
VIRTUELLE
WELTEN

Das Paralleluniversum unserer Daten

Es geht um Werbung, Betrug oder die Optimierung von Geschäftsmodellen: Verbraucherdaten sind ein kostbares Gut, das Kreditgeber und Versicherer genauso interessiert wie Händler und Kriminelle. Kai Rannenberg, Professor für Mobile Business & Multilateral Security an der Goethe-Universität, forscht zur Cybersicherheit. Dirk Frank hat mit dem Wirtschaftsinformatiker über Datenschutz, Hackerangriffe und das Auto als »Handy auf Rädern« gesprochen.

Dirk Frank: Herr Professor Rannenberg, wir sprechen heute virtuell miteinander, über ein gängiges Konferenztool, und da sind wir quasi schon mittendrin im Thema Datenschutz und Datensicherheit, oder?

Kai Rannenberg: Sie haben einiges anklicken müssen, um der Aufzeichnung unseres Gesprächs zuzustimmen. Das folgt den EU-weiten Regeln der Datenschutzgrundverordnung (DSGVO). Viele Konferenzsysteme machen ihren Nutzerinnen und Nutzern nicht in gleicher Weise klar, was wie aufgezeichnet wird. Vielfach werden die Daten auch nicht wie bei diesem System in Europa, also im Schutzbereich der DSGVO, verarbeitet und gespeichert, sondern anderswo – »irgendwo in der Cloud«. Oder es bleibt unklar, wer Zugriff auf die Daten hat, weil die Verwaltung der Systeme von außerhalb Europas erfolgt beziehungsweise gar nicht klar ist, wo die Systeme verwaltet werden. Das Projekt CyberSec4Europe hat mit dem BigBlueButton-Server des Projektpartners TU Delft, den wir gerade für die Aufzeichnung nutzen, schon sehr schnell nach Beginn der Pandemie gezeigt, dass man einen leistungsfähigen Konferenzserver in Europa zuverlässig, mit Open-Source-Software und nach den Regeln der DSGVO betreiben kann – für Besprechungen, große öffentliche Konferenzen, die Lehre und sogar für offizielle Projektbegutachtungen. Das hat uns auch für die Nutzung des inzwischen an der Goethe-Universität aufgebauten BigBlueButton-Servers geholfen. Insgesamt war diese Aktivität für den Datenschutz wie auch die Cybersicherheit wichtig, denn natürlich leisten auch Web-Konferenzsysteme einen wesentlichen Beitrag oder Nichtbeitrag zur Cybersicherheit und damit zur digitalen Souveränität.

Spätestens seit der Coronapandemie haben viele im Beruf damit zu tun, vorher war das wahrscheinlich eher auf einen kleineren Nutzerkreis beschränkt.

Wir haben in Hessen einen sehr wachen Datenschutzbeauftragten. Der hat den hessischen Ausbildungsinstitutionen, speziell den Schulen, vorgeschrieben, mit Systemen zu arbeiten, bei denen man weiß, wo die Daten liegen und dass sie garantiert im Bereich der Datenschutzgrundverordnung bleiben. Ein Anbieter etwa in Frankreich oder Dänemark kann okay sein. Aber die Daten zum Beispiel nach China zu übermitteln, wo rechtsstaatliche Grundsätze nicht in unserem Sinne gelten und die Einhaltung der DSGVO unterstützen, wäre untersagt.

Wie gehen Sie denn damit um, wenn Sie mit Kolleginnen und Kollegen aus den USA konferieren?

Wenn ich mit Kolleginnen und Kollegen in den USA spreche, dann kann ich sie in unser Konferenzsystem einladen. Dabei müssen sie aus den USA über einen Weg dahin gelangen; dieser Weg ist natürlich genauso sicher oder unsicher wie das, was sie in den USA eben vorfinden. Es geht bei den Diskussionen, die in diesem Zusammenhang geführt werden, nicht darum, zu behaupten, dass es keine Rechtsstaatlichkeit in den USA gäbe. Tatsache ist aber, dass eine spezielle Regulierung in den USA existiert, die Dienstanbieter dazu verpflichtet, Abhörmaßnahmen aus Gründen der nationalen Sicherheit zuzulassen, ohne die Kunden darüber zu informieren. Dagegen wurde in den USA geklagt, auch mit Blick auf den damit verbundenen Wettbewerbsnachteil, bislang aber

Bild: ozrimoz/Shutterstock

ohne Erfolg. Die Vorbildfunktion, die Europa beim Thema Datenschutz und Datensicherheit mithilfe zum Beispiel der DSGVO einnimmt, hat natürlich auch den Vorteil, dass sich Firmen und Organisationen weltweit darauf berufen können. Diese europäische Regulierung hat geradezu eine Nachahmungsbewegung bewirkt. In Indien etwa hat man verstanden, dass die Einhaltung der einschlägigen Regeln eine wesentliche Voraussetzung ist, um am europäischen Markt erfolgreich sein zu können.

Wenn man momentan über das Thema Cybersicherheit spricht, kommt man am Krieg gegen die Ukraine nicht vorbei. Man denkt dann natürlich vor allem an Cyberattacken auf die sogenannte Kritische Infrastruktur. Wird dadurch nicht vielleicht auch übersehen, dass Datensicherheit und Datenschutz auch schon in unserer alltäglichen IT-Nutzung eine Rolle spielen?

Angriffe auf Kritische Infrastrukturen hatten wir schon vor dem Krieg, zum Beispiel auf den Deutschen Bundestag, auf Energieversorger, auf Universitäten in Gießen und Berlin, auch auf die Stadt Potsdam. Nach dem, was wir von Kolleginnen und Kollegen aus der Ukraine wissen, ist die Fucht vor Angriffen auf die Kritische Infrastruktur gegenwärtig oft größer als die vor Ausspähung im Internet oder in Mobilfunknetzen, weil die Schäden der Angriffe auf die Kritische Infrastruktur unmittelbarer sind. Aber immer mehr Menschen dort wissen nun auch, dass das eine das andere ermöglicht. Wie weit sich dieser Zusammenhang inzwischen bei uns herumgesprochen hat, ist eine interessante Frage.

Cybersicherheit für Europa

CyberSec4Europe als Pilot für das »European Cybersecurity Competence Centre and Network (ECCC)« entwirft, testet und demonstriert Governance-Strukturen für das ECCC und nutzt dabei Best-Practice-Beispiele, das Wissen und die Erfahrung der 42 Partner. Gleichzeitig arbeitet CyberSec4Europe an sicheren Softwarekomponenten, die Lücken in der Forschung schließen und mit den realen Anwendungsfällen verknüpft sind, etwa in den vertikalen Sektoren digitale Infrastruktur, Finanzen, Behörden und intelligente Städte, Gesundheitswesen und Transport.

Das langfristige Ziel von CyberSec4Europe ist eine Europäische Union, die über alle erforderlichen Fähigkeiten verfügt, um ihre demokratische Gesellschaft zu sichern und aufrechtzuerhalten, die im Einklang mit den europäischen Verfassungswerten lebt, zum Beispiel in Bezug auf den Schutz der Privatsphäre und die Nutzung von Daten, und die eine weltweit führende digitale Wirtschaft hat.

Auf **www.CyberSec4Europe.eu/our-results/books** finden sich zwei E-Books, die die Ergebnisse leicht lesbar zusammenfassen.

Wir haben seit vielen Jahren eine Vielzahl von Apps zur Verfügung, die größtenteils kostenfrei angeboten werden. Aber natürlich zahlt man auch mit seinen Daten. Fehlt hier noch das nötige Bewusstsein?

Ja, leider. Manchmal wird es auch leichtsinnigen Nutzerinnen und Nutzern bewusst, dann aber oft auf schockierende Weise. Es gab einen Aufschrei, als bekannt wurde, dass Cambridge Analytica auf Daten von Facebook Zugriff hatte. Und zwar sowohl auf Daten, die auf dem Facebook-Server lagen, als auch auf Daten, die mit der Facebook-App gesammelt wurden.

Aber auch in »erwachsenen« Lebens- und Konsumwelten kommen Apps massenhaft zum Einsatz, man denke nur an Autos.

Das Auto ist inzwischen im Prinzip auch ein Handy auf Rädern. Im Auto lassen sich natürlich noch viel mehr Informationen einsammeln: Wie reagiert die Fahrerin oder der Fahrer auf Stress, wie wird beschleunigt, wie gebremst et cetera. Die Bewegungsprofile der Personen, die bei Handys auch schon existieren, werden noch greifbarer, wenn man mit dem Auto unterwegs ist. Die Wochenzeitung »Die Zeit« hat einmal eine Website aufgesetzt, die die Bewegungsdaten des Politikers Malte Spitz für einen Zeitraum von sechs Monaten aufzeigt. Der hatte sich von der Telekom seine Handy-Ortungsdaten geben lassen. Auf der Website kann man sehr präzise sehen, wo sich Spitz aufgehalten hat, weil auch die Funkzellengrößen mit in die Animation eingearbeitet wurden. Das hat viele Menschen durchaus aufmerken lassen. Wir erwähnen es auch in unseren Vorlesungen, damit auch unsere Studierenden ein Verständnis dafür bekommen, was digitale Infrastrukturen bereits erfassen.

An Ihrem Lehrstuhl wurde vor einigen Jahren eine App entwickelt, die Datenschutzrisiken aufgespürt hat, um damit den Nutzerinnen und Nutzern die Kontrolle über das Verhalten ihrer Apps zurückzugeben.

Diese App hat es damals auch in die Tagespresse geschafft, speziell wegen der Erkenntnisse bezüglich der Sport-Apps. Diese erfassen über zusätzliche Sensoren, etwa an Armbändern, Körperfunktionen. Mehr Aufklärung ist in solchen Fällen sinnvoll: Datenschutz ist wie Zähneputzen. Es ist unbequem, nicht gerade sexy, manchmal tut es sogar weh, aber es

Prof. Kai Rannenberg

Foto Rannenberg: Elio Germani/Hessische Landesvertretung in Brüssel

zahlt sich langfristig aus. Es gibt wiederum die weitverbreitete Aussage »Ich habe nichts zu verbergen.« Eigentlich hat doch jeder etwas zu verbergen, weil jeder Schwächen hat, die, wenn sie in einem bestimmten Moment zugänglich sind, von Nachteil sein können. Die Freigabe von Daten ist natürlich auch eine Sache der Abwägung. Wenn ich zum Beispiel dringend Hilfe holen muss, dann ist die Tatsache, dass ich dabei geortet werden kann, nicht unbedingt mein größtes Problem.

Die SCHUFA hat jüngst betont, dass sie keine Daten aus Social Networks verarbeitet.

Das haben sie aber erst unter öffentlichem Druck bekannt gegeben. Wir wissen auch nicht, wie das bei allen anderen Kreditauswertungsunternehmen aussieht. Versicherungen sind natürlich sehr interessiert, alle möglichen Daten zu erfahren. Sie können, wenn Sie mehr Daten von sich preisgeben, Ihre Auto-Haftpflichtversicherung zu einem günstigeren Tarif abschließen. Manche Leute sagen, das widerspreche eigentlich dem Versicherungsgedanken, wonach man für eine Schwäche eben nicht abgestraft werden dürfte. Wenn einem diese Art Datenhandel angeboten wird, muss man sich der Tatsache bewusst sein, dass man der kleinere Partner ist. Beim europäischen Verband der Verbraucherschützer gibt es dafür eine eigene Abteilung, die sich um Datenschutz kümmert, und zwar speziell in Haushaltsgegenständen beziehungsweise in den Dienstleistungen, die Verbraucherinnen und Verbraucher ganz normal verwenden. Das kann zum Beispiel Spielzeug sein: Beim sogenannten Internet der Dinge sind die Geräte mit dem Internet verbunden. Spielzeuge sind damit Cloud-Endpunkte, aber darüber werden die Kunden nicht ausreichend informiert, gerade bei den Billiggeräten.

Anfang Dezember gab es den »Momentum CyberSec4EuropeSummit Event« in Brüssel. Worum ging es dabei?

Bei einigen Pilotprojekten zum Thema Cybersicherheit ging es bisher um Hochsicherheitsanwendungen im militärischen Bereich. Wir haben uns in unserem Projekt CyberSec4Europe aber auch gezielt Anwendungen vorgenommen und sieben Anwendungsbereiche adressiert: den Austausch medizinischer Daten, auch weil sich mehr und mehr Therapien darauf beziehen; das elektronische Einkaufen; Bankdaten, speziell das Thema »ich und mein Girokonto«; den Bereich Ausbildung und Zertifizierung von Ausbildungsleistungen beziehungsweise Zulassung zu Ausbildungsinstitutionen. Zwei weitere, ebenfalls im zivilen Bereich, aber nicht direkt mit Relevanz für einzelne Bürgerinnen und Bürger, sind der Schutz von maritimen Infrastrukturen, speziell die Kommunikation zwischen Häfen und Schiffen, und das Thema digitale Wertschöpfungsketten in der Produktion. Diese Wertschöpfungsketten werden ja immer länger, daher müssen die Beteiligten einander vertrauen können. Der siebte Bereich sind dann die Smart Cities; in den Städten kommt bekanntlich immer mehr Digitalisierungstechnik in vielfältigsten Anwendungsszenarien zum Einsatz.

Auch unterwegs immer vernetzt: Moderne Autos sammeln große Datenmengen – für Hersteller, Staat und Werkstatt.

Sie wurden im Vorfeld der Veranstaltung folgendermaßen zitiert: »Cybersicherheit muss mit europäischen Werten wie Freiheit und Respekt für jeden Einzelnen sowie dem Schutz der am meisten gefährdeten Personen verbunden bleiben.«

Stellen Sie sich vor: Ihr neues Gebiss wird irgendwo in Einzelfertigung automatisiert oder semiautomatisiert im Rahmen von Smart-Manufacturing erstellt. Dann geht es ja damit los, dass erstmal Ihr Kopf vermessen werden muss, und alle möglichen personenbezogenen Daten inklusive der Fehler, die Ihre Zähne schon hatten, müssen an den Gebissfertiger übermittelt werden. Anhand der genannten Anwendungsbereiche sieht man, dass die europäischen Werte nicht nur abstrakt behandelt werden, sondern mit Blick auf Menschen im Alltag. Wie läuft das bei »normalen« Menschen, was passiert denen eigentlich gerade? Natürlich hat ein Gebissproduzent ein Interesse daran, die Gebisse präzise zu fertigen, sonst kann er sie am Ende nicht verkaufen. Aber es gibt die Versuchung, die sehr persönlichen Daten der Kundinnen und Kunden auch für andere Dinge zu verwenden. Wichtig ist, dass die Menschen darüber nicht nur entscheiden, sondern auch darauf vertrauen können, dass ihre Entscheidungen von den Lieferantinnen und Lieferanten respektiert und verlässlich technisch umgesetzt werden.

Dr. Dirk Frank arbeitet als Pressereferent an der Goethe-Universität.

frank@pvw.uni-frankfurt.de

Foto: Gabriel Nica/Shutterstock