Reflexion · 29. Juni 2026

← Zurück

Du bist nicht anonym

Das Vertrauen, das du nicht gewählt hast

Klartext: Mit deiner E-Mail-Adresse kann jeder in Sekunden herausfinden, wo du ein Konto hast, und manchmal auch dein Gesicht und deinen Namen. Das ist kein Fehler: So funktioniert das Internet. Die Frage ist nicht, ob sie dich sehen können – das können sie –, sondern wem du zwangsläufig vertrauen musst. Und es gibt nur einen Ort, an dem niemand dazwischensteht: das direkte Gespräch, von einem Gerät zum anderen.

Eine E-Mail-Adresse reicht. Nicht unbedingt deine: irgendeine. Man gibt sie in eine Handvoll kostenloser Tools ein – legal, öffentlich, für jeden zugänglich, der danach suchen will – und in wenigen Sekunden erscheint eine Liste: bei welchen Diensten diese E-Mail registriert ist, manchmal ein Profilbild, manchmal ein Vor- und Nachname, von dem der Besitzer dachte, er hätte ihn niemandem gegeben. Man muss kein Techniker sein. Es wird kein Passwort geknackt. Es wird kein Verbrechen begangen. All diese Informationen waren bereits da – veröffentlicht, registriert oder durchgesickert – und warteten nur darauf, dass sich jemand die Mühe macht, sie zusammenzutragen.

Es ist verlockend, dies als Fehler zu betrachten: eine Lücke, eine Unachtsamkeit, etwas, das jemand beheben sollte. Ist es aber nicht. Es ist die normale Funktionsweise des offenen Webs. Jedes Mal, wenn du dich bei einem Dienst anmeldest, ein Formular ausfüllst, eine Bewertung veröffentlichst oder in einem Leak auftauchst, hinterlässt du eine Spur. Keine dieser Spuren ist für sich genommen schlimm. Das Problem – falls es eines ist – entsteht erst, wenn man sie zusammensetzt, und das Zusammensetzen ist einfach.

An dieser Stelle verteidigen sich viele mit einem vernünftigen Satz: »Ich habe nichts zu verbergen« oder »Ich passe auf meine Konten auf«. Der erste Satz verwechselt Verbergen mit Wählen; wir kommen darauf zurück. Der zweite übersieht, dass du den größten Teil dieser Spuren gar nicht selbst hinterlassen hast: Das Handelsregister, die Website, die gehackt wurde, der Bekannte, der ein Foto mit dir hochgeladen und dich markiert hat. Anonymität im Internet ist fast nie eine Eigenschaft, die man besitzt; sie ist höchstens Dunkelheit: die vorläufige Tatsache, dass sich noch niemand die Mühe gemacht hat, nachzusehen.

Bisher haben wir darüber gesprochen, was eine einzelne Person in wenigen Sekunden von Hand tun kann. Nun lassen wir die Person weg. Was uns fast alle jahrelang geschützt hat, war nicht Anonymität, sondern Desinteresse: Um dich zu finden, muss sich jemand die Mühe machen, nachzusehen, und niemand hat die Zeit, jeden anzusehen. Diese letzte Hürde – die Mühe des Nachsehens – ist genau das, was eine Maschine nicht hat. Ein automatisches System kann diesen Abgleich nicht gegen ein bestimmtes Ziel, sondern gegen eine ganze Bevölkerung durchführen; nicht einmalig, sondern ununterbrochen; nicht aus Verdacht, sondern standardmäßig. Was früher einen Ermittler Stunden pro Person kostete, wird nun bei Millionen gleichzeitig erledigt, ohne jemanden Zeit oder Aufmerksamkeit zu kosten. Man muss nicht mutmaßen, wer das tun wollen würde – ein Unternehmen, eine Gruppe, ein Staat –; es reicht zu verstehen, dass man sich nicht mehr aussuchen muss, wen man ansieht. Man kann jeden ansehen.

Deshalb ist »Können sie mich finden?« die falsche Frage. Die Antwort ist ja, und das wird immer mehr der Fall sein. Die nützliche Frage ist eine andere: Wem und wie sehr muss ich vertrauen, um vernetzt zu leben? Denn das ist es, was du jeden Tag tust, meist ohne darüber nachzudenken. Du vertraust darauf, dass der Dienst, bei dem du dich anmeldest, deine Daten sicher aufbewahrt. Du vertraust darauf, dass dein Netzbetreiber deine Anrufe nicht abhört. Du vertraust darauf, dass die Messaging-App, die alle nutzen – sagen wir WhatsApp –, das tut, was sie

behauptet. Du vertraust dem Server dazwischen, dem Unternehmen, das ihn verwaltet, dem Land, in dem er steht, dem kostenlosen Tool, das jemand ins Netz gestellt hat. Jedes dieser Glieder ist eine Vertrauensentscheidung. Der Unterschied ist, dass du fast keine davon bewusst getroffen hast: Sie waren inbegriffen. Diese Glieder, die sich zwischen dich und die andere Person schieben, nennt man im Fachjargon Vertrauensvermittler; der Name ist weniger wichtig als die Tatsache, dass sie da sind, und dass es viele sind.

Es gibt einen ehrlichen Weg, all das zu überprüfen: Mach es mit dir selbst. Und du brauchst nichts von uns. Öffne deinen Browser, tippe drei oder vier Wörter ein – so etwas wie »was weiß das internet über meine e-mail« – und das Web selbst wird dir die Tools präsentieren. Diese Leichtigkeit ist für sich genommen schon die halbe Antwort: Wenn du sie in zehn Sekunden findest, kann jeder finden, was sie über dich sagen.

Wir bieten dir bewusst keine Liste an. Wenn wir es täten, müsstest du uns vertrauen: darauf, dass wir gut auswählen, dass diese Seiten auch in fünf Jahren noch vertrauenswürdig sind, dass hinter keiner von ihnen – heute oder morgen – jemand mit bösen Absichten steht. Das können wir für Seiten, die wir nicht kontrollieren, nicht versprechen, und wir ziehen es vor, kein Versprechen abzugeben, das wir nicht halten können. Genau darum geht es in diesem Artikel. Aber es selbst zu suchen, hat seinen Preis: Die Suchmaschine unterscheidet nicht zwischen seriös und Falle. Eine Seite aufzubauen, die ein echtes Tool imitiert, deine E-Mail abfragt und sie behält, ist trivial. Bevor man also irgendwo etwas eingibt, sollte man wissen, wie man eine Adresse liest.

Hinweis — Eine Adresse lesen, bevor man ihr vertraut. Eine gefälschte Seite kann bis auf den letzten Pixel einer echten kopieren; was sie fast nie fälschen kann, ist ihre Adresse. Bevor du irgendwo etwas eingibst, lies die Adressleiste, nicht die Seite. Der maßgebliche Name steht links vor dem letzten Teil (`.com`, `.org`, `.de`): Bei `sichere-bank.seltsame-seite.top` ist der wahre Eigentümer nicht deine Bank, sondern `seltsame-seite.top`. Misstraue geänderten Buchstaben (ein `0` statt einem `o`), zusätzlichen Wörtern, Bindestrichen, wo du keine erwartest, und seltsamen Endungen. Das Schloss und das `https` sagen nur, dass die Verbindung verschlüsselt ist – nicht, dass der Eigentümer ehrlich ist –: Auch ein Betrüger hat ein Schloss. Und die ersten Ergebnisse, die als »Anzeige« markiert sind, stehen dort, weil jemand bezahlt hat, nicht, weil sie vertrauenswürdig sind. Jede dieser Prüfungen ist im Grunde dieselbe Frage: Wie sehr vertraue ich dieser Adresse, und warum?

An diesem Punkt ist es sinnvoll, das Gegenteil von all dem zu beschreiben: einen Kanal ohne Vermittler. Zwei Menschen, die sich allein auf dem Gipfel eines Berges unterhalten. Kein Postbote, keine Vermittlungsstelle, kein Server, kein Unternehmen, kein Land dazwischen. Und doch, sieh mal: Auch dort verschwindet das Vertrauen nicht. Wenn du der anderen Person ein Geheimnis erzählst, vertraust du ihr. Dieses Vertrauen lässt sich nicht beseitigen – und das ist auch nicht nötig –, denn es ist das einzige, das du wirklich gewählt hast: Du weißt, wem du vertraust, und warum.

Was es auf dem Berg nicht gibt, ist alles andere. Niemand dazwischen. Und das, und nichts anderes, ist das einzige Modell, das sich auf ehrliche Weise digital reproduzieren lässt: ein direkter Kanal von einem Gerät zum anderen, ohne etwas oder jemanden auf dem Weg. Es beseitigt nicht das Vertrauen – das wäre eine Lüge –; es beseitigt die Vermittler. Es lässt dich allein mit dem einzigen unvermeidlichen Vertrauen, demjenigen, das du gewählt hast. Das ist übrigens die Architektur, von der aus wir diese Seiten schreiben; aber das Argument steht für sich allein, egal wer es baut.

Also nein, du bist nicht anonym, und du wirst es wahrscheinlich auch nie wieder sein. Aber das war ohnehin nie der Kampf, auf den es ankam. Man kann nicht leben – oder surfen –, ohne jemandem zu vertrauen; wer das versucht, ist nicht freier, sondern nur einsamer. Reife bedeutet nicht Misstrauen, was nur eine andere Form von Naivität ist. Reife bedeutet, anspruchsvoll zu sein: zu wissen, wem du dein Vertrauen schenkst, wie viel, im Austausch wofür und – vor allem – zu wissen, wann du es jemandem schenkst, ohne es entschieden zu haben.

Fast nichts im Leben ist schwarz oder weiß; fast alles lebt im Grau dazwischen, und zu lernen, sich in diesem Grau zu bewegen, macht einen großen Teil dessen aus, was Urteilsvermögen bedeutet. Die einzige Ausnahme ist das, was von Haus aus richtig gemacht ist: das, was dich aufgrund seines Designs auffordert, niemand anderem zu vertrauen als der Person, mit der du bereits beschlossen hast zu sprechen. Alles andere – absolut alles andere – ist eine Frage des Wie viel und des Wem.

Anmerkung der Redaktion: Wenn diese Cuadernos Unternehmen oder Produkte nennen, geschieht dies nicht, um sie anzuklagen. Diejenigen, die sie entwickeln, leisten Arbeit, die Millionen von Menschen nutzen und schätzen. Was wir aufzeigen, ist struktureller Natur — das Modell, nicht die Marke. Marken erscheinen als Beispiele, weil der Leser sie erkennt.

Quellen und weiterführende Literatur

- OSINT (Open Source Intelligence) — das Sammeln von Informationen aus bereits öffentlichen Daten; es ist kein Eindringen und keine Spionage.
- Reglamento (UE) 2016/679 (RGPD) — über die Verarbeitung personenbezogener Daten, einschließlich der Zusammenführung von Daten, die einzeln öffentlich waren.
- Öffentliche Register (Handels-, Gerichts-, Grundbücher) — eine legitime und ergiebige Quelle für personenbezogene Daten in fast ganz Europa.
- In dieser selben Sammlung: die Cuadernos Lacre über Ende-zu-Ende-Verschlüsselung und »Was eine Unterschrift nicht reparieren kann« entwickeln denselben Gedanken aus einem anderen Blickwinkel.

← ZurückWas eine Unterschrift nicht in Ordnung bringen kann

Aktuelle Lektüre

- Reflexion · 27. Mai 2026 Was eine Unterschrift nicht in Ordnung bringen kann
- Analyse · 26. Mai 2026 Echte vs. scheinbare Privatsphäre: Die Fragen, die man sich stellen sollte
- Analyse · 25. Mai 2026 Self-Hosting als berufliche Praxis

Nehmen Sie diesen Artikel mit, wohin Sie ihn brauchen.

↓ Markdown ↓ Klartext ↓ PDF

Die Datei wird auf Ihr Gerät heruntergeladen. Von dort aus können Sie sie speichern, in Solo2 importieren oder teilen, wo immer Sie möchten. Cuadernos entscheidet nicht über den Zielort für Sie.

Siegellack-Siegel · SHA-256 d250f8ec87a79d3027f33ff15f4696674f550341988c656ba9022e9fe4e7b66c

Cuadernos Lacre · Eine Publikation von Menzuri Gestión S.L. ·
geschrieben von R.Eugenio · herausgegeben vom Team von Solo2.