus, Hörsturz und Abgeschlagenheit verwendet. Sollten so etwas Dritte erfahren?“

Valerie Wilms, Grüne, Bundestagsabgeordnete: „Nö. Ich weiß gar nicht, in welchem Zusammenhang ich mir dieses Tibonin da angeguckt habe. Das ist nicht schön, sowas nachträglich zu lesen, vor allen Dingen verknüpft mit dem eigenen Namen.“

Panorama: „Also, das kann schaden, wenn da Dinge ans Licht kommen...“

Valerie Wilms, Grüne, Bundestagsabgeordnete: „Natürlich kann es schaden. Insofern haben Sie natürlich nicht ganz Unrecht, man wird damit durchaus erpressbar.“

Wer diese Daten hat, kann jederzeit verfolgen, was die Bundestagsabgeordnete macht, wann und wo. Ihre Daten sind nicht anonym. Ihr Name taucht immer wieder auf. Wie auch die Formulare für ihre digitale Steuererklärung.

O-Ton

Valerie Wilms, Grüne,

Bundestagsabgeordnete:

„Steuerfreie Arbeitgeberzuschüsse, Vorsorgeaufwendungen, sonstiges. Ist alles zu sehen. Scheiße. Entschuldigung, wenn ich das so drastisch sage. Also man wird nicht nur dem Finanzamt gegenüber nackt, sondern auch demjenigen gegenüber, der die Daten hat. Unangenehm.“

Hier geht es nicht um Geheimdienste, die Terroristen jagen. Nein, es sind private Firmen, die alle ausforschen. Und mit den Informationen handeln.

Das herauszufinden hat Monate gedauert. Denn ob die Daten von unseren Rechnern wirklich anonym bleiben, daraus macht die Branche ein Geheimnis.

Deshalb erfinde ich „Anna Rosenberg“. Anna ist so alt wie ich, arbeitet aber in der Datenbranche. Sie soll mein Eintritt in die Welt der Datenhändler sein. Um glaubwürdig zu wirken, lasse ich Fotos von Anna machen. Und erstelle ein Profil auf dem beruflichen Online-Netzwerk „LinkedIn“. Senior Consultant nenne ich mich hier. Und arbeite bei „Meez Technology“. Auch dieses junge hippe Start-Up ist meine Erfindung. Noch eine schicke Internetseite, eine Büronummer – umgeleitet auf mein Handy. Fertig. Und tatsächlich: Mit Anna sprechen die Datenverkäufer sogar sehr offen.

*(das Telefon klingelt)*

O-Ton:

„Anna Rosenberg, Meez Technology.“

Als Anna frage ich mehr als 50 Firmen an. Ich behaupte, einen großen Online-Händler zu vertreten. Schnell finde ich Unternehmen, die mit mir ins Geschäft kommen wollen. Sie versprechen Erstaunliches: *„Wir haben 58 Millionen deutsche Profile“, „Unsere Daten reichen lückenlos drei Jahre zurück“, „Nutzerdaten im Abo schon ab 10.000 Euro im Monat“.*

Am Ende bekomme ich sie sogar kostenlos. Als Probe-Datensatz. Die Informationen von rund drei Millionen deutschen Nutzern, jeder Klick im Netz, über einen vollen Monat. Eine gigantische Datenmenge.

Doch wie sind die Händler überhaupt an die Daten der drei Millionen Deutschen gekommen?

Immer, wenn wir im Internet surfen, steht oben die Adresse der Seite, die so genannte URL. Surfen wir durch das Netz, ändert sie sich jedes Mal mit. Dieses Aktivitätsprotokoll ist für die Datenbranche Gold wert. Sie bekommen es mit einem Trick: Wenn wir uns kostenlose Zusatzprogramme, so genannte „Add-ons“ installieren, laden wir uns oft unbemerkt ein kleines Spionage-Programm herunter. Von nun an wird jede besuchte Seite protokolliert und weitergegeben.

Wir können eines dieser Add-Ons enttarnen: WOT - Web of Trust. Das Netz des Vertrauens verspricht sicheres Surfen, sammelt dabei aber auch die Nutzerdaten ein - und das nicht endgültig anonymisiert. Auf Anfrage bestreitet WOT, dass solche Daten weitergegeben werden.

Der Datenwissenschaftler Andreas Dewes soll uns helfen, die Millionen von Daten auszuwerten. Seine Überzeugung: die Daten sind nicht anonym, aus URLs lassen sich Namen herauslesen. Die könnten aufgezeichnet werden, wenn Nutzer sich irgendwo anmelden: bei ihrem Email-Konto, in online-Shops oder in sozialen Netzwerken. Deshalb programmiert er einen Algorithmus, um Namen aus den Daten zu fischen - mit Erfolg.

O-Ton

Andreas Dewes,

Datenwissenschaftler:

„Für mich war sehr überraschend, wie einfach man eigentlich einen Großteil der Daten de-anonymisieren konnte. Hier kann man eigentlich schön sehen, dass die Privatsphäre des Nutzers in keinsten oder in kaum einer Weise respektiert wird.“

Wir konnten zahlreiche Personen identifizieren. Aber wir zeigen nur diejenigen, die damit einverstanden sind. Etwa der EU-Abgeordnete Martin Häusling. Sein Thema ist brisant: Agrarpolitik. Es geht um Milliarden-Subventionen. In Brüssel und hier in Straßburg wird entschieden. Immer unter Druck durch die Lobbyisten. Die Daten seines Büros verraten, wo er wann ist. Immer wieder Hinweise auf seine Reisen mit der Bahn, Hotelbuchungen bei „Booking.com“.

O-Ton

Martin Häusling, Grüne

Abgeordneter im Europaparlament:

„Das finde ich schon erschreckend, muss ich ehrlich sagen. Wir brauchen als Abgeordnete Vertrauensschutz. Wir müssen auch teilweise arbeiten, ohne dass es die Öffentlichkeit gerade für Hintergrundarbeit erfährt, und wenn wir gleichauf sein wollen mit Lobbyisten, die uns den ganzen Tag hier zuballern, dann müssen wir auch selber Recherchen machen. Ich meine, wenn das bestimmte Lobby-Verbände in die Hand bekommen, da kann man vielleicht nachvollziehen, wer jetzt mit mir kommuniziert, mit wem wir uns treffen, kann ja andere in Schwierigkeiten bringen. Ich meine, was ja eigentlich gar nicht geht, man kann ja meine ganze Arbeit sozusagen da nachvollziehen, die ich mache.“

Ein weiteres konkretes Beispiel: Abstimmungen zu vertraulichen Treffen – einfach nachvollziehbar.

O-Ton

Martin Häusling, Grüne, Abgeordneter im Europaparlament: „Das ist eine Terminfindung, wo wir uns als Grüne-Abgeordnete zusammenfinden zu einem internen Treffen.“

Panorama: „Krass, okay.“

Martin Häusling: „Das ist auch nichts für die Öffentlichkeit, wo wir uns sozusagen als agrarpolitischer Kreis treffen.“

Panorama: „Wann war das? Steht das da?“

Martin Häusling: „Das ist erst noch. Und das sollten eigentlich nur die wissen und nicht sozusagen andere.“

Ausgeforscht sind nicht nur intime Daten von Politikern, sondern auch Geheimnisse von Amtsträgern, etwa der Polizei.

Wir finden einen Kriminalhauptkommissar, der in einem Fall von Computerbetrug ermittelt. Weil der mutmaßliche Täter in Großbritannien ist, bittet der Kommissar dort um Hilfe. Um seine Anfrage auf Englisch zu übersetzen, benutzt er ein Übersetzungsprogramm. „Computerbetrug“ schreibt er, oder schickt auch das interne Aktenzeichen und die „IP-Adresse“. So gelangen die sensiblen Polizeidaten einfach ins Netz. Und werden abgegriffen.

Noch brisanter der Fall eines Richters. Zunächst ist er auf der Suche nach einer neuen Robe für die Arbeit und stöbert durch verschiedene Angebote. Dann sucht er nach „Zeit für die

Knechtschaft“, Sado-Maso-Pornos, in denen Frauen gedemütigt werden. Jede Seite, die er anklickt, wird protokolliert. Auch diese heiklen Daten landen im offenen Verkauf.

O-Ton

Andreas Dewes,

Datenwissenschaftler:

„Wir haben hier zum Beispiel eine Vielzahl an pornografischen Inhalten gefunden. Mit teilweise sehr expliziter Vorliebe. Und mit den Daten kann man sich auch natürlich erpressbar machen. Das heißt, hier ist vorstellbar, dass man auch eine Einflussnahme vornehmen kann anhand von solchen Daten, die natürlich im privaten Sinne auch sehr peinlich sein können, aber natürlich hier bei einer Person, die im öffentlichen Leben steht und die eine staatstragende Funktion hat, auch entsprechende Sicherheitsrelevanz hat.“

Justiz, Polizei – und immer mehr betroffene Bundespolitiker und Mitarbeiter finden wir. Neben Martin Häusling und Valerie Wilms, Waltraud Wolff, Annalena Baerbock, Frank Junge und Lars Klingbeil, netzpolitischer Sprecher der SPD. Die Datenspur geht sogar bis ins Bundeskanzleramt, zu Staatsminister Helge Braun.

In Berlin treffen wir Lars Klingbeil, den netzpolitischen Sprecher der SPD. Selbst sein Büro ist Opfer des Datenraubzuges geworden.

O-Ton

Panorama: „Ist das eine Industrie außer Kontrolle?“

Lars Klingbeil, SPD, Bundestagsabgeordneter: „Ich gebe zu, auch ich habe nicht gewusst, dass solche Sachen identifizierbar sind, vielleicht ist man da naiv an der Stelle, aber da braucht man auf jeden Fall auch Aufklärung darüber, welche Daten eigentlich erhoben werden und was mit den Daten dann passiert. Und wenn es eben nicht reicht, mit Vertrauen zu arbeiten, dann müssen Gesetze her.“

Vielleicht hilft irgendwann ein neues Gesetz, im Moment hilft aber nur eines wirklich: solche Spionageprogramme deaktivieren und entfernen. Etwa das von der Firma WOT.

O-Ton

Panorama: „Und die verkaufen ihre Daten weiter.“

Valerie Wilms, Grüne, Bundestagsabgeordnete: „Die Schlitzohren sind das?“

Panorama: „Genau.“

Valerie Wilms: „Dann gibt es nur eine Maßnahme. Und die werden wir jetzt gleich mal machen. Einstellungen. Erweiterungen. WOT. Und dann, weg damit. Gelöscht. Verschwunden.“

Autoren: Svea Eckert, Jasmin Klofta

Mitarbeit: Kian Badrnejad, Stefanie Helbig, Jan Lukas Strozyk

Kamera: Sven Wettengel

Schnitt: Olaf Hollander

Grafik: Thorben Korpel

Abmoderation:

Bei den Abgeordneten haben unsere Recherchen zu großer Verunsicherung geführt. Laut Informationen von Spiegel online verlangen mehrere Fraktionen im Bundestag jetzt Aufklärung zu diesem Datenskandal. Mehr zu den Geschäften mit den Daten und auch Anregungen, wie man sich besser schützen kann, finden Sie bei uns im Netz unter [www.panorama.de](http://www.panorama.de) - und wenn Sie auf diese Seite gehen, ist das auch völlig in Ordnung.

