Tabelle 1.1 Wertverfall für die bestehenden Akteure am Beispiel Musik, es profitieren die Intermediäre (W. I. R. E. 2015)

Format	Preis [in US-Dollar]	Einnahmen Label [pro Stück, in US-Dollar]	Einnahmen Musiker [pro Stück, in US-Dollar]
Selbst gebrannte CD	9,99	0	8
CD im Einzelhandel	9,99	1	1
Download Album (via *iTunes*)	9,99	5,35	0,94
Download MP3 (via *iTunes*)	0,99	0	0,74
Song anhören (via *Rhapsody*)	Fix	0,009.1	0,002.2
Song anhören (via *Last.fm*)	Fix	0,004	0,000.75
Song anhören (via *Spotify*)	Fix	0,001.6	0,000.29

1.6 Neue digitale Geschäftsmodelle entstehen

Digitale Geschäftsmodelle attackieren die traditionell produkt- und technologieorientierten Unternehmen. *Uber* revolutioniert ohne Taxis und Taxifahrer die Taxibranche, *Skype* ohne eigene Netzwerkinfrastruktur die Telekommunikationsindustrie. Von *Alibaba* bis *Zalando* kann man die digitalen Gewinner analysieren: Selten neue Technologien, meist unterscheidet das Geschäftsmodell die Gewinner von den Verlierern. In der digitalen Welt werden zahlreiche Geschäftsmodelle effektiv und effizienter als in der analogen Welt genutzt. So lassen sich zweiseitige Märkte fast perfekt auf digitalen Plattformen realisieren. Dabei ist es egal, ob es sich um den Verkauf von Produkten und Dienstleistungen, um die Vermittlung von Kompetenzen oder um den Abgleich von Stromnutzung und Stromverbrauch im privaten Umfeld dreht. Fast jedes Geschäft lässt sich zu mehr Transparenz, geringeren Transaktionskosten und damit mehr Wettbewerb transformieren. Die Verlierer dieses Trends sind die früheren Profiteure von „Heimatschutz“, von Quasi-Monopolisten wie Energiekonzernen bis hin zu lokalen Akteuren wie Nachbarschaftsläden.

Der Werkzeughersteller *Hilti* revolutioniert derzeit mit seiner On!TrackSoftware die Betriebsmittelverwaltung von Bauunternehmen. Dazu werden Geräte, Werkzeuge und andere Arbeitsmittel digital erfasst und mit RFID-Tags ausgestattet. Eine Datenbank in der Cloud enthält alle wichtigen Informationen wie Standort, Produktspezifikationen und Wartungstermine. Der Kundennutzen liegt in geringeren Beständen, niedrigeren Kosten, besserer vorbeugender Wartung der Werkzeuge, weniger Ausfäl-

len, sicherer Dokumentation, Echtzeitstandortverfolgung der Werkzeuge und höherer Sicherheit für die Mitarbeitenden. Der Wert für *Hilti* besteht darin, dass das Unternehmen seine Kunden besser kennenlernt und nachvollziehen kann, welche Werkzeuge sie wie oft einsetzen. On!TrackKunden sind im Vergleich zu anderen Kunden außerdem profitabler und loyaler.

Betroffen ist auch die Kreativindustrie, die sich bislang nicht den globalen Effizienzbestrebungen stellen musste. Aber über Crowdsourcing-Plattformen wie *99designs.com* werden Werbeagenturen angegriffen, über *InnoCentive* die technischen Dienstleister und über *Amazon Mechanical Turk* sogar die Niedriglohndienstleister. Outsourcing von einfacher Arbeit, zum Beispiel an Callcenter, hat bereits in den letzten 15 Jahren enorm zugenommen. Nun folgt auch die Kreativindustrie. Der Effekt ist überall gleich: Die Welt wird flach, die indische Kollegin aus Bangalore und der chinesische Freelancer aus Schanghai werden zu direkten Konkurrenten. Damit hat die Globalisierung eine nächste Ebene erreicht: Nach der Globalisierung der physischen Produktwelt erfolgt nun auch die Globalisierung der Dienstleistungsindustrie.

Plattform als goldene Lösung?

Plattformen bilden nach wie vor die Basis für erfolgreiche Geschäftsmodelle. Doch ihr Aufbau ist schwierig und auch Unternehmen mit großer Finanzkraft scheitern. Viele Plattformmanager vergessen auch die Zweiseitigkeit der Märkte: Kunden gibt es nicht nur auf der Nachfrage-, sondern auch auf der Anbieterseite.[1)]

Metaverse – Milliardengeschäft oder Totgeburt?

Das Metaverse als Paralleluniversum für Gesellschaft und Geschäft hat die Fantasie der Investoren angeheizt. Als Mark Zuckerberg jedoch seinen ersten Avatar im Metaverse vorstellte, erntete er vor allem Spott: 10 Milliarden US-Dollar Investitionen wurden hierfür aufgewendet und am Ende sah die Öffentlichkeit ein comicartiges Selfie-Bild von Mark Zuckerberg. Es ist vielen nicht vorstellbar, dass hier Wertschöpfung stattfinden kann.

Was ist nun wirklich das Metaverse? Wie häufig, wenn ein Hype entsteht, gibt es unzählige Definitionen und Begriffsverwirrungen. Wir sehen hier drei konstituierende Merkmale für das Metaverse, unabhängig, in welchem Umfeld und in welcher Industrie dieses stattfindet:

1. Es geht beim Metaverse erstens um eine umfassende Erfahrung, welche auf Virtual, Augmented und Mixed Reality (VR, AR, MR) aufbaut. Real-time-Interaktivität von Menschen und Menschen mit Systemen wird hier ermöglicht. Technologisch spielen hier auch KI-Technologien eine große Rolle.

[1] Siehe in Kapitel 3 zum Plattform-Navigator, wie Plattformen erfolgreich entwickelt werden können.

2. Zweitens dreht es sich beim Metaverse immer um soziale virtuelle Welten, in denen live, synchronisiert und gleichzeitig verschiedenste Aktivitäten stattfinden. Der soziale Charakter darf nicht unterschätzt werden, nicht nur im Gaming, sondern auch in industriellen B2B-Umgebungen (z. B. virtuelle Anlagenbesichtigungen von potenziellen Käufern).
3. Drittens basiert das Metaverse auf Web 3.0, welches die Eigentumsrechte regelt. Es ist interoperativ und dezentralisiert, stellt damit auch ein Gegenmodell zu den zentralisierten Plattform-Geschäftsmodellen von *Amazon* und Co. dar. Wichtige Elemente sind hier die Distributed-Ledger-Technologien (DLT, wie Blockchain) und Non-Fungible Tokens (NFT, nicht austauschbarer Wert), welche eine sichere dezentrale Transaktion und damit wirtschaftliche Aktivitäten ermöglicht.

Im B2C-Kontext wird oft die Frage gestellt: Wird für eine Gucci-Tasche (= NFT) im Metaverse tatsächlich real bezahlt? Einerseits zeigt schon der Kunsthandel, dass Produkte gleichzeitig physisch und virtuell gekauft werden können. Andererseits hat auch das rein virtuelle Produkt einen Wert, der unabhängig von seinen Herstellkosten ist – Herstellkosten von virtuellen Massenwaren haben Grenzkosten gegen Null. Was ist nun die Zahlungsbereitschaft für eine virtuelle Gucci-Tasche? Man wird dies nur durch empirisches Testen herausfinden. Aber Skeptiker sollten sich vor Augen führen, dass das Gaming-Unternehmen *Fortnite* bereits 2021 über 5,8 Milliarden US-Dollar Umsatz mit Avatar-Equipment erzielte. Es wird also schon heute viel für digitale Produkte ausgegeben. Unterstützt wird dies noch durch die Veränderung in der Gesellschaft: Für die heutigen Teenager ist es gemäß Umfragen wichtiger, wie sie online, auf Social Media wirken als in Realität. Warum sollte dann nicht ein digitaler Sneaker der richtigen Marke ebenso eine Zahlungsbereitschaft hervorbringen wie der physische Sneaker oder eine Gucci-Tasche?

In der eigenen Forschung arbeiten wir viel im industriellen Kontext (B2B). Hier könnte ein ähnlicher Trend erwartet werden wie beim Aufkommen des Web 2.0, als alle Medien nur über selbst hergestellte T-Shirts mit eigenen Motiven geschrieben haben. Beim Aufkommen von additiven Fertigungsverfahren (3D-Druck) wurde medienwirksam spekuliert, dass jeder Konsument seinen Modeschmuck selbst designt und herstellt. In Realität lagen jedoch in beiden Feldern die wahren Wertschöpfungspotenziale in B2B-Anwendungen, wie z. B. der Ersatzteilherstellung. Bei unseren laufenden Forschungsarbeiten mit *Siemens* zu „NFTs in Industrial Metaverse“ werden wir sehen, welche Use Cases hier die größten Potenziale haben.

Cyberattacken als neue Bedrohung

Digitalisierte Unternehmen haben jedoch nicht nur Chancen, sondern auch zahlreiche neue Risiken. So sind in jüngerer Zeit häufiger Cyberattacken aufgetreten, das Schadenspotenzial steigert sich. Durch einen solchen Angriff auf *Sony* im Jahr 2014 wurden sensitive Daten auf das Netz freigegeben. Persönliche Daten von *Sony*-Mitar-

beitenden und ihren Familien, E-Mails zwischen Mitarbeitenden, Managementgehälter und Kopien von noch nicht freigegebenen Filmen von *Sony Pictures Entertainment* waren verfügbar. 15 Millionen US-Dollar wurden für Schadensersatzklagen zurückgestellt, Co-CEO Amy Pascal trat zurück. Hinter der Attacke wird Nordkorea als Auftraggeber vermutet, es entstand eine internationale Krise mit politischen Folgen.

Im Rahmen des Stuxnet wurde eine iranische Nuklearanlage zerstört; *USB*-Sticks mit Malware wurden auf dem Betriebsgelände breit verteilt. Es war nur eine Frage der Zeit, bis ein Mitarbeitender einen solchen USB-Stick finden, diesen in ein Gerät stecken und damit die Malware aktivieren würde.

Das Jahr 2022 zeigt hingegen ein ganz neues Ausmaß an Cyberangriffen, mit einem Allzeithoch an Datenleaks. Allein in Deutschland fielen 80 Unternehmen einer Cyberattacke zum Opfer, wobei die Dunkelziffer noch nicht berücksichtigt wurde (CSO 2023). Die Folgen waren oft hohe Umsatzeinbußen, verbunden mit hohen Wiederherstellungskosten für die Datenlandschaft oder in einigen Fällen auch Reputationsschäden.

Der Hackerangriff auf das Unternehmen *Continental* ist ein solches Beispiel. Hacker verschafften sich Zugang zu den Servern des Unternehmens und verbreiteten anschließend 40 Terabyte an sensiblen Daten im Darknet. Darunter befanden sich Informationen über Budget- oder Investitionspläne sowie Mittelungen von Vorstandsmitgliedern. Dieser Angriff bedeutete einen erheblichen Schaden für *Continental* (CSO 2022).

Ein weiteres internationales Beispiel aus dem Jahr 2022 ist das der russischen Hackergruppe Conti, die ganz Costa Rica lahmlegte. Sie griffen das Finanzministerium an, beeinträchtigten so die Import-/Exportindustrie und lösten eine nationale Krise aus. Später versuchten die Hacker erneut, die Sozialversicherungskasse Costa Ricas anzugreifen, was ihnen zwar nicht in gleichem Maße gelang, aber ein großes Chaos verursachte.

Ein weiteres Beispiel, das die Risiken von Cyberangriffen auch für den Endkunden verdeutlicht, war ein Datenleak im Jahr 2022 bei über 500 Millionen Nutzern von *WhatsApp*, einem Unternehmen das zu *Facebook* gehört. Die entsprechenden Daten wurden durch den Hacker in einem Hacker-Community-Forum zum Verkauf angeboten.

Das aktive Management von Zugriffsrechten für Daten gewinnt an Bedeutung. Illegale Datenverkäufe an Banken zur Steuerhinterziehung sind nur die medienwirksame Spitze des Eisberges. Die meisten Schäden in Unternehmen werden nicht bemerkt, da Daten in großen Mengen illegal zu Wettbewerbern diffundieren. Die Funktion des Information Security Officer wird daher nicht nur für Großkonzerne, sondern auch für mittelständische Unternehmen mit hoher Wissensintensität hoch relevant. Die Aufgabe von solchen Datensicherheitsverantwortlichen ist die Entwicklung einer sicheren Datenumgebung, die den zunehmend offenen Geschäftsprozes-

sen gerecht wird, aber gleichzeitig nach außen sicher ist. Typische Probleme in Unternehmen sind das Management von Zutrittsrechten, Netzschwachstellen, physische Schwachstellen im Zugang zu IT-Centern und vor allem Schwachstellen in der User Awareness. Es wird immer üblicher, neben internen Audits Organisationen wie den *Chaos Computer Club* mit gezielten Hackerangriffen zu beauftragen, um die Schwachstellen eines Unternehmens aufzudecken.[2)]

Je höher der Grad der Digitalisierung von Fertigung und Logistik, auch über Unternehmensgrenzen hinweg, und je vernetzter und offener die Wertschöpfungskette, umso anfälliger ist diese für externe Attacken. Dabei gibt es mehrere Felder: 1. Datenverlust, zum Beispiel durch Malware, 2. Datendiebstahl, zum Beispiel Kundendaten von Banken oder Prozessdaten einer Maschine, 3. Fehlverhalten von vernetzten Anlagen oder Produkten, 4. Remote-Steuerung von Anlagen oder Produkten. Stellt man sich beim autonomen Fahren einen Hacker mit verbrecherischen Absichten vor, wird schnell klar, dass der Schaden unermesslich hoch werden kann. Diese Risiken sind in ihren unterschiedlichen Dimensionen zu erfassen und zu bewerten. Die Risikomatrix von Ereigniswahrscheinlichkeit und -ausmaß, ergänzt mit einem qualitativen Risikodialog, wird hier unerlässlich. Das Thema Sicherheit gewinnt bei der Digitalisierungsdebatte stark an Bedeutung.

1.7 Segen und Fluch der Regulierung

Der Umfang der Daten wächst immens. Allein im *Audi A8* wurden im Jahr 2014 über 2000 Datenpunkte abgenommen. Doch was wird damit gemacht? Und noch wichtiger: Wem gehören die Daten? Dem Versicherungsunternehmen, das eine Prämienreduktion bei vorsichtiger Fahrweise anbietet? Dem Automobilhersteller *Audi*? Oder gar den Automobilzulieferern, die über die verschiedenen Marken hinweg eine auf ihr Subsystem konzentrierte Queranalyse durchführen könnten? Oder dem Endkunden, dem Autofahrer? Welche Daten sind in welcher Form verwendbar? Hier sind noch zahlreiche Themen offen.

Uber wird in einigen Ländern verboten, teils aus arbeitsrechtlichen Gründen, teils wegen der Versicherungen, teils als Antwort auf den gewerkschaftlichen Druck der Taxifahrer. Die Frage ist, wie lange sich Fortschritt aufhalten lässt und wo reguliert werden muss. In den Ländern, in denen *Uber* erlaubt ist, setzt sich das Unternehmen mit enormer Geschwindigkeit durch – ein untrügliches Zeichen für Mehrwert bei diesem zweiseitigen Markt. Der nächste Konflikt beim Fahren ist schon vorprogrammiert, wenn autonome Fahrzeuge zugelassen werden. Die Technologie ist auch hier weitgehend vorhanden. In *Stanford* beschäftigt man sich derzeit mit ethischen Fragen

[2] Siehe hierzu auch Kapitel 5 zu Cybersicherheit.

rund um autonomes Fahren: Auch wenn die absolute Zahl der Unfälle und Verkehrstoten mit hoher Wahrscheinlichkeit stark sinken wird, wird es ungeklärte Einzelfälle geben, und diese werden die öffentliche Diskussion bestimmen. Fährt das Fahrzeug nach einer unübersichtlichen Kurve eher in eine Gruppe Rollstuhlfahrer oder in Mutter und Kind, wenn sich der Unfall nicht vermeiden lässt? Solche Entscheidungen lassen sich schwierig programmieren. Menschliches Versagen wird akzeptiert, aber die Anforderungen an computerisierte Entscheidungen sind höher.

Die Regulierung wird früher oder später auch die Kreativindustrie betreffen. Heute wird in ganz Europa über Minimallohnforderungen diskutiert. Wie wird es in Zukunft sein, wenn über die Virtualisierung der Arbeit der indische Callcenter-Mitarbeitende aus Bangalore zum direkten Kollegen und Wettbewerber des Mitarbeitenden in Zürich wird? Wie effektiv sind heutige Gesetze zur Verhinderung von Lohndumping, wenn über Internetplattformen wie *Amazon Mechanical Turk* oder *Clickworker.com* heute schon viel Arbeit von den entwickelten Ländern in Niedriglohnländer verlagert wird? Wie geht man in Europa mit dem Trend zum Freelancer in der digitalen Welt um, bei dem die Mitarbeitenden immer stärker ausgelagert werden, zum Beispiel via Crowdsourcing, für Webdesign oder Programmierung? Gerade in der digitalen Wertschöpfung wird immer stärker virtuell gearbeitet. Wie können Urheberrechte und geistiges Eigentum in der neuen offenen Welt von *YouTube* und Sharing-Plattformen effektiv geschützt werden?

Wie geht man mit Plagiatsthemen und Copyright um in Zeiten von zunehmend erfolgreicher generativer KI, wie ChatGPT, das Text generiert, ohne die Quellen zu identifizieren? Bereits drei Monate nach Veröffentlichung gibt es den ersten wissenschaftlichen Artikel mit ChatGTP als Co-Autor (2023).

Zahlreiche Fragen sind hier noch offen, eines steht jedoch fest: Die Regulierung hinkt der technologischen Entwicklung hinterher. Einige Länder arbeiten mit „experimenteller Gesetzgebung“, auch Deutschland und der Schweiz beispielsweise bei der Zulassung von autonomen Fahrzeugen (2022 bzw. 2023): Hier ist es nun erlaubt, unter bestimmten Bedingungen die Hände komplett vom Steuer zu nehmen. Was technologisch schon lange möglich ist, wird nun unter enger Beobachtung versuchsweise zugelassen. Es ist noch nicht abzusehen, wo es mehr und wo es weniger Regulierungen geben wird. Sicher ist nur, dass sich der Druck verstärken wird: mehr Regulationsforderungen von Gewerkschaften und etablierten Unternehmen, Deregulationsforderungen von den neuen Wettbewerbern.