CORE®

IDENTITÄT UND SICHERHEIT – DIE BEFÄHIGUNG DES NUTZERS DURCH TECHNOLOGISCHE EMANZIPATION

Dr. Waldemar Grudzien
Dr. Mirko Schiefelbein
Holger Friedrich

April 2018
COREtechmonitor | Blogpost

Key Facts

- Identitätsdaten von Nutzern im digitalen Raum hoch exponiert
- Heute verwendetes technologisches Perimeter-Sicherheitsparadigma unsicher und verwundbar
- Aktuell geringer Veränderungsdruck für verändertes Sicherheitsparadigma
- Lösungsansätze für technologische Emanzipation durch einzelne Marktteilnehmer und direkt technologische Anforderungen seitens Regulator
- Nutzer durch veränderte Technologien und Verfahren zur Souveränität über ihre Daten im digitalen Raum zu befähigen

Report

1. Grundsätzliche Unsicherheit der Identitätsdaten

Durch die Nutzung von Apps und Services im Internet hinterlassen Nutzer umfangreiche Spuren. Anders als in der analogen Welt bleiben diese als Daten prinzipiell verfügbar und werden von verschiedenen Diensten zu unterschiedlichen Zwecken ausgewertet und genutzt. Dieses Vorgehen ist im Regelfall durch die Geschäftsbeziehung zwischen Nutzern und Diensteanbietern legitimiert. Zumeist wird dies für die gezielte Schaltung von Werbung verwendet, daneben bieten einige der darauf aufbauenden Informationen und Services Vereinfachungen für Nutzer, z.B. durch Zusatzinformationen zu Strecken oder Verspätungen.

Die zugrundliegenden Daten gehören, und das ist bewusst zu machen, der digitalen Identität des Nutzers an respektive lassen sich ihr zuschreiben; anders formuliert: Nutzer machen Daten zugänglich – und das heißt auch, dass diese Daten ihrer Identität ob gewollt oder nicht zugerechnet werden können. Für die Anbieter dieser Dienste gilt, dass der Nutzer mit seinen Daten mindestens ebenso das Produkt ist wie die von ihnen zur Verfügung gestellten Plattformen und Dienste selbst.

Neben den Formen der vereinbarten Verwendung von Nutzerdaten gibt es jedoch weitere, illegitime respektive illegale Facetten der Datenverwendung. Graubereiche sind berührt, wenn es um die wie auch immer anonymisierte Weitergabe von Daten an Dritte oder um die weitere Verfolgung digitaler Karteileichen geht (nicht mehr genutzte, aber nicht gelöschte Accounts). Zudem können trotz Widerspruchs des Nutzers zur Datensammlung, indem er z.B. das Geolocationing deaktiviert, auch weiterhin alle Quellen durch die Provider zusammengeführt werden.

Davon zu unterscheiden ist der Fall eines Einbruchs in die Integrität von Netzen – seien es Firmennetzwerke, Datenbanken oder heimische Rechner von Verbrauchern –, um Daten zu entwenden. Diese Einbrüche setzen zum Teil direkt bei Sicherheitslücken der Software (und Hardware) an; zum Teil verschaffen sie sich Zugang

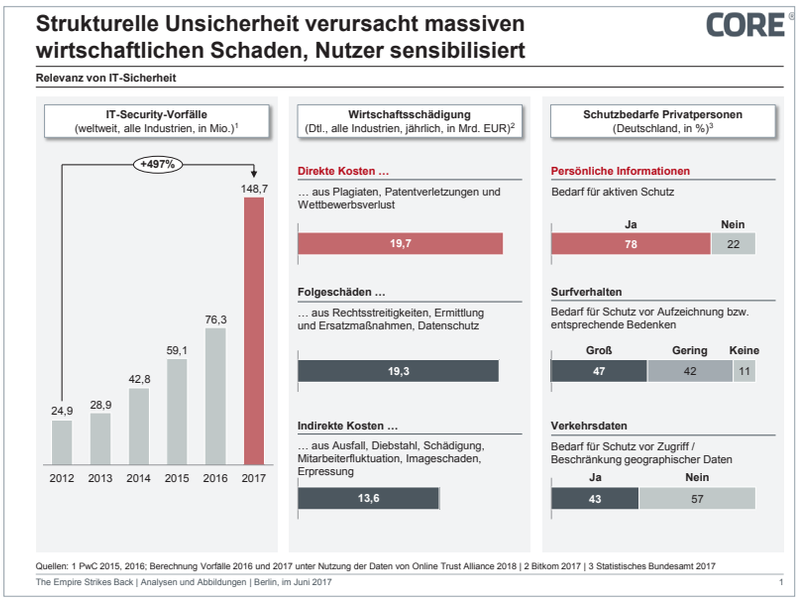

Abbildung 1: Strukturelle Unsicherheit verursacht massiven wirtschaftlichen Schaden, Nutzer sensibilisiert

durch die Erbeutung von Nutzerzugangsdaten, die aufgrund ihrer Einfachheit und ihrer häufigen Wiederverwendung ein großes Risiko darstellen. Ein vergessener Account oder ein einfach zu hackendes Passwort im digitalen Raum sind in der analogen Welt damit zu vergleichen, auf der Straße seinen Ausweis zu zeigen oder ohne Prüfung einen hingehaltenen Zettel zu unterschreiben. Bereits ein Bruch reicht aus, um umfangreiche Analysen zum Verhalten und den Präferenzen von Nutzern durchführen zu können.

Die Konsequenzen für den Nutzer sind unüberschaubar. Die Daten erlauben es vielerlei Gruppen, Schlussfolgerungen zu ziehen. Dies beginnt bei hartnäckiger, personalisierter Werbung, geht über No-Fly-Listen bis zur Anpassung des Scores für Kredite. Der Nutzer hat darüber jegliche Kontrolle verloren, er erfährt weder etwas über die Informationen und ihre Herkunft noch über die Speicherung, Auswertung und Verwendung. Er merkt nur, dass er nicht mehr fliegen kann oder einen höheren Zinssatz für einen Kredit erhält.

Die Regulatorik hat hier bisher einen rein rechtlich getriebenen Ansatz verfolgt, indem sie die unberechtigte Weitergabe von Daten sanktioniert. Der grundsätzlichen Unsicherheit der Technologien, mit denen die Daten oft gespeichert, ausgewertet und genutzt werden, hat sie nichts entgegengesetzt.

2. Geringer inhärenter Veränderungsvektor

Die beteiligten Parteien verfügen über eine nur geringe intrinsische Motivation, an dieser Situation etwas zu ändern. Am Verhalten der Nutzer anzusetzen, ist in den wenigsten Fällen von Erfolg gekrönt, weil kaum Alternativen zur Verfügung stehen und ein Verzicht auf die Nutzung der Apps und Services einem Verlust an Lebensqualität und der digitalen Pflege sozialer Beziehungen gleichkäme.

Seitens der Serviceanbieter haben einige wenige Unternehmen ein Interesse an der Sicherheit von Nutzerdaten und insofern einem Höchstmaß an Sicherheit. Für

viele jedoch bilden der Bezug und die Verwendung von Daten die DNA ihres Geschäftsmodells. Aus gutem Grund – aus Sicht der Serviceanbieter – wird es dem Nutzer schwer gemacht, sein Smartphone datenschutzfreundlich einzustellen. Dabei helfen die Berechtigungseinstellungen des Smartphones kaum weiter, da sich z.B. der Zugriff auf eindeutige Identifikationsnummern wie IMEI oder MAC-Adresse nicht unterbinden lässt.

Schließlich scheint das vorherrschende Technologie-Architektur-Paradigma vermeintlich sicher. Perimeter-Netze – solche, die auf den Umfang (= Perimeter) von Sicherheitszonen setzen – unterscheiden zwischen einem vertrauenswürdigen Netz (z.B. Firmennetz, innen), einer demilitarisierten Zone (DMZ) und einer prinzipiell unsicheren Zone außerhalb. Innerhalb des vertrauenswürdigen Netzes gilt die Annahme, dass jeder Nutzer, jedes Gerät und jede Nachricht, die erfolgreich authentifiziert wurden, vertrauenswürdig seien.

Dies ist ein Trugschluss, wie die immer ähnlich verlaufenden erfolgreichen Angriffe zeigen: Auf Basis eines Methodenmixes aus CSS, CSRF, Injections, Phishing etc. gelangt ein Stück Schadsoftware in das vertrauenswürdige Netz und bildet ein Einfallstor. Der Angreifer bringt ein Remote Access Tool (RAT) ins Netzwerk, bewegt sich dann lateral innerhalb des Netzes, bis er sich höher privilegieren kann und Verwertbares auffindet.

Der Ansatz der Perimeter-Sicherheit trägt im Ergebnis nicht nur bei den Verbrauchern zur Unsicherheit bei, sondern vor allem bei den Anbietern. Sie werden systematisch als Zwischenstationen für Angriffe auf Verbraucher sowie Serviceanbieter genutzt. Schnellere Produktreleases von Apps und Bibliotheken, die ein weit höheres abstraktes Programmieren erlauben, steigern die Komplexität massiv, senken die Transparenz und folglich die Sicherheit.

3. Technologische Emanzipation/Souveränität

3.1 Sicherheits-Architekturen: Perimeter- vs. Zero Trust-Approach

Gegen Perimeter-Netze wäre in einer statischen Welt nichts einzuwenden. „Statisch“ in dem Sinne, dass alle Endpunkte des Netzes keiner größeren Dynamik unterliegen. Tatsächlich ändern sich die Endpunkte jedoch permanent, Endnutzer und technische User bringen neue Smartphones, IoT-Geräte respektive Agenten in ein Netz. Noch schneller als die Endpunkte ändern sich die Applikationen und die um diese postierten Werkzeuge wie IDEs, Libraries, Dev/Ops-Toolchains. Diese Dynamiken führen zu einer weit höheren Zahl systematischer Fehler und eröffnen Verwundbarkeiten für Angreifer. Am gegenüberliegenden, dem als sicher eingestuften Ende des Netzes, sitzen immer noch die gleichen Menschen und folgen einem Link oder öffnen einen Anhang.

Demgegenüber wird bei der Zero Trust Network-Architektur das komplette Netz als unsicher betrachtet, es gibt kein sicheres privilegiertes Netz innen und ein unsicheres Netz außen. Bedrohungen werden als permanent existent im Netz angenommen. Jeder Nutzer, jedes Gerät und jeder Datenfluss muss authentifiziert, autorisiert und verschlüsselt werden. Der Zugang zum Netz hängt somit nicht mehr von der

Lokalisierung in einem internen Netz, sondern einzig vom Zustand und den Credentials des Endgerätes und den Credentials des Nutzers ab. Der Entscheid über eine erneute Authentifizierung und Autorisierung wird auf Basis eines dynamischen Regelwerks unter Kombination verschiedener Einflussgrößen vorgenommen und nicht einer einzigen statischen Schwelle wie eines Eurobetrags, des aktuellen Aufenthaltortes oder der Meldeadresse.

Zero Trust Networks verwenden vorhandene Technologien in neuen Wegen und einer veränderten Komposition, es werden keine neuen Protokolle, Bibliotheken oder Sprachen benötigt. Vorreiter in Zero Trust Networks ist Alphabet/Google, das diese Aktivitäten in seiner Tochter BeyondCorp bündelt und seit 2014 über seine eigene Infrastruktur inklusive Mitarbeiter ausrollt. Apple kann mit seinem deutlich rigideren geschlossenen System aus eng angebundenen iPhones und iOS als Zero Trust Network gesehen werden, in dem Falle sogar für alle Endnutzer.

3.2 Regulatorik: Direkte Regulierung von IT und Technologie

INeben diesem paradigmatischen Wechsel in der Sicherheitsarchitektur stärkt der Regulator mit mehreren Gesetzesinitiativen die Sicherheit von Nutzerdaten. Mit dem IT-Sicherheitsgesetz (IT-SiG) hat der deutsche Gesetzgeber die europäische Richtlinie zur Gewährleistung einer hohen Netzwerk- und Informationssicherheit (NIS-RL) umgesetzt. Seit dem 30. Juni 2017 gilt das IT-SiG für alle sieben sogenannten „kritische Sektoren“, u.a. auch für die Sektoren Finanz- und Versicherungswesen sowie Informationstechnik und Telekommunikation. Die europäische Zahlungsdiensterichtlinie PSD II erhöht insbesondere die Sicherheit der Nutzerdaten im elektronischen Zahlungsverkehr – ab dem 14. September 2019 muss mit dem RTS SCA der letzte sicherheitstechnische Baustein der PSD II eingehalten werden.

IT-SiG wie PSD II fordern ein den Stand der Technik berücksichtigendes Mindestmaß an IT-Sicherheit sowie ein Meldewesen für drohende oder bereits eingetretene schwerwiegende Sicherheitsvorfälle. Berichtsanforderungen runden den Forderungskatalog beider Gesetze ab.

Ab Ende Mai tritt die Datenschutzgrundverordnung in Kraft. Die DSGVO ist das erste Datenschutzgesetz, das durch die Forderung nach technischen Sicherheits-maßnahmen den Datenschutz gewährleisten will. Artikel 32 DSGVO schreibt die angemessene Berücksichtigung des Standes der Technik bei der Umsetzung geeigneter organisatorischer und technischer Maßnahmen vor – eine „Verschlüsselung“ personenbezogener Daten wird dediziert vorgegeben. Ebenfalls erstmalig ist die DSGVO sanktionsbewährt zur effektiven Durchsetzung des Datenschutzes; mit Bußgeldern bis zu 4% des Jahresumsatzes oder max. 20 Mio. EUR.

Mit der Einführung des „Datenschutzes durch Technik und datenschutzfreundliche Voreinstellungen“ (Art. 25) werden durch die DSGVO auch Anforderungen an die Produktentwicklung und -implementierung gestellt – Privacy by Design/ Privacy by Default. Ferner stellen die in den Artikeln 15 bis 20 DSGVO zusammengestellten Betroffenenrechte wie Recht auf Vergessenwerden oder auch Recht auf Datenübertragbarkeit nicht-triviale technische Anforderungen an Diensteanbieter dar.

Die ePrivacy-Verordnung konkretisiert die DSGVO im Bereich der elektronischen Kommunikation und weitet die Datenschutzregelung auch auf sogenannte „Over-The-Top-Kommunikationsanbieter“ (OTT) wie Instant Messaging aus. Bisher fallen nur klassische Telekommunikationsanbieter unter die Regelungen, was aber aufgrund des Bedeutungszuwachses der OTTs kein ausreichendes Schutzniveau mehr darstellt. Die ePrivacy-Verordnung wird aller Voraussicht nach erst in 2019 in Kraft treten. Über den finalen Inhalt dieser letzten der vier maßgeblichen Gesetze kann noch nicht abschließend berichtet werden, jedoch zeichnet sich im derzeitigen Trilog-Verfahren eine „Pro-Datenschutz“-Tendenz ab.
Im Ergebnis wird das regulatorische Vierer-Bündel die IT-Sicherheit und den Datenschutz von Nutzerdaten mit technischen Maßnahmen erhöhen.

3.3 Serviceanbieter: Technologische Kollaboration für Reichweiten

Seitens der Diensteanbieter sind die rein digitalen Spieler (GAFAs) gleich mehrfach im Vorteil: Ihre Lösungen verfügen über eine große Verbreitung, sie setzen Standards in der User Convenience und sind geübt in der Adaption neuer Technologie-Paradigmen. Da ihre Geschäftsmodelle jedoch in weiten Teilen darauf basieren, die Daten von Nutzern zu sammeln, auszuwerten und zu verwerten, können sie genetisch-strukturell nur ein bedingtes Interesse haben, die Souveränität über diese Daten dem Nutzer zu übereignen.
Demgegenüber haben traditionell analoge Marktteilnehmer im Rahmen der Transformation ihrer Geschäftsmodelle erkannt, dass ihre bisher geringere Fokussierung auf Daten ihnen zum Vorteil gereichen kann. Sie kollaborieren, um auf technologischer Basis eine maximale Reichweite zu generieren und fokussieren neben der Funktion zusehends ebenfalls auf Lifestyle.
Mit Blick auf Daten können sie glaubwürdig Lösungen entwickeln, die nicht die Datenhoheit beim Nutzer belassen (dort ist sie im digitalen Raum ohnehin nicht beheimatet), sondern die den Nutzern die Hoheit und Souveränität über ihre Daten zurückgeben. Voraussetzung dafür ist, Transparenz zu schaffen und Sicherheit zu gewährleisten.

Synthese

Die digitale Identität wird weitere Aufwertung und wirtschaftliche Verwertung erfahren. Die Hoheit über seine eigene digitale Identität wird somit zum entscheidenden Faktor für Nutzer, so sie wie im analogen Raum weiterhin ihre Datensouveränität wahren wollen. Für die Wahrung seiner Datensouveränität müssen die beteiligten Stakeholder dem Nutzer geeignete Mittel an die Hand geben. Ein Mittel der Wahl ist sichere Technologie, große Provider haben das erkannt und passen ihre Sicherheitsarchitekturen an die neue dynamische IT an. Regulator und Aufsicht unterstützen mittlerweile den technologischen Lösungsweg mit mehreren aufeinander abgestimmten Gesetzesinitiativen mit dem Ziel, Datensicherheit und Datenschutz durch sichere IT-Systeme zu erreichen. Auf diesen Pfad müssen sich auch Anbieter und Nutzer selbst begeben.

Autoren

Dr. Waldemar Grudzien

Dr. Waldemar Grudzien setzt sich als Transformation Engineer mit den aktuellen regulatorischen Anforderungen und deren technischer Realisierung auseinander. Als promovierter Elektrotechniker war er als Leiter in einem nationalen Bankenverband für die Bereiche Retailbanking und Banktechnologien zuständig.

Mail: waldemar.grudzien@core.se

Dr. Mirko Schiefelbein

Dr. Mirko Schiefelbein verantwortet als Transformation Director die Forschungsaktivitäten des COREinstitutes. Als promovierter Geisteswissenschaftler liegt sein Fokus auf der Erforschung von technologieinduzierten Veränderungen in Organisationen. Unter Mirkos Federführung wurden eine Vielzahl an Veröffentlichungen im Kontext von Technologie-Transformationen publiziert, die von nationalen und internationalen Medien wiederkehrend aufgegriffen wurden.

Mail: mirko.schiefelbein@core.se

Holger Friedrich

Holger Friedrich Holger Friedrich verantwortet seit 2010 die Beratungseinheit von CORE. Er ist seit über 25 Jahren in der Softwareindustrie tätig. Vor der Gründung von CORE hat er ein Technologieunternehmen aufgebaut, wirkte in leitender Position bei marktführenden Technologieanbietern und war u.a. Partner in einer führenden internationalen Strategieberatung.

Mail: holger.friedrich@core.se

COREinstitute
Am Sandwerder 21-23
14109 Berlin | Germany
https://institute.core.se
Phone: +49 30 26344 020
office@coreinstitute.org

CORE SE
Am Sandwerder 21-23
14109 Berlin | Germany
https://www.core.se
Phone: +49 30 26344 020
office@core.se

COREtransform GmbH
Am Sandwerder 21-23
14109 Berlin | Germany
https://www.core.se
Phone: +49 30 26344 020
office@coretransform.de

COREtransform GmbH
Limmatquai 1
8001 Zürich | Helvetia
https://www.core.se
Phone: +41 442 610 143
office@coretransform.ch

COREtransform Ltd.
One Canada Square
London E14 5DY | Great Britain
https://www.core.se
Phone: +44 203 319 0356
office@coretransform.co.uk

COREtransform MEA LLC
DIFC – 105, Currency House, Tower 1
Dubai P.O. Box 506656 I UAE
https://www.core.se
Phone: +971 4 3230633
office@coretransform.ae

April 2018