Bild: Thorsten Hübner

Virtuelle Bodyguards

Wie Sie Ihre Daten im Internet löschen (lassen)

Jeden Tag handeln Tausende Datenbroker mit Ihren persönlichen Informationen im Internet und verdienen damit Milliarden. Das ruft Schutzdienste auf den Plan. Sie versprechen, Ihre Daten zu löschen, sodass Spammer und Betrüger Sie nicht mehr belästigen. Wir klären, was die Dienste taugen, welche Möglichkeiten Sie zusätzlich haben und wann Sie machtlos sind.

Von Torsten Kleinz

Das Angebot klingt verlockend: Sie müssen sich nie wieder selbst um widerrechtlich abgegriffene Daten kümmern, stattdessen übernehmen Dienstleister die Jagd nach E-Mail-Adressen und Telefonnummern in den Fängen von Datenhändlern. Die Hilfe ist oft nur allzu willkommen, denn als Einzelner steht man der Übermacht der Datensammler hilflos gegenüber.

In diesem Artikel untersuchen wir die Methoden und Erfolgsaussichten solcher Datenschutzdienste und geben zusätzlich Tipps, was sie selbst tun können. Auf die Hintergründe des weltweiten Geschäfts mit persönlichen Daten und die aktuelle Rechtslage in der EU und in den USA gehen wir im Artikel auf Seite 124 ein.

Surfshark Incogni

Seit 2021 bietet das in Litauen ansässige, aber in den Niederlanden registrierte Unternehmen Surfshark seinen Dienst Incogni an. Incogni soll E-Mail-Adressen in den Beständen von Datenbrokern aufspüren und deren Löschung fordern. Er ist einer der günstigsten Datenlöscher auf dem Markt, leistet für knapp 70 Euro im Jahr aber auch weniger als die Konkurrenz. Einen kostenlosen Probe-Account gibt es nicht, immerhin kann man bei Nichtgefallen innerhalb von 30 Tagen sein Geld zurückfordern.

c't kompakt

- Schutzdienste verschicken in Ihrem Auftrag automatisierte Löschaufforderungen an Firmen und Datenbroker. Wir haben zwei davon getestet.
- Es gibt jedoch Tausende von Datenbrokern und Sammlern. Die Schutzdienste können nur einen Bruchteil abdecken, sodass Ihre Daten weiter zirkulieren.
- Statt Dienstleister zu beauftragen, ist es oft billiger und effizienter, Accounts manuell zu kündigen und Daten selbst löschen zu lassen.

Das Angebot wirkt auf den ersten Blick aufgeräumt und professionell aufgesetzt. Incogni fragt lediglich die E-Mail-Adresse sowie den Namen ab und verzichtet auf Angaben zu Telefonnummer und Adresse. Nachdem man per Kreditkarte bezahlt hat, soll man per Maus eine rechtsverbindliche Vollmacht unterschreiben, mit der Incogni die Datenlöschung bei verschiedenen Anbietern verlangt. Eine weitere Identitätsprüfung findet nicht statt.

Im Test mit einer deutschen Mailadresse landeten wir nach wenigen Minuten auf einem aufgeräumten Dashboard, das 91 Datenhändler listet. Wer will, kann sich durch die einzelnen Anbieter klicken, bekommt aber nur rudimentäre Informationen. Die Liste reicht von dem deutschen Marktforschungsunternehmen GfK über den Marketing-Anbieter ID5, der Interessenprofile für die Werbeindustrie verknüpft, bis hin zum Videoportal Dailymotion. Incogni fragte uns gar nicht erst, ob wir einen der Dienste tatsächlich nutzen, sondern verschickte sofort die Löschaufforderungen in unserem Namen.

In den folgenden Wochen konnten wir auf dem Dashboard den Fortschritt der Händlerreaktionen und Löschungen verfolgen. Diese können laut Surfshark bis zu 45 Tage dauern. Nach zwei Wochen hatten lediglich 21 der 91 angeschriebenen Anbieter reagiert.

Ob die Anbieter tatsächlich Daten von uns besaßen, erfuhren wir nur im Ausnahmefall. Ein Anbieter schickte seine Antwort nicht nur an Incogni, sondern auch an unsere E-Mail-Adresse und teilte darin mit, dass es überhaupt keinen Datensatz gebe, den man löschen könnte. Im Incogni-Portal wurde der Eintrag dennoch als Erfolg markiert.

Was genau bei welchem Unternehmen gelöscht wird, können Incogni-Kunden nicht beeinflussen: Weder kann man andere Datenbroker außerhalb der vorgefertigten Liste kontaktieren, noch andere persönliche Daten abseits der E-Mail-Adresse tilgen lassen. Das erleichtert es den Datenbrokern, sich dumm zu stellen. Wer bei einem Anbieter nicht mit exakt der gleichen E-Mail-Adresse und der gleichen Namensschreibweise registriert ist, braucht nicht auf Löschung zu hoffen.

Privacy Bee

Der in Atlanta ansässige Anbieter Privacy Bee existiert seit 2020. Er richtet sich hauptsächlich an US-Kunden, da er sich auf den California Consumer Privacy Act (CCPA) beruft.

Die Aufmachung von Privacy Bee weckt sofort Misstrauen. Der Dienst warnt mit alarmistischer Sprache vor den Gefahren für die Privatsphäre, bleibt aber höchst vage, wenn es um den konkreten Nutzen des eigenen Angebots geht. Dafür wirbt die Firma mit begeisterten Zitaten von Medien wie dem US-Techmagazin VentureBeat. Eine einfache Google-Suche zeigt schnell: Dieses Zitat stammt nicht etwa von einem Journalisten, der den Dienst getestet hat, sondern von Harry Maugans selbst, dem CEO von Privacy Bee.

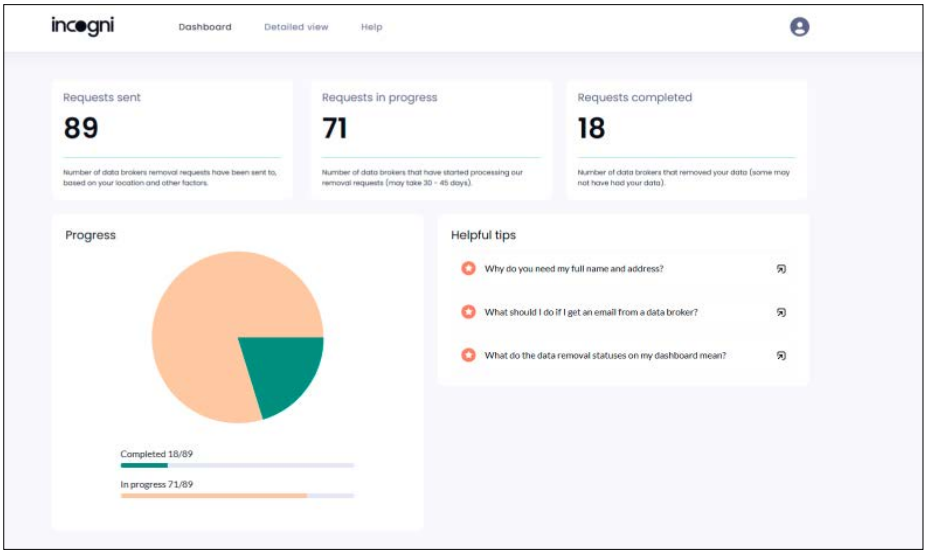
Vor Abschluss eines Abos prüft Privacy Bee kostenlos, wie weit die eigenen Daten schon verbreitet sind: Außer Namen und E-Mail-Adresse kann man auch seine Telefonnummer in den Angeboten von über 282 Datenbrokern suchen lassen. Die meisten davon sind einfache Personensuchmaschinen, die zum Beispiel öffentliche Informationen aus Telefonverzeichnissen oder gar aus Gerichtsunterlagen systematisch scannen und weiterverkaufen.

Doch selbst als wir uns zum Test mit einem Fantasienamen und einer frisch angelegten E-Mail-Adresse anmeldeten, sprang die Risiko-Ampel auf „Medium Risk“ und meldete „38 Exposures“. Die kostenlose „Prüfung“ ist also nichts weiter als Panikmache, die Interessierte zum Abschluss eines kostenpflichtigen Abos für 197 US-Dollar pro Jahr bewegen soll.

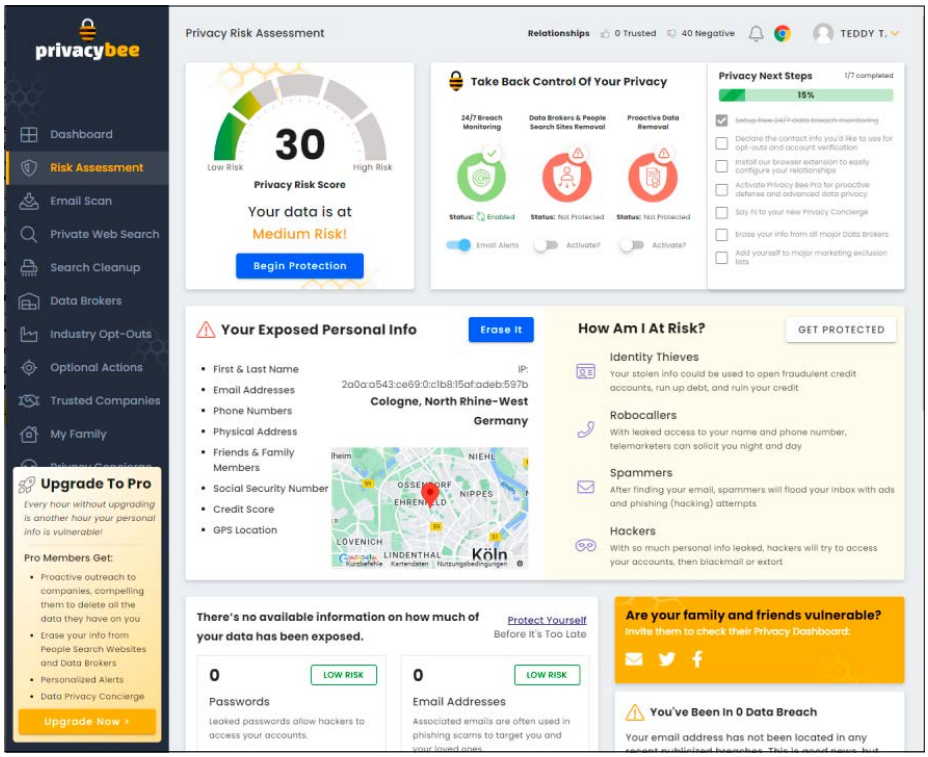
Dazu bietet Privacy Bee eine Reihe von Zusatzleistungen an, darunter eine Browser-Erweiterung, die auf Tracker in Websites hinweist und einen Concierge-Service, der Fragen zur Privatsphäre beantworten soll.

Besondere Vorsicht ist beim E-Mail-Check geboten, mit dem Privacy Bee automatisch die Postfächer seiner Kunden bei Google, Yahoo und Outlook.com durchsuchen und unerwünschte Mails abbestellen will. Dafür verlangt Privacy Bee die Zugangsdaten des E-Mail-Postfachs.

Dies ist generell eine schlechte Idee, denn es besteht die Gefahr, dass das Unternehmen die Daten aus den Scans anderweitig verwendet und an Dritte verkauft. Nicht zuletzt erhalten Spammer durch das automatisierte Klicken auf Opt-Out-Links eine kostenlose Bestätigung, dass ihre E-



Incogni präsentiert sich sehr aufgeräumt, geizt aber mit Informationen. Dass die angeschriebenen Unternehmen mitunter gar keine Daten gelöscht haben, erfährt man hier nicht.



Privacy Bee liefert bedeutend mehr Infos als Incogni, greift aber auch zu aggressiven Verkaufsmethoden. Ungefährdete Nutzer gibt es laut der kostenfreien Ersteinschätzung gar nicht.

Mail gelesen wurde – dadurch kann sich die Spamwelle sogar vergrößern.

Statt die Bedrohung durch Ransomware-Erpresser zu verringern, erhöht Privacy Bee diese sogar. Man stelle sich nur vor, der Dienst würde selbst Opfer eines Erpressers, und dieser würde neben den Namen und Telefonnummern der Kunden auch deren Zugänge zu Mail-Konten erbeuten. Geben Sie deshalb niemals nie einem Dienstleister die Zugangsdaten Ihres E-Mail-Kontos. Selbst wenn er seriöser wirkt als Privacy Bee.

Datenschützer in den USA

Außer einfachen Datenlöschdiensten wie Privacy Bee und Incogni finden sich auch US-Firmen wie Optery und Kanary, die mit aufwendigeren Dienstleistungen werben: Kanary etwa buhlt um Familien, die für 150 US-Dollar pro Jahr Informationen über ihre Kinder innerhalb von 24 Stunden aus der Google-Suche entfernen wollen. Optery verspricht, nicht nur Formschreiben automatisch zu verschicken, sondern in schwierigen Fällen auch menschliche Mitarbeiter mit der Datenlöschung zu betrauen.

Optery ist zwar mit bis zu 25 Dollar pro Monat ein vergleichsweise teures Angebot, informiert die Kunden aber auch klar über die Grenzen des Machbaren. So benennt das Unternehmen mehrere „Dishonorable Data Brokers“, die Löschaufforderungen nicht oder nur unzureichend erfüllen. US-Bürgern steht es dann frei, sich bei der Federal Trade Commission oder dem Generalstaatsanwalt von Kalifornien zu beschweren. Der Dienst plant eine Ausweitung auf den europäischen Raum, konnte auf Anfrage der c’t aber noch keinen Termin nennen. Wir sahen deshalb von einem Test ab.

Vom Schützer zum Broker

Darüber hinaus findet man aber auch Firmen, die inzwischen die Seiten gewechselt haben und vom Datenschützer zum Datenbroker wurden. Das britische Start-up Digi.me entwickelte zum Beispiel ursprünglich eine Software, mit der Nutzer die Datenbestände unterschiedlichster Plattformen gesammelt auf ihren Rechner herunterladen konnten. Inzwischen widmet sich das Unternehmen jedoch einem anderen Kundenkreis: Auf seiner Website wirbt Digi.me um Firmen, die Zugriff auf diese Daten erhalten wollen und betont, dass die Betroffenen dieser Verwertung zugestimmt haben.

Im Oktober 2022 wurde Digi.me vom australischen Datenbroker World Data Exchange übernommen, der Firmenkunden auch Zugang zu Gesundheitsdaten und zu Kontenbewegungen verschaffen will. Auch zahlreiche andere Unternehmen haben sich ähnlich wie Digi.me umorientiert, viele ursprüngliche Datenschutz-Initiativen sind ganz von der Bildfläche verschwunden.

Deformierte Biometriedaten

Besonders invasive Datenverarbeiter wie Clearview AI, die Milliarden von Bildern von Social-Media-Plattformen auswerten und innerhalb einer juristischen Grauzone agieren, werden von den kommerziellen Datenlöschern noch ganz ausgespart. Dabei können solche biometrischen Datensammlungen existenzielle Probleme verursachen: Solche Dienste wurden zum Beispiel genutzt, um Pornodarsteller bloßzustellen oder Teilnehmer von Demonstrationen an Strafverfolger melden. Gegen solche Datensammlungen anzugehen ist zeitaufwendig, wie zum Beispiel der Spiegel-Redakteur Patrick Beuth erfuhr: Erst nach mehreren Monaten und zahlreichen schriftlichen Aufforderungen löschte Clearview AI seine Daten.

Zum Schutz vor biometrischen Datensammlern wie Clearview AI empfiehlt Beuth das Online-Tool Lowkey der Universität Maryland (lowkey.umiacs.umd.edu). Lowkey deformiert Gesichter in Bildern, sodass diese sich deutlich schwieriger automatisiert zuordnen lassen.

Datensparsamkeit

Weil sich Daten, die bereits öffentlich sind oder kommerziell gehandelt werden, oft nicht mehr rückstandslos beseitigen lassen, sollte man den eigenen Datenabdruck im Internet so weit wie möglich minimieren. Verweigern Sie etwa die Herausgabe nicht unbedingt notwendiger Informationen wie Telefonnummern, Geburts- und Adressdaten, wann immer möglich.

Ebenso kann man die Synchronisation verschiedener Datenbestände erschweren, wenn man bei unterschiedlichen Internetdiensten verschiedene E-Mail-Konten verwendet. Viele Online-Shops bieten zum Beispiel einen Gastmodus an. Das ist zwar mitunter unbequemer als einen Kunden-Account anzulegen, aber in der Regel nicht mit gravierenden Nachteilen verbunden. Die Zahlungsdaten müssen Geschäfte bei Bestellungen allerdings weiterhin speichern.

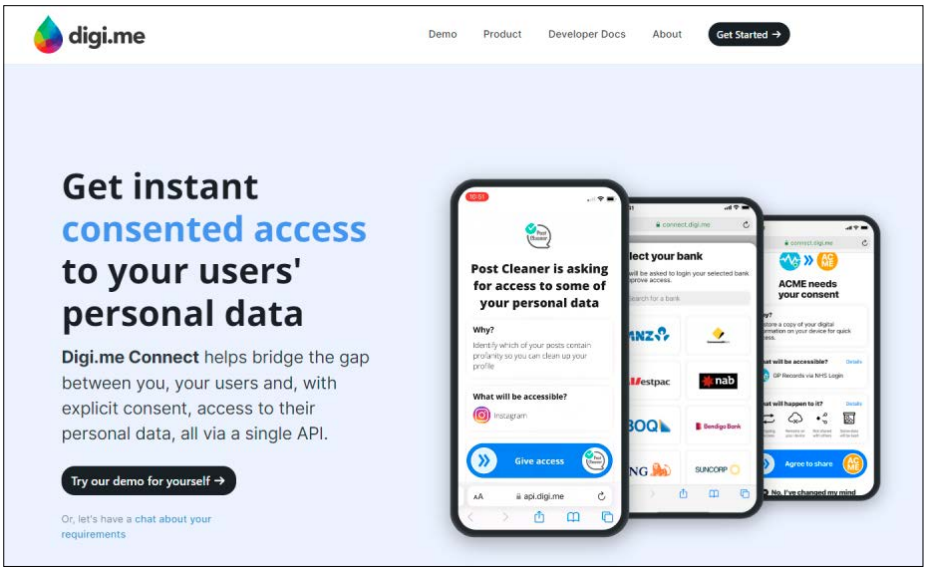
Fazit

Bei den Datenlöschdiensten muss man sehr genau unterscheiden, ob sie sich an

Kunden innerhalb der EU oder in den USA richten. In den USA ist die Rechtslage beim Datenschutz derzeit stark in Bewegung. Kommerzielle Datenlöschdienste können dort mit Sammelklagen und anderen Rechtsmitteln durchaus dazu beitragen, dass Datenhändler den Datenschutz künftig ernster nehmen.

In der EU bringen die bisherigen Schutzanbieter jedoch herzlich wenig. Dienstleister wie Incogni machen oft nicht mehr, als automatisierte Löschaufforderungen an Anbieter zu verschicken, die solche Löschungen bereits ihrerseits weitgehend automatisiert haben. Sie treffen damit nur einen winzigen Teil der Datenhändler und können nicht verhindern, dass die einmal gelöschten Daten am nächsten Tag an anderer Stelle wieder auftauchen. Gegen Leaks im Darknet, die sich aus Ransomware-Angriffen auf Firmen speisen, können sie nichts ausrichten.

Da ist es billiger und effizienter, Accounts manuell zu kündigen und Daten selbst löschen zu lassen. Vordrucke, Adressen und Anleitungen finden Sie etwa auf justdelete.me und aboalarm.de, wenn auch deren Anleitungen nicht immer aktuell sind. Die Löschung ungenutzter Accounts verhindert nicht zuletzt, dass Online-Händler oder Forenbetreiber ihren Datenschatz bei einer Insolvenz an Datenbroker verscherbeln. *(hag@ct.de)* c't



Das Unternehmen Digi.me warb erst dafür, dass Nutzer ihre Daten selbst verwalten können, nun verkauft es den Zugriff auf diese Daten an Firmenkunden.