Online Einkäufe im Internet

©bnenin - stock.adobe.com

Abteilung Marktforschung, Dezember 2019

Studie zur digitalen Sicherheit bei Einkäufen im Internet

Joanneum Research im Auftrag der Kammer für Arbeiter und Angestelle für Steiermark

Meine AK. Ganz groß für mich da. AK-Hotline ✆ 05 7799-0

www.akstmk.at

Online Einkäufe im Internet

Studie zur digitalen Sicherheit bei Einkäufen im Internet

Joanneum Research Digital
Institut für Informations- und Kommunikationstechnologien

DI Dr. Ralph Ankele

Graz, Dezember 2019

Im Auftrag der
Kammer für Arbeiter und Angestellte für Steiermark

Inhalt

1 Zusammenfassung

Die Zahl der Einkäufer im Internet wächst schnell. 2019 haben 62.4 Prozent der Österreicher[1] online eingekauft. Gerade bei der jüngeren Generation ist der Trend zum Einkaufen im Internet noch deutlich schneller am Wachsen. Im letzten Jahr haben, 81 Prozent der 16 bis 24-Jährigen im Internet etwas bestellt (Schultz, Anteil der Online-Käufer an der österreichischen Bevölkerung von 2010 bis 2019 2019).

Die Einkaufmöglichkeiten im Internet verändern sich stetig. Die umsatzstärksten Online Shops in Österreich haben 2018 einen Gesamtumsatz von 1.5 Milliarden Euro erwirtschaftet (Montasell 2019). Klarer Marktführer in Österreich ist Amazon, mit einem Umsatz von 682.3 Millionen Euro, gefolgt von Zalando und Universal mit jeweils 304.3 Millionen Euro bzw. 135.9 Millionen Euro Umsatz. Dabei bewegt sich der Trend beim Einkaufen im Internet mit den neuen Technologien weg vom PC zu Hause, auf Smartphones und andere smarte Geräte der Kunden. Der E-Commerce Markt für das Internet der Dinge kann dabei in drei Kategorien unterteilt werden:

- *Verbundene Geräte für Kunden:* zum Beispiel Smartphones, Smart Homes, und verbundene Autos.
- *Verbunden Geräte für Verkäufer:* zum Beispiel intelligente Getränkeautomaten und verbundene Werbebildschirme.
- *Selbstbezahlende automatisierte Kassensysteme:* zum Beispiel technische Geräte welche automatisiert den Bezahlungsprozess im Hintergrund abwickeln.

Da Kunden beim Einkaufen im Internet nicht vor Ort sind, müssen Sie über das Internet auf Zahlungssysteme zugreifen, welche auch über das Internet möglich sind. Die typischen Zahlungssysteme für das Einkaufen im Internet in Österreich sind Lastschrift/Bankeinzug, Überweisung, Kreditkarten, Vorkasse, Kauf auf Rechnung, mobile Zahlungsmittel mit der Verwendung von Smartphones und Smartwatches, sowie PayPal. In letzter Zeit sind auch noch viele Fintech Unternehmen hinzugekommen, die als Challenger Banken versuchen, die Bezahlsysteme im Internet zu revolutionieren. Zusätzlich ist auch ein Trend zur Bezahlung mit digitalen Zahlungsmitteln oder Kryptowährungen zu beobachten.

Durch den Wechsel von Einkäufen vor Ort in Einkäufe im Internet, sind viele Unternehmen auch auf die technischen Möglichkeiten aufmerksam geworden, dass Kaufverhalten ihrer Kunden verstärkt zu protokollieren und analysieren. Bonusprogramme und Kundenkarten sind dabei ein geschickter Vorwand mit dem sich Unternehmen rechtfertigen, das Kaufverhalten ihrer Kunden zu analysieren. Die bekanntesten Bonusprogramme in Österreich sind der Jö-Bonus-Club und das PAYBACK Bonusprogramm.

[1] Aus Gründen der besseren Lesbarkeit wird ausschließlich die männliche Form verwendet. Sie bezieht sich auf Personen beiderlei Geschlechts.

Während viele Online Shop Betreiber das Kaufverhalten ihrer Kunden mitprotokollieren, um ihre Dienste zu verbessern, gibt es auch andere Motive für das Analysieren der Daten. Dies sind zum Beispiel personalisierte Werbung, das Erstellen von Personenprofilen, individuelle Preisgestaltung, das Anlegen von Bewegungsprofilen, sowie das Verkaufen von personenbezogenen Daten an Drittanbietern.

Viele Kunden sind sich dessen nicht bewusst wo Sie beim Online Einkaufen im Internet ihre Daten hinterlassen. Während den Kunden oft klar ist, dass Sie Daten wie Namen, Anschrift, und Zahlungsdaten an den Händler im Laufe des Bestellprozesses weitergeben, ist vielen nicht bewusst, dass der Online Händler auch die Suchanfragen, das Klickverhalten und vieles mehr speichert und analysiert. Zusätzlich verlinken Werbeanbieter das Suchverhalten in Online Shops und Suchmaschinen (zum Beispiel Google), um den Kunden dann später gezielt Werbung einblenden zu können. Mittels Technologien wie Cross Device Tracking ist es Werbeanbietern auch möglich, Kunden über mehrere Geräte zu verlinken. Dabei kann unter anderem erkannt werden, wenn ein Kunde im Fernsehen einen Werbespot gesehen hat, um diesen Kunden dann gezielt Werbung auf dem Smartphone oder Computer einzublenden.

Doch nicht nur Werbeanbieter und unseriöse Shops versuchen persönliche Daten von Kunden zu sammeln. Cyber-Kriminelle sind auf den Trend zum Einkaufen im Internet aufgesprungen und versuchen durch Malware, Phishing, Abo Fallen und Social Engineering die persönlichen Daten von Kunden, sowie deren Zahlungsinformationen zu stehlen. Viele unseriöse Online Shops versuchen Kunden über unsichere Zahlungsarten, wie Überweisungen und Vorkasse, zu Zahlungen zu überreden, und liefern dann die bestellten Waren nicht. Auch der Identitätsdiebstahl nimmt zu. Dabei verkaufen Cyber-Kriminelle persönliche Daten von Kunden im Dark Web. Ausreichend dafür sind bereits Informationen über die Kreditkarte eines Kunden, die von einem bis 45 US-Dollar gehandelt werden. Vollständige Identifikationspakete werden im Dark Web zwischen 30 und 100 US-Dollar verkauft.

Um Sicher im Internet einkaufen zu können, sind die folgenden Punkte zu beachten:

- Achtung bei augenscheinlich zu niedrigen Preisen.
- Preise in Online Shops sollten transparent aufgelistet sein.
- Vermeiden Sie unsichere Zahlungsmethoden (wie Überweisungen und Vorkasse).
- Benutzen Sie wenn möglich ein oder mehrere Preis-Vergleichsportale.
- Seriöse Anbieter geben Details zu den Liefer-/Versanddiensten auf ihrer Webseite bekannt.
- Lesen Sie die Allgemeinen Geschäftsbedingungen.
- Hat der Online Shop ein E-Commerce-Gütezeichen?
- Sind die Lieferzeiten klar ersichtlich?
- Ist der Leistungsumfang klar beschrieben und aufgelistet?
- Machen Sie von Ihrem Rücktrittsrecht (14 Tage ohne Angabe eines Grundes) Gebrauch, sollte die Waren nicht ihren Erwartungen entsprechen.
- Benutzen Sie unterschiedliche, sichere Passwörter, wenn Sie sich bei Online Shops im Internet registrieren.
- Benutzen Sie wenn möglich eine mehrfache Authentifizierungsmethode, wenn Sie sich bei Online Shops anmelden.
- Vermeiden Sie das Eingeben von persönlichen Daten und Bankinformationen, wenn Sie mit öffentlichen WLANs verbunden sind.

- Benutzen Sie Werbeblocker beim Einkaufen im Internet.
- Studieren Sie die Datenschutzeinstellungen ihres Webbrowsers, und passen Sie diese gegebenenfalls an.
- Vermeiden Sie Kundenkarten und Bonusprogramme, wenn Sie nicht wollen, dass ihr Kaufverhalten analysiert wird.
- Nehmen Sie nicht bei jedem Gewinnspiel im Internet teil.
- Bewahren Sie ihre Anonymität im Internet. Füllen Sie nur die Informationen aus, die unbedingt notwendig sind damit die Dienste funktionieren. Lassen Sie irrelevante Informationen weg.
- Überprüfen Sie regelmäßig ihre Bankkonten und Kreditkarten, die Sie zum Einkaufen im Internet benutzen.

2 Einführung

Einkaufen im Internet ist ein wachsender Trend. 2019 nutzten durchschnittlich 62.4 Prozent der Österreicher im Alter von 16 bis 74 Jahren das Internet zum Online Einkaufen (Schultz, Anteil der Online-Käufer an der österreichischen Bevölkerung von 2010 bis 2019 2019). Bei jungen Erwachsenen (Altersgruppe 16 bis 24-jährigen) haben sogar 81 Prozent in den letzten 12 Monaten im Internet eingekauft. Die jüngere Bevölkerungsgruppe kauft mittlerweile beinahe alles im Internet ein. Sei es von der täglichen Bestellung von Pizza und Nudeln, bis hin zu Elektronischen Geräten, Bekleidung, Büchern und Kosmetikprodukten. Die beliebtesten Produkte sind mit 37 Prozent Bekleidung und Textilien. 25 Prozent kaufen Bücher, Zeitschriften und Zeitungen online. Elektronische Geräte folgen mit 23 Prozent. Der Umsatz vom österreichischen Internet-Einzelhandel 2018 beträgt 3.8 Milliarden Euro und wächst stetig (Schultz, E-Commerce-Umsatz in Österreich von 2006 bis 2017 sowie eine Prognose bis 2018 (in Mrd. Euro) 2019).

Während Einkaufen im Internet immer mehr zunimmt, steigen auch Sicherheit– und Datenschutzbedenken. Vielen Menschen ist unklar, was mit ihren Daten im Internet passiert. Denn auch Cyber-Kriminelle schlafen nicht und haben längst erkannt, dass mit Onlinebetrug sehr viel Geld gemacht werden kann. 2018 wurden in Österreich 19628 Fälle von Cybercrime bei der Polizei zur Anzeige gebracht. Lediglich 37 Prozent davon konnten aufgeklärt werden (Schultz, Entwicklung der Aufklärungsquote von Cybercrime (gesamt) in Österreich von 2006 bis 2018 2019). Weitere Gefahren beim Einkaufen im Internet können direkt von den Betreibern von unseriösen Online Shops ausgehen. Jedoch wird die Privatsphäre ihrer Kunden auch oft von seriösen Händlern ignoriert, um das Kaufverhalten ihrer Kunden detailliert zu analysieren. Einerseits versuchen Händler und Werbeanbieter mehr Informationen zum Kaufverhalten von Kunden herauszubekommen, um ihre Dienste und Services zu verbessern. Andererseits nutzen Werbeanbieter die Daten von Kunden auch um personalisierte Werbung, Personenprofile und persönliche Preisgestaltung von Produkten zu betreiben. Dazu werden, sich im rechtlichen Graubereich befindliche, technische Möglichkeiten genutzt oder der Kunde wird mit einer Informationsflut überlastet, sodass er keine bewusste Entscheidung mehr treffen kann. Viele Kunden stimmen daher der Weitergabe ihrer persönlichen Daten zu, ohne sich dem wirklichen Ausmaß der Datenweitergabe bewusst zu werden.

Diese Studie informiert über die möglichen Gefahren beim Online Einkaufen und gibt Ratschläge zum Sicheren Einkaufen im Internet. Ziel ist es den österreichischen Kunden mehr Bewusstsein über Gefahren beim Einkaufen im Internet zu geben, und die Sicherheit von Einkäufen im Internet zu erhöhen.

3 Methodik

Als Teil dieser Studie wurde eine Literaturrecherche durchgeführt. Dabei wurden aktuelle wissenschaftliche Publikationen, Fachzeitschriften, technische Blogs, Internetforen, und Webseiten von Anbietern von innovativen, technischen Produkten analysiert und ausgewertet. Basierend auf dieser Grundlage und dem technischen Fachwissen der Studienautoren wurden die fachlichen Kapitel der Studie verfasst.

Die Studie ist unterteilt in drei Teile. Zu Beginn wird ein Überblick über den derzeitigen Stand der Technik von Einkaufmöglichkeiten im Internet gegeben. Dies inkludiert unter anderem alle bekannte Zahlungsmittel wie Überweisungen, Nachnahme, Lastschriften, und Kreditkarten, behandelt aber auch neue Technologien wie zum Beispiel mobile Zahlungsmittel, PayPal, Startup Banken und Krypto-währungen. Des Weiteren wird eine Übersicht über Online Stores (Amazon, Apple Store, Play Store) und verschiedenen Kundenkarten und Bonusprogrammen (Jö-Bonus-Club, PAYBACK) gegeben.

Anschließend werden die verschiedenen Zahlungssysteme und Einkaufmöglichkeiten analysiert, und die damit zusammenhängenden Risiken und Gefahren beschrieben. Dabei wurde in erster Linie auf Aufklärung und Wissensvermittlung für Kunden gesetzt. In diesem Zusammenhang wird erläutert, was mit persönlichen Kundendaten konkret passiert. Danach werden typische Praktiken von Cyberkriminellen und schlussendlich datenschutzrechtliche Risiken und Gefahren aufgelistet.

Abschließend werden die Erkenntnisse zusammengefasst und Ratschläge zum Sicheren Einkaufen im Internet gegeben.

4 Online Einkaufmöglichkeiten im Internet

In diesem Kapitel geben wir eine Übersicht über Einkaufsmöglichkeiten im Internet. Zuerst werden die beliebtesten Online Shops in Österreich vorgestellt. Danach werden verschiedenen von Online Shops in Österreich akzeptierten Zahlungssysteme aufgelistet. Außerdem geben wir eine Übersicht über mobile Online Shops, neue mobile Zahlungssysteme und die zukünftigen Online Shops für das Internet der Dinge. Zuletzt geben wir einen Überblick über die größten in Österreich genutzten Bonusprogramme und Kundenkarten die mehrere Einkaufsgeschäfte in einem Bonusprogramm vereinen.

4.1 Übersicht von Einkaufsmöglichkeiten im Internet

Im Folgenden wird zuerst eine Übersicht über online Einkaufsmöglichkeiten in Österreich gegeben, und danach auf die typischen Zahlungsarten für Online Shops eingegangen.

4.1.1 Online Einkaufsmöglichkeiten

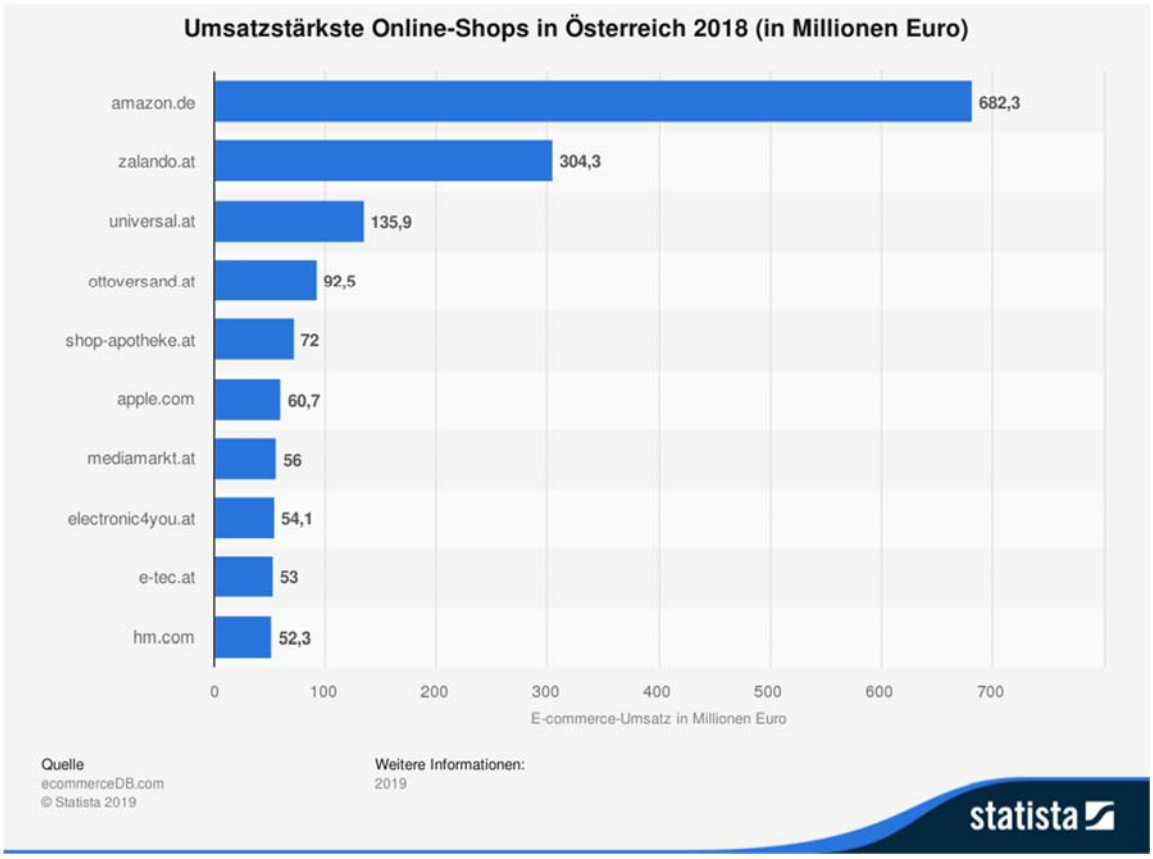

Abbildung 1. Liste der umsatzstärksten Online-Shops in Österreich 2018 (Montasell 2019)

2018 haben die 10 größten Online Shops in Österreich einen Gesamtumsatz von mehr als 1,5 Milliarden Euro gemacht. Der Marktführer Amazon hat davon mit 682.3 Millionen Euro beinahe die

Hälfte des gesamten Umsatzes zu verbuchen. Die zweit und drittplatzierten Online Shops sind Zalando und Universal mit jeweils 304,3 und 135,9 Millionen Euro Umsatz. Die Statistik (siehe Abbildung 1 für mehr Informationen) zeigt, dass in Österreich Einkaufen im Internet ein immer stärker wachsender Trend ist.

4.1.1.1 Amazon

Amazon ist ein in den USA ansässiger Onlineversandhändler mit einem umfangreichen Angebot. Kunden in Österreich (amazon.at) nutzen die Dienste von Amazon Deutschland (amazon.de), wobei Inhalte/Produkte lokal angepasst sind. In Österreich ist Amazon mit 682,3 Millionen Euro Umsatz 2018, der umsatzstärkste Online Shop.

Amazon betreibt neben seinem Online Shop noch weitere Dienste, wie zum Beispiel eine Online Videotheke Amazon Prime Video, einen Musikdienst Amazon Music, eine online Bezahlfunktion Amazon Pay, den Hörbuch Anbieter Audible, die Spracherkennungssoftware Alexa, sowie die Filmdatenbank IMDb. Der Amazon Marketplace ist zum Verkauf von privaten und kommerziellen Produkten gedacht. Amazon verlangt vom Verkäufer pro verkauften Artikel eine Provision von bis zu 15 Prozent und zusätzliche Gebühren für Versand und Logistik.

Die Produktlinie von Amazon umfasst verschiedene Medienartikel (Bücher, Zeitschriften, CD/DVDs, Videos, Software), Baby und Kinderprodukte, Elektronikprodukte, Schönheitspflege und Wellnessprodukte, Lebensmittel, Küchengeräte, Schmuck, Sportartikel, Automobilzubehör, Musikinstrumente, Spielzeug und vieles mehr.

4.1.1.2 Zalando

Zalando ist ein in Deutschland ansässiger Onlineversandhändler, insbesondere für Mode und Schuhe. Der Versandhändler ist mit 304,3 Millionen Euro Umsatz 2018, der zweitstärkste Online Shop in Österreich.

Die Produktlinie von Zalando umfasst hauptsächlich Mode, wie zum Beispiel Herren und Damenbekleidung, Schuhe, Sportmode, Accessoires, sowie Schönheitspflege und Wellnessprodukte.

4.1.1.3 Universal Versand

Universal Versand ist ein in Salzburg ansässiger Onlineversandhändler, mit einem breitgefächerten Onlinesortiment. Der Versandhandel gehört zur Otto Group und ist mit 135,9 Millionen Euro Umsatz der drittgrößte Online Shop in Österreich. Der Online Shop hat seit dem Jahr 2000, das österreichische E-Commerce-Gütesiegel. Das Gütesiegel zertifiziert ein sicheres online Einkaufen, kostenlose Streitschlichtung sowie einen überprüften Kundenservice.

Die Produktlinie von Universal.at umfasst ein breites Mode Sortiment, Haushaltsartikel, Einrichtungsgegenstände, Spielwaren und Unterhaltungselektronik.

4.1.1.4 Otto-Versand

Otto-Versand ist ein in Deutschland ansässiger Onlineversandhändler, mit einem breit gefächerten Angebot, dass auf Mode fokussiert ist. Mit einem Umsatz von 92.5 Millionen Euro ist das

Versandunternehmen das viertgrößte in Österreich. Seit dem Jahr 2011 ist der Otto Versand (ottoversand.at) auch mit dem österreichischen E-Commerce-Gütesiegel ausgezeichnet.

Neben einem Produktkatalog, den es seit 1950 gibt, wurde 1995 der Otto-Online Shop eröffnet. Die Produktlinie von Otto-Versand umfasst Damen und Herrenmode, Sportmode, Technik und Unterhaltungsartikel, sowie Küchengeräte und Haushaltsartikel.

4.1.2 Zahlungssysteme

Das Einkaufen im Internet ist ein zunehmender Trend. Da die Kunden beim Einkaufen im Internet nicht mehr vor Ort sind, müssen Sie auf Zahlungssysteme zurückgreifen die auch über das Internet verfügbar sind. Eine Umfrage des Österreichischen Instituts für angewandte Telekommunikation zeigt, dass die Zahlungsmöglichkeiten beim Einkaufen im Internet für die Kunden eine große Rolle spielen. Die Kunden legen großen Wert darauf, dass sichere Zahlungsmittel angeboten werden, und bewerten diese Online Shops dann als vertrauenswürdiger.

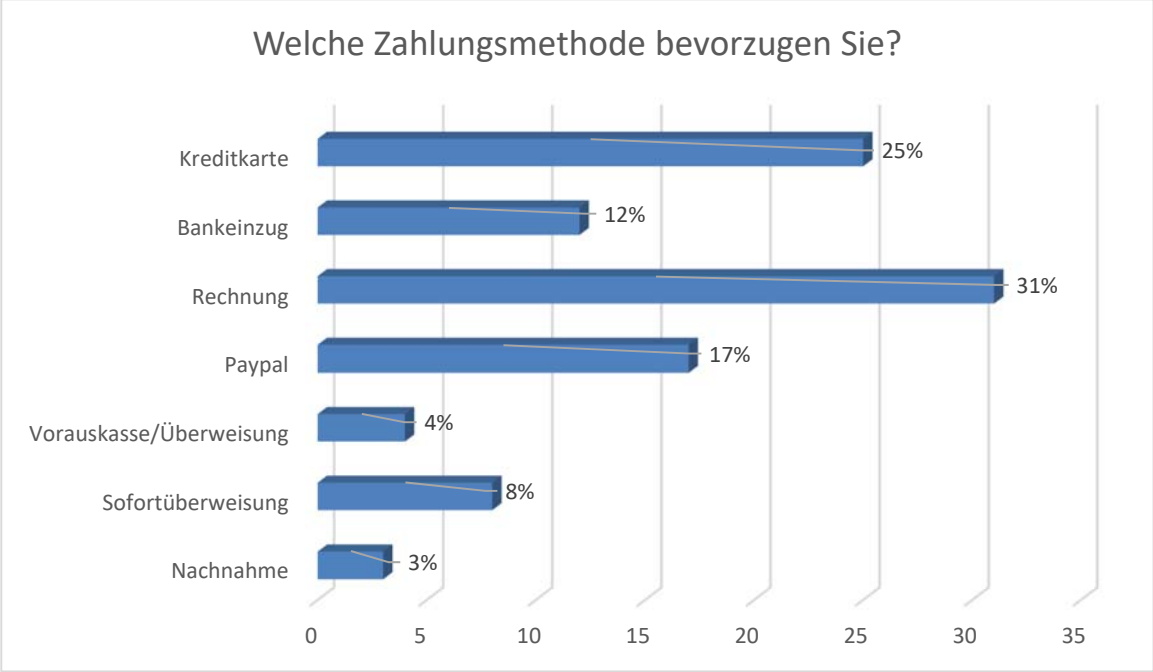

Abbildung 2. Welche Zahlungsmethoden bevorzugen Sie? (Österreichisches E-Commerce-Gütezeichen 2000)

Abbildung 2 listet die bevorzugten Zahlungsmethoden der Österreicher. Dabei zählt die Bezahlung auf Rechnung und Kreditkarten zu den beliebtesten Zahlungsmitteln in Österreich.

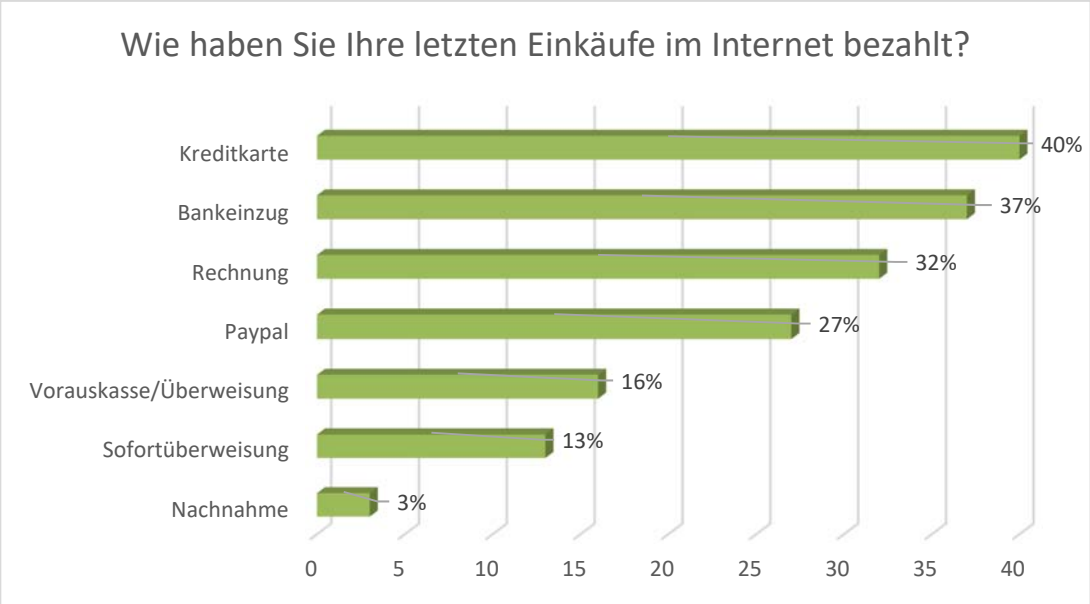

Abbildung 3. Wie haben Sie Ihre letzten Einkäufe im Internet bezahlt? (Österreichisches E-Commerce-Gütezeichen 2000)

Abbildung 3 zeigt auch, dass Kunden in Österreich sehr oft mit Kreditkarte oder mit Bankeinzug in Österreichischen Online Shops einkaufen. Eine weitere Umfrage, hat sich das Zahlungsverhalten von Österreicher nach Betragshöhe angesehen. Abbildung 4 zeigt dabei, dass Kunden ab einer höheren Geldsumme vermehrt zu Bankomat oder Kreditkartenzahlungen greifen.

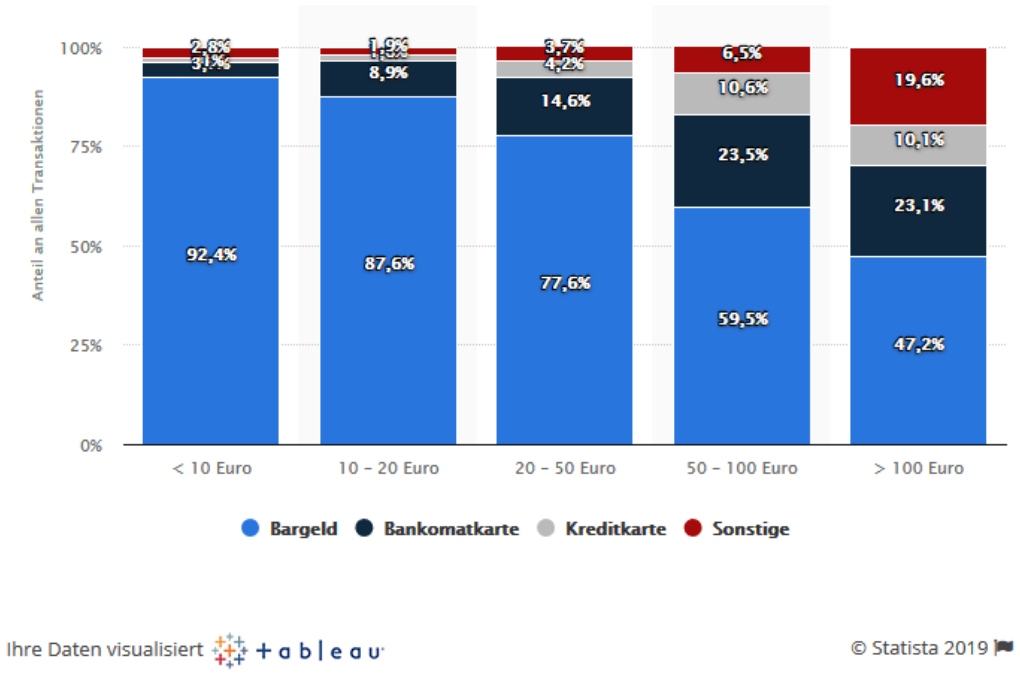

Abbildung 4. Übersicht von Zahlungsmittel in Österreich nach Betragshöhe im Jahr 2016 (Schultz, Anteile von Zahlungsmitteln an allen Transaktionen in Österreich nach Betragshöhe im Jahr 2016 2017)

4.1.2.1 Lastschrift/Bankeinzug

Das Lastschriftverfahren ist ein bargeldloses Zahlungsmittel. Dabei darf ein Zahlungsempfänger eine Forderung (Geld), von einem Zahlungspflichtigen einziehen. Im Gegensatz zu einer Überweisung, wird bei einer Lastschrift der Zahlungsvorgang vom Zahlungsempfänger ausgelöst. Generell wird dabei vom Zahlungsempfänger ein Auftrag an seine Bank gestellt, um die Geldforderung von der Bank des Zahlungspflichtigen einzufordern. Seit 1. November 2010 gilt die SEPA Lastschriftverpflichtung (Europäische Union 2009), welche alle Kreditinstitute in der Europäischen Union (EU) verpflichtet das Lastschriftverfahren umzusetzen. Das Lastschriftverfahren kann generell für öfter auftretende Schuldverhältnisse, wie zum Beispiel Mieten, und andere Abgaben, aber auch bei Online Einkäufen eingesetzt werden. In Österreich ist seit August 2014 das SEPA-Lastschriftverfahren umgesetzt (Österreichische Nationalbank 2019).

4.1.2.2 Überweisung

Die Überweisung ist ein bargeldloses Zahlungsmittel. Dabei löst der zahlungspflichtige Schuldner mit einer Weisung an sein Bankunternehmen, einen Zahlungsauftrag, an dem Zahlungsempfänger, aus. Seit Jänner 2008 können innerhalb von Österreich und ins EU-Ausland (in der Euro-Zone) Überweisungen mittels der SEPA-Überweisung durchgeführt werden. Seit August 2014, ist in Österreich die SEPA-Überweisung umgesetzt (Österreichische Nationalbank 2019).

Für online Einkäufe wird neben einer SEPA-Überweisung oft auch die SOFORT-Überweisung und die eps-Überweisung angeboten. Die SOFORT-Überweisung (Sofort GmbH 2014), ist ein Online Bezahlsystem welches von der Sofort GmbH betrieben wird. Bei dem Zahlungssystem wird die Überweisung von der SOFORT-Überweisung über das Online Banking System des Kunden ausgelöst. Danach informiert es den Händler über die getätigte Überweisung. Die eps-Überweisung (Studiengesellschaft für Zusammenarbeit im Zahlungsverkehr (STUZZA) 2000), ist ein Online Bezahlsystem, das von österreichischen Banken entwickelt wurde. Bei der eps-Überweisung handelt es sich um ein Direkt-Überweisungsverfahren, womit die Zahlungsdaten über eine Schnittstelle an das Online-Banking Systems des Kunden übertragen werden.

4.1.2.3 Kreditkarte

Bei der Bezahlung mit Kreditkarte wird einem Zahlungspflichtigen ein Kredit von den Ausstellern der Kreditkarte gewährt. Die meisten Kreditkarten sind weltweit einsetzbar und werden für tägliche Transaktionen, als auch für das Online Einkaufen immer beliebter. Die vier größten Kreditkartenanbieter in Europa sind Mastercard, Visa, Diners und American Express. Auch in Österreich wird die Kreditkarte ein immer beliebteres Zahlungsmittel. Während 2005 noch 2,17 Millionen Kreditkarten ausgegeben wurden, liegt 2019 die Anzahl der ausgegebenen Kreditkarten bei 3,57 Millionen Stück (siehe Abbildung 5). Das Zahlungsvolumen mit Kreditkarten in Österreich hat sich in den letzten Jahren verdoppelt. Beim Online Einkaufen benutzen 19% der Österreicher am liebsten eine Kreditkarte. 93% der umsatzstärksten Online Shops in Österreich bieten die Möglichkeit zur Bezahlung mittels Kreditkarte an (Schultz 2019).

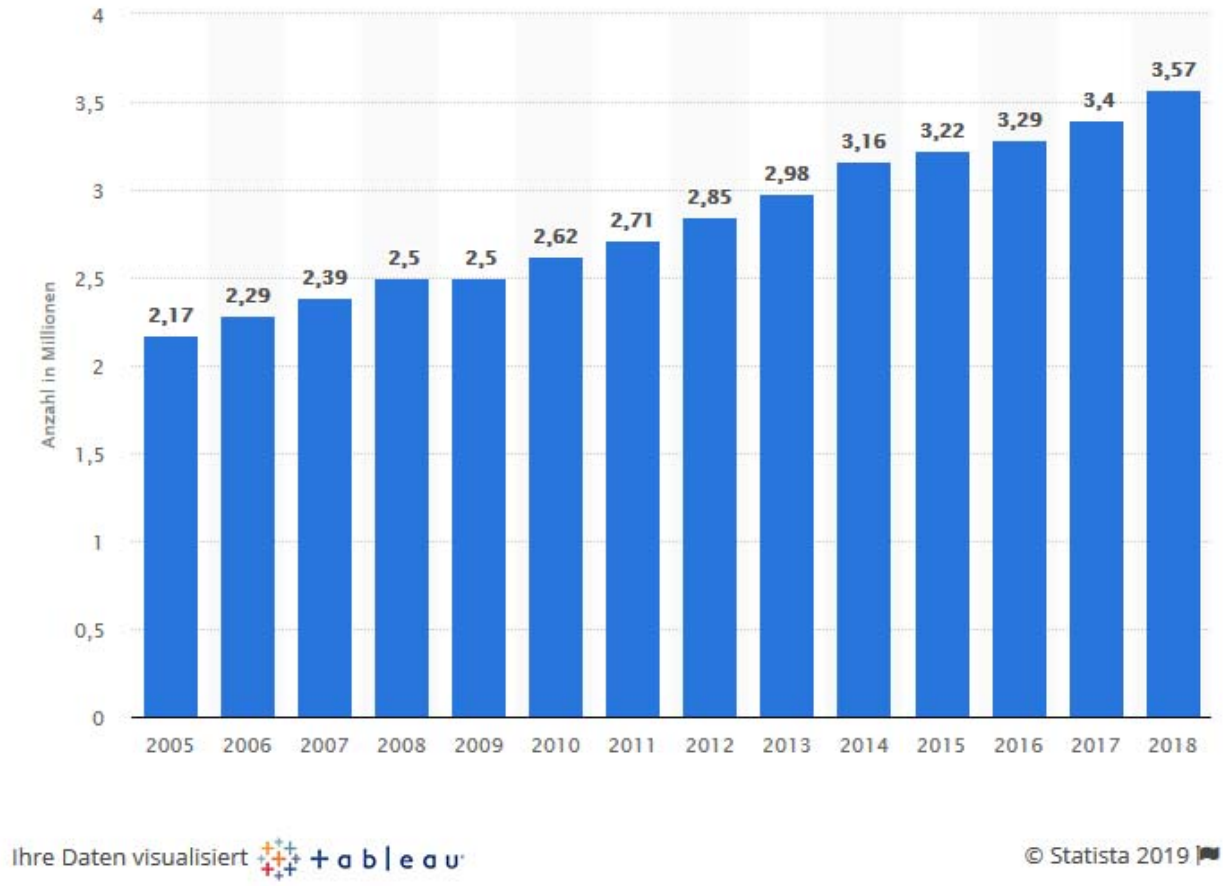

Abbildung 5. Anzahl der ausgegebenen Kreditkarten in Österreich

4.1.2.4 Vorkasse

Die Vorkasse ist eine Zahlungsbedingung, bei welcher der Käufer zuerst eine Zahlung initiiert. Bei erfolgreichem Zahlungseingang versendet, der Verkäufer die Waren dann. Während nach allgemeinem Kaufrecht die Zahlung und die Übergabe der Ware gleichzeitig erfolgen muss, ist dies bei der Vorkasse nicht der Fall. Beim online Einkaufen wird oft Vorkasse mit dem Versprechen angeboten damit den Versandprozess beschleunigen zu können. Als Zahlungsmittel kann eine beliebige Zahlungsart benutzt werden, wobei oft eine Überweisung vom Verkäufer bevorzugt wird.

4.1.2.5 Kauf auf Rechnung

Bei dem Kauf auf Rechnung muss der Käufer eine Zahlung erst initiieren, sobald er die Waren erhalten hat. Oft wird dem Käufer eine fix festgelegte Frist (meistens zwischen 14 und 30 Tagen nach Erhalt der Rechnung) eingeräumt, um die Rechnung zu begleichen. Der Kauf auf Rechnung ist aus Sicht des Kunden eines der sichersten Zahlungsverfahren, da diese die Waren zuerst kontrollieren kann, und erst danach die Rechnung begleichen muss. Für die Zahlung kann oft eine normale Banküberweisung getätigt werden.

In Österreich gibt es beim Onlineeinkauf auch die Möglichkeit mit dem Zahlungsanbieter Klarna (Klarna Bank 2005) zu bezahlen. Klarna ist dabei als Vermittler zwischen Händler und Kunden tätig, und versichert dabei dem Händler das Risiko des Zahlungsausfalles. Damit erreicht Klarna

eine höhere Akzeptanz bei Händlern. Die Kunden müssen im Anschluss die Rechnung bei Klarna begleichen. Dies ist sowohl als Sofortüberweisung als auch als Ratenkauf möglich.

4.1.2.6 Mobile Zahlungsmittel

Mobile Zahlungsmittel sind eine elektronische Zahlungsform unter Verwendung von mobilen Telefonen, Tablets, sowie Smartwatches. Diese mobilen Zahlungsmittel werden oft für Micropayments (für Beträge bis zu fünf Euro) benutzt. In Österreich ist das Paybox Zahlungssystem bekannt. Paybox ist ein SMS-Zahlungsverfahren, welches von der Mobilkom Austria vertrieben wird. Die Bezahlung von Paybox funktioniert über eine Lastschrift auf einem österreichischen Bankkonto.

4.1.2.7 PayPal

PayPal ist ein in den USA ansässiger Onlinebezahldienst, welcher vor allem beim Onlineeinkauf genutzt werden kann. Hierbei bietet PayPal seinen Nutzern ein virtuelles Konto, das von einem regulären Bankkonto aufgeladen werden kann. Die Identität des Kontos wird über eine E-Mail-Adresse definiert. Mit dem virtuellen Konto können dann Zahlungen, wie zum Beispiel für das Onlineeinkaufen, durchgeführt werden. PayPal fungiert beim Onlineeinkauf als Dienstleister für den Zahlungstransfer. Der Vorteil von PayPal im Vergleich zu normalen Überweisungen ist, dass die getätigten Zahlungen oft sofort dem Zahlungsempfänger gutgeschrieben werden, und damit die Lieferzeiten beim Onlineeinkaufen verkürzt werden.

4.1.2.8 Startup-Banken

Startup-Banken, oft auch Challenger Banken genannt, sind Fintech Unternehmen die finanziellen Technologien und Zahlungsmittel anbieten. Diese Banken unterscheiden sich von normalen Banken durch den Einsatz von modernen, innovativen Technologien, welche die komplexen Abläufe und Kosten in traditionellen Banken reduzieren. Die Kontoführung und Zahlungen werden oft per Smartphone durchgeführt. Diese Startup Banken bieten Debit Karten für Onlineeinkäufe an. Diese müssen entweder zuerst von einem traditionellen Bankkonto aufgeladen werden oder müssen ein normales Bankkonto hinterlegt haben.

In Österreich sind N26 (N26 2013) und Revolut (Revolut 2015) bekannt. Beide Banken bieten ein normales Bankkonto an, welches über das Smartphone verwaltet wird. Die Kunden haben eine Debitkarte von Mastercard oder Visa, mit welchen Geldabhebungen, sowie Onlineeinkäufe durchgeführt werden können.

4.1.2.9 Kryptowährungen

Kryptowährungen sind digitale Zahlungsmittel, die auf Basis eines dezentralen Buchungssystems funktionieren. Diese digitalen Zahlungsmittel basieren auf kryptographischen Technologien, unter anderem der Blockchain-Technologie und digitalen Signaturen. Kryptowährungen sind verteilte, unabhängige Zahlungssysteme, welche in einer digitalen Brieftasche, auch Wallet genannt, gespeichert werden. Als Zahlungsmittel für die tägliche Nutzung oder für das Onlineeinkaufen sind Kryptowährungen weniger geeignet, da die Wechselkurse oft sehr stark fluktuieren und häufig Transaktionsgebühren bezahlt werden müssen. Des Weiteren unterliegen Kryptowährungen

keinen staatlichen Regulationen, weshalb der Wert oft nur an Angebot und Nachfrage gebunden ist.

Die wohl bekannteste Kryptowährung ist Bitcoin mit einem aktuellen Wechselkurs von 1BTC = 7779.21€ (Stand 09.10.2019) (CoinMarketCap 2019). Das Ziel von Bitcoin ist es, eine verteilte Version von elektronischem Bargeld zu ermöglichen, und Online Zahlungen von Partei zu Partei zu senden, ohne ein Finanzinstitut bemühen zu müssen (Nakamoto 2008).

4.2 Mobile Online Stores

Mobile Shopping, in eigenen Online Shops, welche für mobile Geräte (Smartphones, Smartwatches, Tablets) optimiert sind, wurden erstmals 2002 probiert. Während bei den ersten Versuchen, oft die Bildschirmgrößen, der damaligen Mobiltelefone, noch zu klein waren, ist das mobile Onlineeinkaufen heutzutage nicht mehr wegzudenken. Der Einkaufsvorgang wird dabei komplett am Mobiltelefon durchgeführt. Dies ist durch den Einsatz von neuen Technologien und speziellen Shopping Apps sowie mobilen Online Shops möglich. Wenn 2013 noch ein Umsatz von 200 Millionen Euro durch Einkaufen via Mobiltelefone erzielt wurde, ist 2019 ein Umsatz von 800 Millionen Euro erreicht worden (Schultz, Ausgaben beim Einkauf via Smartphone in Österreich von 2013 bis 2019 (in Millionen Euro) 2019) (siehe Abbildung 6).

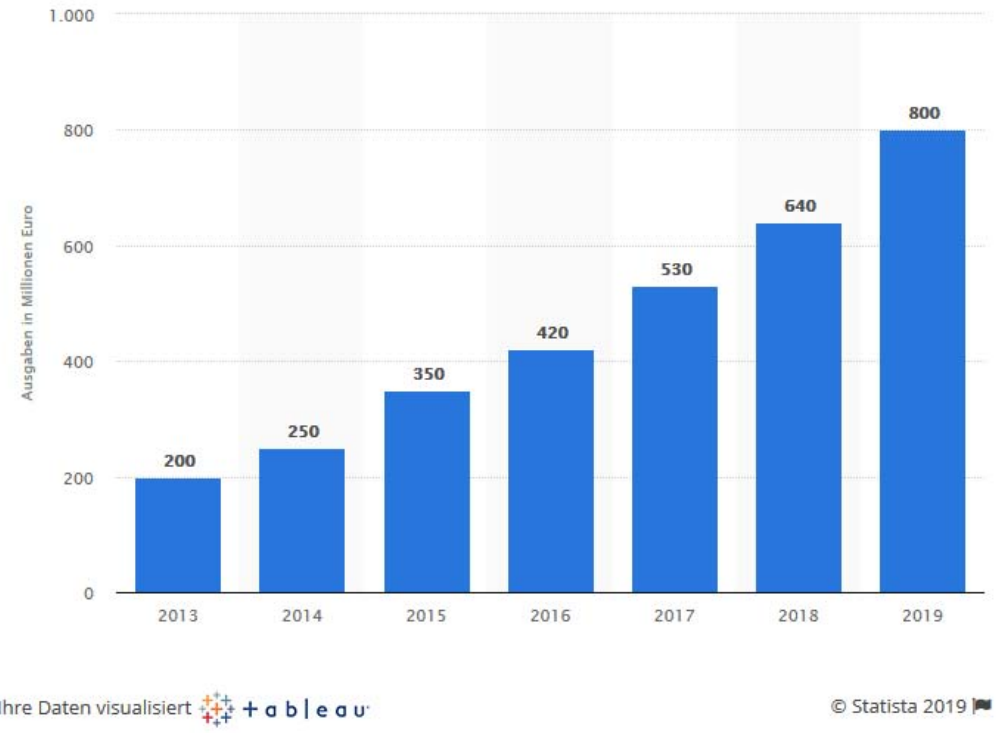

Abbildung 6. Ausgaben beim Einkauf via Smartphone (in Millionen Euro)

4.2.1 Online Shops für Smartphones und Apps

Online Shops am Smartphone werden jedoch nicht nur für den klassischen Onlinehandel benutzt, sondern man kann damit auch Dienstleistungen (zum Beispiel Netflix, Spotify) und neue

Software/Apps kaufen. Zusätzlich hat sich der Trend von kostenpflichtigen Apps, auf kostenlose Apps, mit In-App Käufen verschoben. Bei In-App Käufen, können Zusatzfunktionen und neue Features zu einer kostenlosen Basisapplikation dazukauft werden. Die Apps und Dienstleistungen werden meistens direkt vom Smartphone Anbieter in einem Online Shop bereitgestellt. Diese sind unter anderem der Apple Store für iPhones und der Google Play Store für Android Mobiltelefone. Neue Features in Apps werden oft direkt über den jeweiligen Online Shop als In-App Käufe angeboten.

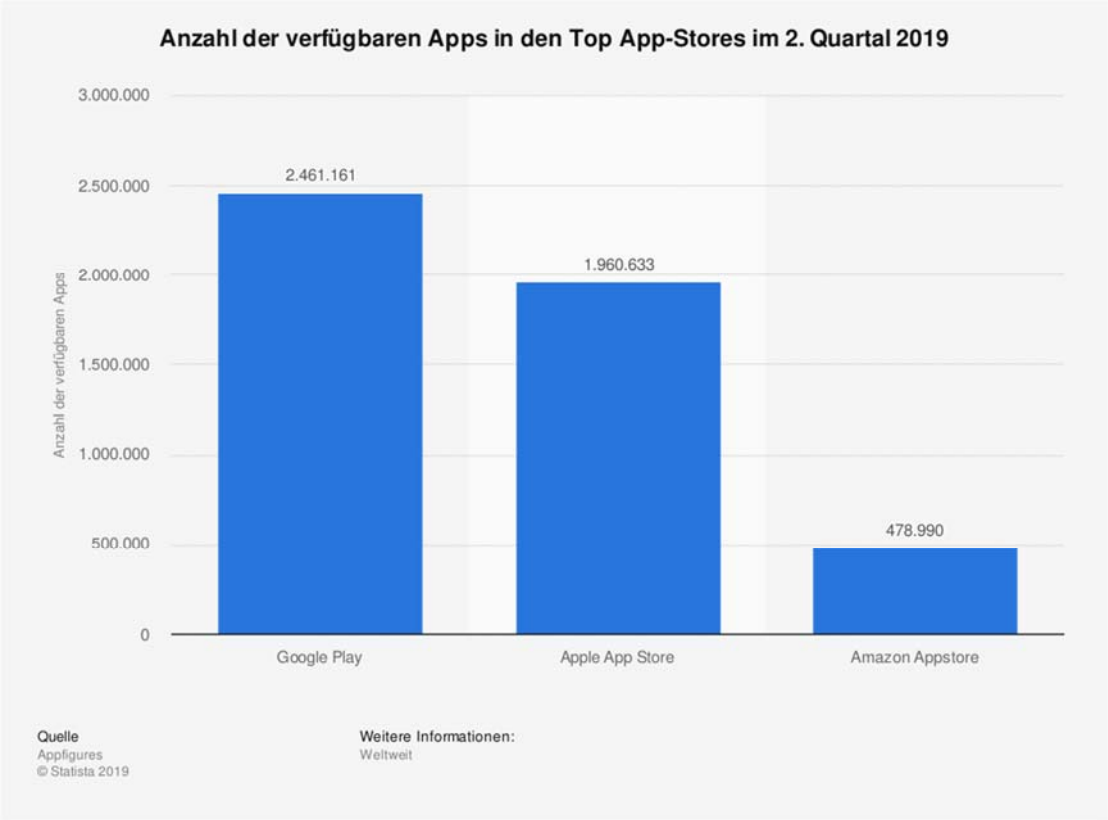

Abbildung 7. Anzahl der verfügbaren Applikationen in den Top App-stores (Rabe 2019)

4.2.1.1 Apple Store

Der Apple App Store ist eine digitale Plattform zum Vertrieb von mobilen Applikationen für iOS, tvOS und watchOS. Der Store wurde 2008 geschaffen und ist seitdem von 500 angebotenen Applikationen auf ca. 1,9 Millionen gewachsen (siehe Abbildung 7). Kunden müssen sich mit ihrer Apple ID einloggen, und können dann kostenlose oder kostenpflichtige Applikationen erwerben.

4.2.1.2 Google Play Store

Der Google Play Store, früher auch Android Market genannt, ist eine digitale Plattform zum Vertrieb vom mobilen Applikationen für Android. Der Store wurde 2008 geschaffen und umfasst mittlerweile ca. 2,4 Millionen mobile Applikationen (siehe Abbildung 7). Kunden müssen sich mit ihrem Google Account einloggen, und können dann kostenlose oder kostenpflichtige Applikationen erwerben.

4.2.2 Mobile Bezahlsysteme

Mobile Bezahlsysteme verwenden mobile Endgeräte zur Initiierung, Autorisierung und Realisierung der Zahlung. Dabei werden oft Mobiltelefone, Tablets, Smart Watches sowie verschiedene Geräte aus dem Internet der Dinge (IoT) verwendet. Die bekanntesten mobilen Zahlungssysteme sind unter anderem Apple Pay und Google Pay.

4.2.2.1 Apple Pay

Apple Pay ist ein mobiles Zahlungssystem, welches auf den mobilen Geräten (iPhone, Apple Watch) von Apple angeboten wird. Es wurde 2014 das erste Mal in den USA in Betrieb genommen, und ist seit 24. April 2019 auch in Österreich verfügbar. Beim Bezahlen mit Apple Pay vergibt Apple für jede gespeicherte Kreditkarte eine Device Account Nummer, welche dem Verkäufer anstatt der Kreditkartennummer weitergegeben wird. Sobald die Zahlung mit dem Mobiltelefon initiiert wird, wird diese Device Account Nummer übertragen und im Banknetzwerk mit der hinterlegten Kreditkarte verglichen. Dadurch sieht der Verkäufer nie die echte Kreditkarte, kann aber trotzdem von einer gültigen Zahlung ausgehen.

4.2.2.2 Google Pay

Google Pay, früher auch Android Pay genannt, ist ein mobiles Zahlungsmittel, welches auf den mobilen Geräten für Android angeboten wird. Außerdem ist es ab iOS Version 9.0 auch auf Apple Geräten verfügbar. Es erschien erstmals 2015 in den USA, und ist mittlerweile in vielen Staaten weltweit zurzeit jedoch noch nicht in Österreich verfügbar. Kunden können jedoch verschiedene europäische Kreditkarten und Startup Banken benutzen, und auf diese Weise Google Pay auch in Österreich nutzen. Die Funktionalität von Google Pay ist jener von Apple Pay sehr ähnlich, und benutzt sogenannte „Tokens“, um die realen Kreditkartendaten nicht mit den Zahlungsterminals oder Applikationen austauschen zu müssen.

4.2.3 Online Shops für das Internet der Dinge

Das Internet der Dinge vernetzt verschiedenste Technologien und Geräte, welche zuvor nicht verbunden waren. Dabei werden eingebettete Systeme, kabellose Sensornetzwerke, Kontrollsysteme, Automationssysteme (Gebäudeautomatisierung) mit neuen Technologien, wie zum Beispiel Echtzeitanalysesystemen und Künstlicher Intelligenz verbunden. Man kann das Internet der Dinge in vier Kategorien aufteilen:

- Industrie 4.0, auch Intelligente Industrie genannt (Englisch: Smart Industry)
- Intelligente Städte (Englisch: Smart City)
- Intelligentes Zuhause (Englisch: Smart Home)
- Intelligente Dinge (Englisch: Smart Devices)

In einer Studie (siehe Abbildung 8) zur Anzahl der IoT Geräte im Haushalt (Janson 2018) im deutschsprachigen Raum, haben ca. 9% der Befragten angegeben, intelligente Glühbirnen, ca. 8% einen virtuellen Assistenten (z.B. Amazon Echo) und ca. 4 % intelligente Haushaltsgeräte (z.B. Kühlschränke, Waschmaschinen) zu benutzen. Während in Österreich zurzeit der Anteil am

intelligenten Zuhause bei ca. 15% liegt, sollte sich der Markt voraussichtlich bis 2023 auf ca. 32% verdoppeln (Kurier.at 2018).

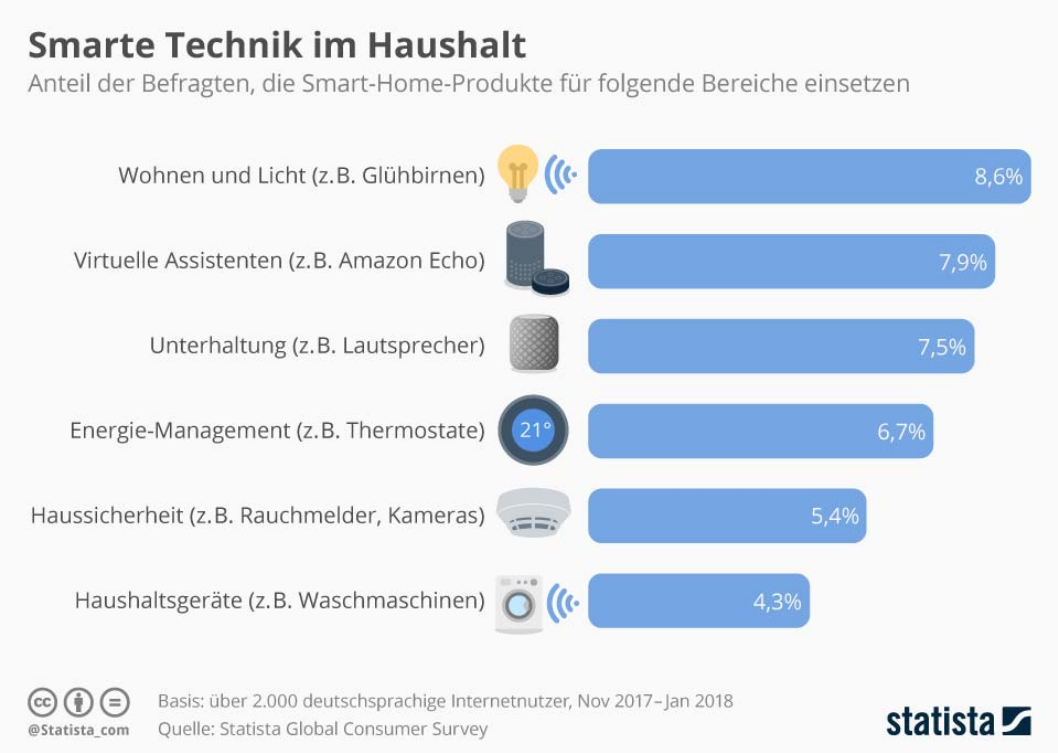

Abbildung 8. Anzahl der IoT Geräte im Haushalt (Janson 2018)

Mit dem schnellen Wachstum von IoT Netzwerken und den neuen technologischen Trends wird auch der E-Commerce Markt stark beeinflusst. Durch die Vernetzung von alltäglich benutzten Geräten und Kommunikationsmitteln, ergeben sich viele Möglichkeiten, um Kunden schneller und einfacher zu erreichen.

E-Commerce im Internet der Dinge kann in drei Kategorien geteilt werden:

- *Vernetzte Geräte für Kunden:* Das inkludiert alles, was sich auf den Kunden fokussiert, beginnend bei intelligenten Uhren, elektronischen Ringen, Bändern und Aufklebern, bis hin zu intelligenten Häusern und Wohnungen sowie vernetzten Autos.
- *Vernetzte Geräte für Verkäufer:* Das inkludiert alles aus der Sicht des Verkäufers, wie zum Beispiel intelligente Getränkeautomaten, Verkaufskioske und intelligente, vernetzte Werbebildschirme.
- *Selbstbezahlende automatisierte Kassensysteme:* Dies inkludiert alle neuen technologischen Geräte, mit welchen ein Kunde direkt Waren bestellen kann, und der Bezahlungsprozess im Hintergrund automatisch abgewickelt wird.

Beispiele für automatisierte Kassensysteme sind unter anderem in Bahn und Busstationen, in denen man direkt mit dem Mobiltelefon durch das Benutzen der NFC Fähigkeit des Smartphones eine Fahrkarte entwertet. Weitere Beispiele sind die Möglichkeit kleine Beträge mit dem Scannen eines Barcodes oder QR Codes zu bezahlen. Des weiteren ermöglicht Amazon (Zimmer 2018) mit

seinem intelligenten Lautsprecher Amazon Echo, dass Kunden direkt per Sprachsteuerung essentielle Produkte aus dem Amazon Shop bestellen können. Zusätzlich entwickelte Amazon 2014 den Amazon Dash Button (Amazon 2014), ein kleines elektronisches Gerät, das zum Beispiel auf die Waschmaschine geklebt werden kann. Sobald das Waschmittel ausgeht, ermöglicht es dem Kunden per Knopfdruck neues Waschmittel zu bestellen. Auch intelligente Fernseher und Kühlschränke werden immer beliebter. Intelligente Fernseher sind mit dem Internet verbunden und ermöglichen damit das Abspielen von Videos von Youtube, Netflix, Amazon Prime Video und vielen anderen Video Streaming Diensten. Dabei können die Kunden entweder ein Abo kaufen, oder Filme direkt in der Onlinemediathek sehen. Intelligente Kühlschränke (Smart-Wohnen.de 2019) sind teilweise mit Kameras und Scannern ausgestattet, und bieten eine Auflistung von den im Kühlschrank befindlichen Produkten und das Erstellen von Einkaufszettel. In naher Zukunft wird es vermutlich auch möglich sein, dass intelligente Kühlschränke den Einkauf für die Kunden erledigen (Redaktion 2017).

4.3 Bonusprogramme/Kundenkarten

Kundenkarten sind eine effiziente Methode zur Bindung von Kunden, sowie um den Kunden zu widerholten Einkäufen zu veranlassen. Aus der Sicht eines Kunden bieten diese Programme oft Ermäßigungen, umsatzbasierte Rabatte und Gutschriften, Spezialgeschenke, Zugang zu limitierten Produkten, spezielle Services, sowie Zugang zu Veranstaltungen, Magazinen und eine regelmäßige Kommunikation mit dem Geschäft/Händler. Aus der Sicht des Händlers dienen Kundenkarten oft nicht nur dazu, Kunden an sich zu binden sondern darüber hinaus, das Kaufverhalten von Kunden zu analysieren und Kundenprofile zu erstellen.

In Österreich besitzen 7% der Kunden zumindest eine Kundenkarte, 46% der Kunden zumindest zwei bis fünf Kundenkarten, 26% der Kunden sechs bis zehn Kundenkarten, 4% der Kunden 11 bis 15 Kundenkarten, und 17% der Kunden benutzen gar keine Kundenkarte (Schultz, Wie viele Kundenkarten besitzen Sie bzw. an wie vielen Cashback-Programmen nehmen Sie teil? 2018) (siehe Abbildung 9).

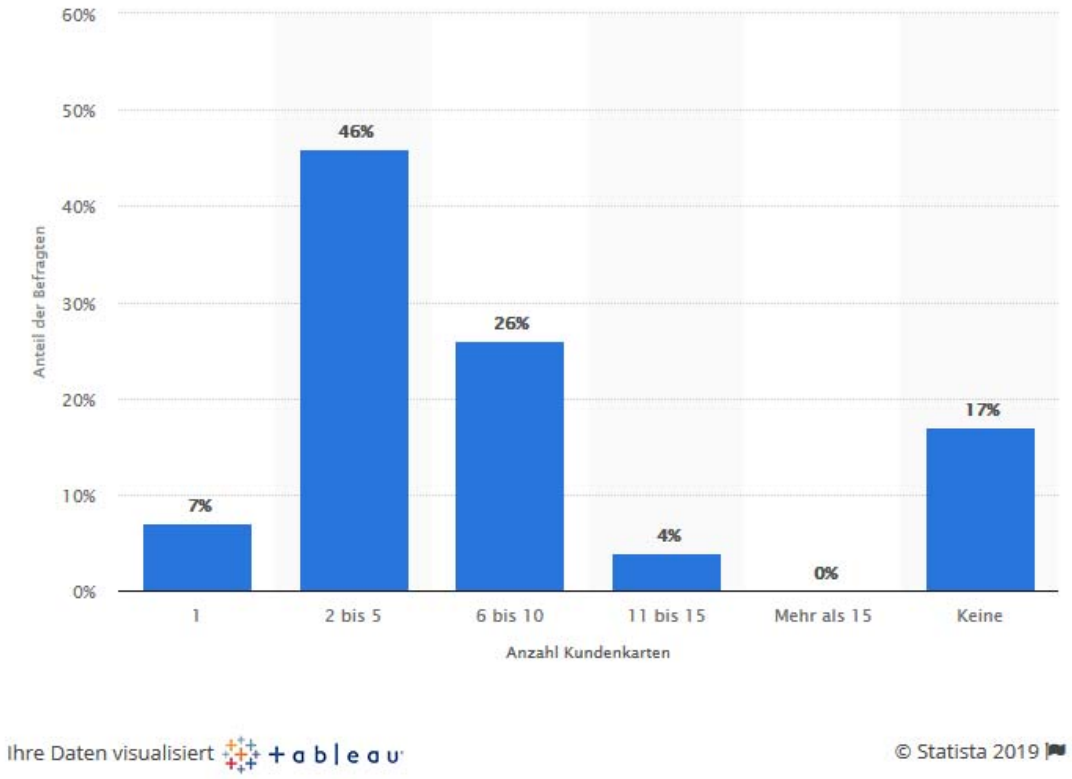

Abbildung 9 Anzahl der Kundenkarten

Es gibt verschiedene Arten von Kundenkarten. Einige bieten spezifische Funktionen an, andere bieten mehrere Funktionen gleichzeitig. Die Kundenkarten können unterteilt werden in:

- Kundenkarten zum Rabatt sammeln (z.B.: Ikea Family Card, Saturn Kundenkarte)
- Kundenkarten mit Zahlungsfunktion (z.B.: spezielle Kreditkarten)
- Bonuskarten in Vielfliegerprogrammen (z.B.: Miles & More)
- Regionalkarten (z.B.: ÖBB Card)
- Gebündelte Bonusprogramme (z.B.: Jö-Bonus-Club, PAYBACK)

Besonders interessant für den Kunden sind oft gebündelte Kundenkarten, wie zum Beispiel die Jö-Bonus-Club Karte und die PAYBACK Karte, welche mehrere größere Konzerne vereint. Dabei ist es dann möglich Bonuspunkte bei mehreren Konzernen übergreifend zu sammeln, und später einzulösen.

4.3.1 Jö-Bonus-Club

Der Jö-Bonus-Club (Jö Bonus Club GmbH 2019) ist ein Bonusprogramm von mehreren Unternehmen in Österreich, welches im Mai 2019 gegründet wurde. Die teilnehmenden Unternehmen sind unter anderem: die Rewe Group Austria (Billa, Bipa, Merkur), ADEG, Penny Markt, Libro, Interio, Bawag PSK, Zgonc und die OMV. Kunden können durch Vorweisen ihrer Jö-Karte Bonuspunkte sammeln und diese dann gegen Rabatte und Sonderaktionen bei jedem der teilnehmenden Partnerunternehmen einlösen.

4.3.2 PAYBACK

PAYBACK (PAYBACK 2000) ist ein Bonusprogramm, das in Deutschland seit 2000 und in Österreich seit 2018, besteht. Seit 2010 gehört PAYBACK zu American Express. In Österreich nehmen einige Unternehmen als Partner an dem Programm teil. Partnerunternehmen sind unter anderem: BP, DM, Fressnapf, Burger King, Nordsee, Sehen Wutscher, Austrian Airlines, Universal Versand, Otto Versand, Shop Apotheke, Expedia, Liferando.at, und OETicket. Die PAYBACK Karte funktioniert ähnlich wie die Jö-Bonus-Club Karte. Bei jeder Bezahlung bei einem PAYBACK Partner Unternehmen wird die PAYBACK Karte gescannt und Punkte zwischen 0.5-4% der Kaufsumme vergeben. Diese Punkte können dann gegen Prämien, Warengutscheine oder weitere Rabatte eingetauscht werden.

5 Mögliche Gefahren bei Online Einkäufen im Internet

In diesem Kapitel wird auf die möglichen Gefahren beim Einkaufen im Internet näher eingegangen. Zuerst wird eine kurze Übersicht gegeben, was mit personenbezogenen Daten passiert, die direkt oder indirekt beim Einkaufen im Internet an einen Händler weitergegeben werden. Danach werden die verschiedenen Möglichkeiten für Cyber-Kriminelle diskutiert, welche auf illegale Weise persönliche Daten von Kunden zu stehlen oder Kunden beim Einkaufen im Internet zu bestehlen. Zuletzt werden datenschutzrechtliche Bedenken adressiert, die zu tragen kommen, wenn Onlineeinkäufe im Internet getätigt werden. Dabei wird auf Fragen eingegangen, wie zum Beispiel: Wo werden Daten hinterlassen? Wer nutzt die Daten? Warum werde ich im Internet verfolgt? Wie werde ich im Internet verfolgt? Was sind die rechtlichen Rahmenbedingungen und wie sieht die Realität aus?

5.1 Was passiert mit meinen Daten im Internet?

Beim Einkaufen im Internet entstehen sehr viele Daten. Dies beginnt mit den Daten die bei einer Bestellung eingegeben werden, zum Beispiel der Name, die Adresse, und die Zahlungsinformation. Dabei handelt es sich um Daten, welche ein Kunde freiwillig und bewusst dem Händler weitergibt. Daneben existiert jedoch noch eine zweite Kategorie an personenbezogenen Daten. Diese entstehen durch die Interaktion und Nutzung des Online Shops und werden vom Händler gesammelt.

Doch was sind personenbezogenen Daten? Nach der EU-Datenschutz-Grundverordnung (Wirtschaftskammer Österreich 2019) sind das alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen. Dabei wird unter identifizierbar verstanden, dass eine Person entweder direkt oder indirekt, mittels Zuordnung einer Identifikation, wie zum Beispiel einem Namen, einer Nummer, Standortdaten oder einer Online-Kennung, zu einem oder mehreren Merkmalen, identifiziert wird. Dies inkludiert Merkmale wie jene der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person. Beispiele dafür sind der Name, die Wohnadresse, das Geburtsdatum, oder die Religionszugehörigkeit.

Online Shops sind aus vielerlei Gründen an den personenbezogenen Daten ihrer Kunden interessiert. In erster Linie sollte natürlich eine Bestellung auch bei den Kunden ankommen, wofür natürlich Informationen gebraucht werden. Oft bleibt es jedoch nicht nur bei diesen Daten. Wenn Internetbenutzer Suchanfragen in Online Shops eingeben, sich für Newsletter registrieren, oder einfach so im Internet herumbrowsen, werten viele Werbeanbieter diese Daten aus. Das Ziel der Anbieter ist oft die Verbesserung ihrer Dienste und Services. Die Datenverarbeitung nutzt damit in erster Linie den Konsumenten, da er damit schneller die gewünschten Dinge findet, und die Nutzung von Diensten gratis erhält. Allerdings ist damit oft nicht Schluss. Viele Anbieter sammeln und verarbeiten die Daten von Kunden nicht nur zum Verbesserern ihrer Dienste, sondern auch für personalisierte Werbung, Erstellung von Personenprofilen, Informationen zum Nutzerverhalten, das Anlegen von Bewegungsprofilen, zur individuellem Preisgestaltung und vieles mehr. So können die Werbeanbieter ihren Kunden garantieren, dass diese personalisierten Werbeanzeigen

bei der richtigen Zielgruppe landen. Viele Konsumenten kennen das vermutlich, wenn man zum Beispiel einen Urlaub bucht, und dann mehrere Wochen später immer noch Werbung zu Hotels und Mietautos am Rand von Webseiten bekommt. Eine Lokalisierung von Konsumenten durch das Anlegen von Bewegungsprofilen, ist insbesondere interessant, um Online-Angebote richtig zu steuern. Dabei können Online Shops dann in Zusammenarbeit mit Werbeanbietern regional oder national begrenzt Produkte gezielt anbieten.

Ein weiterer Faktor ist natürlich auch der Weiterverkauf von gesammelten personenbezogenen Daten an Drittanbieter. Dies ermöglicht Drittanbietern eine genaue Zuweisung von Kunden in Zielgruppen ohne zuvor Daten zu sammeln. Zusätzlich werden Informationen zum Onlineverhalten von Kunden auch von Banken und anderen Kreditunternehmen bei der Überprüfung der Kreditwürdigkeit benutzt. Auch viele Versicherungsunternehmen sind natürlich am Verhalten und dem Onlineeinkaufsprofil ihrer Kunden interessiert. Während für viele Unternehmen Kundendaten aus wirtschaftlicher Sicht interessant sind, zeigen auch Staaten Interesse an persönlichen Daten. Dies zeigt die Diskussion über eine EU-weite Vorratsdatenspeicherung (Al-Youssef 2019) sowie der Abhörskandal um die Geheimdienste der NSA (Niesen 2017).

5.2 Cyber-Kriminalität

Unter Cyber-Kriminalität oder Internetkriminalität versteht man Straftaten, welche im Internet stattfinden oder durch Technologien aus dem Internet ermöglicht werden. Die Arten von Cyber-Kriminalität sind sehr vielfältig und reichen von Identitätsdiebstahl, Urheberrechtsverletzungen, Betrug beim Online Shoppen, bis hin zu Cyber-Terrorismus und dem Verbreiten von Kinderpornographie. Speziell mit dem technischen Fortschritt im Internet, und der zunehmenden Vernetzung von Geräten (durch das Internet der Dinge), hat sich die Kriminalität teilweise auch ins Internet verlagert.

Abbildung 10 zeigt die Ergebnisse einer Umfrage von KPMG (KMPG 2019), bei der 340 österreichische Unternehmen befragt wurden, um die Arten von Cyber-Attacken auf Unternehmen festzustellen. Dabei hat sich ergeben, dass 47% der Unternehmen von Malware Angriffe betroffen waren, weitere 47% von Phishing Attacken, 29% der Unternehmen von Angriffen mit Cryptolocker und Ransomeware, 29% der Unternehmen von direkten Angriffen auf ihre Webseiten oder Webapplikationen, 16% waren von Social Engineering Angriffen betroffen und 14% der Angriffe waren Denial of Service Attacken.

Eine weitere Umfrage (Schultz, Mit welchen Internet-Betrugsarten waren Sie bereits konfrontiert? 2019) unter 1000 Onlineeinkäufern im Internet zeigt auf, dass 15% der Onlineeinkäufer schon gefälschte Zahlungsaufforderungen bekommen hatten, 15% der Onlineeinkäufer hatten Schadsoftware erhalten, weitere 15% waren mit Abofallen konfrontiert, 12% der Onlineeinkäufer hatten es mit vermeintlichen Gratisangeboten zu tun, und 10% der Onlineeinkäufer haben schon einmal etwas bestellt, jedoch trotz Zahlung keine Lieferung erhalten.

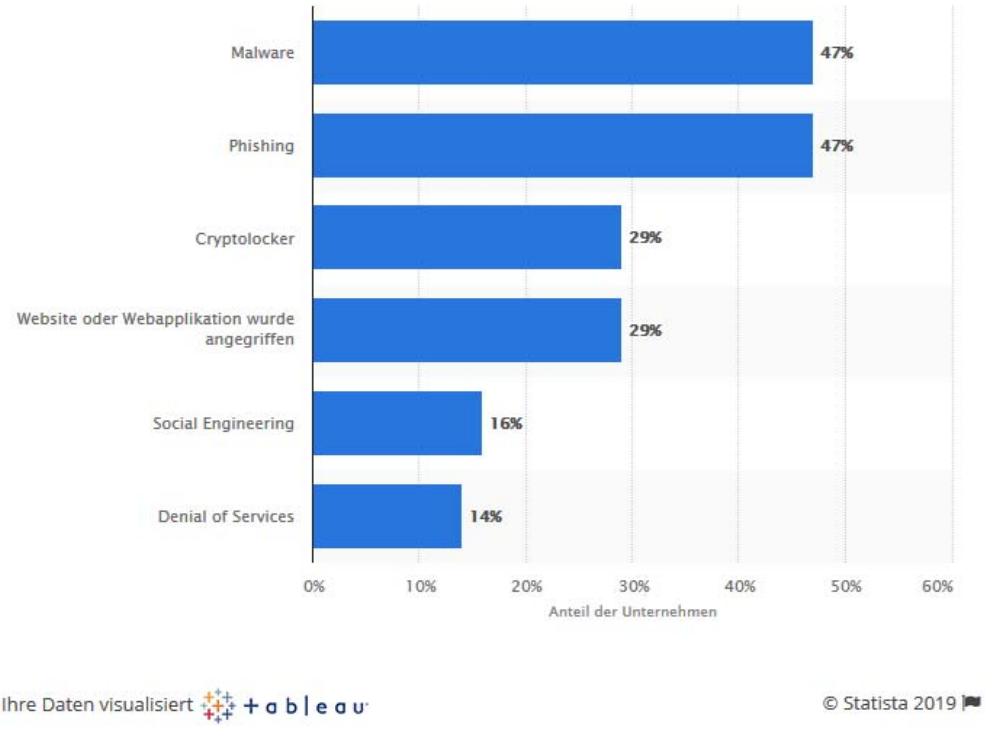

Abbildung 10. Arten von Cyberangriffen auf Unternehmen in 2018 (Schultz, Welche Arten von Cyberangriffen haben Sie 2018 in Ihrem Unternehmen identifiziert? 2019)

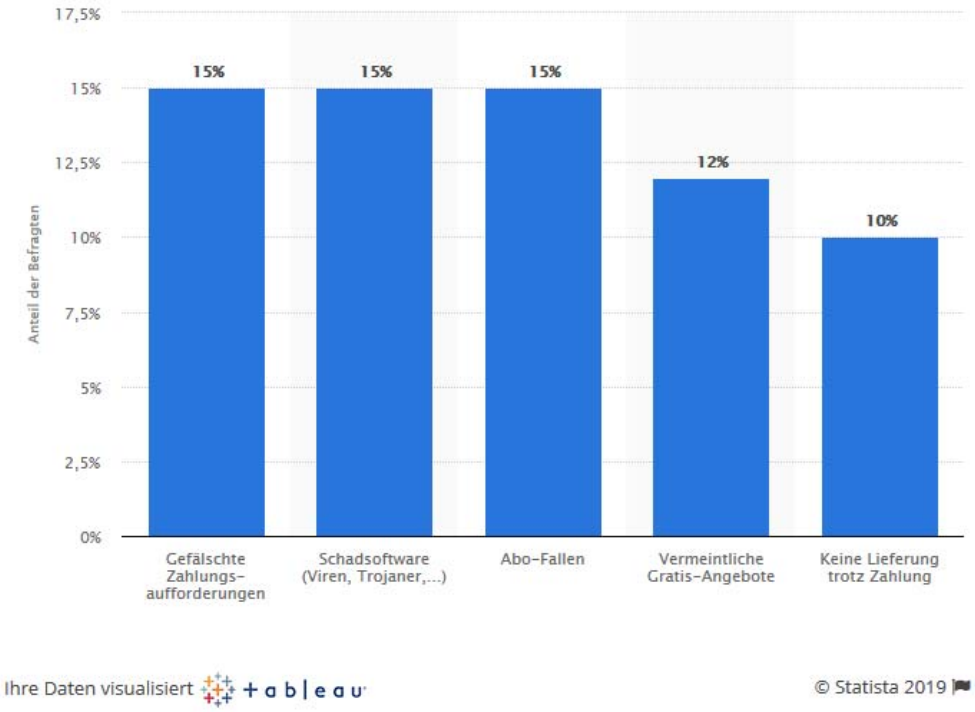

Abbildung 11. Auflistung von den typischen Internet Betrugsarten (Schultz, Mit welchen Internet-Betrugsarten waren Sie bereits konfrontiert? 2019)

In Abbildung 12 und Abbildung 13 sind die angezeigten Fälle von Cybercrime in Österreich von 2004 bis 2018 aufgelistet, sowie die angezeigten Fälle von Internetbetrug in Österreich von 2006 bis 2018. Man kann dabei erkennen, dass Internetbetrug den Großteil der Angriffe im Internet ausmacht. Die Daten stammen aus der Polizeilichen Kriminalstatistik, weshalb die Dunkelziffer deutlich höher sein dürfte. Im Jahr 2018 wurden 19.628 Fälle von Cybercrime bei der Polizei zur Anzeige gebracht, wovon 37% der Fälle aufgeklärt werden konnten (Schultz, Entwicklung der Aufklärungsquote von Cybercrime (gesamt) in Österreich von 2006 bis 2018 2019). Von den insgesamt 19.628 Fällen, handelt es sich bei 13.328 Fällen um Internetbetrug. Der Anstieg von Internetkriminalität von 2017 auf 2018 ist mit 16,8% auch sehr stark steigend.

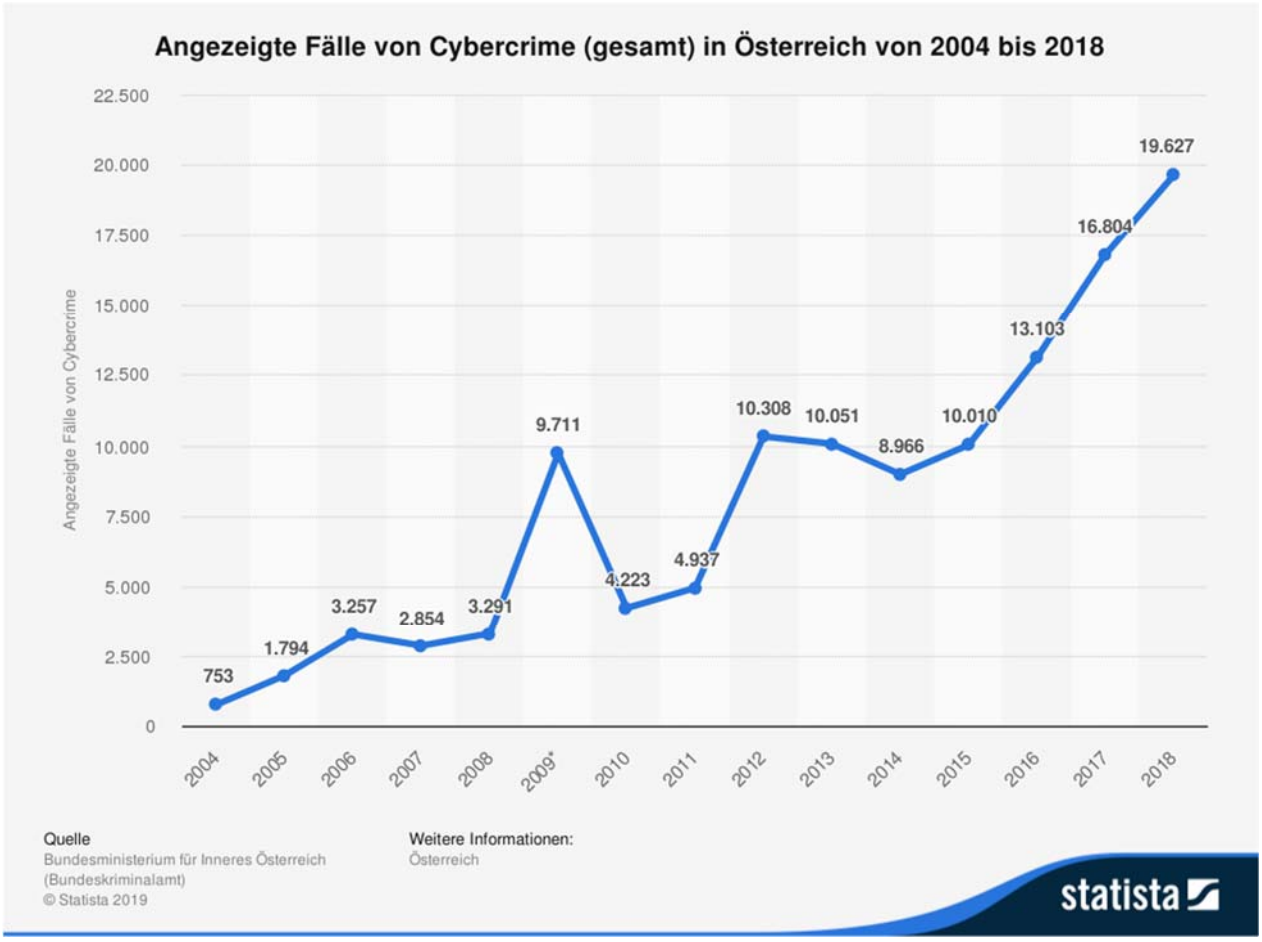

Abbildung 12. Cybercrime in Österreich (Schultz, Angezeigte Fälle von Cybercrime (gesamt) in Österreich von 2004 bis 2018 2019)

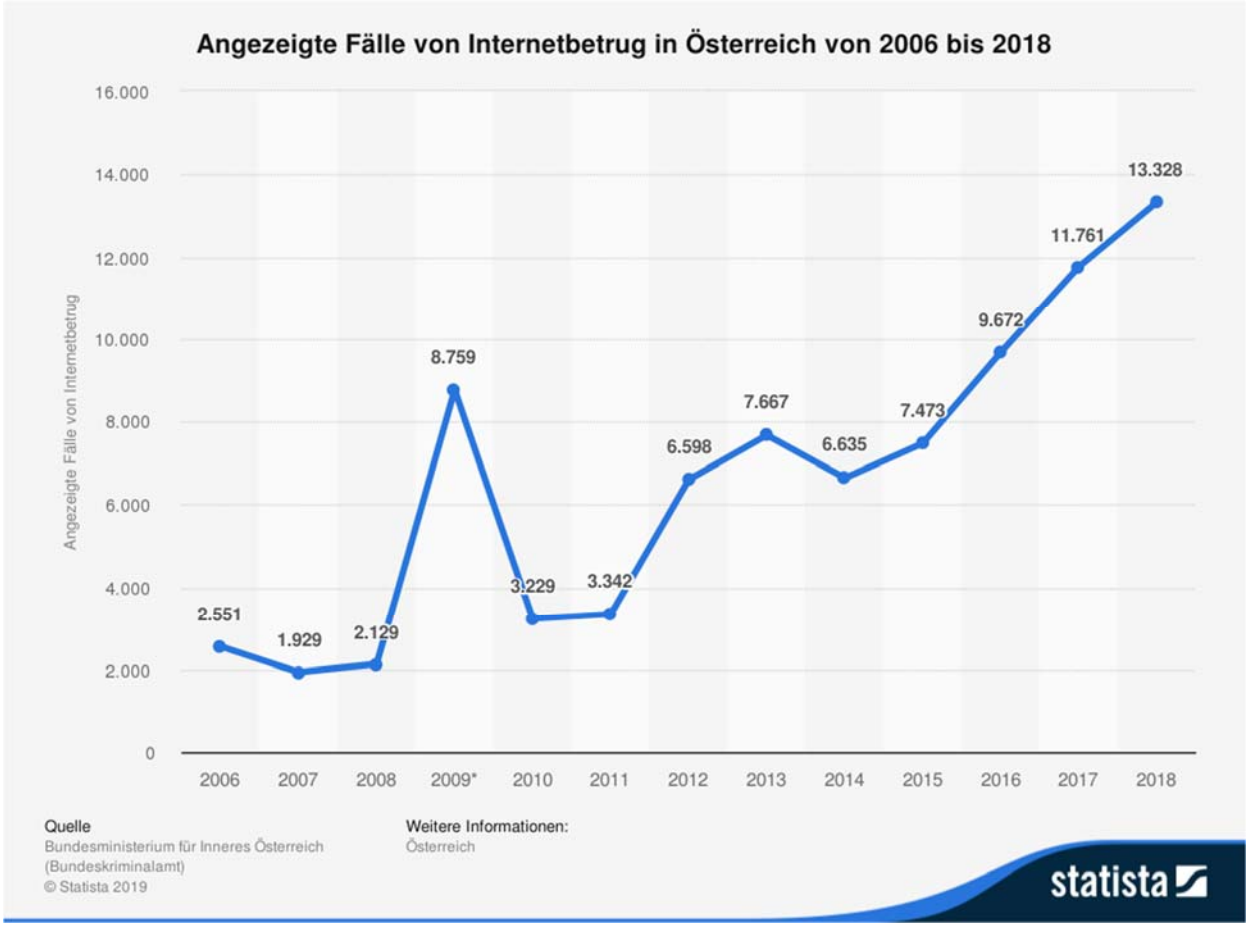

Abbildung 13. Internetbetrug in Österreich (Schultz, Angezeigte Fälle von Internetbetrug in Österreich von 2006 bis 2018 2019)

5.2.1 Identitätsdiebstahl

Beim Identitätsdiebstahl werden personenbezogene Daten einer natürlichen Person missbräuchlich verwendet. Im Vergleich zu einem typischen Diebstahl, wo einer Person etwas weggenommen wird, kann der Geschädigte beim Identitätsdiebstahl seine Identität immer noch weiterverwenden. Beim Identitätsdiebstahl wird, durch das Vortäuschen von falschen Tatsachen, Phishing oder Social Engineering, versucht die persönlichen Daten zu entwenden. Cyberkriminelle nutzen dabei auch öffentlich zugängliche Informationen, welche viele Nutzer durch schlecht konfigurierte Social Media Plattformen öffentlich zugänglich machen.

Erfolgreich gestohlene oder gesammelte Informationen können dann von Cyberkriminellen benutzt werden, um Onlineprofile mit diesen Daten zu erstellen. Dies kann von einfachen Onlineprofilen bis hin zu Bankkonten und Reisepässen führen. Das Ziel von Identitätsdiebstählen ist es oft, einen betrügerischen Vermögensvorteil zu bekommen oder den echten Inhaber der Identität in Misskredit zu bringen. Im ersten Fall, wird oft ein Bankkonto oder ein Zahlungsdienst mit der gefälschten Identität eröffnet und dann Kredite, Dienstleistungen oder Waren bestellt.

Oft werden die gestohlenen Identitäten oder Onlineprofile auch an andere Cyberkriminelle weiterverkauft. Das Dark Web bietet dafür verschiedenste Möglichkeiten und Interessenten. Die Preise von gestohlenen persönlichen Daten und Ausweisdokumenten reichen dabei im

Durchschnitt von einem US Dollar bis zu mehreren hundert US Dollar (siehe Abbildung 14 und (Symantec 2019)).

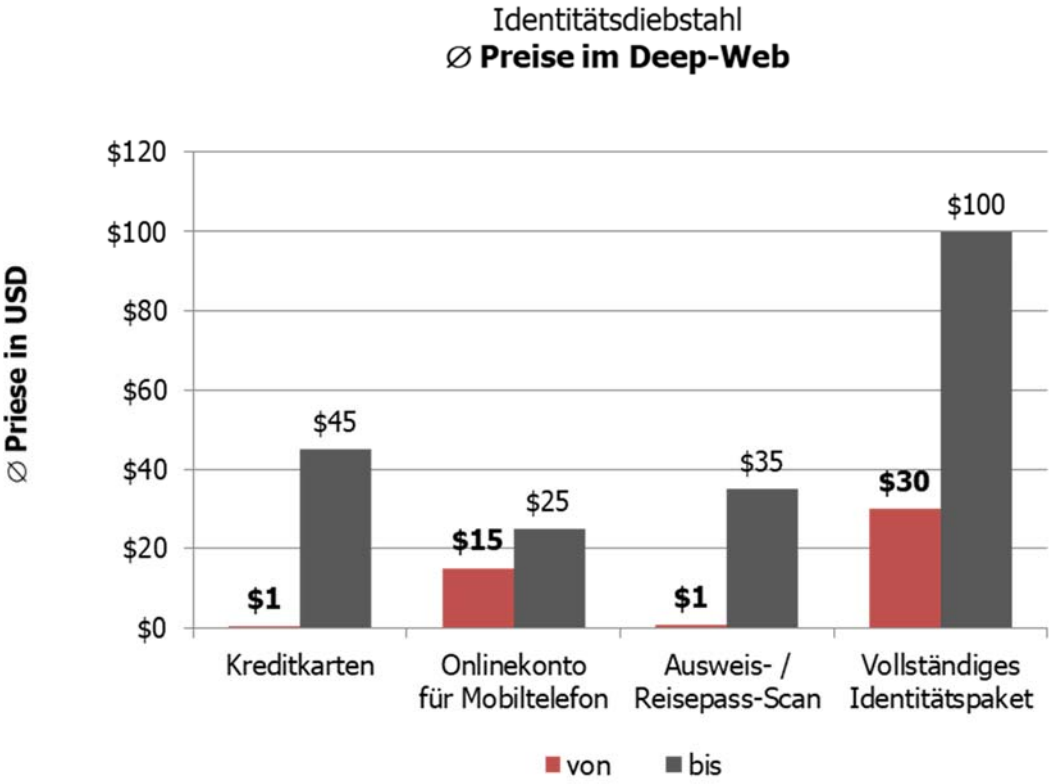

Abbildung 14. Durchschnittspreise für gestohlene Identitätsdaten im Dark Web (Symantec 2019)

5.2.2 Internetbetrug und Erpressung

Internetbetrug kann als Generalisierung von verschiedenen Betrugsarten im Internet gesehen werden. Allgemein unterscheidet man zwischen Phishing, Identitätsdiebstahl, Eingehungsbetrug, Information/Daten Diebstahl sowie Abofallen. Die Gefahren reichen dabei von betrügerischen Angeboten in Online Shops und Verkaufsplattformen, bis hin zu manipulierten Zahlungssystemen und gefälschten Webseiten. Die Gefahr Opfer von Internetbetrug zu werden lauert beinahe überall. Soziale Netzwerke, Emails, sowie unseriöse Online Shops gibt es sehr häufig im Internet. Die Abofalle ist einige der am weitesten verbreiteten unseriösen Geschäftspraktiken von Cyberkriminellen. Dabei werden Internetangebote oft so gestaltet, dass es für den Kunden nicht ersichtlich ist, dass es sich bei dem Kauf um ein Abo Angebot handelt. Oft wird dem Kunden von einem unseriösen Online Shop auch angeboten eine Dienstleistung zu beziehen. Danach wird einige Zeit später eine weitere Rechnung an den Kunden geschickt, mit dem Hinweis, dass es sich bei der Dienstleistung um ein Abo gehandelt hat, und die gesetzliche Widerrufspflicht abgelaufen sei. Dabei wird oft auf die Gutgläubigkeit von Kunden gesetzt, um diese zum Zahlen zu bewegen. Sollte die Zahlung nicht durchgeführt werden, wird oft noch mit Rechtsanwaltsbriefen und Inkassobüros gedroht.

Zum Erkennen von unseriösen Online Shops in Österreich gibt es von watchlist-internet.at eine Liste von betrügerischen Online Shops (Watchlist Internet 2019)[2]. Weitere Hinweise auf einen gefälschten oder unseriösen Online Shop sind auffällige Internetadressen, das Angebot von ausschließlich unsicheren Zahlungsmethoden (Vorkasse/Überweisung), auffallend günstige Preise, Kundenbewertungen, welche in einem kurzen Zeitraum verfasst wurden, oder ein fehlendes Impressum auf der Webseite. In Österreich gibt es seit dem Jahr 2000 auch das Österreichische E-Commerce-Gütezeichen, welches jährlich erneuert wird und als sichtbares Zeichen für seriöse Onlineanbieter steht (Österreichisches E-Commerce-Gütezeichen 2000)[3].

5.2.3 Phishing

Unter Phishing fallen alle Versuche, an die persönlichen Daten von Internetnutzern zu kommen, sei es über gefälschte Webseiten, Email unter dem Vorwand von anderen Personen oder Instituten zu stammen, oder der Nutzung anderer Kommunikationsmittel. Hinter einem Phishing Angriff stehen finanzielle Motive von Cyberkriminellen. Das Ziel von Phishingangriffen ist es, ahnungslose Internetbenutzer dazu zu verleiten auf Links zu klicken oder kompromittierte Dateien zu öffnen, um damit die persönlichen Zugangsdaten zu Bankkonten, oder Online Shopping Plattformen zu bekommen. Typisch ist dabei die Imitierung von vertrauenswürdigen Webseiten. Dabei wird oft das Corporate Design sowie Firmenlogos, Layouts und Schriftarten kopiert, um die gefälschte Webseite/Email authentisch wirken zu lassen. Zusätzlich wird beim Empfänger gezielt der Eindruck erweckt, z.B. unter dem Vorwand einer notwendigen Sicherheitsüberprüfung, dass dieses Phishing Email sehr wichtig sei. Während in der Vergangenheit Phishing Emails oft anhand schlechter Grammatik oder offensichtlichen Fehlern schnell von echten Emails unterschieden werden konnten, werden Phishing Attacken immer professioneller. Als Methoden zur Verschleierung werden oft HTML Emails benutzt, welche mittels Link Spoofing in dem Verweisziel den echten Link anzeigen, jedoch danach auf eine gefälschte Webseite verlinken. Weitere Varianten sind das Ausnutzen der Mehrdeutigkeit von Buchstaben bei verschiedenen Schriftarten (In einigen Schriftarten ist die Zahl „1“ grafisch sehr ähnlich zum Kleinbuchstaben „l“). Ein Beispiel einer Phishing Email ist in Abbildung 15 aufgelistet.

5.2.4 Social Engineering

Unter Social Engineering versteht man, das gezielte Manipulieren von Personen, um bestimmte Verhaltensweisen hervorzurufen oder um Zugriff zu vertraulichen Informationen zu erhalten. Des Weiteren kann Social Engineering benutzt werden, um eine Person zum Kauf eines Produktes zu bewegen. Eine Spezialform des Social Engineerings ist das Social Hacking, bei welcher das persönliche Umfeld einer fremden Person ausspioniert wird, um in ein Computersystem einzudringen. Die Strategie von Cyber-Kriminellen beim Social Engineering ist oft, sich als Autoritätsperson auszugeben. Dabei meldet sich ein Cyber-Krimineller bei seinen Opfern per Telefon und gibt sich als führender Mitarbeiter oder EDV-Techniker aus. Die Opfer werden dann

[2] https://www.watchlist-internet.at/liste-online-shops/ Abgerufen: 25.10.2019

[3] https://www.guetezeichen.at/zertifizierte-websites/guetezeichen/ Abgerufen: 25.10.2019

oft durch firmeninternes Wissen oder durch Fachjargons getäuscht. Zusätzlich werden die Opfer dann auch noch durch zeitliche Fristen und durch andere Stressfaktoren zur Mitarbeit gezwungen.

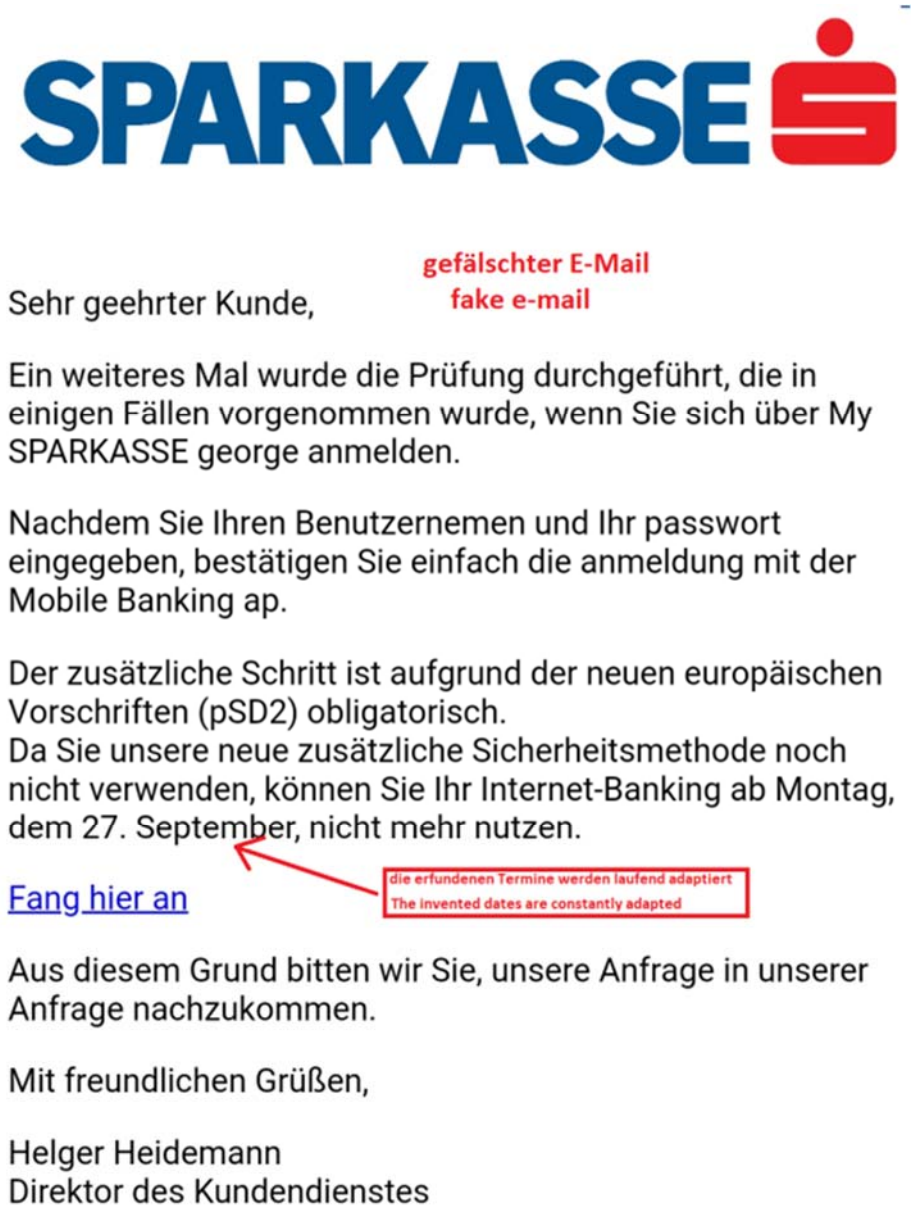

Abbildung 15. Beispiel eines Phishing Emails (Sparkasse.at 2019)

Auch beim Online-Shopping werden oft Social Engineering Techniken von unseriösen Online Shops benutzt, welche oft mit Phishing Attacken kombiniert werden. Dabei wird zum Beispiel eine Webseite präpariert, die nach dem Zahlungsvorgang eine Fehlermeldung anzeigt. Kurze Zeit später meldet sich dann ein „Mitarbeiter“ der Firma und bietet seine Hilfe bei dem Zahlungsvorgang an. Wenn ein Kunde dann seine Zahlungsdaten per Telefon durchgibt, können diese dann für beliebige andere Zwecke missbraucht werden. Zur Verschleierung werden dann oft die echten Waren oder Dienstleistungen bestellt, um den Kunden in Sicherheit zu wiegen. Meistens jedoch auch zu einem höheren Preis als bei der originalen Bestellung durch den Kunden.

5.3 Datenschutz/Privatsphäre

Als Privatsphäre wird im Allgemeinen der nichtöffentliche Bereich bezeichnet, in welchem ein Mensch unbeirrt von äußeren Einflüssen, sein Recht auf freie Entfaltung seiner Persönlichkeit wahrnehmen kann. Ziel des Datenschutzes ist der Schutz der Privatsphäre. Grundsätzlich dient der Datenschutz dem Schutz vor missbräuchlicher Sammlung, Verarbeitung und Auswertung von Daten. Zum Schutz personenbezogener Daten von natürlichen Personen in Österreich gilt seit 25. Mai 2018 die EU-Datenschutz-Grundverordnung (Rechtsinformationssystem des Bundes 2019). Zusätzlich gelten in Österreich noch zwei Anpassungen am EU-Datenschutzgesetz, mit dem Datenschutz-Anpassungsgesetz 2018 (Rechtsinformationsystem des Bundes 2018) und dem Datenschutz-Deregulierungs-Gesetz 2018 (Rechtsinformationssystem des Bundes 2018).

5.3.1 Datenspuren beim Online Shopping - Wo werden Daten hinterlassen?

Online Einkaufen ist ein boomender Markt, der durch die zunehmende Digitalisierung noch stärker wächst (Futurezone.at 2019). Nichtsdestotrotz wird immer noch ein Großteil der Einkäufe offline, also in Geschäften vor Ort getätigt. Um Daten über das Kaufverhalten von Kunden abzugreifen, will der Handel jedoch auch von den offline gekauften Artikeln und Dienstleistungen, online Daten beziehen, um diese zu analysieren und in so genannte User Profile überzuführen. Doch wo werden beim online und offline Einkaufen Daten hinterlassen?

Im Allgemeinen kann davon ausgegangen werden, dass Online Shop Anbieter und Werbungsanbieter auf möglichst allen Geräten versuchen Informationen über Kunden zu protokollieren. Bei Geräten umfasst dies Mobiltelefone, Tablets, Laptops, Smart Watches, Bluetooth Kopfhörer, Autoradios, Navigationssysteme und andere. Zusammengefasst, das Verhalten eines Kunden wird überall protokolliert, wo eine kabellose Verbindung möglich ist, also WLAN oder Bluetooth eingeschalten ist.

Eine wichtige Frage, die sich stellt, ist: Wo hinterlasse ich als Kunde bewusst oder unbewusst Informationen und Daten, die von Werbeanbietern und Online Shops aufgegriffen und verarbeitet werden können? Auf mobilen Geräten wie Smartphones und Laptops greifen Werbeanbieter oft auf den Webbrowser-Verlauf, den Webbrowser-Cache-Speicher, besuchte Webseiten, Formulardaten, Zeiten des Zugriffes, Klickverhalten auf Webseiten, IP Adressen, Cookies, verschiedenste Browsereinstellungen, welche oft beim Browser Fingerprinting benutzt werden, und viele andere Einstellungen und Verläufe zu, auf welche die Anbieter Zugriff haben.

5.3.2 Wer nutzt die Daten? Wer verfolgt mich im Internet?

Nachdem nun klar ist, dass man beim online Einkaufen sehr einfach eine Datenspur im Internet hinterlässt, stellt sich die Fragen: Wer nutzt diese Daten? Wer protokolliert mein Verhalten eigentlich im Internet, und beim online Einkaufen?

Im Allgemeinen kann davon ausgegangen werden, dass beinahe jeder Anbieter von Webseiten oder Betreiber von Online Plattformen daran interessiert ist, Daten zu sammeln und zu analysieren. Dies umfasst Infrastrukturanbieter, Einkaufshäuser, Einzelhandel, Hotellerie, Tourismusgebiete, Werbedienstleister, Verkehrsbetriebe, Städte/Verwaltung, Flughäfen, und viele mehr. Oftmals sind

die Anbieter gar nicht an allen Daten interessiert oder verstehen die entsprechenden Technologien nicht. Darüber hinaus sammeln und analysieren viele Anbieter die Daten gar nicht selbst, sondern beziehen die Daten bzw. Ergebnisse von Drittanbietern. Diese Drittanbieter, die mit Kundendaten handeln, werden oft Informationsvermittler, oder auf Englisch Data Broker genannt. Ein Informationsvermittler bezieht Kundendaten von verschiedenen Quellen, filtert und analysiert diese Daten, um sie später an andere Firmen weiter zu verkaufen. Dabei werden die Daten nicht verkauft, sondern nur Lizenzen für eine zeitlich beschränkte Nutzung weitergeben.

Ein bekanntes Beispiel, bei dem Werbeanbieter mehr Informationen über eine Person sammeln als gewollt, war 2012 das Kaufhaus Target (Hill 2012). Anhand von Kundenprofilen basierend auf dem Suchverhalten der Kunden hat Target seinen Kunden passende Gutscheine zugeschickt. Ein Vater hat daraufhin eine Beschwerde bei dem Kaufhaus eingereicht, nachdem seine Teenagertochter Gutscheine für Baby Utensilien bekommen hatte. Nach einer Entschuldigung des Unternehmens, meldete sich der Vater kurz darauf jedoch ein weiteres Mal. Er hatte von seiner Tochter erfahren, dass sie schwanger sei.

Ein weiteres Beispiel für Firmen, die Daten von Kunden sammeln, um Benutzerverhalten zu analysieren und Kundenprofile zu erstellen, ist Facebook. Facebook (Martin Stepanek 2016) schaltet gezielt Werbung für Kunden, analysiert das Klickverhalten, und welche Werbungen angesehen werden. Zusätzlich kann Facebook auch durch das Abgleichen von Kundendaten herausfinden, wie viel Geld nach einer gezielten Werbeschaltung ausgegeben wurde.

5.3.3 Warum werde ich im Internet verfolgt? Was machen Online Shops mit meinen Daten?

Wir haben nun gesehen, dass Onlineanbieter Daten und Verhalten von Kunden sammeln und analysieren. Doch die Frage, stellt sich nun, warum das Verhalten von Kunden protokolliert wird? Was machen Online Shops mit den gesammelten oder über Drittanbieter erhaltenen Daten?

Während einige großen Internetkonzerne in erste Linie Produkte und/oder Dienstleistungen verkaufen und anbieten, wie zum Beispiel Google, Facebook und Amazon, sind diese Anbieter jedoch oft diejenigen, welche am meisten Gewinn mit dem Sammeln und Analysieren von Daten verdienen. Dies passiert dann oft durch den Verkauf von personalisierter Werbung, wofür Anbieter natürlich einige Informationen über den Kunden haben müssen, um gezielt Werbung schalten zu können. Zusätzlich erhöht sich der Gewinn dieser Internetkonzerne durch die Verbesserung von Services. Oft sind große Internetkonzerne und Online Shops nicht an einer alleinigen Nutzung der Daten interessiert, sondern sind auch bereit, die Daten weiterzuverkaufen oder sie durch zeitlich begrenzte Nutzung zu vermieten. Beim Verkauf von Daten an Drittanbieter, sind viele dieser Anbieter daran interessiert diese Daten zur Vervollständigung ihrer Personenprofile zu verwenden. Auch das Nutzerverhalten und ein mögliches Bewegungsprofil von Kunden ist bei Werbeanbietern sehr gefragt.

Auch in österreichischen Online Shops werden massiv Daten gesammelt (Wimmer 2018). Nicht nur online, sondern auch offline werden in österreichischen Kaufhäusern Daten gesammelt, welche dann auch online weiterverwendet werden können. Seit 2013 gibt es bei Billa in Österreich teilweise elektronische Supermarkt-Preisschilder (Gruber 2013). Während die Anbieter argumentieren, dass damit die Preise an jene von Mitbewerbern angepasst werden, können diese jedoch auch für personalisierte Preise verwendet werden. Des Weiteren benutzt Billa seit 2015 iBeacons

(Futurezone.at 2015). Diese können benutzt werden um per Bluetooth Informationen und Nachrichten zu den Smartphones der Kunden zu schicken. Damit kann dem Kunden gezielt Werbung geschalten werden. Laut Billa wird die Technologie jedoch nur benutzt, um die Billa Kundenkarte bei der Kassa automatisch auf dem Display anzuzeigen.

5.3.4 Wie werde ich im Internet verfolgt? Welche technischen Möglichkeiten werden verwendet?

Zum Analysieren von Kundenverhalten und um Kunden beim Online Einkaufen wieder zu erkennen, gibt es viele verschiedene Technologien und technische Hilfsmittel. Im Allgemeinen möchten Anbieter von Online Shops Kunden, welche schon einmal im Online Shop eingekauft haben, das Eingeben von Rechnungsdaten und der Versandinformationen ersparen. Zusätzlich sollte es natürlich möglich sein, einen Einkauf zu starten, und dann noch ein bisschen über einige Produkte zu recherchieren, um den Einkauf dann dort fortzusetzen, wo man aufgehört hat. Manchmal benutzen Kunden auch mehrere Browser Fenster und sollten dann immer noch einen gemeinsamen Einkaufskorb haben. Der Heilige Gral des Online Shoppens für Anbieter ist es natürlich, wenn ein Kunde einen Einkauf am Laptop beginnt, und diesen dann am Smartphone beenden kann. Dies kann durch die neuesten Technologien wie zum Beispiel Cross-Device-Tracking ermöglicht werden.

5.3.4.1 Cookies

Ein HTTP-Cookie ist eine Datei, welche vom Webbrowser auf dem Computer beim Besuch von Webseiten gespeichert wird, und verschiedenste Informationen enthalten kann. Der Webserver, auf welchen die Webseite liegt, kann dann bei einem weiteren Besuch der Webseite Informationen aus dem Cookie auslesen. Dies ist hilfreich, um eine Session aufrecht zu erhalten. Benutzt wird es zum Beispiel sobald man sich bei einem Online Shop wie Amazon einloggt, und dann später nochmal Amazon besucht. Diese Session Cookies werden für Online Banking, Social Media Plattformen, Webmail Zugängen und vieles mehr benutzt.

Während Cookies im Allgemeinen sinnvoll sind, können sie auch missbräuchlich verwendet werden, um Benutzerverhalten zu protokollieren. Diese so genannten Tracking Cookies, sind meistens Third-Party-Cookies, also Cookies welche von einem Drittanbieter auf einer Webseite angeboten werden. Meistens sind dies Cookies, welche von Werbeanbietern wie Google, Facebook oder anderen zusätzlich auf einer Webseite mitgesendet werden. Damit ist es möglich, dass Anbieter wie Google oder Facebook, das Verhalten von Benutzern auch auf fremden Webseiten mit verfolgen können.

Seit 2018 müssen Webseitenanbieter für alle Cookies, mit der Ausnahme von unbedingt notwendigen Cookies, zuerst um die Zustimmung des Benutzers fragen. Dies ist reguliert in der ePrivacy Regulation von der Europäischen Union (Koch 2019).

5.3.4.2 ETags

HTTP ETags, oder auch entity-tags, sind ein Header Feld im HTTP Standard. Es wird benutzt, um Änderungen an Ressourcen, wie zum Beispiel Bilder oder Formulardaten, zu erkennen und wird zum Speichern der Ressourcen verwendet. Im Prinzip wird erkannt, ob eine Ressource verändert

worden ist und neu geladen werden muss, oder ob es unnötig ist, die Ressource neu zu laden und sie von einem lokalen, schnelleren Cache Speicher geladen werden kann.

Während viele Internetbenutzer mittlerweile Drittanbieter Cookies blockieren und Werbungsblocker installiert haben, haben Werbeanbieter andere Techniken gefunden, um Benutzerverhalten zu protokollieren. ETags können genauso wie Cookies benutzt werden, um Benutzer zu verfolgen. Nachdem ETags genauso wie Cookies im Webbrowser Cache gespeichert werden, können Werbeanbieter ETags einfach wiederholen, um damit festzulegen, dass diese fix vorhanden sind, um Benutzerinformationen damit zu protokollieren.

5.3.4.3 Digitaler Fingerabdruck

Sollten Cookies nicht verfügbar sein, weil der Webbrowser diese nicht speichert oder blockiert, und sollte zusätzlich die IP Adresse des Internetbenutzers nicht ersichtlich sein, oder regelmäßig wechseln, gibt es immer noch Möglichkeiten Kunden direkt zuzuordnen. Diese Möglichkeit bleibt oftmals auch bestehen, wenn der Kunde zwischen verschiedenen Webbrowsern hin- und herwechselt in der Hoffnung sich beim online Einkaufen Preisvorteile zu verschaffen. Der digitale Fingerabdruck eines Computers, oft auch Geräteabdruck oder Browser Fingerabdruck genannt, ist eine Kombination aus Informationen über ein Gerät, um es zu identifizieren. Ein sehr sinnvoller Einsatz dieser Technologien ist beispielsweise bei der Erkennung von Identitätsdiebstahl oder beim Kreditkartenbetrug. Allerdings können diese Technologien auch z.B. von Werbeanbietern missbräuchlich verwendet werden.

Der digitale Fingerabdruck basiert auf verschiedenste Einstellungen eines Webbrowsers, die dieser einem Webserver zur Verfügung stellt, um eine Webseite oder einen Online Shop grafisch korrekt darzustellen. Dies umfasst bei Webbrowsern Informationen zum Datum, Datumsformat, Zeitzone, unterstützte und bevorzugte Sprachen, Software Versionen, Displayauflösung, unterstützte und bevorzugte Schriftarten, unterstützte Audio und Video Formate, Liste der Webbrowser Plug-Ins, und vieles mehr. Oft ist damit eine eindeutige Identifikation der Geräte möglich. Wissenschaftler von der Electronic Frontier Foundation haben in einer Studie (Eckersley 2014) nachgewiesen, dass bei 286.777 Webbrowsern nur ein identer Fingerabdruck der Webbrowser auftritt.

5.3.4.4 Canvas Fingerprinting

Eine weitere Technologie zur eindeutigen Identifikation von Internetnutzern ohne Verwendung von Cookies ist Canvas Fingerprinting. Damit einher geht die Möglichkeit, Benutzerverhalten zu analysieren, um gezielt Werbung zu schalten oder Preise individuell auf Kunden anzupassen.

Canvas Fingerprinting nutzt neueste Technologien vom HTML5 Standard. Dabei wird der Effekt genutzt, dass in einem HTML Canvas Element die Textdarstellung abhängig vom Betriebssystem, der Grafikkarte, den Grafiktreiber, dem Webbrowser und den installierten Schriftarten ist, und zwischen verschiedenen Internetbenutzern variiert. Dabei wird beim Laden der Webseite ein versteckter Text in einem Canvas Element angezeigt. Dann wird dieser Text mit JavaScript ausgelesen und ein kryptographischer Hash Wert über den ausgelesenen Text berechnet, welcher eine eindeutigen Identifikation zurückliefert. In einer Studie (Acar, et al. 2014) von 2014 wurde nachgewiesen das 5,5% der Top 100000 Webseiten diese Technologie benutzen und eine weitere

Studie (Eckersley 2014) hat eine eindeutige Identifikation von Computern mit einer Genauigkeit von 83,6% ergeben.

5.3.4.5 Beacons

Beacons sind kleine elektronische Geräte, welche eine Lokalisierung von Geräten wie zum Beispiel Smartphones ermöglichen. Des Weiteren können Beacons benutzt werden, um Bewegungsprofile, Einkaufsverhalten und gezielte Werbung zu ermöglichen. Beacons funktionieren mit verschiedenen kabellosen Technologien, wie zum Beispiel Ultraschall, WLAN, Bluetooth und über das Web. Während in einer freien Umgebung GPS benutzt werden kann, um Benutzer zu verfolgen, ist dieses in Gebäuden oft nicht möglich. Außerdem ist das WLAN optimierte Tracking oft sehr ungenau. Um dennoch das Kaufverhalten, und den Ort von Benutzern gezielt festzustellen, können Beacons eingesetzt werden. Dafür werden oft Bluetooth, WLAN oder auch Ultraschall Beacons benutzt.

Die Funktionsweise dieser Beacons ist wie folgt: Ein Kaufhaus kann Beacons im Geschäft verteilt platzieren. Sobald ein Kunde mit einem Smartphone daran vorbeigeht, wird das Bluetooth/WLAN/Ultraschallsignal auf der App des Werbeanbieters erkannt und kann dann eine entsprechende Aktion auslösen. Mögliche Aktionen sind eine gezielte Werbeeinspielung für den Kunden oder die Weitergabe der Position des Kunden, um ein Bewegungsprofil zu erstellen.

Eine andere Art von Beacons sind Web Beacons, auch Zählpixel genannt. Diese werden oft beim gezielten online Shopping über Werbeemails benutzt. Dabei wird eine kleine oft nur 1x1 Pixel große Grafik per HTML Email mitgesendet, die vom Webserver des Anbieters geladen wird sobald der Kunde das Email ansieht oder die Webseite öffnet. Der Webserver kann dann die IP Adresse und weitere über Browser Fingerprinting ermittelte Informationen abgreifen, speichern und weiter analysieren.

Beacons werden beinahe von allen größeren Internetkonzernen angeboten, wie zum Beispiel iBeacons von Apple, Eddystone von Google, AltBeacons und GeoBeacons. Anwendungsbeispiele für Beacons sind beispielsweise im Transportwesen die U-Bahnen in London, welche WLAN-Tracking benutzen (O'Malley 2019). Des Weiteren benutzt Billa seit 2015 iBeacons (Futurezone.at 2015). Diese können benutzt werden, um per Bluetooth Informationen und Nachrichten zu den Smartphones der Kunden zu schicken. Dies kann auch genutzt werden, um zielgerichtet Werbung für Kunden zu schalten. Billa benutzt die iBeacons um automatisch die Billa Kundenkarte auf dem Display bei der Kassa anzuzeigen.

5.3.4.6 Cross Device Tracking

Cross Device Tracking bezeichnet die Technologien, welche verwendet werden, um Kunden über mehrere Geräte zu identifizieren. Mit der zunehmenden Vernetzung von Geräten, hat sich auch das Einkaufsverhalten von Kunden geändert. Während die meisten Kunden früher offline in einem Kaufhaus eingekauft haben, können die neuesten Produkte alle nun direkt im Internet erworben werden, oftmals auch von der Couch aus über das Smartphone. Dadurch hat sich auch der Fokus von Werbeanbietern und Online Shop Betreibern geändert, da normale Emails oder Werbesendungen oftmals nicht mehr gelesen werden.

Das Ziel von Cross Device Tracking ist es Kunden, welche sich Produkte im Fernsehen oder beim Online Shoppen am Computer angesehen haben, auch auf ihren Smartphones zu erkennen, um ihnen gezielt personalisierte Werbung zuzusenden. Dabei ist das Ziel von Werbeanbietern, einen Link von einer Person zwischen allen Geräten zu schaffen, die sie benutzen. Dies inkludiert persönliche Computer und Laptops, Smartphones, Smart TVs, Tablets und Smart Watches. Ein Beispielszenario hierbei wäre ein Kunde, welcher am Laptop einen Einkauf beginnt und sich über Winterschuhe informiert. Später wechselt er auf das Smartphone, um weiter nach Winterschuhen zu suchen. Aus Sicht des Werbeanbieters sollten dem Kunden dann optimaler Weise gezielt Angebote für Winterschuhe eingeblendet werden und die Suchanfragen vom Computer sollten mitberücksichtigt werden. Ein weiteres Szenario, wäre ein Kunde, der bei einer Werbetafel vorbeigeht und vor dieser stehen bleibt. Dieser Kunde sollte dann gezielt Werbung mit dem Kontext der Werbetafel auf seine persönlichen Geräte (Smartphone, Smart TV, persönlicher Computer, …) angezeigt bekommen.

Die Technologien, die Cross Device Tracking ermöglichen, sind oft Ultraschall Beacons, also für das menschliche Gehör, unhörbare Töne, welche zum Beispiel von einem Smart TV während einer Werbesendung ausgesendet werden. Diese werden dann vom Mikrophon eines anderen Gerätes, zum Beispiel dem Smartphone des Kunden, aufgefangen. 2017 hat eine Studie (Arp, et al. 2017) aufgezeigt, dass 234 Androidapplikationen Werbeanbieter inkludiert hatten, welche ohne dem Wissen der Kunden Ultraschallsignale aufgezeichnet haben. Diese Signale wurden über Werbesendungen in Fernsehprogrammen ausgesendet, um zu messen, welcher Kunde die Werbesendungen angesehen hat, und wie lange. Cross Device Tracking kann außerdem benutzt werden, um Kundenprofile zu erstellen, Kaufverhalten zu analysieren, anonyme Benutzer zu deanonymiseren und kann auch zur Massenüberwachung eingesetzt werden.

5.3.5 Was sind die rechtlichen Rahmenbedingungen? Wie sieht die Realität aus?

5.3.5.1 Rechtliche Rahmenbedingungen in Österreich

In Österreich gilt seit Mai 2018 die Datenschutz-Grundverordnung und das österreichische Datenschutzgesetz in der Fassung des Datenschutz-Anpassungsgesetz 2018 und des Datenschutz-Deregulierung Gesetzes 2018. Im Speziellen sind damit einige Gesetze in Kraft getreten, welche die Überwachung und das Tracking von Kunden verbieten oder erschweren.

Artikel 6 (European Union 2016) der EU Datenschutz-Grundverordnung (DSGVO) regelt die Rechtmäßigkeit der Verarbeitung von personenbezogenen Daten. Besonders interessant ist hier Punkt f.)

„die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.“ (European Union 2016)

Dieser Punkt regelt damit die Verarbeitung von personenbezogenen Daten, erlaubt jedoch bei berechtigten Interesse die Verarbeitung von Daten, was auch die Verarbeitung durch Dritte erlaubt.

Insbesondere interessant in Bezug auf Tracking von Kunden während eines Onlineeinkaufes, ist hierbei der Erwägungsgrund 47 (European Union 2018) von Artikel 6 der EU Datenschutz Grundverordnung.

„… Die Verarbeitung personenbezogener Daten zum Zwecke der Direktwerbung kann als eine einem berechtigten Interesse dienende Verarbeitung betrachtet werden." (European Union 2018)

Dieser Artikel erlaubt dabei die Verarbeitung von personenbezogenen Daten, um Kunden gezielte Werbung zu schalten, und regelt dies als berechtigtes Interesse für die Verarbeitung von personenbezogenen Daten.

Zum Schutz von personenbezogenen Daten kann in Österreich auch das Telekommunikationsgesetz 2003 (Rechtsinformationssystem des Bundes 2011) herangezogen werden.

§93 (3) *„Das Mithören, Abhören, Aufzeichnen, Abfangen oder sonstige Überwachen von Nachrichten und der damit verbundenen Verkehrs- und Standortdaten sowie die Weitergabe von Informationen darüber durch andere Personen als einen Benutzer ohne Einwilligung aller beteiligten Benutzer ist unzulässig. Dies gilt nicht für die Aufzeichnung und Rückverfolgung von Telefongesprächen im Rahmen der Entgegennahme von Notrufen und die Fälle der Fangschaltung sowie für eine technische Speicherung, die für die Weiterleitung einer Nachricht erforderlich ist."* (Rechtsinformationssystem des Bundes 2011)

Dieses Gesetz regelt im Allgemeinen die Verarbeitung von Standortdaten, und kann damit auch auf gezielte Werbemaßnahmen, welche oft standortbezogen einem Kunden angezeigt werden, angewendet werden.

5.3.5.2 Die Realität von Datenschutz beim Online Einkaufen

Die Realität von Datenschutz beim online Einkaufen weicht jedoch oft von den Europäischen Datenschutzgesetzen ab. Oft werden rechtliche Graubereiche ausgenutzt, um Kundendaten zu sammeln und auszuwerten. Dabei wird der Kunde sehr oft zur Zustimmung der Nutzung seiner Daten, und zur Weitergabe der Daten an Dritte aufgefordert. Viele Kunden geben hierbei ihre Zustimmung. Des Weiteren wird dem Kunden auch die Möglichkeit offeriert, dass dieser seine Zustimmung jederzeit wiederrufen kann. Das Problem dabei ist jedoch, dass viele Menschen gar nicht wissen, wer Sie – und in welchem Ausmaß – trackt. Dabei ist Kunden oftmals einerseits unklar in welchem Ausmaß personenbezogenen oder ortsbezogene Daten über sie gesammelt und verarbeitet werden, aber auch welche ihrer Daten an Drittanbieter weiterverkauft und verarbeitet werden. Oft werden Kunden dabei auch unter Druck gesetzt, wie zum Beispiel, dass ein Service oder eine Bestellung nur möglich ist, wenn eine Zustimmung zur Verarbeitung der Daten gegeben wird.

Im Grundsatz muss man sich immer die Frage stellen, womit große Internetkonzerne Geld verdienen. Außerdem sollte man sich vor Augen führen, dass nichts im Internet gratis ist. Sollte ein Service gratis angeboten werden, bezahlt der Kunde sehr oft mit der Weitergabe seine personenbezogenen Daten. Ein Beispiel dafür ist Facebook, welches vor Kurzem eine Strafe von 5 Milliarden US Dollar gezahlt hat, im Zusammenhang mit dem Cambridge Analytica Datenschutzskandal (Cooper 2019), jedoch einen Gewinn von 22 Milliarden US Dollar 2018 (Rabe, Umsatz und Nettoergebnis von Facebook weltweit in den Jahren 2007 bis 2018 (in Millionen US-

Dollar) 2019) gemacht hatte. Facebook macht rund 98,5 Prozent seiner Umsätze (55 Milliarden US Dollar im Jahr 2018) mit Werbung. Ein weiteres negatives Beispiel ist Google, welches über Google Maps den Standort seiner Benutzer auch dann trackt, wenn Tracking im Webbrowser vom Benutzer explizit deaktiviert ist (Melchior 2018). Auch Google hat 2019 eine Strafe von 1.7 Milliarden US-Dollar in der EU gezahlt, weil es seine marktbeherrschende Stellung im Online-Werbemarkt missbraucht. Google hat einen Umsatz von 136 Milliarden US-Dollar 2018 gemacht, und einen Gewinn von 30 Milliarden US-Dollar (Sokolov 2019).

6 Ratschläge zum Sicheren Einkaufen im Internet

In diesem Kapitel geben wir Tipps und Ratschläge für sicheres Einkaufen im Internet. Da immer mehr Menschen in Online Shops über das Internet einkaufen, steigt auch das Risiko, dass es zu Pannen kommt. Dies können verspätete Lieferungen sein oder Händler, welche den Umtausch oder die Rückerstattung von Produkten nicht erlauben. Allerdings steigt auch die Zahl unseriöser Online Shops und Cyber-Kriminelle, welche aus wirtschaftlichem Interesse versuchen Kunden zu schädigen.

Damit Sie keine schlimme Überraschung beim Einkaufen im Internet erleben, und damit erst gar keine Probleme entstehen, sollten Sie folgende Ratschläge für das sichere Einkaufen im Internet beachten.

- **Zu billige Preise:** Bei zu billigen Preisen ist Vorsicht geboten. Im Allgemeinen gilt, dass niemand etwas zu verschenken hat. Oft lohnt sich ein Vergleich von Preisen auf Vergleichsplattformen. Sollten die Preise bei einem Online Shop sehr viel günstiger sein als überall anders, ist oft etwas falsch dabei. Oft handelt es sich in diesem Fall um Fälschungen oder es kommen hohe Versandkosten auf den Kunden dazu.
- **Transparente Preise:** Um eine versteckte Kostenfalle zu vermeiden, ist es beim Einkaufen im Internet sehr wichtig, dass Preise transparent aufgeschlüsselt werden. Daher sollten Sie beim Einkauf darauf achten, dass neben dem Produktpreis auch die Kosten für Verpackung und Transport angegeben sind. Während im Onlinehandel sehr oft die Preise transparent angegeben sind, ist leider bei Flugbuchungen genau das Gegenteil der Fall. Daher lohnt es sich oftmals Vergleichsplattformen zu benutzen, welche das Gepäck und die Zahlungsart mitberücksichtigen.
- **Zahlungsmethoden:** Alle größeren Online Shops bieten verschiedenste Zahlungsmethoden an. Dabei sollten Sie darauf achten, eine sichere Zahlungsmethode zu benutzen. Gerade bei der ersten Bestellung und bei unseriöse aussehenden Online Shops sollten Sie besonders vorsichtig sein. Vermeiden Sie daher Zahlungen auf Vorkasse oder Banküberweisungen bevor die Waren geliefert werden.
- **Vergleichs/Bewertung Plattformen:** Im Allgemeinen ist es hilfreich vor einem Kauf im Internet die Preise zu vergleichen. Verschiedene Vergleichsplattformen bieten dafür ihre Dienste im Internet an. Doch passen Sie auch hier auf, da oft die Angebote von manchen Herstellern trotzdem bevorzugt gereiht sind oder nicht alle Anbieter verglichen werden. Zusätzlich ist es sehr hilfreich, wenn andere Kunden schon bei einem Online Shop gekauft haben und eine Bewertung des Produktes und Kaufprozesses abgegeben haben. Auch hier sollte man auf die Anzahl der Bewertungen, das Datum der Bewertungen achten und berücksichtigen, ob es sich nur um eine Bewertung handelt oder ob auch ein Kommentar dabeisteht. Oft werden diese Bewertungen auch vom Händler selbst erstellt oder über eine Klickfarm im Internet gekauft.

- **Liefer/Versand Service:** Beim Online Einkaufen ist natürlich auch der Versand der im Internet bestellten Waren sehr wichtig. Seriöse Anbieter geben Informationen zu dem Versanddienstleister bekannt und bieten oft mehrere Möglichkeiten an. Während ein Standardversand oft erst ab einer gewissen Einkaufssumme gratis ist, kann oft ein Premiumversand ausgewählt werden, der schneller liefert. Da viele Versanddienstleister während der Arbeitszeit Pakete zustellen, ist es oft auch interessant, direkt zu einer Abholstation in der Nähe des Wohnortes liefern zu lassen.
- **Allgemeine Geschäftsbedingungen (AGB):** Die Allgemeinen Geschäftsbedingungen werden von vielen Kunden oft ignoriert, jedoch ist es hilfreich, kurz einen Blick darauf zu werfen. Die AGBs sollten transparent und leicht verständlich geschrieben sein, und alles Wichtige zum Einkauf abdecken. Man kann unseriöse Onlinehändler oft daran erkennen, dass keine AGBs vorhanden sind.
- **Authentizität:** Seriöse Online Shops haben detaillierte Informationen über sich selbst im Impressum stehen. Dies umfasst den Firmennamen, die Anschrift, eine Telefonnummer und Email Adresse, sowie eine zugehörige Kontaktperson oder Kontaktstelle. Zusätzlich haben viele Online Shops ein Zertifikat oder in Österreich auch das E-Commerce-Gütezeichen, dass die Qualität und die Kundenfreundlichkeit des Online Shops bestätigt.
- **Lieferzeiten:** Die Lieferzeiten der online gekauften Waren sollten schon vor dem Abschluss des Einkaufes ersichtlich sein. Neben einem Standardversand wird dabei von vielen Anbietern ein kostenpflichtiger Premiumversand angeboten, welche oft eine Zustellung am nächsten Tag ermöglicht.
- **Leistungsumfang:** Die Artikelbeschreibungen in Online Shops sollten natürlich der Wahrheit entsprechen. Die Garantiebedingungen sollten klar ersichtlich sein. Oft findet man mehr Informationen zur Garantie in den Allgemeinen Geschäftsbedingungen. Es lohnt sich auch einen Artikel auf Vergleichsplattformen zu vergleichen, oder einfach bei einer Internetsuchmaschine danach zu suchen. Oft findet man dann mehr Informationen zu einem Artikel.
- **Rücktrittsrechte:** Kunden in Österreich können von einem online abgeschlossenen Vertrag, wie zum Beispiel beim Einkaufen im Internet, innerhalb von 14 Tagen ohne Angabe eines Grundes, zurücktreten. Dies ist in Österreich im Fern- und Auswärtsgeschäfte-Gesetz geregelt.
- **Passwörter:** Benutzen Sie schwer zu erratende Passwörter, und verschiedene Passwörter für verschiedene Dienste im Internet. Sollte ein Passwort von Ihnen gestohlen werden, dann sind nicht alle anderen Dienste kompromittiert. Passwörter, die den Namen des Haustieres und seinen Geburtstag enthalten oder 123456 sind nicht sicher! Wenn möglich nutzen Sie Passwort-Safes. Speichern Sie keine Passwörter auf Geräten, welche andere Personen nutzen können.
- **Multifaktor Authentifizierung:** Mit der europäischen Zahlungsrichtlinie PSD2 (Payment Service Direktive) sind Banken verpflichtet eine 2-Faktor Authentifizierung bei Bankgeschäften online zu verlangen. Dabei muss sich ein Kunde für ein Bankgeschäft mit zumindest 2 Faktoren authentifizieren, wobei einer zum Beispiel das Wissen eines Passwortes ist, und der zweite Faktor der Besitz eines Smartphones, wo ein TAN Code

hingeschickt wird. Dies erschwert das Hacken von Bankkonten und sollte, wenn möglich auch beim Einkaufen im Internet eingesetzt werden.

- **Öffentliche WLANs:** Während öffentliche WLANs eine Reduktion der mobilen Datennutzung ermöglichen, bergen sie auch erhebliche Sicherheitsrisiken. Sie können davon ausgehen, dass der Besitzer des öffentlichen WLANs ihre kompletten Daten, welche zwischen Ihrem Computer und der Webseite übertragen werden, im Klartext mitlesen kann. Geben Sie daher in Ihnen unbekannten WLAN Netzen niemals ihre Bankdaten oder andere persönliche Daten oder Anmeldeinformationen an. Sollten Sie dennoch wichtige Informationen übertragen müssen, können Sie mit einem VPN (Virtuelles Privates Netzwerk) eine geschützte Verbindung herstellen.
- **Werbeblocker:** Ein Werbeblocker blockiert das Laden von Werbeanzeigen auf Webseiten in Ihrem Webbrowser. Damit werden viele Werbeanzeigen entfernt, zusätzlich können die Webseiten schneller geladen werden. Auch ihre Privatsphäre und ihre Sicherheit beim Online Einkauf wird erhöht, da die Werbeanbieter oft nicht mehr in der Lage sind ihr Kauf- und Suchverhalten zu verfolgen. Des Weiteren wird das Risiko von Malware durch Werbung weiter eingeschränkt.
- **Datenschutzeinstellungen:** In unser zunehmenden gläsernen Gesellschaft, in welcher Begriffe wie Big Data und konstante Überwachung keine Seltenheit mehr sind, werden auch beim Einkaufen im Internet massiv Daten gesammelt. Während Webbrowser und online Einkaufsportale verschiedenste Einstellungen und individuelle Profile anbieten, haben viele Kunden die standardmäßigen Einstellungen nie verändert. Für mehr Datensicherheit im Internet ist es sehr wichtig diese Einstellungen anzupassen, da viele Kunden oft mehr Informationen preisgeben als ihnen bewusst ist. Im Allgemeinen gilt: geben Sie nur die nötigsten Informationen im Internet an, um die Funktion des jeweiligen Dienstes zu ermöglichen.
- **Kundenkarten und Bonusprogramme:** Während viele Geschäfte mit Rabatten und Bonuspunkten Kunden an sich binden wollen, ist die wirkliche Ersparnis oft sehr gering. Die meisten Rabatte sind umsatzgebunden, und viele Kunden machen oft keine Preisvergleiche. Zusätzlich verliert man durch den Einsatz von Kundenkarten oder der Teilnahme an Bonusprogrammen seine Anonymität beim Einkaufen. Viele Unternehmen nutzen die Informationen vom Kaufverhalten, um Ihnen Werbung zuzuschicken und personalisierte Angebote zu machen.
- **Gewinnspiele:** Nehmen Sie nicht an jedem Gewinnspiel im Internet teil. Oft besteht deren Zweck darin, gezielt Kunden zu fangen und persönliche Daten zu erhalten. Je mehr Daten Sie eingeben müssen, desto unseriöser ist das Gewinnspiel. Lassen Sie die Finger von Gewinnspielen mit dem Motto: „Sie sind der 100.000 Besucher der Webseite und haben ein iPhone gewonnen!“. Im besten Fall, bekommen Sie danach mehr Spam Emails, im Schlimmsten Fall sind Sie in eine Abo-Falle geraten.
- **Anonymität:** Wenn möglich versuchen Sie im Internet anonym zu bleiben. Oft müssen beim Einkaufen im Internet nicht alle Felder in einem Formular ausgefüllt werden. Füllen Sie nur die wirklich verpflichtenden Felder aus, und lassen Sie irrelevante Informationen leer. Ein Onlinehändler muss zum Beispiel nicht unbedingt ihr Geburtsdatum kennen. Geben Sie keine Zahlungsinformationen und Details zu Ihrer Person an Fremde weiter.

Nutzen Sie verschiedenen E-Mail-Adressen, und benutzen Sie ein Pseudonym das nicht Ihren Namen enthält.

- **Bankkonten und Kreditkarten regelmäßig überprüfen:** Überprüfen Sie regelmäßig ihre Bankkonten und Kreditkarten, mit welchen Sie im Internet einkaufen. Sollten Sie irgendwelche Unregelmäßigkeiten oder unberechtigte Abbuchungen entdecken, melden Sie diese Ihrem Bankunternehmen und verlangen Sie eine Rückerstattung. Einige Kreditkartenanbieter und viele Startup Banken ermöglichen auch, dass Ihre Karte für Online Transaktionen gesperrt wird, sollten Sie die Karte online nicht benutzen. Des Weiteren gibt es von einigen Anbietern die Möglichkeit, virtuelle Kreditkarten für das online shoppen zu verwenden, welche sich nach jeder Transaktion ändern.

7 Referenzen

Acar, Gunes, Christian Eubank, Steven Englehardt, Marc Juarez, Arvind Narayanan, und Claudia diaz. „The Web Never Forgets: Persistent Tracking Mechanisms in the Wild.“ 3. 11 2014. https://securehomes.esat.kuleuven.be/~gacar/sticky/the_web_never_forgets.pdf (Zugriff am 30. 10 2019).

Al-Youssef, Muzayen. *Die Vorratsdatenspeicherung soll EU-weit zurückkehren.* 07. 06 2019. https://www.derstandard.at/story/2000104478424/die-vorratsdatenspeicherung-soll-zurueckkehren (Zugriff am 06. 11 2019).

Amazon. *Meine Dash Buttons.* 2014. https://www.amazon.de/b?ie=UTF8&node=15144565031 (Zugriff am 17. 10 2019).

Arp, Daniel, Erwin Quiring, Christian Wressnegger, und Konrad Rieck. „Privacy Threats through Ultrasonic Side Channels on Mobile Devices.“ In *IEEE European Symposium on Security and Privacy (EuroS&P)*. Paris, Frankreich: IEEE, 2017.

CoinMarketCap. *Top 100 Kryptowährungen nach Börsenwert .* 2019. https://coinmarketcap.com/de/ (Zugriff am 09. 10 2019).

Cooper, Daniel. *Facebook will pay $5 billion fine for Cambridge Analytica data breaches.* 24. 07 2019. https://www.engadget.com/2019/07/24/facebook-will-pay-5-billion-fine-for-cambridge-analytica-data-b/?guccounter=1&guce_referrer=aHR0cHM6Ly93d3cuZ29vZ2xlLmNvbS91cmw_c2E9dCZyY3Q9aiZxPSZlc3JjPXMmc291cmNlPXdlYiZjZD0xOCZjYWQ9cmphJnVhY3Q9OCZ2ZWQ9MmFoVUtFd2pGX1p (Zugriff am 05. 11 2019).

Eckersley, Peter. „How Unique Is Your Web Browser?“ 2014. https://panopticlick.eff.org/static/browser-uniqueness.pdf (Zugriff am 30. 10 2019).

Europäische Union. „VERORDNUNG (EG) Nr. 924/2009 DES EUROPÄISCHEN PARLAMENTS UND DES RATES vom 16. September 2009 über grenzüberschreitende Zahlungen in der Gemeinschaft und zur Aufhebung der Verordnung (EG) Nr. 2560/2001.“ 16. 09 2009. https://eur-lex.europa.eu/legal-content/DE/TXT/PDF/?uri=CELEX:32009R0924&from=DE (Zugriff am 02. 10 2019).

European Union. *Art. 6 – EU-DSGVO – Rechtmäßigkeit der Verarbeitung.* 27. 04 2016. https://www.datenschutz-grundverordnung.eu/grundverordnung/art-6-ds-gvo/ (Zugriff am 31. 10 2019).

—. *Erwägungsgrund 47 EU DS-GVO.* 2018. http://www.privacy-regulation.eu/de/erwaegungsgrund-47-DS-GVO.htm (Zugriff am 31. 10 2019).

Futurezone.at. *Billa testet iBeacons in elf Filialen.* 17. 08 2015. https://futurezone.at/digital-life/billa-testet-ibeacons-in-elf-filialen/147.504.497 (Zugriff am 29. 10 2019).

—. *Studie: Österreicher shoppen am liebsten online.* 29. 10 2019. https://futurezone.at/digital-life/studie-oesterreicher-shoppen-am-liebsten-online/400660364 (Zugriff am 29. 10 2019).

Gruber, Gregor. *E-Ink-Technik erobert Supermarkt-Preisschilder.* 26. 06 2013. https://futurezone.at/b2b/e-ink-technik-erobert-supermarkt-preisschilder/24.598.234 (Zugriff am 29. 10 2019).

Hill, Kashmir. *How Target Figured Out A Teen Girl Was Pregnant Before Her Father Did.* 16. 02 2012. https://www.forbes.com/sites/kashmirhill/2012/02/16/how-target-figured-out-a-teen-girl-was-pregnant-before-her-father-did/#39e89f0a6668 (Zugriff am 29. 10 2019).

Janson, Matthias. *Smarte Technik im Haushalt .* 27. 02 2018. https://de.statista.com/infografik/13058/smarte-technik-im-haushalt/ (Zugriff am 16. 10 2019).

Jö Bonus Club GmbH. *Jö Bonus Club.* 2019. https://www.joe-club.at/ (Zugriff am 2019. 10 11).

Klarna Bank. *Klarna AB.* 2005. https://www.klarna.com/at/ (Zugriff am 10. 10 2019).

KMPG. *Cyber Security Studie 2019 - Strategien österreichischer Unternehmen im Kampf gegen Cyberkriminalität.* 2019. https://home.kpmg/at/de/home/insights/2019/05/studie-cyber-security-in-oesterreich-2019.html (Zugriff am 25. 10 2019).

Koch, Richie. *Cookies, the GDPR, and the ePrivacy Directive.* 2019. https://gdpr.eu/cookies/ (Zugriff am 30. 10 2019).

Kurier.at. *Darüber spricht das Netz: Internet of Things.* 03. 12 2018. https://kurier.at/wirtschaft/darueber-spricht-das-netz-internet-of-things/400342453 (Zugriff am 16. 10 2019).

Martin Stepanek, Patrick Dax. *Facebook weiß, wo du einkaufst - User meist ahnungslos.* 16. 06 2016. https://futurezone.at/digital-life/facebook-weiss-wo-du-einkaufst-user-meist-ahnungslos/204.886.642 (Zugriff am 29. 10 2019).

Melchior, Laura. *Google trackt User - auch wenn sie den Standort deaktivieren.* 14. 08 2018. https://www.internetworld.at/online-marketing/google/google-trackt-user-standort-deaktivieren-1634572.html (Zugriff am 05. 11 2019).

Montasell, Gerhard. *Umsatzstärkste Online-Shops in Österreich 2018 (in Millionen Euro).* 13. 09 2019. https://de.statista.com/statistik/daten/studie/860119/umfrage/top-online-shops-oesterreich-ecommercedb/ (Zugriff am 06. 11 2019).

N26. *N26 #DieMobileBank.* 2013. https://n26.com/de-at (Zugriff am 10. 10 2019).

Nakamoto, Satoshi. „Bitcoin: A Peer-to-Peer Electronic Cash System.“ 31. 10 2008. https://bitcoin.org/bitcoin.pdf (Zugriff am 2019. 10 09).

Niesen, Claudia. *Alles Wichtige zur NSA-Affäre.* 16. 02 2017. https://www.spiegel.de/politik/deutschland/nsa-affaere-worum-geht-es-a-1134779.html (Zugriff am 06. 11 2019).

O'Malley, James. *TfL is going to track all London Underground users using Wi-Fi.* 22. 05 2019. https://www.wired.co.uk/article/london-underground-wifi-tracking (Zugriff am 30. 10 2019).

Österreichische Nationalbank. *SEPA-Lastschriftverfahren.* 2019. https://www.oenb.at/Zahlungsverkehr/SEPA/SEPA-Zahlungsinstrumente/SEPA-Lastschriftverfahren.html (Zugriff am 04. 10 2019).

—. *SEPA-Überweisung.* 2019. https://www.oenb.at/Zahlungsverkehr/SEPA/SEPA-Zahlungsinstrumente/SEPA-Ueberweisung.html (Zugriff am 04. 10 2019).

Österreichisches E-Commerce-Gütezeichen . *Österreichisches E-Commerce-gütezeichen Zertifizierte Websites.* 2000. https://www.guetezeichen.at/zertifizierte-websites/guetezeichen/ (Zugriff am 25. 10 2019).

PAYBACK. *PAYBACK.* 2000. https://www.payback.at/ (Zugriff am 11. 10 2019).

Rabe, L. *Anzahl der verfügbaren Apps in den Top App-Stores im 2. Quartal 2019.* 07. 08 2019. https://de.statista.com/statistik/daten/studie/208599/umfrage/anzahl-der-apps-in-den-top-app-stores/ (Zugriff am 14. 10 2019).

—. *Umsatz und Nettoergebnis von Facebook weltweit in den Jahren 2007 bis 2018 (in Millionen US-Dollar).* 09. 08 2019. https://de.statista.com/statistik/daten/studie/217061/umfrage/umsatz-gewinn-von-facebook-weltweit/ (Zugriff am 05. 11 2019).

Rechtsinformationssystem des Bundes. *Datenschutz-Deregulierungs-Gesetz 2018.* 2018. https://www.ris.bka.gv.at/Dokumente/BgblAuth/BGBLA_2018_I_24/BGBLA_2018_I_24.html (Zugriff am 28. 10 2019).

—. *Datenschutzgesetz – DSG.* 2019. https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=bundesnormen&Gesetzesnummer=10001597 (Zugriff am 28. 10 2019).

—. *Telekommunikationsgesetz 2003 - TKG 2003.* 11. 05 2011. https://www.ris.bka.gv.at/GeltendeFassung.wxe?Abfrage=Bundesnormen&Gesetzesnummer=20002849&FassungVom=2011-05-18 (Zugriff am 05. 11 2019).

Rechtsinformationsystem des Bundes. *Datenschutz-Anpassungsgesetz 2018.* 2018. https://www.ris.bka.gv.at/Dokumente/RegV/REGV_COO_2026_100_2_1367515/REGV_COO_2026_100_2_1367515.html (Zugriff am 28. 10 2019).

Redaktion, A1. *Erledigt der Kühlschrank bald den Einkauf?* 07. 08 2017. https://www.a1.net/connectlife/pd/erledigt-der-kuehlschrank-bald-den-einkauf/ (Zugriff am 17. 10 2019).

Revolut. *Revolut.* 2015. https://www.revolut.com/de-AT/ (Zugriff am 10. 10 2019).

Schultz, Eva. *Anteil der Online-Käufer an der österreichischen Bevölkerung von 2010 bis 2019.* 28. 10 2019. https://de.statista.com/statistik/daten/studie/298302/umfrage/nutzung-von-online-shopping-in-oesterreich/ (Zugriff am 08. 11 2019).

—. *Angezeigte Fälle von Cybercrime (gesamt) in Österreich von 2004 bis 2018.* 09. 08 2019. https://de.statista.com/statistik/daten/studie/294141/umfrage/cybercrime-in-oesterreich/ (Zugriff am 18. 10 2019).

—. *Angezeigte Fälle von Internetbetrug in Österreich von 2006 bis 2018.* 03. 05 2019. https://de.statista.com/statistik/daten/studie/527857/umfrage/angezeigte-faelle-von-internetbetrug-in-oesterreich/ (Zugriff am 18. 10 2019).

—. *Anteile von Zahlungsmitteln an allen Transaktionen in Österreich nach Betragshöhe im Jahr 2016.* 04. 04 2017.

https://de.statista.com/statistik/daten/studie/695248/umfrage/zahlungsmittelanteile-in-oesterreich-nach-betragshoehe/ (Zugriff am 06. 11 2019).

—. *Anzahl der ausgegebenen Kreditkarten in Österreich in den Jahren 2005 bis 2018 (in Mio.).* 22. 08 2019. https://de.statista.com/statistik/daten/studie/739896/umfrage/anzahl-der-ausgegebenen-kreditkarten-in-oesterreich/ (Zugriff am 2019. 10 09).

—. *Ausgaben beim Einkauf via Smartphone in Österreich von 2013 bis 2019 (in Millionen Euro).* 17. 07 2019. https://de.statista.com/statistik/daten/studie/568222/umfrage/mobile-commerce-ausgaben-in-oesterreich/ (Zugriff am 11. 10 2019).

—. *E-Commerce-Umsatz in Österreich von 2006 bis 2017 sowie eine Prognose bis 2018 (in Mrd. Euro).* 22. 10 2019. https://de.statista.com/statistik/daten/studie/317206/umfrage/brutto-jahresumsatz-im-internet-einzelhandel-in-oesterreich/ (Zugriff am 08. 11 2019).

—. *Entwicklung der Aufklärungsquote von Cybercrime (gesamt) in Österreich von 2006 bis 2018.* 09. 05 2019. https://de.statista.com/statistik/daten/studie/680995/umfrage/aufklaerungsquote-von-cybercrime-in-oesterreich/ (Zugriff am 25. 10 2019).

—. *Mit welchen Internet-Betrugsarten waren Sie bereits konfrontiert?* 14. 08 2019. https://de.statista.com/statistik/daten/studie/777022/umfrage/erfahrungen-von-online-kaeufern-mit-internet-betrug-in-oesterreich/ (Zugriff am 18. 10 2019).

—. *Welche Arten von Cyberangriffen haben Sie 2018 in Ihrem Unternehmen identifiziert?* 23. 07 2019. https://de.statista.com/statistik/daten/studie/552495/umfrage/arten-von-cyberangriffen-auf-unternehmen-in-oesterreich/ (Zugriff am 18. 10 2019).

—. „Wie viele Kundenkarten besitzen Sie bzw. an wie vielen Cashback-Programmen nehmen Sie teil?“ 13. 12 2018. https://de.statista.com/statistik/daten/studie/950276/umfrage/umfrage-zum-besitz-von-kundenkarten-in-oesterreich/ (Zugriff am 2019. 10 10).

Smart-Wohnen.de. *Hallo Kühlschrank, ist noch Milch vorhanden?* 2019. https://www.smart-wohnen.de/haus-garten/artikel/hallo-kuehlschrank-ist-noch-milch-vorhanden/ (Zugriff am 17. 10 2019).

Sofort GmbH. *SOFORT-Überweisung.* 2014. https://www.klarna.com/sofort/ (Zugriff am 04. 10 2019).

Sokolov, Daniel AJ. *Google-Mutter Alphabet erzielt 2018 über 30 Milliarden US-Dollar Reingewinn.* 05. 02 2019. https://www.heise.de/newsticker/meldung/Alphabets-Jahresnettogewinn-hoch-wie-nie-4297688.html (Zugriff am 05. 11 2019).

Sparkasse.at. *Muster von Phishing-E-Mails.* 27. 09 2019. https://www.sparkasse.at/sicherheitscenter/wichtige-sicherheitstipps/muster-mails (Zugriff am 24. 10 2019).

Studiengesellschaft für Zusammenarbeit im Zahlungsverkehr (STUZZA). *eps-Überweisung.* 2000. https://www.eps-ueberweisung.at/ (Zugriff am 04. 10 2019).

Symantec. „Internet Security Threat Report .“ 02 2019. https://www.symantec.com/content/dam/symantec/docs/reports/istr-24-2019-en.pdf (Zugriff am 21. 10 2019).

Watchlist Internet. *Liste betrügerischer Online-Shops.* 2019. https://www.watchlist-internet.at/liste-online-shops/ (Zugriff am 25. 10 2019).

Wimmer, Barbara. *Überwachungskapitalismus: Wie unser Online-Verhalten ausgewertet wird.* 20. 02 2018. https://futurezone.at/netzpolitik/ueberwachungskapitalismus-wie-unser-online-verhalten-ausgewertet-wird/400003922 (Zugriff am 29. 10 2019).

Wirtschaftskammer Österreich. *EU-Datenschutz-Grundverordnung (DSGVO): Wichtige Begriffsbestimmungen.* 25. 03 2019. https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Wichtige-Begriffsbestimmu.html (Zugriff am 06. 11 2019).

Zimmer, Daniela. *Amazon lässt mit Alexa bezahlen.* 20. 06 2018. https://www.internetworld.at/e-commerce/amazon/amazon-laesst-alexa-bezahlen-1633863.html (Zugriff am 17. 10 2019).