



Evgeny Chereshevnev (Foto: Stifterverband)

Aufstand im Internet der Dinge

VERÖFFENTLICHT AM 04.08.2017

Ein internationales Team um den IT-Security-Experten Evgeny Chereshevnev entwickelt eine Software, die digitale Nutzerdaten hundertprozentig verschlüsselbar machen soll. Jeder Internetnutzer kann dann eigenständig entscheiden, wem und unter welchen Bedingungen er seine Daten zur Verfügung stellt. Ein Interview über ein Projekt, das auch die Spielregeln von Big Data verändern könnte.



LESEZEIT: 9 MINUTEN

TEXT:

ERNST TIMUR DIEHN >

Vor einigen Jahren ließen Sie sich einen Biochip in Ihre linke Hand implantieren.

Damals entwickelten wir den Prototyp eines einheitlichen, digitalen Schlüsselsystems. Das Implantat ist zwölf Millimeter groß, besitzt einen eingebauten Speicherchip und eine Antenne. Es steuert meine Computer und mein Handy an und identifiziert mich ohne PINs oder Fingerabdruck. Über den Chip kann ich mich digital ausweisen, bräuchte also keinen Pass oder andere Ausweise mehr mit mir herumzutragen. Man könnte medizinische Patienten- oder Versicherungsdaten auf dem Chip direkt lesbar machen. Auch jeder Kaufvorgang ließe sich abwickeln, indem ich einfach die Hand über ein mit Sensoren bestücktes Bezahlterminal halte. Wahrscheinlich werden schon in zehn Jahren ähnliche Möglichkeiten digitaler Identifizierung zum Alltag gehören.

Als Träger des Chips fühlen Sie sich als lebender Teil des Internets der Dinge ...

Wir programmierten den Chip darauf, mit anderen smarten Objekten zu interagieren – zum Beispiel mit Türen, in die elektronische Sensoren eingebaut sind. Ich mache mit der Hand eine Wink- oder

Wischbewegung und schon öffnet oder schließt der Chip die Tür. Klappte die Funkübertragung aber nicht oder konnte das digitale System mich nicht mehr identifizieren, kam ich prompt nicht mehr in mein Büro und noch nicht einmal mehr auf das Firmengelände. Das war ein bisschen so, als ob es mich gar nicht mehr geben würde ...

Natürlich haben Sie das Problem behoben.

Trotzdem wurde auch gleich das Wachpersonal nervös, obwohl die Jungs mich persönlich kannten. Solche und ähnliche Erfahrungen stimmen mich nachdenklich.

BIG BROTHER IM SMART HOME



Foto: iStock/ Chesky_W

Ihre Experimente klingen schon interessant. Aber wer ist denn in dieser Form überhaupt mit dem gerade entstehenden Internet der Dinge verbunden?

Ob mit oder ohne Biochip bekommt die Qualität von Apps und digitalen Services einen immer höheren Stellenwert: Störungen betreffen schon lange nicht mehr nur ein beliebiges technisches Gerät, das Sie besitzen, sondern beeinträchtigen unmittelbar Ihre Lebensqualität. Stellen Sie sich vor, Sie würden wegen eines Bugs oder weil Sie gehackt worden sind alle Ihre Dokumente, Log-ins, Pässe und Kontozugänge verlieren. Um Ähnliches erleben zu können, wird man im Internet der Dinge sicher keinen Biochip tragen müssen. Dank der Experimente mit dem Chip konnte ich mir jedenfalls ein Bild davon machen, wie es sich für uns Menschen anfühlen könnte, ein Sensor, ein Smart Device, für ein stetig anwachsendes Kommunikationssystem zu sein. Noch im Jahr 1992 waren Computer Werkzeuge und wir ganz eindeutig die Nutzer. Schon im Jahr 2020 wird es schätzungsweise bereits 50 Milliarden Geräte mit eigenständiger digitaler Sensorik geben. Die meisten werden rund um die Uhr Daten – auch über uns und unser Verhalten – aufnehmen und an andere smarte Dinge weitersenden. Das alles macht Themen wie Privacy-Management, Datenschutz und Cybersecurity wirklich brisant. Man fängt an, gängige Szenarien anders zu betrachten: Was bedeutet es zum Beispiel, in einem smarten Haus zu leben, das permanent Ihr Verhalten scannt, analysiert und diese Daten an andere weitergibt?

Die meisten neuen digitalen Services, die das Internet der Dinge ermöglicht, werden sinnvoll sein. Das wäre zumindest zu erhoffen. Und für viele Dienstleistungen werden wir nicht einmal etwas bezahlen müssen ...

Falls ein digitaler Service im Netz frei verfügbar sein sollte, bedeutet das, dass Ihre Nutzerdaten – also Sie

selbst – zum Produkt geworden sind. Was macht einen smarten Kühlschrank denn aus der Sicht seiner Produzenten smart? Dank eingebauter Sensoren weiß der Kühlschrank, wer Sie sind, welche Nahrungsmittel Sie einkaufen, wann Sie welche Zahlungsarten verwenden. Diese Daten werden zum Unternehmen gesendet, das das Gerät gebaut hat. Der Konzern verwendet Ihr Verhalten als Rohstoff ...

... natürlich auch, um das Produkt zu verbessern ...

... und für Big-Data-Analysen. Oder er verkauft diese Daten weiter. Wir lassen uns auf mehr und mehr Services ein, die vor allem deshalb „smart“ genannt werden können, weil sie auf geschickte Art Daten über uns sammeln.

NUTZERDATEN SMART MANAGEN

So weit, so bekannt.

Schon heute tracken mehr als 2.000 Netzwerke unsere Bewegungen, um mithilfe automatisierter Bot-Technologien unsere digitalen Neigungen zu analysieren. Viele der Apps, an die wir uns gewöhnt haben, versenden ständig sensible Daten über uns. Fitnesstracker sammeln zum Beispiel Daten über unsere Gesundheit und unseren Körper. Auch das Offlinetracking mit WLAN- und Bluetooth-Signalen wird in Flughäfen oder Geschäften wie selbstverständlich eingeführt. Am Ende entsteht ein riesiges Netz aus intelligenten Dingen, die die ganze Zeit Daten miteinander tauschen. Zudem sollen jetzt ganze Regierungen, Verwaltungen, Städte „smart“ gemacht werden, nicht nur Häuser und Autos. Letztlich bedeutet das: Unsere sozialen Systeme verschmelzen zu einem riesigen digitalen Sensorsystem. Und nur wenn wir den berühmten „I agree“-Button drücken, den „Geschäftsbedingungen“ zustimmen und unsere Privacy-Rechte auf unsere persönlichen Nutzerdaten abtreten, können wir diese ganzen neuen digitalen Programme und Services überhaupt nutzen. Diese Praxis kennen wir doch schon ...

Viele User haben sich an diese Vorgehensweise gewöhnt. Und wir mögen ja auch die „smarten Leistungen“, die uns bereits angeboten werden.

Bevor ich meine Erfahrungen mit dem Chip gemacht habe – der ja über Jahre ständig weiter Daten über mich sammelt, damit ich noch besser mit smarten Dingen interagieren kann –, habe ich auch gedacht: „Wow, ich möchte in einem smarten Haus, in einer smarten Stadt wohnen. Was für eine fantastische Zukunft!“ Mittlerweile beunruhigt mich die Vorstellung eher. Smart sollte doch vor allem die Art sein, wie wir unsere eigenen Nutzerdaten managen, digital verschlüsseln und verwalten. Wir sollten mit unseren digitalen Daten so verfahren können wie mit Dingen, die uns physisch gehören, zum Beispiel unseren Autos. Falls Sie mein Auto nutzen möchten, können Sie das gerne tun – aber nur, wenn es mir sinnvoll erscheint und nach meinen Bedingungen.

Im Moment scheinen digitale Nutzerdaten allen möglichen Akteuren zu gehören, außer den 'Nutzern' selbst – also uns!



EVGENY CHERESHNEV

Evgeny
Chereshevnev
(Foto:
Stifterverband)

Nachvollziehbar.

Angenommen also, ein medizinisches Forschungsinstitut möchte Ihre medizinischen Daten digital abrufen und für eine klinische Studie verwenden. Falls Sie das Anliegen überzeugt, würden Sie Ihre medizinischen

Daten doch sicher gerne zur Verfügung stellen, oder?

Falls es nur die wirklich studienrelevanten Daten betrifft ... sicher.

Also ohne Ihre komplette Mail- und Surfhistorie, ohne Ihre Geostandortsdaten, Ihre Wohndaten oder andere sensible Informationen, dank derer ein Big-Data-Analyst zum Beispiel auch Ihre angebliche Kreditwürdigkeit herauslesen kann. So läuft das aber nicht. Im Moment scheinen digitale Nutzerdaten allen möglichen Akteuren zu gehören, außer den „Nutzern“ selbst – also uns!

Sie haben namhafte IT-Größen, die beispielsweise für Google oder Symantec tätig waren, von Ihrer Idee überzeugen können, eine Software zu entwickeln, die sämtliche digitalen Fingerabdrücke im Netz hundertprozentig verschlüsseln soll. Wie kommen Sie darauf, dass das technisch überhaupt klappen kann?

Es gibt bereits Software, die es prinzipiell ermöglicht, sichere Verschlüsselungscodes zu schreiben. Unser Produkt wird eine Art weißes Rauschen erzeugen, durch das man Ihren digitalen Fußabdruck nicht mehr zurückverfolgen kann. Dabei bleiben Ihre digitalen Daten für den eigenen Gebrauch identifizierbar. Flankiert wird das Ganze von einem KI-basierten System, das in Echtzeit alle Gefahrenquellen im Netz untersucht, um ständig neue passende Schutzmaßnahmen zu entwickeln. Sogenannte Tracker lesen neue Software im Netz aus, die von Data-Minern oder Hackern benutzt werden könnten. Ein weiterer Kern der neuen Technologie wird Daten unbegrenzt und sicher in der Cloud speichern, aufgeteilt nach verschiedenen Identitäten wie „Familie“, „Arbeit“ oder „privat“. Für die sichere Identifizierung unserer User halten wir bereits die notwendigen US-Patente – zum Beispiel zur verschlüsselten Übertragung biometrischer Daten und digitaler Fingerprints.



EVGENY CHERESHNEV

Evgeny Chereshnev ist Chief Executive Officer von **Biolink Tech** . Er war Global Vice President of Consumer Marketing bei Kaspersky Lab, einem international tätigen Unternehmen für Softwaresicherheit und Cybersecurity. Sein Blog BionicMan erregte internationale Aufmerksamkeit.

Wird das Endprodukt wie eine externe Festplatte aussehen, die ich an meinen Computer anschließe?

Wir werden unseren Service als App anbieten. Sie laden die Software herunter und erhalten regelmäßige Updates. Der Kunde zahlt zum Beispiel zehn Dollar im Monat und erhält dafür Updates und Software für die permanente Verschlüsselung jeglichen Datenverkehrs, zur effizienten Schadsoftwarebekämpfung und zur Erzeugung des weißen Rauschens. In Zukunft könnte sich jeder User auch mit einem eigenen Blockchain-System ausstatten, das die gesamte Datenumgebung steuert.

Was wird noch notwendig sein, um das Projekt überhaupt realistisch umzusetzen?

Aus Sicherheitsgründen entwickeln wir Teams in verschiedenen Teilen der Welt. Ein Teil unseres Produkts wird in Singapur und Irland entstehen, weil in beiden Ländern neue Technologien und Start-ups besonders gefördert werden. Dort werden vor allem auch neue Patente und geistiges Eigentum ernsthaft geschützt. Alles, was mit der Verschlüsselung zu tun hat, entsteht in Europa. E-Commerce oder das Entwickeln von Cryptocurrency und digitalen Bezahlssystemen wird die Unterstützung der besten Rechtsexperten benötigen. Softwareentwickler und Mathematikexperten arbeiten in virtuellen Teams. Wenn das Coden beendet ist, wir also ein konkretes Produkt anbieten können, werden wir mit den wichtigsten Hardwareproduzenten verhandeln. Wir stehen schon jetzt mit den Entscheidern dieser Branche in regelmäßigem Kontakt.

Sie klingen entschlossen ...

Bevor wir dieses Projekt starteten, habe ich weltweit mit Hunderten der besten IT-Sicherheitsexperten, mit Firmenbesitzern und namhaften Game-Changern aus der IT-Branche diskutiert. Alle zeigten sich für die Idee sehr offen, viele boten mir ihre Unterstützung an. Manche zeigten sich besonders sensibilisiert, weil sie beim Thema Datenschutz an die Zukunft ihrer Kinder und Enkel denken. Vielen Entscheidern in der Branche ist klar, dass die Herausforderungen in Sachen Privacy-Management und Cybersecurity dringend gelöst werden müssen. Wir sind übrigens auch bereit, mit der Data-Mining-Industrie zu verhandeln, um eine gemeinsame Ebene zu finden. Im Sinne der vielen Millionen Nutzer in der digitalen Welt sollten wir

uns gemeinsam darum bemühen, zu einer Servicequalität zurückzufinden, die verloren gegangen ist.

QUELLE: [HTTPS://MERTON-MAGAZIN.DE/AUFSTAND-IM-INTERNET-DER-DINGE](https://merton-magazin.de/aufstand-im-internet-der-dinge)