Wie Carrier den digitalen Alltag ihrer Kunden mit Schutzdiensten sichern können

Clemens Aumann, Joachim Hauk, Carolin Obernolte

> Jeder digitale Dienst hat eine Schattenseite: Welche Daten durch ihn erhoben und verwendet werden, ist für (Privat-)Kunden vollständig intransparent.

> Endkunden wünschen sich grundsätzlich Dienste, die ihre personenbezogenen Daten so wenig wie möglich erheben, auswerten und speichern.

> Carriern bietet sich die Chance, die Schnittstelle zum Kunden zurückzugewinnen, indem sie ihre Kunden in dieser asymmetrischen Informations- und Machtkonstellation unterstützen und sich selbst im Bereich Sicherheit und Schutz hervorragend positionieren.

Das Internet verbindet uns alle. Internetdienste unterschiedlichster Art bieten diverse Nutzungsmöglichkeiten für jedermann. Insbesondere Endkunden profitieren von einer Vielfalt an Leistungen, die ihnen das Leben erleichtern oder es interessanter gestalten.

Der tägliche Zwist: Bequemlichkeit vs. Datenpreisgabe

Die Vielzahl an Diensten reicht von kostenloser weltweiter Telefonie über Skype über den Austausch von Neuigkeiten bei Facebook bis hin zum Teilen von Fotos mit Freunden und Bekannten bei Instagram und der Kommunikation per Videobotschaften mit Snapchat. Onlineshopping-Dienste ermöglichen Besorgungen flexibel von Zuhause aus und Smart-Home-Lösungen vernetzen das Zuhause, sodass man auch aus der Ferne über das Smartphone Lampen, Heizkörper und Fernseher bedienen kann. Was für ein Komfort, wenn man nicht einmal mehr das Haus verlassen muss, um einzukaufen, und nicht einmal mehr aufstehen muss, um Geräte an- und auszuschalten!

Aber damit nicht genug: Wearables wie Smartwatches bieten die Möglichkeit, Körpervitaldaten zu sammeln und auszuwerten, um sich darauf basierend gesundheitsbewusster zu verhalten. Wer sich an einem Ort nicht auskennt, muss nicht etwa zur Tourismusinformation gehen oder Passanten nach dem Weg fragen, sondern nur noch auf dem Smartphone die Ortungsfunktion betätigen und sich anschließend mithilfe der Navigation zum gewünschten Ort führen lassen. Diese Anwendungsfälle sind nur einige der zahlreichen Beispiele aus der Praxis. Die Vorteile all dieser Anwendungsfälle lassen sich unter Schlagwörtern wie Digitalization, Sharing und Convenience zusammenfassen. Der Nützlichkeit dieser Dienste stehen allerdings auch vielfältige Risiken für die Endkunden gegenüber. Alles hat seinen Preis – in diesem Fall nicht nur einen monetären: Den höchsten Preis zahlen Endkunden mit der Preisgabe ihrer Daten.

Anbieter von Internetdiensten generieren große Mengen personenbezogener Daten und werten diese anschließend aus, um detaillierte Kundenprofile erstellen zu können. Diese werden von Anbietern verwendet, um Werbemaßnahmen und generell alle Arten von Informationen gezielt auf die Interessen der Endkunden zuzuschneiden. Dieses Vorgehen der Anbieter wird den Endkunden jedoch nicht transparent gemacht. Der Kunde kann lediglich durch die auf ihn zugeschnittenen Werbeanzeigen und Botschaften darauf schließen, dass durch das Generieren und Auswerten seiner Daten ständig Rückschlüsse auf seine Persönlichkeit gezogen werden. Die Sammlung und Auswertung der Daten stellen jedoch nicht die einzigen Risiken für Endkunden dar. Viele Anbieter von Internetdiensten speichern die Daten ihrer Kunden und geben sie gegebenenfalls sogar an Dritte

weiter. Was anschließend mit den Daten passiert, wird den Endkunden vorenthalten. Riskant für Endkunden ist auch die Tatsache, dass Anbieter von Internetdiensten ihre Kunden nicht vollständig vor Hacking-Angriffen und Spionage schützen können, da die Unternehmen oft selbst Opfer von massiven Cyber-Angriffen sind.

Endkunden sind also nicht mehr Herr über ihre persönlichen Daten. Weder können sie kontrollieren, welche Daten erfasst und analysiert werden, noch können sie vorgeben, wann und wie lange ihre Daten gespeichert werden. Um diese Risiken zu umgehen, müssten Endkunden auf Internetdienste verzichten. Umgekehrt erhalten sie aber keine ökonomische Kompensation für ihre Datennutzung beziehungsweise keinen Anteil an dem damit erzeugten Mehrwert für das nutzende Unternehmen, obwohl einer aktuellen Studie des Ponemon Instituts zufolge Endkunden durchaus bewusst ist, welchen Wert ihre Daten haben.[1]

Was können also diejenigen tun, die von den Internetdiensten profitieren möchten, ihre persönlichen Daten aber dennoch schützen wollen? Könnten Schutzdienste dem Endkunden entsprechend seiner individuellen Schutzbedürftigkeit das passende Schutzmodell bieten? Wäre ein solches Schutzmodell aus Sicht der Kunden überhaupt hilfreich und erwünscht?

Zentrale Thesen zum Schutz der persönlichen Daten aus Kundensicht

1. Intransparenz bei Endkunden hinsichtlich Datenverwendung: Bei Endkunden herrscht eine weitgehende bis vollkommende Intransparenz über die Erfassung, Verarbeitung, Analyse und Speicherung ihrer Daten. Der Eurobarometer-Studie zum Thema Datenschutz zufolge gaben 50 Prozent der Befragten an, nur teilweise Kontrolle über ihre Daten zu haben. 35 Prozent der Befragten gaben an, gar keine Kontrolle über die Daten, die sie teilen, zu haben.[2]

2. Risiko der Komplettüberwachung und Ausspähung: Endkunden nehmen bei der Nutzung von Internetdiensten Überwachung und Ausspähung verstärkt als Risiken wahr. Die Eurobarometer-Studie zeigt, dass 50 Prozent der Befragten

1 *Vgl. Studie mit Endkunden aus Europa, USA und Japan, erhoben in verschiedenen Kategorien. Beispiel: Gesundheitszustand 35$;Kaufhistorie17,80$, Arbeitgeber/Ausbildungsstatus: 8,50$, aktueller geographischer Ort: 5,10$. Ponemon Institut, Datenschutz und Sicherheit in einer vernetzten Welt: Eine Umfrage unter Endkunden aus den USA, Europa und Japan, 03/2015, S. 17.*

2 *Vgl. Schiavoni, Data Protection Tracker 4Q15, Ovum.*

besorgt darüber sind, Opfer von Datenmissbrauchsfällen zu werden. 32 Prozent der Befragten befürchten, dass ihre Informationen ohne ihr Wissen verwendet oder sogar gestohlen (29 Prozent) werden.[3]

3. Fehlendes Vertrauen der Endkunden gegenüber datenverarbeitenden Unternehmen: Endkunden müssen ihre Daten Anbietern von Internetdiensten anvertrauen, wenn sie deren Dienste nutzen möchten. Jedoch zeigen Endkunden ein verstärktes Misstrauen gegenüber diesen Unternehmen, wenn es um die Handhabung ihrer personenbezogenen Daten geht. Die Eurobarometer-Studie hat ergeben, dass 78 Prozent der Endkunden es schwer finden, den Unternehmen zu trauen, die ihre persönlichen Daten verarbeiten. Auch wenn fast 80 Prozent der befragten Endkunden Misstrauen gegenüber datenverarbeitenden Unternehmen hegt, nutzt dennoch die Mehrheit der Endkunden die Dienste dieser Anbieter, da sie auf den Nutzen oder Komfort, den diese Dienste bieten, nicht verzichten möchten. Die Akquisition von WhatsApp durch Facebook Anfang 2014 untermauert dies beispielhaft: Als bekannt wurde, dass Facebook WhatsApp aufkaufen würde, gab es eine Welle der Aufruhr, da Facebook nicht die endkundenfreundlichsten Datenschutzbestimmungen aufweist. Es wurde befürchtet, WhatsApp würde sich den Datenschutzbestimmungen von Facebook fügen müssen, wodurch die Sicherheit der Nutzerdaten als gefährdet angesehen wurde.[4] Viele Endkunden hatten sich im Rahmen der Suche nach einer sichereren Chat-Alternative für Threema entschieden. Auch wenn Threema in der Tat einen deutlich endkundenfreundlicheren Umgang mit den personenbezogenen Daten ihrer Nutzer vorweist,[5] konnte sich dieser Dienst mittelfristig nicht gegen WhatsApp durchsetzen und erreicht mit zirka 3,5 Millionen Nutzern bei Weitem keine vergleichbaren Nutzerzahlen (Stand: Juni 2015).[6] WhatsApp ist weltweit weiterhin führender Messaging-Anbieter (Stand: Februar 2016).[7] Dies könnte dadurch erklärt werden, dass die Mehrheit der Nutzer nicht dazu bereit war, den Aufwand auf sich zu nehmen, um eine alternative sichere Lösung zu suchen und zu nutzen.

3 Vgl. Schiavoni, Data Protection Tracker 4Q15, Ovum.

4 Vgl. Radke, WhatsApp: Hinweise auf Zusammenführung mit Facebook, 2016: http://www.heise.de/newsticker/meldung/WhatsApp-Hinweise-auf-Zusammenfuehrung-mit-Facebook-3082755.html.

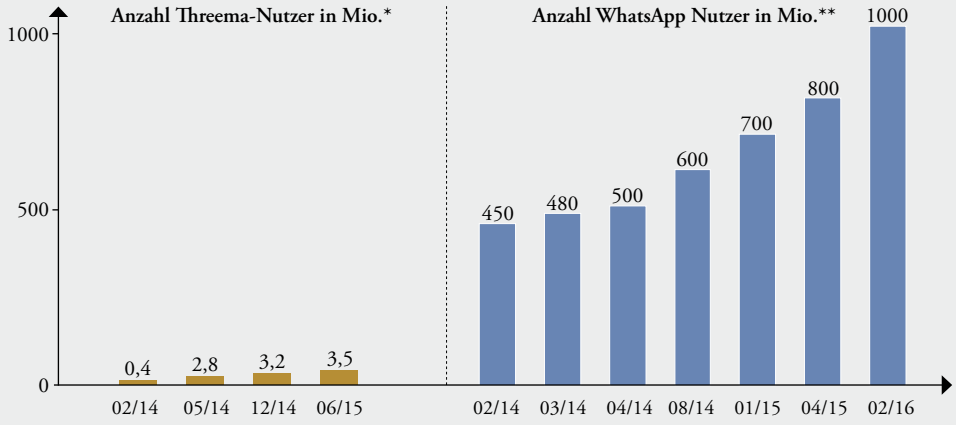
5 Vgl. Stiftung Warentest (Hrsg.) WhatsApp und Alternativen: Datenschutz im Test, https://www.test.de/WhatsApp-und-Alternativen-Datenschutz-im-Test-4675013-0/.

6 Vgl. Statista (Hrsg.) http://de.statista.com/statistik/daten/studie/445619/umfrage/nutzer-des-schweizer-messaging-dienstes-threema/.

7 Vgl. Statista (Hrsg.) http://de.statista.com/statistik/daten/studie/285230/umfrage/aktive-nutzer-von-whatsapp-weltweit/.

4. Steigende Beunruhigung bei der Nutzung von Internet-Diensten: Die Vergangenheit weist diverse Vorfälle auf, in denen Unternehmen aufgrund von Sicherheitslücken und Hackerangriffen Kundendaten verloren haben. Im Oktober 2013 zum Beispiel wurden drei Millionen Kreditkarteninformationen von Adobe-Kunden gestohlen.[8] Aufgrund solcher und weiterer Vorfälle steigt nicht nur das Angstlevel der Endkunden hinsichtlich Malware und Cyber-Attacken, sondern auch das Bewusstsein über die Werthaltigkeit ihrer Daten. Sie befürchten immer häufiger, potenzielle Opfer von Datenmissbrauchsfällen oder Identitätsklau zu werden. Das meist allzu defensive Informationsverhalten vieler Unternehmen in Fällen von Datenmissbrauch oder Sicherheitslücken verstärkt diese Bedenken.[9] Trotz dieser Befürchtungen geht die Mehrheit der Endkunden jedoch nicht sorgsam mit ihren Daten um. Eine Studie der GSMA zum Thema Wahrnehmung von Datenschutzbestimmungen der mobilen Internetnutzer hat ergeben, dass 80 Prozent der Nutzer von Internetdiensten oder Apps die Datenschutzhinweise akzeptieren, ohne sie zu lesen, da diese zu lang oder legalistisch sind.[10] Dies impliziert, dass Endkunden mit den derzeitigen Datenschutzbestimmungen oftmals überfordert sind.

Abbildung 1: Vergleich der Nutzerzahlen von Threema und WhatsApp



* *Statista (Hrsg.), Anzahl der Nutzer des Schweizer Messengers Threema von Februar 2014 bis Juni 2015 (in Mio.), http://de.statista.com/statistik/daten/studie/445619/umfrage/nutzer-des-schweizer-messaging-dienstes-threema/.*

** *Statista (Hrsg.), Anzahl der aktiven Nutzer von WhatsApp weltweit von Februar 2014 bis Februar 2016 http://de.statista.com/statistik/daten/studie/285230/umfrage/aktive-nutzer-von-whatsapp-weltweit/.*

Quelle: Detecon

8 *Vgl. Little, Personal Data and the Big Trust Opportunity, 2014, S. 14.*

9 *Vgl. Rybak, In the Age of Cyber Smash and Grabs: Safeguarding Customer Loyalty, Ring-Fencing Customer Data, Current Analysis, 2015, S. 3.*

10 *Vgl. Schiavoni, Data Protection Tracker 4Q15, Ovum, S. 19.*

5. Steigende Nachfrage von Schutzdiensten: Endkunden verlangen nicht nur vermehrt Sicherheit bei der Nutzung von Internetdiensten, sondern fordern auch verstärkt ein, selbst entscheiden zu können, welche Daten sie wo und in welchem Maße freigeben. Der GSMA-Studie zufolge würden 60 Prozent der befragten Endkunden gerne ein einheitliches Regelkonstrukt zum Schutz ihrer Daten festlegen wollen und wünschen sich, dass alle Anbieter diese Bestimmung einheitlich einhalten.[11] Auch wenn die meisten Kundenlösungen noch immer unverständlich und zu technisch für den Durchschnittsnutzer sind, befassen sich immer mehr Endkunden mit dem Thema Sicherheit, da die Bedeutsamkeit und Notwendigkeit von Sicherheitslösungen aus Sicht der Endkunden steigt.[12] Allerdings müssen Endkunden bislang weitestgehend selbst aktiv werden, wenn sie ihre Daten schützen wollen, da sie keine aktive und weitreichende Hilfe oder entsprechenden Services hierfür erhalten. Einer Studie von Orange zum Thema Verhaltensänderung von Endkunden hinsichtlich Datenschutz zufolge haben 37 Prozent der Befragten das Gefühl, Unternehmen oder Organisationen würden sie nicht über ein persönliches Datenmanagement unterrichten.[13] Endkunden haben eher das Gefühl, trotz vorherig vereinbarter Datenschutzbestimmungen auf die guten Absichten der Anbieter angewiesen zu sein. Sie befürchten, dass Anbieter ihre Daten für mehr verwenden als ursprünglich vereinbart: „[customers] are concerned that companies are using their data for more than was initially agreed."[14]

6. Weniger Vertrauen in OTTs als in Telekommunikationsanbieter: Endkunden nehmen OTTs als Unternehmen wahr, die von den Daten ihrer Kunden profitieren wollen. Telekommunikationsanbieter werden von Endkunden hingegen eher als „Durchreicher" von Daten wahrgenommen und daher eher als vertrauenswürdig eingeschätzt, wenn es um die Handhabung personenbezogener Daten geht: „[…] [Operators] are often seen as more trustworthy than internet companies or other service providers and can position themselves more strongly in terms of protecting their customer's privacy."[15] Der GSMA-Studie zufolge werden Telekommunikationsanbieter sogar als Ansprechpartner der Endkunden bei Problemen rund um das Thema Daten- oder Privatsphäre-Schutz gesehen, da 58 Prozent der Befragten Telekommunikationsanbieter um Hilfe bei solchen Problemen bitten.[16] Einer aktuellen Studie von Syniverse zufolge hat jedoch das Vertrauen von Endkunden in Mobilfunkanbieter nachgelassen: Die Befragten sollten sich

11 Vgl. Schiavoni, Data Protection Tracker 4Q15, Ovum, S. 19.
12 Vgl. Mohr-McClune, Zeitgeist Communications: Speaking in Confidence, Current Analysis, 2015, S. 3.
13 Vgl. Schiavoni, Data Protection Tracker 4Q15, Ovum, S. 22.
14 Vgl. Schiavoni, Data Protection Tracker 4Q15, Ovum, S. 25.
15 Vgl. Schiavoni, Data Protection Tracker 4Q15, Ovum, S. 6.
16 Vgl. Schiavoni, Data Protection Tracker 4Q15, Ovum, S. 19.

dazu äußern, ob sich ihr Vertrauen gegenüber Mobilfunkanbietern hinsichtlich des Schutzes ihrer personenbezogenen Daten geändert habe.[17] Die Hälfte der Befragten gaben an, dass sie Mobilfunkanbietern seit den letzten drei Jahren „weniger" vertrauen, 35 Prozent vertrauen ihnen „genauso" und 15 Prozent trauen ihnen „mehr" als vorher.[18] Dies impliziert, dass Endkunden in den letzten Jahren gegenüber Mobilfunkanbietern hinsichtlich Datensicherheit immer skeptischer geworden sind. Grundsätzlich gilt aber, dass Endkunden solche Anbieter, die ihnen mehr Kontrolle und Transparenz beim Management ihrer Daten verschaffen, positiver wahrnehmen als andere, die ihnen Transparenz erschweren oder gar verwehren: „Consumers appear to increasingly trust and use companies that are willing to offer them greater control through tools that are easy to use."[19]

Diese Kundensicht zeigt deutlich, dass sich Endkunden grundsätzlich Dienste wünschen, bei denen ihre personenbezogenen Daten so wenig wie möglich erhoben, ausgewertet und gespeichert werden. Da in der Realität solche Dienste derzeit jedoch kaum angeboten werden, müssen Kunden einen Kontrollverlust über ihre Daten in Kauf nehmen. Sie werden jedoch zunehmend sensibel für das Thema Sicherheit und Datenschutz, so dass wir grundsätzlich einen Bedarf nach Schutzdiensten ableiten können. Da sich viele Endkunden oftmals inhaltlich nicht mit Datenschutzbestimmungen zurechtfinden, sollte ein Angebot auf intuitive, einfach zu verstehende und einfach zu nutzende Sicherheitsdienste zielen, mithilfe derer sie die Sicherheit ihrer Daten managen können. Für Endkunden stellen Schutzdienste, eine vertrauensbildende Maßnahme dar, die ihnen Transparenz und Kontrolle über die Verwertung ihrer Daten verschafft.[20] Aufgrund der Interessenskonflikte ist die Glaubwürdigkeit der Dienste-Anbieter stark eingeschränkt. Da der Kunde zudem mehrere Anbieter parallel verwendet, leidet zudem die Übersichtlichkeit. Ein relevantes, weil Dienste übergreifendes und gleichzeitig unabhängiges Schutzangebot können aus unserer Sicht nur Regulierungsbehörden, Netzbetreiber oder ganz neue Unternehmen schaffen. Netzbetreiber sind hierfür unserer Meinung nach in der besten Position: Bei ihnen laufen die Verkehre zusammen, sie verfügen über die Kundenbeziehungen und sind weniger schwerfällig als staatliche Behörden. Gegenüber aufkommenden Start-ups haben sie (noch) den Vorteil größerer Reichweite durch Kundenstamm, Markenbekanntheit und -vertrauen.

17 *Vgl. Syniverse (Hrsg.): In dieser Studie wurde die Einstellung von Endkunden im Hinblick auf Datenschutz abgefragt. Es wurden mehr als 8.000 Endkunden aus acht Ländern befragt.*

18 *Vgl. Syniverse (Hrsg.) The Mobile Privacy Predicament, S. 12, https://www.syniverse.com/assets/files/custom_content/Mobile-Privacy-Predicament-Report.pdf.*

19 *Vgl. Schiavoni, Data Protection Tracker 4Q15, Ovum, S. 25.*

20 *Vgl. Schiavoni, Data Protection Tracker 4Q15, Ovum, S. 6.*

Zentrale Argumente für das Angebot von Schutzdiensten aus Sicht der Telekommunikationsanbieter

Regionale Repräsentation und große Erreichbarkeit: Große Telekommunikationsanbieter decken ein breites geographisches Spektrum mit eigenen Tochterfirmen oder Partnern ab. In den abgedeckten Ländern sind sie zudem durch ein meist flächendeckendes Netzwerk an Shops und durch die sehr gute Erreichbarkeit auf digitalen sowie telefonischen Kanälen mit großen Serviceeinheiten, die diese Kanäle bedienen, einfach erreichbar, was gerade in Problem- und Krisenfällen eine grundsätzlich hohe Reaktions- und Handlungsfähigkeit erlaubt.[21] Als Telekommunikationsdienstleister vor Ort, die damit auch nationaler Rechtsprechung unterliegen, sind Carrier trotz multinationaler Repräsentation juristisch greifbarer – was als vertrauensbildende Dimension in der Markenpositionierung eingebracht werden kann.

Daten- und Kommunikationssicherheit ist Teil des Kerngeschäfts: Die Sicherheit der Netze und der darauf laufenden Kommunikation ist für Telekommunikationsanbieter seit langem Teil des Kerngeschäfts. Sie beschäftigen sich konstant mit diesen Themen und verfügen über eine entsprechende Expertise auf technischer, prozessualer und regulatorischer Ebene. Daher sind sie besonders befähigt, den zunehmenden regulatorischen Druck bezüglich Datenschutz und Datensicherheit operativ sowie produktiv umzusetzen.[22] Sie können in ihrem Ökosystem Datensicherheit auf dem Nutzungs-, Verarbeitungs-, und Transportation-Layer kontrollieren, was ein solches Angebot zusätzlich glaubwürdig macht. Dies setzt aber auch eine entsprechende Sensibilisierung und Akzentuierung des Themas voraus sowie die Anpassung entsprechender Handlungs- und Notfallpläne im Fall eines Sicherheitsvorfalls.[23]

IT-Kompetenz und Trend zu Cloud-Produkten: Die meisten Telekommunikationsanbieter haben bereits eine ausgeprägte IT-Kompetenz, wenn nicht sogar eigene Bereiche oder Geschäftszweige, deren Kerngeschäft IT-Entwicklung und -Betrieb für Kunden beinhaltet. Mit der zunehmenden Bedeutung von Cloud-Produkten und den entsprechenden Angeboten großer Telcos bekommen diese Angebote zusätzlichen Impetus, müssen sich aber auch hier erhöhten Sicherheitsanforderungen stellen.[24]

21 Vgl. Clark-Dickson, Data Mobile operators' consumer mobile security strategies, Informa, 2014.
22 Vgl. Little, Personal Data and the Big Trust Opportunity, Ovum, 2014.
23 Vgl. Rybak, In the Age of Cyber Smash and Grabs: Safeguarding Customer. Loyalty, Ring-Fencing Customer Data, Current Analysis, 2015.
24 Vgl. Schiavoni, Data Protection Tracker 4Q15, Ovum.

Einfache Prozessierbarkeit von Sicherheitsdienstleistungen im Geschäftsmodell: Der Charakter von Kommunikationsdienstleistungen als Dauerschuldverhältnis ist konsistent mit dem Geschäftsmodell von Schutzdiensten, die auch kontinuierlichen oder zeitraumbezogenen Charakter haben. Solche Schutzdienste können damit einfach als Zusatzoption zu bestehenden Verträgen oder als Einzelprodukt angeboten werden. Entsprechende Abrechnungsmöglichkeiten sind gegeben (und auch Kapazitäten für Drittanbieter oder Partner meist Teil des bisherigen Geschäftsmodells.[25] Auch entsprechende Vertriebs- und Servicekompetenzen liegen vor bzw. können einfach ausgebaut werden.

In Summe sind Telekommunikationsdienstleister sowohl aus Kundensicht als auch auf Basis ihres Brandings und der notwendigen Kompetenzen sehr gut positioniert, um die Rolle als Wächter der Datensicherheit des Kunden zu übernehmen. Die nächste Frage ist, wie ein solches Angebot aussehen kann, das heißt, welche Gestaltungselemente und Abstufungen kundenseitig gewünscht sind und Sinn machen, um ein attraktives Angebot zu realisieren.

Chance nutzen: ein Schutz-Portfolio schrittweise aufbauen (Protection as a Service)

Eine Monetarisierung mag sowohl durch explizite Schutzleistungen als auch durch ein übergreifendes Premium-Preismodell auf Basis wahrgenommener Markendimensionen erfolgen. Aus unserer Sicht bietet sich ein schrittweiser Aufbau an, der beide Ansätze kombiniert:

Die grundlegende Achse ist die Wirkungstiefe des Schutzes. Eine nur geringe Wirkungstiefe wird dann erzielt, wenn der Kunde von seinem Anbieter Informationen

- eher selten, zum Beispiel bei Vertragsabschluss oder anlässlich signifikanter Risiken…
- primär auf vom Anbieter selber angebotene beziehungsweise verwendete Dienste und Daten…
- überwiegend nur in allgemein gehaltener Form…
- zu eher generellen Risiken

erhält.

Von diesem Basiszustand aus ließe sich ein Schutzportfolio schrittweise entlang von drei zentralen Dimensionen entwickeln:

25 Vgl. Clark-Dickson, Data Mobile operators' consumer mobile security strategies, Informa, 2014.

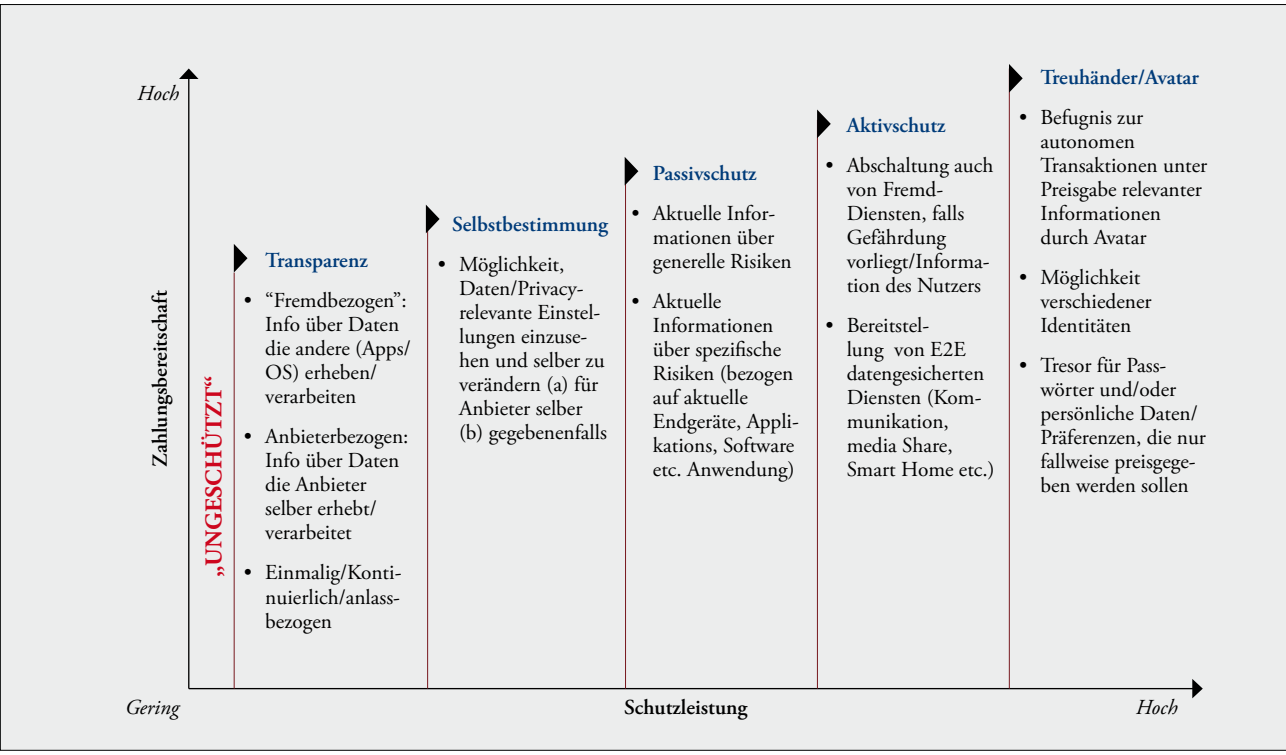
1. Aktualität, Art und Umfang der Risikoprüfungen, das heißt die Frage, ob es nur um Dienste, welche der Carrier selbst anbietet, oder (etwas/sehr) darüber hinaus geht,

2. Personalisierungsgrad der Sicherheitsinformation, das heißt Prüfung beziehungsweise Information nur bei Betroffenheit der installierten und genutzten Dienste,

3. Aktionsintensität, das heißt reine Information oder eine konkrete Handlungsaufforderung.

Wir gehen davon aus, dass mit einer tiefgreifenden Schutzleistung eine erhöhte Zahlungsbereitschaft einhergeht. Die in der folgenden Abbildung dargestellte Portfolio-Evolution beginnt mit der Schaffung der Transparenz als „vertrauensbildende Maßnahme" und entwickelt sich schrittweise bis hin zu einem Avatar, der verschiedenste virtuelle Identitäten für den Kunden gegenüber anderen

Abbildung 2: Potenzielle Schutzdienste für Carrier



Quelle: Detecon

26 *Vgl. Deuker, Aumann, Albers, Duschinski, „Bekommen statt Suchen – Warum wir unsere Interaktion zukünftig an Smart Agents übergeben", in: Detecon Management Report, 3/2011, S. 8-17.*

virtuellen Transaktionspartnern übernehmen kann.[26] Für die Portfolio-Cluster „Transparenz" und „Selbstbestimmung" sehen wir nur die Positionierung und den Marken-Goodwill mit einhergehender Premium-Preissetzung als Monetarisierungsansatz. Mit dem Cluster „Passiv-Schutz" ergibt sich unseres Erachtens die Chance, diesen als eigens bepreisten Service anzubieten.

Carrier besetzten bislang diese Schutzfunktion nicht übergreifend. Es gibt aber erste OTT-Anbieter, welche sich aktiv in Richtung Schutzfunktion und Datensicherheit positionieren. Ein Beispiele ist Digi.mem eine App, die sich aus der Funktion einer personenbezogenen Speicherung von persönlichen Social-Media-Inhalten zu einer Sicherungsfunktion entwickelt hat. Dies App nutzen bereits 350.000 Kunden aus verschiedenen Ländern. Die Firma will später im Jahr 2016 den Funktionsumfang in Richtung Content Sharing von durch Kunden freigegebenen Profilen erweitern. Weiter ist da der Konkurrent Datacoup, der bereits vom Kunden freigegebene Profilinformationen an interessierte Datenkäufer verkauft und dem Kunden dafür Payouts zahlt. Datacoup ist allerdings bislang nur in den USA aktiv. Dies zeigt, dass sich bereits Pioniere in dieser Lücke positionieren. Telcos müssen also schnell handeln, um das „Window of opportunity" zu nutzen, solange es noch existiert.

Nachfrage heute und morgen: ein kurzer Check

Auf den ersten Blick erscheint der oben skizzierte Avatar als weit entfernte Vision. Doch schaut man auf die bereits vorhandenen sowie aktuell pilotierten und damit greifbaren Entwicklungen, dann entsteht schnell der Eindruck, dass wir mit einem Fuß schon „in der Matrix" stehen:

Betrachte ich den Fernseher – oder betrachtet er mich? 2 SmartTVs mit Webcam, 3 Laptops, 2 Pads und 3 Smartphones machen schon mal 15 Kameras und 10 Mikrofone. 1 Trainingsuhr und 1 ActionCam macht mit den Smartphones und Pads dann 7 Geräte mit GPS/Ortungsfunktion. Auf der Einkaufsliste stehen noch Sensoren und Kameras zur Sicherung des Smart Home. Gelesene Datenschutzrichtlinie von 107 Apps aus der letzten Zählung: 2, verstanden: 0. Wer weiß, wann diese Geräte welche Daten übermitteln und wer auf Geräte oder Daten Zugriff hat oder haben könnte? Der Besitzer meistens nicht.

Gestalked im Supermarkt?! Ist das Smartphone-WLAN jetzt an oder aus? Viele vergessen oft, es auszuschalten – die Energieersparnis erscheint zu gering. Woran man nicht denkt: Das Smartphone teilt sich (seine MAC) auch jedem WiFi-Zugang freudig mit, an dem man im Tagesverlauf vorbeikommt. Unternehmen wie Euclid machen sich das zunutze und erstellen für zahlungsbereite Handels-

unternehmen Bewegungsprofile, die auf der Geräte-ID basieren. Wie lange man wann in welchem Supermarkt war, vor welchen Regalen man länger stand und wo man schnell vorbeigelaufen ist, wird dadurch ersichtlich. Für diese Datenbereitstellung sollte es Rabattpunkte geben. Mindestens.

Zahlen mit der schönen Stimme statt mit dem „guten Namen"? Sprache wird als bequeme Steuerungsmöglichkeit immer beliebter werden. Das aktuell von Google „Hands Free" getestete Zahlen per Sprachbefehl erscheint nach den Steuerungen von iPhone, Xbox, Amazon Fire und Google Now als logischer und bequemer Evolutionsschritt. Dass Stimmmuster gegenüber einer PIN Vorteile haben, ist unbestritten. Nur setzt dies auch ein ununterbrochenes Mitlauschen der Geräte voraus. Lässt sich überhaupt prüfen, ob Kamera und Mikrophon wirklich ausgeschaltet sind – und bleiben? Hören die Anbieter der Dienste immer mit?

Wie sieht die Zukunft aus? Eine weitere Vernetzung von persönlichen Endgeräten aller Art, eine Zunahme von verbundenen Devices für verbesserte Unternehmensprozesse – all dies wird zu einer exponentiell ansteigenden Dichte von uns umgebenden Sensoren führen. Darüber hinaus wird auch die Anzahl der Netzzugangspunkte für eben diese Sensoren deutlich zunehmen. Die Wahrscheinlichkeit, sich bewusst oder unbewusst mitzuteilen, steigt damit in allen Lebensbereichen signifikant an. Etwas unheimlich wird es, wenn man sich die Möglichkeiten der Verknüpfung von Daten vor Augen führt: Der Fernseher weiß, was man gerade sieht, der Pulsmesser zeichnet auf, was man dabei empfindet – das ist hervorragend für die Werbewirkungsmessung! Die Autoversicherung glaubt auf Basis von Daten zu wissen, in welchem Maße man sich an die Gesetze von Physik und Verkehr hält – und passt daraufhin die Tarife an. Die Krankenversicherung glaubt zu wissen, ob, wann und wie viel man sich bewegt und im örtlichen Weindepot einkauft. Bekommt man noch eine Versicherung, wenn man sich nicht tracken lässt?

Die meisten Nutzer scheinen die Risiken derzeit noch nicht allzu sehr zu schrecken. Die Nutzerzahlen großer Plattformen wie Facebook und WhatsApp haben unter der vielfachen Kritik nicht signifikant gelitten. Der Netzwerkeffekt – der entscheidende Punkt für den Einzelnen, dass die Mehrheit seiner Kontakte ebenfalls wechselt – spielt gerade den großen Playern in die Hände. Aus Nutzersicht wird das Risiko darüber hinaus noch als tendenziell gering betrachtet. Beispielsweise gilt bei WhatsApp das Risiko von ungesicherten Nachrichten gemeinhin als vernachlässigbar. Diese Sicht wird jedoch mit jedem Digitalisierungsschritt unverhältnismäßiger: Ein vollständig digitalisierter Alltag ist dann zwangsläufig auch ein vollständig dokumentierter und verwertbarer Alltag.

Das größte Risiko sehen wir in der Beschneidung der informationellen Neutralität: Was passiert, wenn auf Basis des vollerfassten Verhaltens einer Person dieser ausschließlich Informationen zur Verfügung gestellt werden, die andere (Systeme) als relevant betrachten? Anstatt bei Weltgeschehen und Einkäufen das voll verfügbare Spektrum sehen zu können, wird einer Person dann nur ein angereichertes Spiegelbild der scheinbaren Interessen und Neigungen gegeben. Greifbarer und im Alltag anzutreffen sind und bleiben „klassische" Risiken wie Identitätsdiebstahl, Transaktionsbetrüge oder Erpressungen. All diese Risiken werden zukünftig durch die fortschreitende tiefere Durchdringung des persönlichen Alltags mit digitalen Diensten multipliziert.

Carrier sollten Position beziehen – und zwar schnell

Zusammenfassend haben wir fünf Hypothesen formuliert, entlang derer sich Handlungsnotwendigkeiten für Carrier schrittweise bestimmen lassen:

1. Treiber auf Nachfrageseite: Die im Rahmen der Digitalisierung bei den Nutzern von Telekommunikationsdiensten entstehenden Unsicherheiten werden rasant zunehmen.

2. Chance für Carrier: Carrier sind im bestehenden Marktsystem die grundsätzlich geeignetste Entität, um Dienste-übergreifend, reaktionsschnell und einer Vielzahl von Kunden Transparenz und Schutz zu verschaffen.

3. Zeitdruck für Carrier: Je länger die Carrier mit einer Positionierung „gegenüber" den OTT zögern, umso mehr werden sie als deren Unterstützer betrachtet.

4. Bewertungs- und Entwicklungsbedarf für Carrier: Die Monetarisierung der möglichen Themen rund um Kundendaten wird derzeit fast ausschließlich aus dem Aspekt der „klassischen" Big Data-Brille betrachtet. Der Schutzaspekt ist im Hinblick auf seinen möglichen Mehrwert nach unserer Erfahrung bislang nicht betrachtet worden.

5. Handlungsbedarf für Carrier: Nicht jeder Carrier wird von seinen Kunden bereits jetzt als ausreichend geeignet wahrgenommen, um als vertrauenswürdige Schutzinstanz gelten zu können.

Es ist folglich dringend geboten, dass Carrier jetzt zunächst die für sie relevante und mögliche Positionierung bestimmen. Eine schrittweise und markentechnisch auch glaubwürdige Emanzipierung vom OTT-Big-Brother-Modell und eine Ermündigung des Telekommunikationsnutzers sind möglich. Sie kann sich am oben aufgezeigten Evolutionsmodell für Schutzdienste orientieren. Start-ups adressieren bereits relevante Elemente dieses Modells. Angesichts des notwendigen Kompetenzaufbaus und der zu erwartenden Produktentwicklungsphase ist jetzt die Zeit zu handeln. Das Schutzbedürfnis des digital durchleuchteten Kunden ist eine große Chance, die Verluste an der Kundenschnittstelle gegenüber den OTTs wieder wettzumachen. Aus unserer Sicht können sie sogar mehr als vollständig ausgeglichen werden.