Business Punk

WORK HARD. **PLAY** HARD.

AUSGABE 01_2014 6,90 Euro WWW.BUSINESS-PUNK.COM

NETFLIX
Die „House of Cards"-Erfinder wollen das deutsche Fernsehen plattmachen

SNAPCHAT
Selbstzerstörung als Prinzip: Darum pfeifen die Typen mit der Fotoapp auf die Facebook-Kohle

HASS IM BÜRO
Das Arschloch muss weg. So wird man es los

INSIDE „STROMBERG"
CAST UND CREW VERRATEN: ALLES

FUCK OFF, NSA!

Mit PIRATE BAY kämpfte er gegen die Webzensur, jetzt zieht Peter Sunde in den Krieg gegen den Abhörterror

PLUS DOSSIER IT-SICHERHEIT
NO-SPY-STARTUPS /// JAGD AUF SCHNÜFFLER /// CROWD GEGEN HACKER

ITALIEN, SPANIEN € 7,95
SCHWEIZ SFR 12
4 191709 506002 01

SCHLÜSSEL-

Text: **Christian Cohrs**

Am Ende ist es natürlich egal, ob es um sensible Gesundheitsdaten geht, den Aufenthaltsort eines Handybesitzers oder Männer in grünen Pullovern. Aber die Pullovermänner sind eben anschaulicher, wenn Felix Bauer erklärt, wie er die Auswertung großer Datenmengen mit dem Datenschutz versöhnen will.

Der Pulloverträger, den Bauer als Erklärhilfe aussucht, gehört zu den Besuchern der Innovation Days, einer Art Leistungsschau der deutschen Forschungsdickschiffe Max-Planck- und Fraunhofer-Gesellschaft sowie Helmholtz- und Leibniz-Gemeinschaft. Ende Dezember präsentieren sie im DDB Forum an der Berliner Friedrichstraße, woran in deutschen Laboren getüftelt wird: Steuersoftware für menschenähnliche Roboter, künstliche Schließmuskel, so was. Im Atrium zwischen den Vortragssälen stehen weiße Besprechungsboxen mit den Namen von Dax-Konzernen, die hier Talente und Ideen suchen.

Was aber, wenn das hier keine Roadshow für Forscher wäre, sondern hochvertraulich, fragt Bauer. Wenn jemand draußen zwar wissen dürfte, dass hier Männer in Pullovern rumlaufen, aber nicht, wie viele einen grünen Pulli tragen? Dann könnte seine Erfindung dafür sorgen, dass alle Daten, die den Raum verlassen so weit anonymisiert sind, dass sie keine Rückschlüsse auf bestimmte Personen zulassen.

Aircloak heißt die Technik, die Bauer mit anderen Wissenschaftlern am Max-Planck-Institut für Softwaresysteme in Kaiserslautern entwickelt hat. Sie soll das Problem lösen, dass immer wertvolle Informationen verloren gehen, sobald man sensible Daten wie Krankenakten anonymisiert. Durch Aircloak wird ein Zugriff auf die kompletten Daten möglich, da sie verschlüsselt auf einen Hochsicherheitsserver gelangen und bei der Antwort auf jede Anfrage Anonymität sichergestellt wird. Etwa, indem Aircloak Ergebnisse bei kleinen Mengen mit Rauschen belegt, also statt exakter Zahlen Von-bis-Angaben ausspuckt oder Antworten ganz verweigert, wenn diese eine eindeutige Identifizierbarkeit ermöglichen könnten.

Basis von Aircloak ist ein TPM, ein Chip, der Computer mit Sicherheitsfunktionen ausstattet, sie aber zugleich eindeutig identifizierbar macht – und User damit kontrollierbar. „Wir drehen den Spieß um“, sagt Bauer. Statt zum Ausbremsen von Raubkopierern nutzt seine Hardware den Chip nicht nur zur Versiegelung der Daten, sondern auch, um die Funktionsweise von Aircloak für Außenstehende transparent und kontrollierbar zu machen.

Zum Zeitpunkt der Innovation Days gibt es einen Prototyp. Doch Bauer hat schon potenzielle Kunden im Blick, neben der Medizinforschung etwa Mobilfunkfirmen. Die säßen auf Bergen von Kundendaten, könnten sie aber aus rechtlichen Gründen nur eingeschränkt auswerten. Und selbst wenn ihnen unter Auflagen mehr erlaubt wäre: „Den Firmen ist klar, dass sie es nicht verkacken dürfen“, sagt er. Darum ist er optimistisch, nach dem Auslaufen des Existenzgründerstipendiums in knapp einem

-BRANCHE

Mit German Angst zum Weltmarktführer: Deutsche Startups entdecken Datenschutz als Standortvorteil und machen sichere Kommunikation zum Business

Jahr die Patente übernehmen und ausgründen zu können.

Erste Rückmeldungen machen Mut. Nicht nur von möglichen Kunden, sondern auch von Datenschützern: „Solche Ansätze würden wir gerne häufiger sehen“, lobt das Landeszentrum für Datenschutz Schleswig-Holstein. Im Januar hat Bauer ein internationales Unternehmen gefunden, das Aircloak testen will. „Das ist das erste Mal, dass wir echte Daten drauf loslassen können.“ Die Chancen stehen gut, dass aus dem Uni-Projekt bald eine Firma wird.

Anonymität, Datenschutz, Security – alles Themen, die gemeinhin nicht mit der Startup-Szene assoziiert werden. Dabei gibt es in Deutschland eine ganze Reihe junger IT-Firmen, die dem Internet ein wenig Privatsphäre zurückgeben wollen. Hier schlummert ein gigantisches Business. NSA-Skandal und der im Januar bekannt gewordene Diebstahl von 16 Millionen E-Mail-Adressen haben auch dem Arglosesten klargemacht, dass Sicherheit im Web mehr bedeutet als die Installation eines Virenscanners. Laut einer im Oktober 2013 veröffentlichten Studie zweier Ökonomen der University of Colorado Boulder wären Internetnutzer sogar bereit, dafür zu zahlen: 1,19 Dollar, um künftig ihren Aufenthaltsort zu verschleiern. Die Geheimhaltung all ihrer Kontakte wäre ihnen sogar 4,05 Dollar wert. Dieser Bewusstseinswandel befeuert eine ganze Branche, die nun schwankt zwischen Dankbarkeit, endlich nicht mehr als paranoid zu gelten, und Ambitionen auf die Weltmarkführerschaft.

Simon Specka tendiert zu Letzterem. „Wir wollen eine Marke aufbauen, die für mehr Privacy und Security im Internet steht“, sagt der Gründer von Zenmate. Das Berliner Startup launchte seine Erweiterung für Googles Chrome-Browser im Juni 2013, eine Woche nach dem Beginn der NSA-Affäre. Mit dem Plug-in können User anonym und geschützt vor Mitlesern surfen. „Wir sind selbst immer ein bisschen paranoid gewesen und haben uns immer weitestgehend gesichert“, sagt Specka. Wie sein Mitgründer war er im Studium oft unterwegs und im Ausland, ging nur über verschlüsselte VPN-Verbindungen ins Netz.

Dieser Weg zu mehr Schutz persönlicher Daten im Netz ist jedoch vergleichsweise umständlich und

\\Aircloak

Ursprünglich wurde an Felix Bauers Institut ein Weg gesucht, der Werbeindustrie datenschutzkonformen Zugriff auf Kundendaten zu ermöglichen. Das erwies sich als kompliziert und teuer, brachte die Wissenschaftler aber auf die Idee für ihre Technologie, mit der Datenbanken weitreichend ausgewertet werden können und die Anonymität trotzdem garantiert bleibt.

\\Protonet

„Das Design stand von Anfang an", sagt Ali Jelveh über seinen orangefarbenen Serverwürfel. Ebenso die Idee, dass der sofort nach dem Aufstellen einsatzbereit sein soll. Ein paar Dutzend der ab 3400 Euro teuren Geräte hat er bereits verkauft. Im kommenden Jahr sollen es bis zu 1000 werden. Dabei mag helfen, dass eine preiswertere Version in Arbeit ist.

»Es ist ganz geil, die Firewall eines Landes auszutricksen. Aber wir sind nicht in der Position, uns mit der chinesischen Regierung anzulegen«

SIMON SPECKA \\ *Zenmate*

setzt technische Kenntnisse voraus. So kamen die beiden auf die Idee mit dem Plug-in, über das sich das sichere Internet per Klick an- und ausschalten lässt. „Wir haben das Rad nicht neu erfunden", sagt Specka, „sondern es einfacher gemacht und schöner verpackt." Klingt simpel, doch dahinter stecken eine Menge Know-how und eine Infrastruktur mit Servern auf mehreren Kontinenten.

Nur fünf Prozent der annähernd eine Million User kommen aus Deutschland, beinahe dreimal so viele aus den USA, 38 Prozent aus Südkorea. Dort ging Zenmate im vergangenen November viral, was den Berlinern in nur drei Tagen 200 000 Downloads bescherte. Vor allem die europäischen Kunden verfolgten einen, so nennt Specka es, „hedonistischen Approach". Sie nutzen Zenmate, um sich als Surfer aus den USA auszugeben und in Deutschland gesperrte Musikclips angucken zu können oder um Videodienste wie Hulu zu unblocken. Global betrachtet wachse jedoch die Zahl der Nutzer, die sich durch das Plug-in Sicherheit verschaffen wollen. Beispielsweise beim Onlinebanking in einem öffentlichen W-Lan. Und dann gibt es noch die Gruppe der vom freien Web Ausgesperrten, „die in ihren Ländern fundamental in ihren Internetrechten, wie wir sie verstehen, beschnitten werden", beschreibt sie Specka. Diese Leute, „die nicht einmal auf Wikipedia zugreifen können", liegen ihm sichtlich am Herzen.

Specka mag die „Revoluzzer-Schiene", auf ein Wettrüsten mit Chinas Great Firewall will er sich aber nicht einlassen. Zenmates mit jedem Kunden steigende Serverkosten werden mit Wagniskapital bezahlt, das Startup muss bald Geld verdienen. Darum soll aus dem kostenlosen Dienst ein Freemium-Modell erwachsen. Die Bezahlversion könnte die Anonymisierung weitertreiben, sagt Specka, und den Browserfingerprint „durch den Mixer jagen". Denn diese sehr individuellen Daten werden als Tracking-Alternative zu den von vielen Surfern geblockten Cookies immer beliebter.

Schon jetzt hat Specka – es geht ihm schließlich um den Aufbau einer Marke – weiter gehende Pläne. „Nach dem Surfen wollen wir im nächsten Schritt die Onlinekommunikation privater und sicherer machen." Aktuell tüfteln die Berliner an einem Tool, das Schluss machen soll mit den Awkward-Momenten, wie man sie von Facebook kennt, wenn beim Geburtstagsgruß an die Ex immer gleich das Liebesgesäusel vergangener Tage mitaufpoppt. Wie das Anonymisierungs-Plug-in soll auch der geplante Kommunikationsdienst browserbasiert sein. Wieder geht es darum, vorhandene Technik simpel zu machen und schön zu verpacken, dass sie jeder nutzen kann.

Die Notwendigkeit einer besseren Absicherung ihrer Daten haben auch Firmen erkannt. „Oft geht es nur noch darum, welche Lösung eingesetzt wird, und nicht ob", sagt Thomas Gutsche, Mitgründer von Tutanota. Früher hat der Hannoveraner bei PricewaterhouseCoopers gearbeitet und mit sensiblen Daten zu tun gehabt. Viele Klienten hätten diese am liebsten per Dropbox übermittelt. „Für ein renommiertes Unternehmen natürlich ein absolutes No-Go", sagt Gutsche. Angestoßen von dieser Sorglosigkeit, überlegte er mit Freunden, wo das größte Verbesserungspotenzial liegt, wenn es um den Austausch vertraulicher Daten geht. „Da kamen wir ganz schnell auf E-Mails."

Mehr Sicherheit soll auch hier ein Plug-in bringen. Jedoch nicht für den Browser, sondern für Outlook. Ist es aktiviert, werden E-Mails per End-to-End-Verschlüsselung über einen Tutanova-Server verschickt. Hat der Empfänger das Plug-in nicht, erhält er alternativ einen Link. Ein Klick, und er kann die verschlüsselte Mail über eine sichere Verbindung direkt im Browser aufrufen und nach Eingabe eines per SMS übermittelten Codes lesen. In beiden Fällen werden die Mails auf den Rechnern der Absender und Empfänger lokal ver- und entschlüsselt. Das Verfahren von Tutanota ist – anders als De-Mail – zwar nicht behördlich anerkannt, dafür ohne kompliziertes Anmelde- und Verfizierungsprozedere und in Verbindung mit normalen Mailadressen nutzbar.

Als Kunden hat Gutsche Personen ausgemacht, „die tagtäglich mit personenbezogenen, datenschutzrelevanten Daten umgehen": Rechtsanwälte, Steuerberater, Wirtschaftsprüfer, Unternehmensberater.

\\Zenmate

„Das Internet wurde nicht mit der Idee entwickelt, dass irgendwann das ganze Leben digitalisiert ist", sagt Simon Specka (l.). Damit trotzdem noch ein Rest Privatsphäre bleibt, haben er und sein Mitgründer Markus Hanel ein Plug-in entwickelt, mit dem sich sicher und anonym surfen lässt. Denn: „Du gehst ja auch nicht aufs Klo und lässt die Tür offen."

\\Tutanota

E-Mails sind für die Übermittlung vertraulicher Daten so geeignet wie Postkarten. Das wollen Matthias Pfau, Thomas Gutsche und Arne Möhle (v.l.) ändern, indem sie über eine Cloudlösung sichere End-to-End-Verschlüsselung direkt aus dem Mailprogramm anbieten. Außerdem startet im Frühjahr ihr kostenloser Webmail-Dienst Tutanota Free. Apps für Smartphones sollen später folgen.

\\Secusmart

„Bei den professionell Paranoiden spielt Sexiness keine so große Rolle", sagt Hans-Christoph Quelle. Da inzwischen aber nicht mehr nur Agenten die Notwendigkeit sicherer Handys erkannt haben, sondern auch ästhetisch anspruchsvollere Kunden wie Politiker und Geschäftsleute, stattet seine Dusseldorfer Firma Blackberry-Smartphones mit einem Sicherheitschip aus.

Auch ein paar „Hidden Champions" hätten bereits Interesse bekundet. „Die wollen geheime Unterlagen wie Entwicklungspläne mit ausländischen Töchtern oder Partnern sicher austauschen."

Wenn selbst Schraubenhersteller über eine Absicherung ihrer Kommunikationswege nachdenken, eröffnet sich Hans-Christoph Quelle ein Milliardenmarkt. Nachdem er zunächst für Nokia an sicherer Sprachübertragung gearbeitet hatte, gründete Quelle 2007 Secusmart. Zwei Jahre später bekam das Düsseldorfer Startup den Zuschlag, die Bundesregierung mit sicheren Handys zu beliefern. Weil aber viele Politiker ihr iPhone dem sicheren Telefon vorzogen, entwickelte Quelle die Idee, „Security so weit zu bringen, dass sie nicht mehr stört". Das Ergebnis war eine Micro-SD-Karte, die aus einem Blackberry Z10 ein Smartphone mit sicherem und privatem Bereich für Apps macht. Nachdem Secusmart der deutschen Regierung und den Bundesministerien bereits 2000 „Merkel-Handys" verkaufen konnte, nimmt Quelle nun verstärkt ausländische Behörden und Firmenkunden ins Visier: Auf der Cebit wird seine Firma eine abhörsichere Festnetz-Telekommunikationsanlage vorstellen, die „Merkel-Infrastruktur", so der etwas ungelenke, aber sicher verkaufsförderliche Name.

Seit nicht mehr nur Paranoiker sich für IT-Sicherheit interessieren, taugt das Thema sogar zum Hardware-Hype. Das bewies Anfang 2013 das Startup Protonet. Per Crowdfunding sammelten die Hamburger das Vierfache der benötigten 50 000 Euro ein, um ihre orangefarbene Box auf den Markt zu bringen. Das Konzept, eine Art private Cloud, die man sich ins Büro stellt, traf auf das schon damals wachsende Bedürfnis, wieder Herr über die eigenen Daten zu sein. Dabei betont Protonet-Mitgründer Ali Jelveh: „Wir sind eine Software-Company." Protonet ist nicht als Datensafe gedacht, sondern als ein Server, auf dem Software läuft, die gemeinschaftliches Arbeiten vereinfacht. Kritiker schossen sich trotzdem darauf ein, Protonet Sicherheitslücken nachzuweisen. Das Startup nimmt es sportlich und ist bemüht, Schwachstellen zu beseitigen. Doch Jelveh weiß: „Wenn die NSA wo reinwill, schafft die das auch."

Den Schnüfflern es zumindest schwer zu machen ist das Ziel von Secucloud, ebenfalls aus Hamburg. Gründer Dennis Monner hat früher Firewall-Hardware gebaut und festgestellt, dass viele Kunden überfordert waren, die 10 000 Euro teuren Geräte

\\Secucloud

Große Sorgen um die NSA müssten sich deutsche Surfer eher nicht machen, aber um Kriminelle, die ihre Kreditkartennummer ausspähen, sagt Dennis Monner (u.r.). Damit auch diese Sorge verschwindet, will ihnen der Chef von Secucloud eine rote Box ins Wohnzimmer stellen, die sämtlichen Traffic über die Server seiner Sicherheitsfirma leitet. Außerdem plant er, Internet-Serviceprovidern anzubieten, die Router ihrer Kunden mit seiner Software auszustatten.

> »Der Präsident eines Landes hat sein amerikanisches Handy weggeschmissen und gesagt: ›Ich will das, was Frau Merkel hat‹«
>
> **HANS-CHRISTOPH QUELLE** \\ *Secusmart*

richtig einzustellen. So kam er auf die Idee, statt hochkomplexer Hardwaresysteme eine Cloudlösung zu entwickeln. Secucloud leitet den kompletten Traffic der Kunden über eigene Server, die durch High-End-Firewalls gesichert sind.

Dass Monner in diesem Frühjahr trotzdem eine rote Kiste auf den Markt bringt, hat eher mit Psychologie zu tun. „Die Leute wollen etwas anfassen", sagt Monner. Und: „Die Box ist gar nicht intelligent." Denn im Grunde steckt in der Secubox+ nur ein W-Lan-Router, der alle Daten verschlüsselt an Secucloud schickt. Der Psychotrick funktioniert so gut, dass Monners Crowdfunding bei Seedmatch den von Protonet aufgestellten Rekord kassierte und 500 000 Euro statt der geplanten 50 000 Euro einbrachte.

Obschon die Kampagne auch als Testballon für Marktakzeptanz gedacht war, verweist sie auf ein Problem deutscher Security-Startups: „Wenn jemand in den USA eine coole Idee hat, bekommt er 5 Mio. Dollar und legt los", sagt Monner. Hierzulande sei das leider noch nicht so.

Doch das Interesse an der Branche wächst dank beständiger Skandale stetig, und der Standort Deutschland profitiert jedes Mal davon. „Die amerikanische Kryptoindustrie hat sich desavouiert", sagt Secusmart-Chef Quelle. Deutschland sieht er in einer guten Position, denn die Größe des Heimatmarkts sei zwar entscheidend. Nicht minder wichtig aber sind die rechtlichen Rahmenbedingungen. „Die Gesetze sind in Deutschland, wie sie sind", sagt Dennis Monner von Secucloud, der Einbau von Backdoors etwa ist anders als in den USA verboten. Das sei von Vorteil für die weltweite Vermarktung. Auch Tutanota-Gründer Gutsche bezeichnet es als „echten Mehrwert bei einer Internationalisierung", nicht dem Patriot Act unterworfen zu sein.

Mögen deutsche Gründer oft mit rechtlichen Rahmenbedingungen hadern, in diesem Fall sind sie ganz zufrieden: „Sinnvolle Gesetze muss man nicht ändern", sagt Felix Bauer von Aircloak, „aber man kann versuchen, technische Lösungen für die Einschränkungen zu finden, die aus diesen Gesetzen entstehen." Und wenn irgendjemand doch meint, die Gesetze ändern zu müssen, weil die Vorratsdatenspeicherung kommt? Dann empfiehlt Simon Specka Arnold Schwarzenegger: „Break the rules, not the law. But break the rules." ▮