KFV - SICHER LEBEN 26

KRIMINALITÄT DER ZUKUNFT

Technologische und gesellschaftliche Entwicklungen mit Auswirkungen auf Eigentumskriminalität

KFV - SICHER LEBEN. BAND 26
KRIMINALITÄT DER ZUKUNFT
Technologische und gesellschaftliche Entwicklungen
mit Auswirkungen auf Eigentumskriminalität
Wien, 2021.

MEDIENINHABER UND HERAUSGEBER
KFV (Kuratorium für Verkehrssicherheit)

AUTOR*INNEN
Dr. Georg Plattner
Dr. Claudia Riccabona-Zecha
Mag. Dagmar Lehner

KFV - SICHER LEBEN 26

KRIMINALITÄT DER ZUKUNFT

Technologische und gesellschaftliche Entwicklungen mit Auswirkungen auf Eigentumskriminalität

INHALT

1 EINLEITUNG

Nicht erst seit dem weltweiten Ausbruch der Corona-Pandemie, welche die Gesundheitssysteme der westlichen Welt größtenteils unvorbereitet traf und unsere Gegenwart nachhaltig verändert hat, sollte es mehr als offensichtlich sein, dass ein Blick in die Zukunft – selbst in die nicht allzu entfernte – schwierig ist. Gleichzeitig ist die vorausschauende Trendanalyse eines der wichtigsten Instrumente jeder Form der Präventionsarbeit. Dies gilt ebenso im Bereich der Kriminalität – weniger in dem Sinne, Verbrechen zu verhindern, bevor sie passieren, als dass gesellschaftliche, technologische oder politische Entwicklungen frühzeitig erkannt und antizipiert werden. So kann eine vorausschauende Präventionsarbeit dazu beitragen, dass die Kehrseite des Fortschritts immer auch Teil der Überlegungen für Zivilgesellschaft, Exekutive und Gesetzgeber bleibt.

Gewisse Entwicklungen sind offensichtlich, und es gibt starke Indikatoren, die auf Herausforderungen im Bereich Kriminalität hinweisen. Dass beispielsweise der Klimawandel über kurz oder lang auch Auswirkungen auf die strafrechtliche Beurteilung des Umgangs von Menschen oder Wirtschaftsunternehmen mit der Natur hat, ist ein sehr wahrscheinliches Szenario. Zu deutlich ist die Notwendigkeit, dem Raubbau der Menschen an der Natur und den gesellschaftsbedrohenden Folgen durch den Klimawandel Einhalt zu gebieten.

Andere Entwicklungen sind technologischer Natur und stellen die Kehrseite von wichtigem Fortschritt dar. Nichtsdestotrotz muss auch über diese negativen Aspekte gesprochen werden, um die Innovation hier nicht kriminellen Akteur*innen zu überlassen. Die bevorstehende Neuaufstellung des Mobilfunknetzes durch den Umstieg auf 5G birgt auch Risiken und Sicherheitsprobleme, die frühzeitig angesprochen und angegangen werden müssen. Gleiches gilt für die kommenden Meilensteine der Computertechnologie: die Weiterentwicklungen auf dem Gebiet der künstlichen Intelligenz und den Aufstieg der Quantencomputer. Beide Entwicklungen haben nicht nur enormes positives Potenzial im Sinne des technischen Fortschritts, sondern verbergen in sich auch enorme Risiken durch die Verwendung in kriminellen Strukturen. Der digitale Raum und seine Sicherheit sind wohl das innovativste Feld der Kriminalität allgemein, sowohl im privaten als auch im gewerblichen Bereich. Die Vernetzung von Betrieben ist ein Zukunftsthema, das nicht nur Produktionsabläufe und Dienstleistungen massiv vereinfachen wird, sondern natürlich auch diese Unternehmen angreifbar macht. Auch hier sind in der nahen Zukunft große Fortschritte und damit auch große Risiken zu erwarten, die frühzeitig erkannt und bekämpft werden müssen.

Zu guter Letzt verändert sich auch die Struktur unserer Gesellschaft. Die Fortschritte in der Medizin, aber auch im sozialen Bereich führen dazu, dass Menschen immer älter werden. Menschen in der nachberuflichen Lebensphase sind die am stärksten wachsende Bevölkerungsgruppe in Europa und auch in Österreich. Das macht sie schon auf Grund ihrer großen Zahl zu einem beliebten Ziel Krimineller. Aber auch andere Merkmale dieser sozialen Gruppe (vertrauensvoll, ungeübt in neueren Technologien) machen sie anfälliger für bestimmte Arten von Verbrechen. Daher ist auch diese Gruppe besonders in den Blick zu nehmen, um sie bestmöglich vor Verbrechen zu schützen.

Das KFV hat mit dem vorliegenden Projekt die wichtigsten Zukunftsthemen im Bereich Eigentumskriminalität im Überblick zusammengestellt und erste Ansätze zu deren Prävention präsentiert. Die einzelnen Themen werden in Einzelberichten detailliert vertieft und der Fokus auf die Präventionsarbeit gelegt, die nötig sein wird. Mit diesem innovativen Forschungsprojekt will das KFV einen Beitrag dazu leisten, Österreich sicher in die Zukunft zu begleiten.

2 DIE ZUKUNFT DER KRIMINALITÄT – HERAUSFORDERUNGEN, CHANCEN, INNOVATIONEN

Kriminalität und ihre Prävention bedeuten immer auch eine Art Katz-und-Maus-Spiel zwischen jenen, die illegale Handlungen setzen wollen, und den staatlichen Strafverfolgungsbehörden. Speziell technologische Entwicklungen führen hier oftmals zu Situationen, in denen die Prävention der Kriminalität einen Schritt voraus sein könnte oder müsste, de facto jedoch hinterherhinkt. Denn oft ist eine Sicherheitslücke oder eine Produktschwäche so lange unbekannt, bis sie ausgenutzt wird.

Das bedeutet, dass speziell Kriminalitätsfelder, die innovativ oder neuartig sind, immer eine besondere Herausforderung für Strafverfolgungsbehörden darstellen. Sie müssen hier oftmals zunächst vor allem reagieren – denn selbst wenn die Schwachpunkte ungefähr bekannt sind, ist die Art und Weise, in der eine kriminelle Handlung letztendlich gesetzt wird, oft nicht direkt vorhersehbar. Und die Innovationskraft nicht nur auf Seiten des Gesetzes, sondern auch auf Seiten der Kriminellen, führt zu einem ständigen Wettrennen um das nächste Schlupfloch. Es ist daher von besonderem Interesse, nicht nur für die Forschungscommunity, sondern auch für die Strafverfolgungsbehörden, präventiv auch frühzeitig mögliche Risiken anzusprechen, die in Zusammenhang mit gesellschaftlichen und technologischen Veränderungen stehen. So kann Präventionsarbeit ansetzen, noch bevor Kriminelle durch ihr Handeln zu Reaktionen zwingen.

Die hier vorliegende Forschungsarbeit hat es sich zum Ziel gesetzt, wichtige Entwicklungen im digitalen wie im gesellschaftlichen Leben zu analysieren und auf ihre Risiken durch Kriminelle hin zu untersuchen. Wie werden sich unaufhaltsame gesellschaftliche Veränderungen auf Kriminalität auswirken? Wie könnte technologischer Fortschritt dazu beitragen, ganz neue Formen von Kriminalität zu erzeugen? Wo werden altbekannte Verbrechen lediglich an den technologischen Wandel angepasst? Hierfür wurden zum einen Innovationen im digitalen Bereich untersucht und ihre Risiken herausgearbeitet. Zum anderen werden zwei gesellschaftliche Phänomene (der Klimawandel und die Überalterung westlicher Gesellschaften) herausgegriffen, um auch hier zu zeigen, wie diese Veränderungen natürlich auch von krimineller Innovation betroffen sein können.

Diese Arbeit stellt eine Übersicht über technologische Entwicklungen, Risiken für neue oder alte Formen von Kriminalität sowie rechtliches Handlungspotenzial dar. Jedes der Kapitel dient als Übersicht zu einem komplexen Themengebiet mit komplexen Konsequenzen auf vielen Ebenen. In weiterer Folge soll diese erste Überblicksarbeit dazu dienen, spezifische und fokussierte Projekte zu befruchten, um so jeder der hier aufgeworfenen Problemstellungen gerecht zu werden.

3 VERNETZUNG: FLUCH UND SEGEN FÜR UNTERNEHMEN

3.1 INTERNET OF THINGS BEI UNTERNEHMEN, INDUSTRIE 4.0 UND DIGITALISIERUNG

Österreichs Wirtschaft ist, wie die der anderen EU-Mitgliedsstaaten auch, von einem starken Übergewicht von kleinen und mittleren Unternehmen gekennzeichnet: „Die insgesamt rund 329.000 KMU der marktorientierten Wirtschaft stellen 99,6 Prozent der österreichischen Unternehmen. Sie beschäftigten im Erhebungsjahr 2016 rund zwei Millionen Menschen (68 Prozent der Arbeitsplätze) und erwirtschafteten 63 Prozent der Umsätze (455 Mrd. Euro) sowie 62 Prozent der Bruttowertschöpfung (123 Mrd. Euro)“ (Bundesministerium Digitalisierung und Wirtschaftsstandort, 2019). Die überwiegende Mehrzahl dieser Unternehmen (87 Prozent) hat weniger als zehn Beschäftigte. Kleine und mittlere Unternehmen spielen darüber hinaus auch eine wichtige Rolle in der Lehrlingsausbildung.

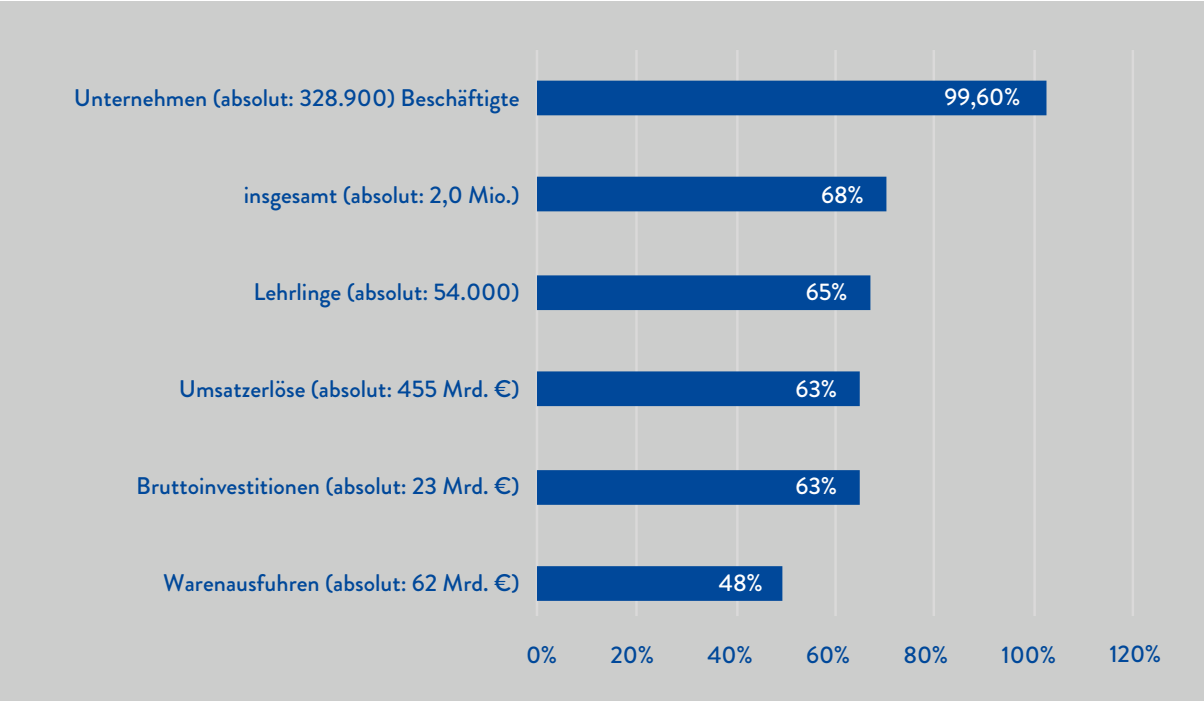

ABBILDUNG 1: Anteil der KMU an allen Unternehmen in Österreich. Quelle: BMDW 2019

Anhand dieser Zahlen ist klar ersichtlich, welchen hohen Wert KMU für den Wirtschaftsstandort Österreich besitzen und welch große Rolle sie auch gesamtgesellschaftlich spielen. Die KMU hatten außerdem großen Anteil an der sehr guten Krisenbewältigung der österreichischen Wirtschaft in den Folgen der Krisenjahre ab 2008 (Wirtschaftskammer Österreich, 2017, S. 14).

Die Digitalisierung der heimischen KMU war bereits 2015 höher als im EU-Durchschnitt, jedoch weiterhin deutlich geringer als bei Großunternehmen (ebda., 18). Österreichische KMU nutzen im EU-Vergleich überdurchschnittlich häufig digitale Informations- und Kommunikationstechnologien. Beinahe jedes Unternehmen mit mindestens zehn Beschäftigten verfügt über einen Internetzugang, und 88 Prozent aller österreichischen KMU hatten bereits 2016

eine eigene Homepage (77% im EU-Durchschnitt). Fast 50 Prozent nutzten 2016 soziale Medien, mindestens 40 Prozent nutzen entweder Warenwirtschafts- bzw. Projektmanagement-Tools oder Software-Lösungen zur Kundenpflege (Wirtschaftskammer Österreich, 2019, S. 8). Eine kürzlich veröffentlichte Studie des Instituts für Höhere Studien (IHS) in Wien zeigt jedoch ein hohes Maß an kritischer Distanz zum Thema der Digitalisierung bei KMU (Gangl & Sonntag, 2020). Besonders KMUs aus Sparten mit traditionell hohem Kund*innenkontakt zeigten sich hier besonders skeptisch, was den Mehrwert der Digitalisierung betrifft. Fehlende Motivation zur Digitalisierung wird als Hauptmotiv ausgemacht, bedingt durch Priorisierung anderer Bereiche, fehlendes Wissen oder die befürchteten hohen Kosten.

Ebenso ein Thema für den österreichischen Wirtschaftsstandort ist Industrie 4.0, die auf Basis eingebetteter (smarter, vernetzter) Systeme (teil-)autonome Maschinen zu einer neuartigen, hochkomplexen Strukturierung im sogenannten Internet of Things (Internet der Dinge, IoT) zusammenführt. Ging es in der ersten Phase vor allem um Anwendung im Bereich Remote Monitoring und Remote Control (standortunabhängige, digitale Wartung von Maschinen und deren Bedienung), so hat sich das Feld seitdem enorm weiterentwickelt. Neue, digitale Services, die auf Apps oder digitalen Assistenten basieren, oder vorausschauende Wartung im Industriebereich sind die nächste Stufe dieser digitalen Evolution. In Österreich wurde hier im Jahr 2016 zuletzt eine Studie zu Kenntnisstand und Einstellung von österreichischen Unternehmen durchgeführt (Lassnig et al., 2016). In dieser Studie wird ein allgemein großes Interesse an der Evolution, die durch die Entwicklungen hin zu Industrie 4.0 ermöglicht wird, dokumentiert, und die Rahmenbedingungen für eine weitere Digitalisierung der Industrie werden als positiv gewertet.

Die wichtigste Veränderung, die die Digitalisierung bringen wird, ist vor allem eine weitere Vernetzung von Unternehmensprozessen, sowohl für die üblichen Geschäftsbereiche (IT – Information Technology) als auch für die Produktionsanlagen und -technologien (OT – Operational Technology). Je vernetzter diese Bereiche werden, umso mehr verändern und verstärken sich auch die Schutzziele dieser Bereiche (Verein Industrie 4.0, 2019).

Die unter dem Schlagwort IoT zusammengefasste neue Rolle, die digitale, smarte Technologie in unserer Gesellschaft spielen wird, ist eines der relevantesten Themen für Unternehmen, um zukunftsfit zu werden. Eine deutsche Studie zum Thema (Vogt, 2019) zeigt, dass IoT ein sich ständig weiterentwickelnder Prozess ist, den Unternehmen durchaus aktiv durchleben, aber oftmals auch von den Anforderungen überfordert sind. Die zuvor angesprochene IHS-Studie zeigt, dass dieses generelle Interesse bei gleichzeitiger Angst vor großen Umwälzungen durchaus auch auf Österreich zutrifft.

3.2 WAS KOMMT: RISIKEN UND CHANCEN IN DER ZUKUNFT

Die Digitalisierung fast aller Wirtschaftsunternehmen wird sich nicht aufhalten lassen, sondern wird im Gegenteil in der Zukunft weiter an Fahrt aufnehmen. Unternehmen, die sich dieser Entwicklung skeptisch gegenüberstellen, werden mittelfristig an Wettbewerbsfähigkeit verlieren. Daher ist die Digitalisierung mit Sicherheit die größte Herausforderung, der sich österreichische Unternehmen in den nächsten Jahren gegenüber sehen werden.

Diese Entwicklung bietet natürlich Chancen und Risiken für die heimischen Betriebe. Zum einen die große Chance, neue Kund*innen zu akquirieren, indem frühzeitig in Digitalisierung investiert wird. Für eine gute Cybersicherheitsstrategie und eine damit verbundene aktive Digitalisierung sprechen daher auch wirtschaftliche Gründe, wie auch eine Studie des KFV im Jahr 2019 ergab: Die Befragung von 500 österreichischen KMU zeigte, dass Cybersicherheit nach wie vor von einigen Unternehmen eher als Belastung und Kostenfaktor gesehen wird. Die primäre Botschaft der im zweiten Studienteil befragten Expert*innen war unisono, dass Prävention gerade für kleine und mittlere Unternehmen enorme Vorteile bringt. Wenngleich es keinen direkten „return on investment“ gibt, stärkt ein angemessener Schutz vor Cyberkriminellen das Unternehmen jedenfalls enorm. Daher lautet wohl die zentrale Botschaft an Unternehmen, dass man nicht erst aktiv werden darf, nachdem man Opfer geworden ist. Die Expert*innen forderten die Unternehmen auf, Sicherheit als Chance zu begreifen. Durch einen adäquaten Level an IT- und Cybersicherheit, aber auch ein modernes Digitalisierungskonzept, können sich Unternehmen im Wettbewerb hervorheben und damit ihren Ruf als zuverlässige und sichere Partner verbessern. Gerade kleine und mittlere Unternehmen sind oft Teil einer Produktionskette, und hier sind Verlässlichkeit und Sicherheit wichtige Faktoren.

Dies gilt natürlich in geringerem Maße auch für die digitale Vernetzung, die Einbettung von Unternehmen in das Internet of Things und die „Versmartung“ von Betriebsprozessen. Diese können eine Vielzahl von Prozessen vereinfachen, die Anknüpfung an Auftraggeber oder andere Teile der Herstellungskette wird vereinfacht, und man schafft sich einen Wettbewerbsvorteil durch Differenzierung von der Konkurrenz.

Selbstverständlich bringen diese Entwicklungen auch ihre Schattenseiten mit sich: Das Hauptrisiko der Digitalisierung ist natürlich die Gefahr, Opfer von Cyberangriffen zu werden. Und gerade KMU sind besonders anfällig dafür, Opfer von Cyberkriminellen zu werden, wie verschiedene Studien zeigen. Als Gründe für die besondere Anfälligkeit kleiner und mittlerer Betriebe werden vor allem mangelnde Ressourcen für Schutzmaßnahmen und fehlende Lösungskompetenz angeführt (Fearn, 2019). Während größere Unternehmen in den vergangenen Jahren ihre Sicherheitsvorkehrungen sukzessive verbessert haben und auch bedeutende Ressourcen in die Cybersicherheit stecken, wird dieses Thema von kleinen und mittleren Unternehmen oft noch immer stiefmütterlich behandelt. Viele KMU unterschätzen laut bisher durchgeführter Studien aber auch schlicht und ergreifend das Risiko, dem sie ausgesetzt

sind. Eine in Deutschland durchgeführte Studie zeigt, dass viele Unternehmen scheinbar davon ausgehen, dass das Risiko zwar allgemein sehr hoch ist, dies jedoch nicht für sie gilt (Sauermann, 2019). Dies wissen auch Kriminelle und machen sich diesen Umstand zunutze. Die Unterschätzung der Gefahren und die geringeren Ressourcen, um eine effektive Prävention für das eigene Unternehmen aufzubauen, führen dazu, dass die Gefahr, die für KMU von Cyberkriminellen ausgeht, weiter steigen wird.

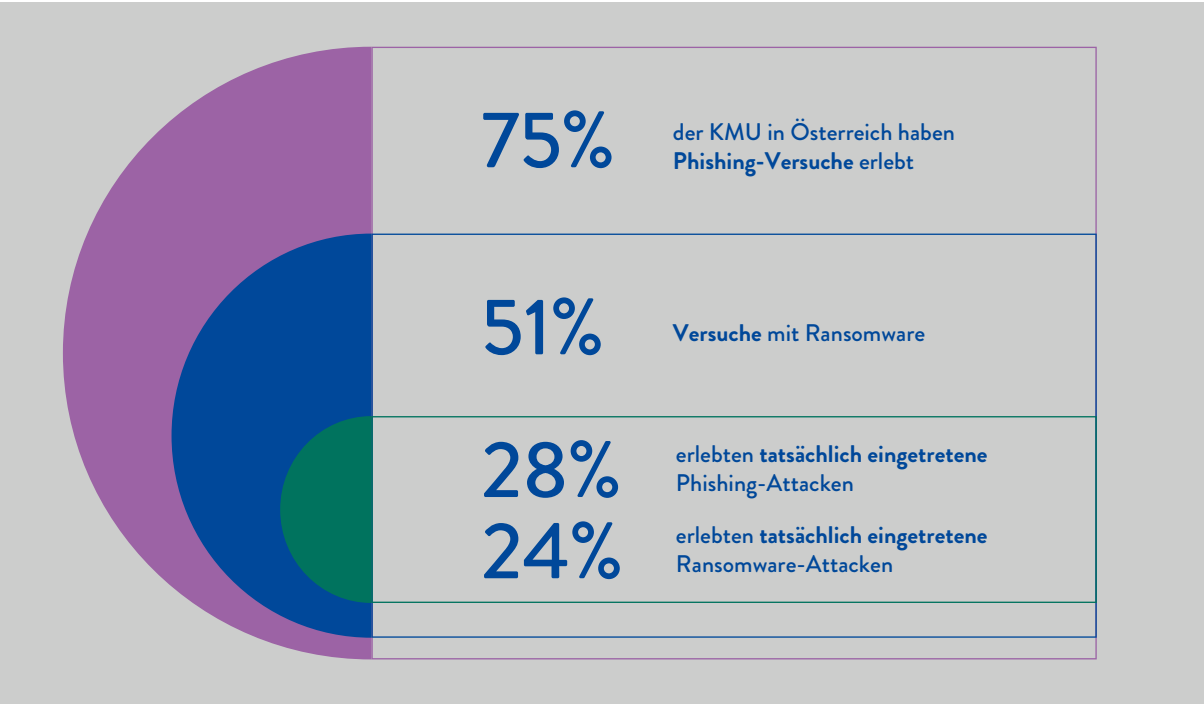

ABBILDUNG 2: Überblick versuchte und eingetretene Attacken. Quelle: Gallup Institut 2019

Auch der Schaden, den diese Unternehmen erleiden, ist signifikant. Im Vereinigten Königreich ergab eine Studie, dass jede Attacke auf Unternehmen (10-49 MitarbeiterInnen) durchschnittlich Kosten von 65.000 £ nach sich zieht. Aufgerechnet würde das bedeuten, dass 80 Prozent sämtlicher durch Cyberkriminalität entstandener Schäden von dieser Unternehmenskategorie getragen werden (Prosser, 2019).

Das KFV hat im Jahr 2019 eine quantitative Befragung österreichischer KMU durchgeführt, um deren Betroffenheit und Sicherheit im Bereich Cyberkriminalität zu eruieren. In der quantitativen Befragung wurde unterschieden zwischen versuchten und eingetretenen Fällen von Cyberkriminalität, da diese Unterscheidung für die Einschätzung der generellen Gefahrenlage durchaus von Interesse ist. Ein Versuch zeigt zum einen, dass Kriminelle nach wie vor großen Tatendrang an den Tag legen, eine niedrige oder hohe Quote an erfolgreichen Fällen zeigt andererseits, wie gut Unternehmen für die Gefahren sensibilisiert sind, wie gut sie geschützt sind und kann damit auch erste Rückschlüsse auf den allgemeinen Kenntnisstand von Unternehmen in Bezug auf ihre Cybersicherheit geben.

Versuchte Cyberattacken hat die überwältigende Mehrzahl der befragten KMU bereits erlebt. Die zwei am häufigsten versuchten Formen von Internetkriminalität bei KMU in Österreich sind Phishing und Schadsoftware (Ransomware, Viren, Trojaner). Über drei Viertel der befragten KMU haben bereits Phishing-Versuche in ihrem Unternehmen erlebt, und mehr als die Hälfte sah sich bereits mit Schadsoftware konfrontiert. Im Vergleich zum Vorjahr kam es bei allen Versuchen zu einem Rückgang. Cyberattacken sind den meisten österreichischen Unternehmen also bekannt, und Erfahrungen sind vorhanden. In der Zukunft wird es weiterhin darum gehen, sich bestmöglich gegen Angriffe von außen zu schützen und die Sicherheit vor Cyberattacken zu erhöhen.

In diesem Zusammenhang stehen auch die Herausforderungen, die auf vernetzte Betriebe mit IoT-Komponenten zukommen, speziell in der Industrie. Hier wird vor allem ein gesteigertes Bewusstsein für Produktions-IT (Operational Technology, OT) gefordert sein. Betriebe im Produktionssektor waren bisher entweder nicht digitalisiert oder hatten keine Anbindung an das Internet. Daher gab es für die verwendeten Maschinen bzw. technisches Gerät im Produktionskreislauf oft nicht den Bedarf, sie speziell abzusichern oder komplexe, regelmäßig wechselnde Passwörter zu verwenden, wie es in der IT bereits seit Jahren Standard ist. Darüber hinaus arbeiten viele Firmen mit „einer flachen und damit unsicheren Netzarchitektur, wodurch sich eingeschleuste Schadsoftware leicht in einem Netzwerk ausbreiten kann“, so die Plattform Industrie 4.0 in ihrem Sicherheits-Leitfaden (Verein Industrie 4.0, 2019, S. 10). Hier wird mit zunehmender Vernetzung der wichtigste Nachholbedarf für smarte Unternehmen gegeben sein.

4 DIE ZUKUNFT IST DIGITAL: INNOVATIONEN UND IHRE BEDEUTUNG FÜR CYBERKRIMINALITÄT

4.1 5G: NEUES ZEITALTER DER MOBILFUNKTECHNOLOGIE

4.1.1 WAS IST 5G? WAS IST DER STATUS QUO IN ÖSTERREICH?

Die fünfte Generation ("5G") des Mobilfunks wird in Europa seit 2019 aufgebaut, noch befindet sich das Projekt allerdings auch in Österreich in der Frühphase. Während bislang vor allem in der Wirtschaft große Datenmengen noch über Kabel transportiert wurden und die Anwendungen wenig mobil waren, haben die Ankunft des Smartphones und die damit verbundenen Innovationen in den Bereichen Smart Living und Smart Factory den Löwenanteil des Datenverkehrs auf mobile Endgeräte verlagert. Zwar kann der jetzige Mobilfunkstandard – 4G-LTE – diese Aufgaben bereits erfüllen; doch langsam stößt diese Generation an ihre Kapazitätsgrenzen.

5G soll es ermöglichen, im Mobilfunknetz mit bis zu 10 Gbit/s Daten zu transportieren, und die Latenzzeiten auf bis zu unter einer Millisekunde zu drücken; das Netz wird als die Antwort auf den immer steigenden Datenverbrauch weltweit gesehen, da es in der Lage sein wird, eine Unmenge an Daten gleichzeitig zu verarbeiten. Damit ist es nicht nur möglich, die private Nutzung digitaler Dienste zu beschleunigen und zu revolutionieren (virtuelle Realität, Smart Home etc.), sondern auch in der Wirtschaft durch die gesteigerten Möglichkeiten des Internet of Things und der vernetzten Produktion und Dienstleistung eine enorme Evolution zu ermöglichen. Darüber hinaus wird 5G die Netzgrundlage für das autonome Fahren und einen großen Schritt vorwärts in der Robotik schaffen.

Die deutsche Telekom preist außerdem die zukünftige Flexibilität hinsichtlich Datengeschwindigkeit, Netzkapazität, Reaktionszeit und Datensicherheit. Diese technologische Innovation verbinde die digitale mit der physischen Welt. Ein weiterer großer Vorteil von 5G ist der Energieverbrauch, der auf ein Zehntel im Vergleich zum bisherigen Netzstandard sinken soll. Dies bedeutet, dass bei sogenannten Machine-to-Machine-Anwendungen (dem automatisierten Informationsaustausch zwischen Endgeräten oder mit einer zentralen Leitstelle) der Akkutausch nur noch ungefähr alle zehn Jahre notwendig wäre (Mey, 2019).
Darüber hinaus betont die Telekom auch die Möglichkeit, anforderungsspezifische Lösungen zu schaffen:

> *Bei 5G wird es eine Vielzahl von Netzebenen geben, die parallel unterschiedliche Anwendungen bedienen können, zum Beispiel für Kunden aus der Industrie. Jede Anwendung erhält eine eigene und passende Ebene. Diese Technologie, das Netz sozusagen in unterschiedliche „Scheiben" zu schneiden, nennt sich Network Slicing. Basis dafür sind Technologien wie die Virtualisierung von Netzwerk-Funktionen (NFV) und Software-definierte Netze (SDN). Dank der dadurch entstehenden Flexibilität können reale Netzkapazitäten abhängig vom Bedarf zu virtuellen Netzbereichen zusammengeschaltet werden, d.h., auch kundenspezifische Lösungen sind möglich* (Deutsche Telekom, 2019).

Die große Herausforderung beim Ausbau von 5G ist der Ausbau der landesweiten Glasfaserinfrastruktur. Die direkte Anbindung aller Mobilfunkstationen an das Glasfasernetz wird bei der 5. Mobilfunkgeneration weiter an Bedeutung gewinnen, um die Vorteile der Innovation nutzen zu können. Darüber hinaus muss auch die Verfügbarkeit geeigneter Funkfrequenzen gewährleistet sein, um 5G vollumfänglich nutzbar zu machen. Hohe Datenraten benötigen entsprechend große Frequenzressourcen, also Frequenzkanäle mit hohen Bandbreiten. Die jetzt genutzten Trägerfrequenzen sind jedoch eher im unteren Bereich angesiedelt. Eine weitere Herausforderung ist die Dichte, in der die Trägerfrequenzen sich befinden müssten, um 5G in seinem gesamten Potenzial flächendeckend zu ermöglichen: Die Reichweite der „small cells" genannten Funkbasisstationen beträgt typischerweise unter 100 Metern, was dazu führt, dass sie in geringerem Abstand zueinander als bisher aufgestellt werden müssen. Somit wird 5G in seiner vollen Frequenzbreite zumindest in den ersten Jahren nur dort zum Volleinsatz kommen, wo zusätzliche Kapazitäten in den bestehenden Netzen benötigt werden (große Industriebetriebe, Krankenhäuser, kritische Infrastruktur generell, Stadtzentren) (Graff, 2019; Forum Mobilkommunikation (FMK), 2018; Kapilavai & Schreier, 2019; Informationszentrum Mobilfunk, kein Datum).

In Österreich startete der Ausbau von 5G im Januar 2020. Die Hauptakteure im Ausbau des neuen digitalen Standards sind die Mobilfunkriesen A1, Magenta Telekom und Drei. Alle drei sind überzeugt davon, hier einen großen Schritt in die Zukunft zu tätigen. Mitte 2020 ist 5G bereits in allen neun Bundesländern von einem oder mehreren Anbietern nutzbar, jedoch nicht flächendeckend, sondern nur ortsweise und nur im niedrigen Frequenzbereich von 3,4 bis 3,8 GHz.

4.1.2 5G UND EIGENTUMSKRIMINALITÄT

Jede Innovation führt auch immer automatisch zu neuen Bedrohungslagen durch Kriminelle. Gerade im Digitalisierungsbereich setzen sich Kriminelle frühzeitig auf neue Technologien, da diese oft mit mangelndem Schutz ausgestattet sind oder die Entwickler*innen genügend Sicherheitslücken noch nicht geschlossen oder noch gar nicht entdeckt haben.

Auch die Entwicklung und flächendeckende Einführung von 5G wird dazu führen, dass Kriminelle systematisch nach Schwachstellen im System suchen werden, um daraus Profit zu schlagen. Die wohl größte Verbesserung gegenüber den vorangegangenen Mobilfunk-Standards ist die stärkere Verschlüsselung von Daten und die bessere Verifizierung von Netzwerknutzer*innen (IT-daily.net, 2019). Wenngleich die Europäische Kommission in ihrem Bericht zur Risikobewertung von 5G zu dem Schluss kommt, dass vor allem Staaten und staatliche Attacken ein Risiko für die Sicherheit im 5G-Netz sind (Europäische Kommission, 2019; Fanta, 2019), sind deshalb keineswegs nur kritische und/oder staatliche Akteure gefährdet.

Selbstverständlich ergeben sich durch diese Evolution des Mobilfunks auch neue Möglichkeiten für kriminelle, nicht-staatliche Akteur*innen, um Schaden anzurichten und verschiedenste Eigentumsdelikte zu begehen. Der Informationsdiebstahl kann zum einen über eine

offensichtliche Schwachstelle erfolgen: Gefälschte mobile Basisstationen können weiterhin (wie auch schon bei 4G) dazu genutzt werden, sich direkt alle möglichen Arten von Informationen von allen Geräten zu holen, die sich in dem Empfangsradius der Station befinden (Greiner, 2019). Dies ist eine der aufwendigeren Möglichkeiten, die 5G für Kriminelle bietet.

Das offensichtlichste Risiko ist schlicht und ergreifend die massiv steigende Anzahl an Geräten, die im Mobilfunknetz operieren. Auch wenn Verschlüsselung und Verifizierung verbessert werden, kann dies nicht verhindern, dass Geräte übernommen werden, speziell wenn mit der Menge an Geräten im Netz nicht auch gleichzeitig das Bewusstsein zu Passwortsicherheit erhöht wird. Bereits jetzt sind vor allem Geräte, die nicht täglich aktiv genutzt werden, jene, die am schwächsten geschützt sind – Produktionsmaschinen und OT-Geräte oder die einzelnen Smart-Home-Geräte (IT-daily.net, 2019). Darüber hinaus ergeben sich noch weitere Sicherheitsprobleme, die zu einem neuen Standard der Cybersicherheit, vor allem bei Unternehmen, führen müssen:

> *Der erste Schritt besteht darin, nicht mehr blind unseren Geräten zu vertrauen. Bevor wir einem Gerät den Zugriff auf Unternehmensinhalte oder Cloud-Dienste erlauben, müssen wir sicherstellen, dass es strengste Sicherheitstests besteht. Bevor man ein 5G-Gerät ins Firmennetzwerk einbindet, sollte geklärt sein, dass es keinem Rooting oder Jailbreaking unterzogen wurde. Es sollte außerdem stets die neueste und sicherste Version des Betriebssystems ausführen und alle Sicherheitspatches installiert haben* (IT-Daily.net, 2020).

Werden diese Standards – sowohl im Eigenheim als auch in vernetzten Betrieben – nicht rigoros umgesetzt, ist die Sicherheit sämtlicher Daten, die über dieses Netzwerk laufen, kompromittiert. Das bedeutet, dass die Sicherheit der Endgeräte, die man in seinem eigenen Netzwerk nutzt, eine direkte Auswirkung auf die Sicherheit sämtlicher im Netzwerk befindlichen Daten und Prozesse hat. Dies kann dann beispielsweise dazu führen, dass ein unsicherer smarter Kühlschrank das Einfallstor für Cyberkriminelle ist, die dann auf Daten aus einem eigentlich gesicherten Laptop zugreifen können. Vernetzte Unternehmen hingegen werden ihre Vulnerabilität durch die Einführung von 5G und die damit verbundene massive Ausweitung von smarten Geräten in ihren Produktions- oder Dienstleistungsabläufen ebenso einem aufwendigen Screening unterziehen müssen. Die bereits in Kapitel 3.2 aufgezeigten Gefahren und Schutzmaßnahmen werden dadurch also bedeutender denn je.

Auch die klassischen Cyberattacken der Eigentumskriminalität – Phishing und DDoS-Attacken, um anschließend Geldzahlungen zu erpressen – werden durch 5G erleichtert werden. Durch die enorme mögliche Geschwindigkeit, mit der Daten transportiert werden, ist beispielsweise für DDoS-Attacken eine weit geringere Anzahl an übernommenen Geräten notwendig als bisher, um einen Server zu überfordern, und die Attacken werden außerdem in weit höherer Geschwindigkeit erfolgen können (Bocetta, 2020). Dies kann dazu führen, dass speziell kleine und mittlere Unternehmen, die bereits jetzt nicht optimal vor dieser Art von Angriffen geschützt sind, wieder vermehrt ins Fadenkreuz solcher Attacken geraten. Denn die Anzahl von DDoS-Attacken sank in den letzten Jahren rapide. Durch 5G wird diese Taktik nicht nur wieder erfolgsversprechender, sondern auch kostengünstiger und risikoärmer für Kriminelle.

Auch für die organisierte Kriminalität ergeben sich durch 5G neue Angriffsmöglichkeiten. Die Europäische Kommission weist in ihrer Risikoeinschätzung des neuen Mobilfunkstandards auf die Gefahr hin, dass kriminelle Organisationen die Netzwerkarchitektur direkt angreifen und die Kontrolle über einen kritischen Bereich erlangen könnten. Damit könnten sie nicht nur mit einem Netzausfall für einzelne Unternehmen drohen (und diese Drohung für Erpressung nutzen), sondern auch den Mobilfunk gesamt stören und damit die Anbieter als Erpressungsopfer angreifen (Europäische Kommission, 2019, S. 28 f.). Ebenso könnte man dadurch direkt Endnutzer*innen angreifen, indem man zum Beispiel eine gefälschte Nachricht in das Netzwerk einspeist, die z.B. dazu auffordert, einen kompromittierten Link anzuklicken. Da diese Nachricht den Anschein erwecken würde, als würde sie vom Netzanbieter direkt kommen, wird das Erkennen der Gefahr bedeutend erschwert (Phishing). Außerdem könnte eine kriminelle Organisation auf diesem Weg auch Zugang zu vertraulichen Daten von Endnutzer*innen in einem Netzwerk erhalten und so zum Beispiel die Second-Factor-Authentifizierungs-Codes auslesen (ebda.).

Unsere digitale Zukunft ist untrennbar mit 5G verknüpft. Bereits in der Gegenwart ist der sichere Umgang mit moderner Technik ein zentraler Stolperstein. Passwortsicherheit, Sicherheitsupdates und ein exaktes Wissen darüber, welche Geräte im eigenen Netzwerk hängen und alle diese Geräte adäquat abzusichern wird in Zukunft dazu führen, dass die vertraute Art des Elektrogerätekaufs verändert werden muss: Die digitale Sicherheit wird ein zentraler Aspekt jeder Anschaffung werden müssen, und ein (rudimentäres) Sicherheitskonzept auch für das Eigenheim bzw. die im Alltagsgebrauch verwendeten digitalen Geräte wird für jede einzelne Person ein wichtiger Schritt, um sich selbst vor den neuen Gefahren zu schützen.

4.1.3 5G UND RECHT

Fact Box – relevante Rechtsquellen:

- EU-Recht: **EU-Empfehlung zur Cybersicherheit der 5G-Netze**: enthält Maßnahmen für die Bewertung von Cybersicherheitsrisiken, EU-weit koordinierte Risikobewertung, Risikomanagementmaßnahmen
- Österreich: **Telekom-Netzsicherheitsverordnung 2020**: Informationspflichten für Betreiber elektron. Kommunikationsnetze und Anbieter elektron. Kommunikationsdienste bei Sicherheitsvorfällen.

Im Detail:

a) EU-Recht

Da viele kritische Dienste von 5G-Netzen abhängig wären, wären die Folgen systemischer und weitverbreiteter Störungen besonders gravierend. Die Gewährleistung der Cybersicherheit von 5G-Netzen ist daher ein Thema von strategischer Bedeutung für die Union. Dazu erging die **Empfehlung (EU) 2019/534 der Kom v 26. 3. 2019 - Cybersicherheit der 5G-Netze (ABl L 2019/88, 42)**:

In den ErwGr wird ausgeführt, dass ausländische Investitionen in strategische Sektoren, der Erwerb kritischer Anlagen, Technologien und Infrastrukturen in der Union sowie die Versorgung mit kritischer Ausrüstung eine Gefahr für die Sicherheit der Union darstellen könnten. Mit den in der Empfehlung enthaltenen Maßnahmen soll bis 30.6.2019 zunächst eine Bewertung der Cybersicherheitsrisiken für 5G-Netze auf nationaler Ebene stattfinden und sollen die erforderlichen Sicherheitsmaßnahmen durch die Mitgliedsstaaten ergriffen werden. In weiterer Folge soll basierend auf der nationalen Risikobewertung eine koordinierte Risikobewertung auf Unionsebene gemeinsam entwickelt und bis 1.10.2019 durchgeführt werden. Abschließend soll bis 31.12.2019 ein Instrumentarium mit geeigneten, wirksamen und angemessenen möglichen Risikomanagementmaßnahmen zur Minderung der auf nationaler und Unionsebene ermittelten Cybersicherheitsrisiken vereinbart werden. Die Auswirkungen der Empfehlung im Hinblick auf die Festlegung geeigneter Vorgehensweisen soll bis 1.2020 bewertet werden (siehe weiter unten 4.5).

b) Österreich

Telekom-Netzsicherheitsverordnung 2020 (TK-NSiV 2020)
Verordnung der Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH) über Verpflichtungen von Betreibern elektronischer Kommunikationsnetze und Anbietern elektronischer Kommunikationsdienste iZm Mindestsicherheitsmaßnahmen unter Berücksichtigung von 5G-Netzen sowie mit Informationspflichten bei Sicherheitsvorfällen.

Mit dieser Verordnung werden Informationspflichten von Betreibern elektronischer Kommunikationsnetze und Anbietern elektronischer Kommunikationsdienste bei Sicherheitsvorfällen iZm elektronischen Kommunikationsnetzen und -diensten festgelegt, die zu beträchtlichen Auswirkungen auf den Netzbetrieb oder die Dienstebereitstellung geführt haben. Außerdem wird das Vorgehen der Regulierungsbehörde bei derartigen Sicherheitsvorfällen geregelt.

4.2 DIE ZUKUNFT IN DER WOLKE – CLOUD SECURITY ALS ZENTRALE PRÄVENTIONSAUFGABE

4.2.1 WAS IST: STATUS QUO DER CLOUD SOLUTIONS UND SECURITY IN ÖSTERREICH

Die Nutzung von Cloud-Diensten hat in Österreich in den letzten Jahren zugenommen, im privaten wie im gewerblichen Bereich. Cloud Computing bezeichnet in der Regel eine IT-Infrastruktur, in der Rechenleistung oder Anwendungssoftware als Dienstleistung zur Verfügung gestellt werden, ohne dass diese auf dem lokalen Rechner installiert sein muss.

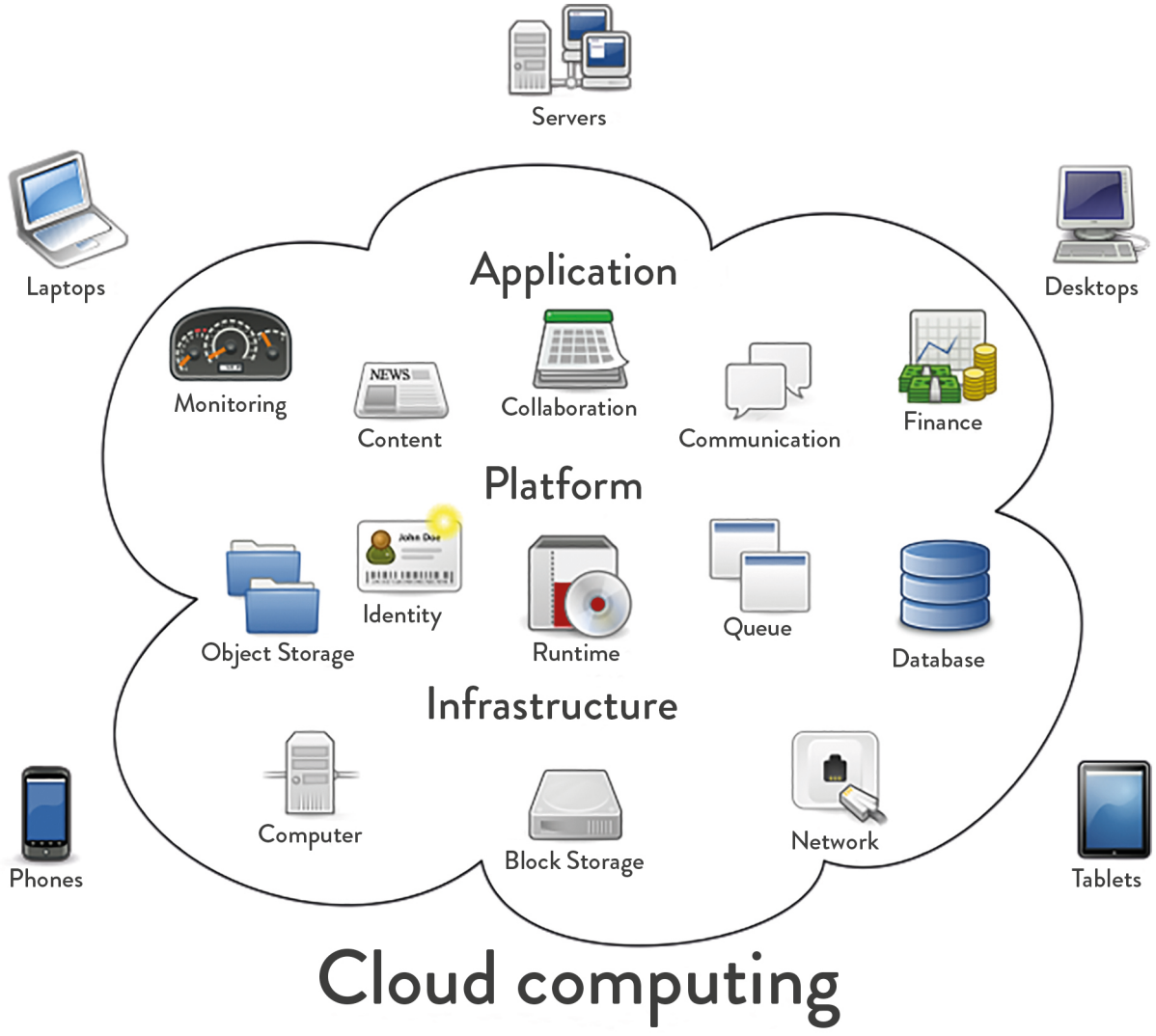

ABBILDUNG 3: Elemente des Cloud Computing, Quelle: Sam Johnston / CC BY-SA

Cloud Computing beinhaltet vier verschiedene Service-Modelle, laut der 2011 veröffentlichten und weitgehend akzeptierten Definition des National Institute of Standards and Technology (NIST) (Mell & Grance, 2011):

- **Software as a Service (SaaS):** Hier wird der Zugang zu Software und Anwendungsprogrammen zur Verfügung gestellt. Gängige Beispiele sind E-Mail, Kalender- und Office-Tools (z.B. Microsoft Office 365).
- **Platform as a Service (PaaS):** Dieses Modell bietet den Zugang von Programmierungs- oder Laufzeitumgebungen mit flexiblen Rechen- und Datenkapazitäten. Damit können Nutzer*innen ihre eigenen Software-Anwendungen entwickeln oder lassen diese ausführen, in einer vom Service-Provider bereitgestellten Umgebung.
- **Infrastructure as a Service (IaaS):** Hier bietet die Cloud den Nutzungszugang zu virtualisierten Hardware-Ressourcen wie Rechnern, Netzen und Speichern. Damit können Nutzer*innen ihren eigenen Computer-Cluster gestalten und sind daher für Betrieb und

Funktion selbst verantwortlich. Ein Beispiel hierfür sind die virtuellen Server der Amazon Elastic Compute Cloude (EC2).

- **Function as a Service (FaaS):** In diesem Modell werden Funktionsinhalte angeboten, die immer wieder genutzt werden oder viel Rechenleistung benötigen.

Die wohl allgemein am meisten genutzten und in der Alltagssprache als Cloud Computing verstandenen Modelle sind hierbei SaaS und IaaS. Neben den Servicemodellen unterscheidet die NIST-Definition außerdem noch zwischen verschiedenen Liefermodellen:

- **Public Cloud:** Das Angebot gilt der breiten Öffentlichkeit und wird über das Internet zur Verfügung gestellt.
- **Private Cloud:** Diese wird nur für die Organisation, die die Cloud erworben hat, betrieben. Das Hosten kann intern oder durch Dritte erfolgen.
- **Hybrid Cloud:** bietet einen kombinierten Zugang zu IT-Infrastrukturen aus beiden oben genannten Formen.
- **Community Cloud:** Ähnlich wie die Public Cloud, jedoch für einen kleineren Nutzer*innenkreis (z.B. mehrere Behörden, Universitäten oder Firmen mit ähnlichem Profil).

Für Privatpersonen sind Cloud-Lösungen längst fixer Bestandteil des Alltags: Mit Dropbox, Google Drive oder Apples ICloud hat man seine Dateien immer griffbereit, über Gmail hat man außerdem ständig Zugriff auf seine E-Mails, Kalendereinträge und erstellte oder dort gespeicherte Dokumente. Hinzu kommt eine Vielzahl von kleinen oder spezialisierten Cloud-Lösungen für die private Nutzung. Zahlen zur Verbreitung bei Privatpersonen sind schwierig zu erlangen.

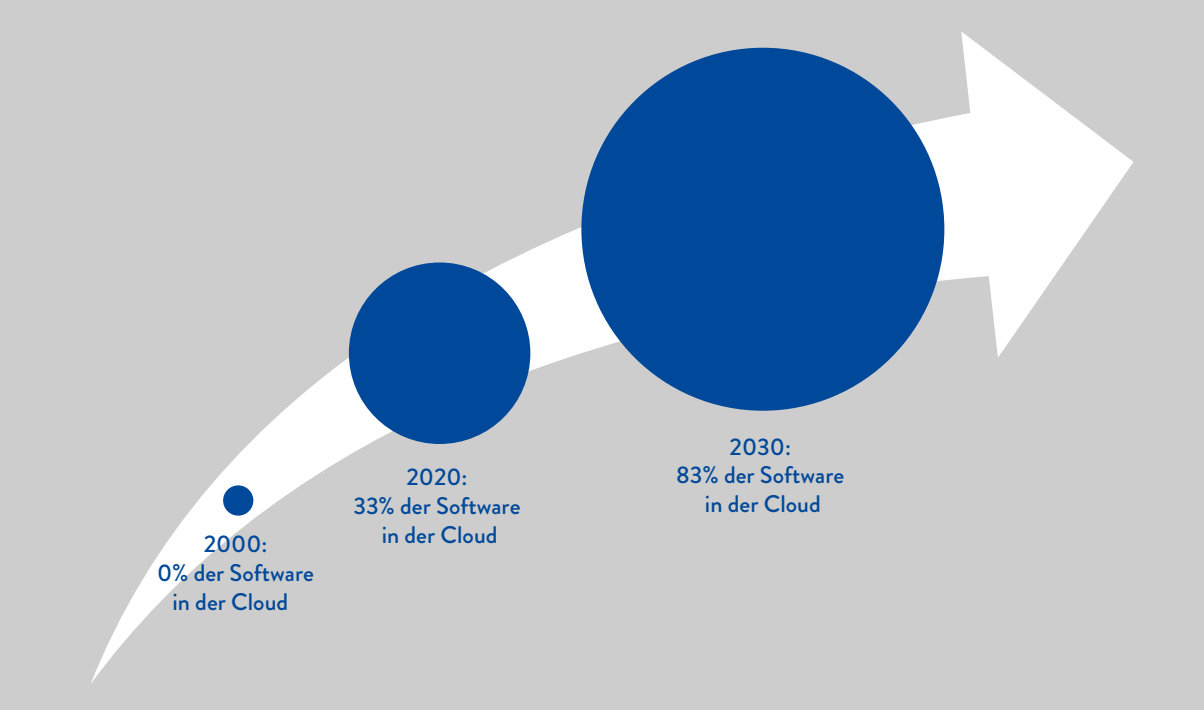

ABBILDUNG 4: Entwicklung von SaaS 2000-2030
Quelle: https://www.bvp.com/assets/media/bessemer-state-of-the-cloud-2020.pdf

Hingegen gibt es eine Vielzahl von Studien zur Cloud-Nutzung von Unternehmen. Zum einen kann der Digital Economy and Society Index (DESI) Auskunft dazu geben, ein jährlich erscheinender Bericht zum Fortschritt der Digitalisierung durchgeführt von der EU. In diesem Bericht liegt Österreichs Wirtschaft im Bereich Cloud-Dienste unter dem EU-Schnitt: Knapp 12 Prozent der österreichischen Unternehmen nutzen demnach Cloud-Dienste mit „mittelhoher Komplexität" (Europäische Kommission, 2020, S. 8). Im Gegensatz dazu stellt die diesjährige repräsentative Monitoring-Studie zum Thema Verbreitung und Nutzung von Cloud-Diensten in Unternehmen eine weit höhere Verbreitung fest: Laut deren Ergebnissen setzt mittlerweile knapp jedes zweite Unternehmen ab 20 Mitarbeiter*innen (47 Prozent) auf Cloud Computing (KPMG Advisory GmbH, 2020, S. 9). Dieser Wert ist im Vergleich zum Nachbarland Deutschland zwar nach wie vor gering (hier sind es über drei Viertel der Unternehmen, ebda.), aber doch bedeutend höher als die Zahlen des DESI-Indexes. Grund hierfür ist vermutlich die breitere Definition von Cloud-Computing in der Studie von KPMG.

In der Nutzung von Cloud-Lösungen zeigt sich in der detaillierten KPMG-Studie ein großer Unterschied zwischen Großunternehmen (ab 250 Mitarbeiter*innen) und kleineren: Während mehr als die Hälfte der großen Unternehmen auf Multi Cloud Computing setzen, ist für kleinere Unternehmen entweder Private oder Public Cloud Computing – und nicht die Kombination der beiden – die Lösung der Wahl. Unternehmen nutzen vor allem US-amerikanische Cloud Services; europäische Lösungen spielen lediglich eine Nischenrolle (ebda., S.10).

4.2.2 WAS KOMMT: RISIKEN UND CHANCEN IN DER ZUKUNFT

Laut dem umfassenden KPMG-Cloud Monitor hat bereits jedes zweite Unternehmen, das auf Cloud-Lösungen setzt, Ausfälle durch technische Probleme beim Provider erlebt. Dies unterstreicht die Notwendigkeit, dass man sich als Unternehmen mit diesem Risiko auseinander setzen und entsprechende Absicherungen schaffen muss. Auf die Ausfälle reagiert hat jedoch lediglich ein knappes Viertel der befragten Unternehmen. Eine Lösung hierfür wäre der Umstieg auf Multi-Cloud-Lösungen, um Ausfälle sofort kompensieren zu können. Dies ist jedoch auch eine Herausforderung für die Unternehmen, da hier ein standardisiertes Vorgehen notwendig ist, um die verschiedenen Provider und deren Dienste unter einen Hut zu bringen. Jedenfalls brauchen Unternehmen auf jeden Fall detaillierte Notfallpläne, um adäquat reagieren zu können, sollte es doch einmal zu einem Ausfall des genutzten Cloud-Dienstes kommen.

Betreffend Sicherheitsvorfällen im System schneiden die Unternehmen mit Public Cloud Lösungen signifikant besser ab als die Unternehmen, die auf ein unternehmensinternes IT-System setzen, wenngleich beide Seiten hohe Verdachtsfälle und tatsächliche Vorfälle hatten: 59 Prozent der Unternehmen mit Public Cloud-Lösungen gaben an, dass es zu einem Sicherheitsvorfall oder einem Verdacht in Hinblick auf die Datensicherheit kam (28% tatsächliche Vorfälle, 31% Verdachtsfälle). Bei den Unternehmen mit internen Lösungen waren es 74 Prozent (29% tatsächliche Fälle, 45% Verdacht).

Für Unternehmen ist ein Cloud-Sicherheitskonzept die wichtigste Präventionsmaßnahme,

um sowohl Ausfälle als auch Angriffe adäquat abfangen zu können. Knapp 40 Prozent der befragten Unternehmen verfügen jedoch über kein spezifisches Cloud-Sicherheitskonzept (ebda., S.29). Hinzu kommt auch ein großes Grundvertrauen der Nutzer*innen in die Cloud. Laut der KPMG-Studie setzt mehr als die Hälfte der befragten Unternehmen auch kritische Anwendungen, Umgebungen und Workflows über eine Public Cloud ein.

Je mehr Unternehmen ihre internen Abläufe in die Cloud verlagern, desto wichtiger wird ein inklusives, durchdachtes Sicherheitskonzept, das auf all diese Risiken vorbereitet ist. Hier wird in Zukunft der große Nachholbedarf sein, denn die Digitalisierung von Unternehmen wird mit einem weiteren Ausbau der Cloud-Infrastruktur einhergehen. In Zukunft werden weite Teile der Unternehmens-Infrastruktur digital „in der Wolke" verortet sein, was es Kriminellen ermöglicht, digital einzubrechen und die geheimsten und kritischsten Unterlagen abzuziehen, die es bislang nur in den Safes und Sicherheitsschränken zu holen gab. Die momentane Absicherung der Cloud ist aber nach wie vor eher ein kleines Vorhängeschloss als ein massiver Safe. Hier herrscht Nachholbedarf für Unternehmen in Österreich.

Doch natürlich steckt in der Entwicklung hin zum Cloud-Computing auch eine Vielzahl an Chancen für Unternehmen. Die Cloud ist der Treiber der Digitalisierung, und eine aktive Cloud-Computing-Unternehmensstrategie führt zu Wettbewerbsvorteilen und einer flexibleren Position im Markt. Sie bewirkt die Erschließung neuer Geschäftsmöglichkeiten oder die schnellere Kooperation in einer Produktionskette. Ein strategisches Cloud- und Sicherheitskonzept ist auch hier der größte Arbeitsschritt, der aber auch gleichzeitig dem Unternehmen schnell wirtschaftliche Vorteile sichern kann.

Für private Nutzer*innen von Cloud-Diensten sind die Risiken ähnlich wie in jeder Interaktion im digitalen Raum. Schwache Passwörter laden zum Datendiebstahl ein, Phishing, Ransomware und fehlende Zwei- oder Mehrfaktor-Authentifizierung sind die klassischen Sicherheitslücken für die privaten User*innen. Je mehr Daten in der Cloud gespeichert werden, umso wichtiger ist eine adäquate Sicherung derselben. Waren es früher vielleicht noch die Gruppenarbeiten, die in der Dropbox gespeichert wurden, sind es nun private Fotos, die zur Erpressung genutzt werden können, kritische Dokumente oder sogar Zugangsdaten, die in der Cloud gesichert und damit abgreifbar sind. Bislang wird die Cloud als unbedacht nebenher laufendes Feature betrachtet, das hilfreich ist und viele Dinge erleichtert. Dass dahinter ein großes Sicherheitsrisiko steckt, das von Kriminellen in Zukunft noch leichter ausgenutzt werden kann, ist noch selten in der Wahrnehmung der privaten Nutzer*innen angekommen. Hier ist es in der Zukunft notwendig, mit Präventionsmaßnahmen frühzeitig zu verhindern, dass hochsensible Daten zu einer leichten Beute werden können.

Aus Sicht der DSGVO gibt es für Cloud-Computing – sowohl im privaten als auch im gewerblichen Gebrauch – einen zentralen systemischen Fehler, der im Juli 2020 durch ein Urteil des EuGH nochmals betont wurde: Der oberste EU-Gerichtshof kippte die Vereinbarung zwischen der EU und den Vereinigten Staaten von Amerika zum Datenaustausch zwischen den zwei Akteuren („Privacy Shield"). In ihrer Entscheidung zu Gunsten der Kläger rund um den Öster-

reicher Maximilian Schrems berufen sich die Richter*innen unter anderem auf die fehlenden Einschränkungen der behördlichen Überwachungsprogramme der USA. Das bedeutet, dass momentan für Daten, die aus der EU bei US-Cloudanbieter*innen gespeichert sind, kein der DSGVO entsprechender Datenschutz existiert. Die Berliner Datenschutzbeauftragte Maja Smoltczyk hat hierzu eine klare und weitreichende Empfehlung abgegeben. „Sie ruft Datenverarbeiter [sic!] dazu auf, alle Daten europäischer Nutzer umgehend auch nach Europa zu verlangen. Und weiter: Firmen, die Cloud-Services in Anspruch nehmen, sollen zu Anbietern in der EU oder anderen Ländern mit „angemessenem Datenschutzniveau" wechseln" (derstandard.at, 2020). Das Problem hierbei ist jedoch, dass es kaum europäische Cloud-Lösungen gibt, die mit ihrer US-Konkurrenz mithalten können. Aus datenschutzrechtlicher Perspektive ist hier eine aktive politische Entscheidung hin zu europäischen Cloud-Lösungen unbedingt erforderlich, um Datenschutz rechtskonform garantieren zu können.

Für User*innen wird es essenziell sein, sich bewusst zu sein, dass die Speicherung von Daten in der Cloud immer ein Sicherheitsrisiko ist. Dieses kann mit den gängigen Vorkehrungen minimiert werden – ein starkes, regelmäßig wechselndes Passwort, keine sensiblen Daten in unsicheren Clouds speichern oder den automatischen Cloud-Login auf bekannte und vertrauenswürdige Netzwerke beschränken – jedoch erfordert auch diese neue Technologie vor allem eine bewusste Auseinandersetzung mit ihrer Sicherheitsarchitektur.

4.2.3 CLOUD COMPUTING UND RECHT

Mit der **NIS-Richtlinie** (Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6.7.2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (siehe unten 4.5) existiert seit 2016 die erste EU-weite Rechtsvorschrift zum Thema Cybersicherheit. Ihr Ziel ist es, ein gleichmäßig hohes Sicherheitsniveau von Netz- und Informationssystemen in der gesamten EU zu erreichen. Somit wurde ein einheitlicher Rechtsrahmen für den EU-weiten Aufbau nationaler Kapazitäten für die Cybersicherheit, eine stärkere Zusammenarbeit der Mitgliedsstaaten der Europäischen Union sowie Mindestsicherheitsanforderungen an und Meldepflichten für kritische Infrastrukturen sowie für bestimmte Anbieter digitaler Dienste wie Cloud-Services und Online-Marktplätze geschaffen.

4.3 RADIKALE INNOVATION: KÜNSTLICHE INTELLIGENZ UND QUANTENCOMPUTER ALS GAME CHANGER IN DER CYBERSICHERHEIT

4.3.1 WAS SIND QUANTENCOMPUTER UND KI? WIE IST DER TECHNISCHE STATUS QUO?

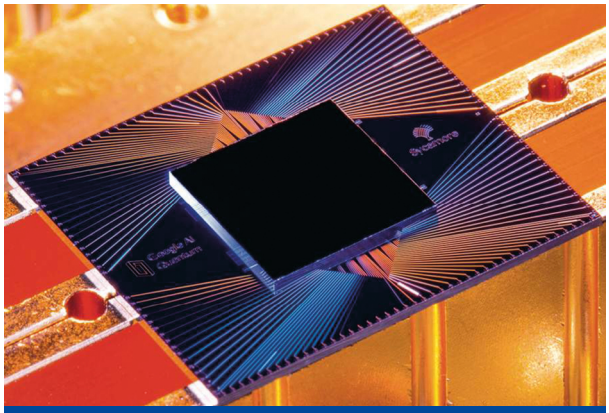

ABBILDUNG 5: Der Sycamore-Chip von Google, Quelle: google

ABBILDUNG 6: In diesem Kabelsalat wird der Chip bis auf den absoluten Temperatur-Nullpunkt gekühlt, Quelle: google

Diese Ankündigung schlug im Oktober 2019 ein wie eine Bombe: Google gab bekannt, dass sein Quantencomputer „Sycamore" „quantum supremacy" erreicht hatte – dies bedeutet, Googles Maschine hatte eine Kalkulation durchgeführt, die kein klassischer Computer in einer realistischen Zeitspanne auszurechnen in der Lage gewesen wäre. In der Community führte das zu Spekulationen über das Ende des klassischen Computerzeitalters – und damit auch das Ende jeder bisher bekannten Form von Cybersicherheit (Coakley, 2019).

Quantencomputer funktionieren, im Gegensatz zu traditionellen Rechenmaschinen, nicht auf Basis der Mikroelektronik, sondern folgen dem Prinzip der Quantenmechanik. Während ein klassischer Computer auf Basis einer binären Speichereinheit – dem Bit – rechnet (0 und 1), nutzt der Quantencomputer ein sogenanntes Qubit als Einheit. Damit kann der Quantencomputer nicht nur 0 oder 1 darstellen, sondern auch einen dazwischen schwebenden Zustand oder beide Positionen gleichzeitig („Superposition"). Das bekannte Beispiel von Schrödingers Katze, die gleichzeitig tot und lebendig in einer Kiste existiert, ist ein Beispiel für die Quantentheorie[1]. Dank dieser Superpositionen ist der Quantencomputer in der Lage, viele Zahlen parallel zu verarbeiten, während der klassische Computer immer nur einen Rechen-

1 In dem Gedankenexperiment befinden sich in einem geschlossenen Kasten eine Katze und ein instabiler Atomkern, der innerhalb einer bestimmten Zeitspanne mit einer gewissen Wahrscheinlichkeit zerfällt. Der Zerfall löst mittels eines Geigerzählers die Freisetzung von Giftgas aus, welches die Katze tötet. Gemäß der Quantentheorie wäre die Katze, bis die Kiste geöffnet wird und damit eine „Messung" des Zustandes durchgeführt wird, gleichzeitig tot und lebendig.

schritt nach dem anderen gehen kann. In der Theorie können Quantenrechner also viele Lösungsschritte gleichzeitig durchführen (Krempl, 2019). Der Quantencomputer wird also die Verarbeitungsgeschwindigkeit und -fähigkeit von Computern massiv erhöhen, was wahrscheinlich zu großen Durchbrüchen in allen möglichen Bereichen führen wird, wie z.B. in den Naturwissenschaften oder in der Medizin. Um diese Rechenprozesse durchführen zu können, muss der Quantencomputer in einer Umgebung gehalten werden, die bis an den absoluten Temperatur-Nullpunkt heruntergekühlt werden muss.

Vorreiter in der Quantenforschung sind die USA, Russland und China auf staatlicher Ebene, wobei in den USA die Zusammenarbeit zwischen privater Wirtschaft, öffentlichem Sektor und akademischer Welt weit mehr ausgebaut ist als in Russland und China, wo die Forschung auf staatlicher Ebene konzentriert wird (Weyrauch & Schmitz, 2019). Auf EU-Ebene wurde erst 2018 das Quantum Technologies Flagship (QTF) gegründet, eine Forschungsinitiative, die Forschungseinrichtungen, die Industrie und öffentliche Geldgeber*innen zusammenbringt, um die EU in diesem Bereich wettbewerbsfähig zu machen. Bis 2021 soll das Projekt voll implementiert sein (Europäische Kommission, 2020).

Künstliche Intelligenz (KI) ist hingegen schon länger nicht mehr bloße Theorie. Bereits 1956 fand die Gründungsveranstaltung der künstlichen Intelligenz als akademisches Fachgebiet am Dartmouth College in New Hampshire statt. Seitdem entwickelte es sich von einem faszinierenden Diskussionsthema für akademische Kreise zu einem vollständigen Teilgebiet der Informatik, welches sich mit der Automatisierung intelligenten Verhaltens und dem maschinellen Lernen befasst. Künstliche Intelligenz bezeichnet die Automatisierung intelligenten Verhaltens sowie maschinelles Lernen. Die Disziplin beschäftigt sich daher vor allem mit Methoden, die es einem Computer ermöglichen, Aufgaben zu lösen, die Intelligenz erfordern würden, wenn sie ein Mensch lösen würde.

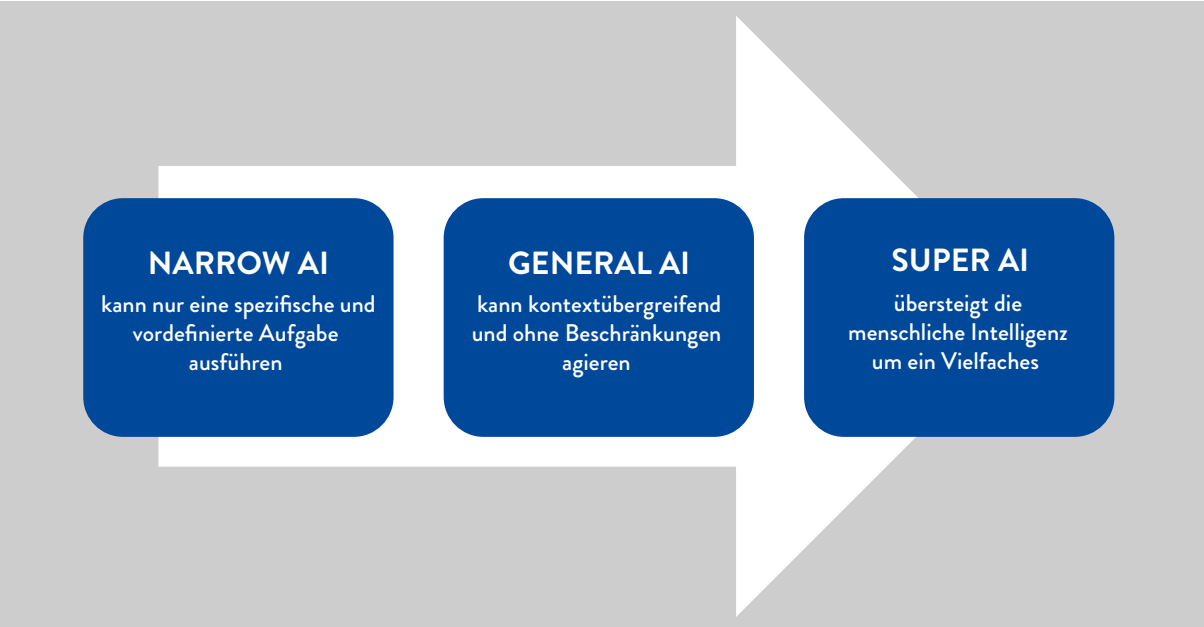

ABBILDUNG 7: Die drei Entwicklungsstufen von KI. Quelle: epicinsights.com

Grob kann in der KI unterschieden werden zwischen starker (General) und schwacher (Narrow) KI sowie dem Ausblick auf eine Super KI. Die schwache KI ist längst in unserem Alltag integriert und kaum mehr wegzudenken: bei Privatpersonen zum Beispiel bei Sprachassistenten (Amazons Alexa, OK Google, Apples Siri u.a.), aber auch bei Produktempfehlungen kommt KI zum Einsatz. Unternehmen schätzen enge KI in ihrer Datenanalyse, um Geschwindigkeit und Zuverlässigkeit zu erhöhen. Dies ist der momentane Status quo der Entwicklung. KI wird für eine spezifische und klar umrissene Aufgabe genutzt, da schwache KI ihre Informationen aus bestimmten Datensätzen entnehmen kann und somit an diese gebunden ist.

In der zweiten Stufe, der starken oder General KI, gibt es für die künstliche Intelligenz keine Beschränkungen mehr. Das System ist dann im Stande, sein Wissen und seine Fähigkeiten in ganz unterschiedlichen Kontexten anzuwenden. Damit kann KI jede gestellte Aufgabe ausführen, auf dem selben Niveau wie Menschen, vermutlich jedoch schneller und effizienter. Es wird erwartet, dass in dieser Stufe von der KI argumentiert, unter Unsicherheit geurteilt, geplant und sogar kreative und einfallsreiche Wege gefunden werden können. Diese Stufe der KI ist noch Zukunftsmusik, sie wird Expert*innenschätzungen zufolge wohl zwischen 2030 und 2060 Realität.

Super KI würde die menschliche Intelligenz dementsprechend schließlich um ein Vielfaches übersteigen (Wenzel, 2020). In einem Vortrag beim US-Think Tank Council on Foreign Relations (CFR) beschreibt der Director of Engineering bei Google, Ray Kurzweil, die Möglichkeit einer Symbiose zwischen KI und Mensch, von der vor allem die Menschheit profitieren würde: Er rechne damit, dass bereits im Jahr 2045 „(...) mit Hilfe einer hybriden KI möglich sein [soll], eine Neocortex-Verbindung zu Cloudsystemen, sogar zu anderen Menschen, herzustellen. Die Daten, auf die wir damit über unser Gehirn zugreifen könnten, wären quasi unendlich. Das würde nicht nur die technische Evolution rasant voranbringen, sondern auch unsere eigene." (ebda.)

4.3.2 WAS KOMMT: RISIKEN UND CHANCEN IN DER ZUKUNFT

Wie bereits aus der kurzen und reduzierten Beschreibung des Potenzials der Quantencomputer ersichtlich wurde, bringen diese monumentale Veränderungen für alle Formen unseres digitalen Lebens, sobald sie der Laborphase entwachsen sind. Die Konsequenzen des Aufstiegs der Quantencomputer sind auch für die Cybersicherheit enorm und potenziell allumfassend. Wie bei den meisten technologischen Neuerungen wird es die Frage sein, welche Seite als erste das Potenzial dieser bahnbrechenden Technologie ausnutzen wird: jene, die ein System schützen will, oder jene, die in das System eindringen will.

Was bereits klar scheint, ist, dass Quantencomputer sämtliche gängigen Kryptosysteme, Sicherheitsprotokolle und andere Schutzmechanismen obsolet machen werden. Die schiere Kraft des Quantencomputers und die Gleichzeitigkeit seiner Aktionen werden die jetzt bekannten Sicherungsprotokolle mit Leichtigkeit ausspielen. Das bedeutet, dass Staaten und Unternehmen bereits jetzt aktiv werden müssen, um auf das Gefahrenpotenzial durch Quan-

tencomputer vorbereitet zu sein. Diese Entwicklung wäre zu revolutionär, um den bisher oft gewählten Umgang mit Cyberkriminalität – passives Warten und Reagieren auf Gefahren – als Handlungsoption zu betrachten (Wallden & Kashefi, 2019). Staaten und Konzerne müssen zusammenarbeiten, um umfassende Konzepte zu entwickeln, um das Potenzial, aber auch die Gefahr von Quantencomputern zu bemessen und geeignete Strategien zu entwickeln. Die Europäische Union hat mit ihrem QTF-Programm bereits einen Schritt in die richtige Richtung gesetzt. Die nächsten Jahre werden zeigen, ob sie in der Lage ist, eine für die Mitgliedsstaaten, aber in weiterer Folge auch für europäische Unternehmen und ihre Bürger*innen geeignete Präventionsmechanismen zu entwickeln.

Eine der zentralen Fragen für die Quantenzukunft wird sein, welche Akteur*innen Zugang zu dieser Technologie haben werden. Werden nur Staaten bzw. globale Konzerne diese Technologie verwenden können oder werden in absehbarer Zeit die Kosten für den Betrieb eines Quantencomputers auch für nichtstaatliche Akteur*innen (wie z.B. kriminelle Organisationen) tragbar sein? Unter anderem von diesen Fragen hängt ab, wie Staaten sich auf die Normalisierung der Quantentechnologie vorbereiten müssen. Es macht einen großen Unterschied für die Cyberverteidigung, ob man mit einem staatlichen Gegner konfrontiert ist oder mit einer Organisation. Eine mögliche Herangehensweise könnte die Etablierung eines internationalen Nicht-Verbreitungsregimes sein, ähnlich wie beim legalen Besitz von Atomwaffen, die eine ähnliche disruptive Rolle in der Kriegsführung spielten, wie es Quantencomputer im Cybersicherheitsbereich und der digitalen Kriegsführung spielen könnten.

Künstliche Intelligenz andererseits ist in ihrer rudimentären Form bereits fester Bestandteil der digitalen Gegenwart. Für Cyberkriminelle würde eine Weiterentwicklung von KI besonders in vier Aktivitäten Erleichterungen schaffen (Huang, 2017):

- Cyber-Hacking: Hier könnte AI dazu dienen, den Effekt einer Attacke zu vervielfachen und so Cyberkriminellen den Angriff von mehr Zielen in kürzerer Zeit ermöglichen. Dies bedeutet vor allem ein erhöhtes Risiko für unsere immer weiter verknüpfte Infrastruktur.
- Coding: KI wird dazu führen, dass das Erlernen von Kodiersprachen nicht mehr notwendig sein wird, um zu coden. Dies wird durch die künstliche Intelligenz übernommen. Das bedeutet natürlich auch, dass es für Kriminelle enorm einfach werden wird, eigene Schadsoftware zu entwickeln. Damit steigt sowohl die Quantität der Täter*innen enorm an als auch die Qualität, da eine Maschine schnell sehr komplexe Codes schreiben kann.
- Deepfakes (siehe Kapitel 4.4): Hier wird nicht nur unsere Perzeption von Wahrheit und Realität in Frage gestellt werden („seeing is believing“ hat als Leitspruch ausgedient). Durch KI-basierte Software können lebensechte Fälschungen sowohl im Video- als auch im Audiobereich erstellt werden, die für Erpressungen und Betrug verwendet werden können.
- Automatisierung von Angriffen: KI wird mittels Maschinenlernen Prozesse bei Cyberattacken automatisieren können, um so die Zahl der Angriffe zu erhöhen, zu verkomplizieren oder sogar zu verschleiern. KI würde in der Lage sein, aus einem fehlgeschlagenen Angriff zu lernen und diesen Lernprozess in der nächsten Attacke automatisch zu inkorporieren.

Natürlich kann gerade künstliche Intelligenz auch für die „Gegenseite“ enorme Vorteile bringen. So wie Kriminelle KI für eine Verbesserung ihres Angriffspotenzials nutzen werden, werden Cybersecurity-Akteur*innen künstliche Intelligenz dazu verwenden, Cyberverteidigungen zu automatisieren, die Schwachstellen selbst zu finden und zu schließen und somit ihre Systeme abzusichern (Shamiulla, 2019).

Quantencomputer und künstliche Intelligenz haben das Potenzial, unser komplettes Cybersicherheitskonzept zu revolutionieren. Bisher bekannte und erprobte Formen der Cyberabwehr werden durch diese Technologien komplett obsolet. Staaten und Organisationen müssen hier frühzeitig und umfassend tätig werden, um unsere Gesellschaft fit für die Quantenzukunft zu machen.

4.4 SCHWACHSTELLE MENSCH – DEEP FAKES

4.4.1 WAS SIND DEEP FAKES?

Deep Fakes sind die nächste Stufe der Video- und Audiomanipulation. Dahinter steckt eine Form von künstlicher Intelligenz, die durch „deep learning“ – eine Subform von KI, eine Aneinanderreihung von Algorithmen, die lernen können und zur intelligenten Entscheidungsfindung befähigt sind – in der Lage ist, Gesichter in Videos zu ersetzen oder eine Stimme perfekt nachzuahmen. Hierzu wird das System dazu programmiert, Videosequenzen und Fotos oder Audiodateien der Zielperson zu studieren und aus verschiedensten Winkeln aufzuzeichnen. Anschließend ahmt das System Verhalten und Sprachverhalten nach. Im Code jedes Deep Fakes steckt ein neuronales Netz, genannt Autoencoder. Dieses wird darauf trainiert, Daten zu verkleinern, um sie anschließend wieder zu vergrößern. Bei der erneuten Vergrößerung versucht der Autoencoder dann, wieder möglichst nah an das Original zu kommen, indem er lernt, wichtige Daten von unwichtigen zu unterscheiden. So lernt das neuronale Netz, wie das Gesicht aussieht und ist anschließend in der Lage, dieses selbstständig zu erzeugen – auch in Bewegung (IONOS.at, 2020).

> *Um Gesichter effektiv auszutauschen, müssen zwei Köpfe erkannt werden: das Gesicht, das im Originalmaterial auftaucht, und jenes, mit dem man den Tausch durchführen möchte. Dafür setzt man einen Eingang (den Encoder) und zwei Ausgänge (die Decoder) an. Der Encoder analysiert jegliches Material, während die beiden Decoder jeweils einen unterschiedlichen Output generieren: Gesicht A oder Gesicht B* (IONOS.at, 2020).

Der Algorithmus fügt also Gesicht B in das Video von Gesicht A ein (siehe auch Abbildung 8). Dies ist auch der größte Unterschied zu den bereits länger bekannten Face-Swap-Fakes: Ein Deep Fake kopiert nicht Bildmaterial in ein anderes Bild, sondern erstellt komplett neues Material; denn nur so kann auch die Mimik passend ausfallen. In einem viralen Video hat so die Nachrichtenplattform Buzzfeed mit Hilfe des Schauspielers Jordan Peele ein Deep-Fake-Video von Präsident Obama produziert, in dem dieser seinen Nachfolger Donald Trump als „Vollidioten“ bezeichnet.

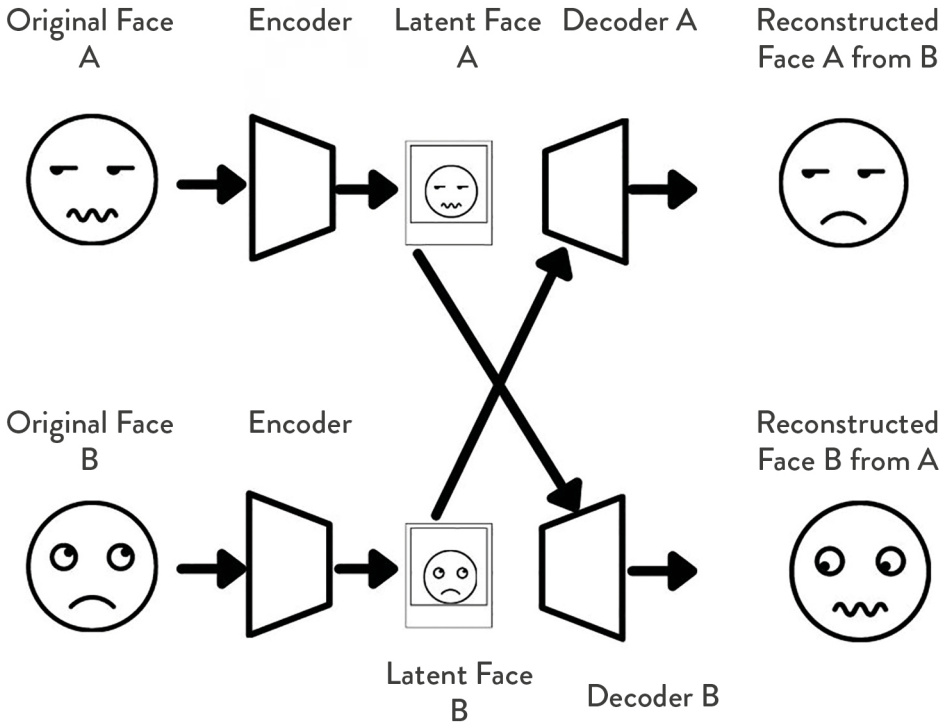

ABBILDUNG 8: Entstehung eines Deep Fakes (eigene Darstellung)

Auf eine vergleichbare Weise ist dann ein Deep-Fake-Code auch in der Lage, aus einem ausreichend großen Pool an Audio-Snippets eine komplett neue Aufnahme zu erstellen. Somit kann in einer Kombination aus Video- und Audio-Manipulation einer Person, von der Gesicht und Stimme bekannt sind, eine komplett künstlich produzierte Rede erstellt werden.

In der Popkultur hatten Deep Fakes ihren ersten großen Auftritt in den letzten beiden Filmen der Star Wars Franchise: Die Schauspielerin Carrie Fisher (Prinzessin Leia) verstarb, noch bevor die Episoden VII und IX gedreht werden konnten. Das Filmstudio beauftragte daraufhin eine andere Schauspielerin, die Rolle zu übernehmen, und setzte dann mit Hilfe eines Deep-Fake-Systems das Gesicht der Verstorbenen auf.

Auch im Alltag werden rudimentäre Formen von Deep Fakes immer beliebter. Es gibt eine Reihe von sehr erfolgreichen gesichtsverändernden Apps, die auf Deep-Fake-Technologie basieren. Die bekannteste dieser Apps ist „FaceApp“, die die Gesichter ihrer User*innen altern lässt oder deren Geschlecht ändert oder eine Kombination von zwei unterschiedlichen Gesichtern produziert. Die zweite bekannte App hierzu ist „FakeApp“ und ermöglichte das Austauschen von Gesichtern in Videos.

4.4.2 DEEP FAKES ALS HERAUSFORDERUNG FÜR UNSERE WAHRNEHMUNG VON REALITÄT

Deep Fakes sind für die allermeisten Menschen, die damit in Berührung kommen, zunächst harmloser Spaß, ein Gimmick auf ihren Smartphones, mit dem sich Paare ihre zukünftigen Kinder als die Kombination ihrer beiden Gesichter erstellen lassen können oder mit denen man einmal selbst eine Rolle in einem Musikvideo oder einer Filmszene übernehmen kann. Doch diese Technologie birgt auch für Kriminelle enormes Potenzial:

- Der CEO-Fraud ist bereits heute ein auch in Österreich vorkommendes Delikt. Hier geben sich Täter*innen als Geschäftsführer*in (CEO) des Unternehmens aus und veranlassen eine*n Mitarbeiter*in zur Überweisung eines größeren Geldbetrages ins Ausland. Mit Hilfe ausgeklügelter Deep Fakes wird diese Betrugsform noch schwieriger für die Mitarbeiter*innen zu erkennen.
- Weiterentwicklung des Enkel-/Neffentricks: Durch die Erstellung hochwertiger Deep Fakes können auch Privatpersonen zur Zahlung von Geldbeträgen bewegt werden, indem die Betrüger*innen vorgeben, nahe Verwandte zu sein, die sich in einer Notlage befinden.
- Erpressung mit Deep Fakes: Bereits jetzt gibt es im Internet Deep Fakes, in denen User (zumeist Männer) Frauen, denen sie aus verschiedenen Gründen Schaden zufügen wollen, in pornografische Videos hineinmanipulieren. Dies geschieht momentan zwar vor allem aus non-monetären Motiven und dient eher der gesellschaftlichen Ächtung des Opfers. Doch natürlich können solche Videos auch produziert werden, um von Personen Geld zu erpressen, damit das Deep-Fake-Video nicht publik wird.

Auf einer gesamtgesellschaftlichen Ebene wird die Weiterentwicklung von KI und damit auch der Qualität von Deep Fakes dazu führen, dass unsere Perzeption von Realität immer mehr in Frage gestellt wird. Feindlich gesinnte Akteur*innen werden in Zukunft mit niedrigen Kosten sehr überzeugende Fake News zu beinahe jedem Thema erzeugen können und so nicht nur unsere Gegenwart, sondern auch die Vergangenheit nachträglich zu manipulieren versuchen. Der einzige Schutz für die Gesellschaft vor solchen Entwicklungen ist Investition in Gegentechnologien, die das Entdecken und zweifelsfreie Identifizieren von solchen Fälschungen ermöglichen. Hinzu kommt der Auftrag an Bildungsinstitutionen und Organisationen, die Menschen zum kritischen Umgang mit digitaler Realität zu erziehen, um den Zweifel an der Authentizität digitaler Information zur Handlungsmaxime zu machen.

4.4.3 DEEP FAKES UND RECHT

Fact Box – relevante Rechtsquellen:

Konkrete Vorschriften und Judikatur fehlen bis dato, aber Verstöße möglich gegen:

- **Zivilrechtlich:** Urheberrecht, Allgemeine Persönlichkeitsrechte (Bildnisschutz/§ 78 UrhG, Schutz der persönlichen Ehre), Verletzung des höchstpersönlichen Lebensbereichs nach §§ 6, 7 sowie 7a Mediengesetz (z.B. Nacktbilder), DSGVO, UWG, § 1330 ABGB (Ehren-

beleidigung) > Ansprüche auf Beseitigung/Unterlassung (Löschung von Web-Inhalten, § 33 MedienG), Schadenersatz

- **Strafrechtlich:** UrhG (zB § 91) Verletzungen der Ehre iSd §§ 111, 113 und 115 StGB (Üble Nachrede Verleumdung, Beleidigung), Vergehen der fortgesetzten Belästigung im Wege einer Telekommunikation oder eines Computersystems nach § 107c StGB („Cybermobbing")

Aktuelle rechtliche Fragestellungen:

- Derzeit existieren keine ausreichenden Gesetze im Umgang mit Deep Fakes, in Diskussion sind z.B.:
  - Regelungen, die eindeutig eine Grenze zwischen einer zulässigen Bearbeitung von Videos und deren Verbreitung und unzulässigen Täuschungen ziehen.
  - Inpflichtnahme von Social-Media-Betreibern, ihre Dienste stärker auf Manipulationen zu kontrollieren.
  - Festlegung einer Grenze, die den Einsatz von Deep Fakes in Kunst, Bildung und Wissenschaft ermöglicht und transparent macht, andererseits Missbrauch unter Strafe stellt.
  - Reglementierung von Deep-Fake-Software ab einem bestimmten Grad der Perfektion.
  - Wahrung der Interessen von durch Deep Fakes geschädigten Privatpersonen.
- Notwendig sind die Sicherung unabhängiger Medien sowie der Ausbau der technischen Gegenwehr, um Fälschungen automatisch erkennen zu können (digitales Wasserzeichen, Blockchain-Technologie).

4.5 RECHT UND DIE KRIMINALITÄT DER ZUKUNFT

4.5.1 AKTUELLE RECHTSLAGE

Die Zukunft der Kriminalität bedeutet auch zugleich Herausforderungen für den Rechtsstaat. Die hohe Innovationskraft und die Geschwindigkeit der Digitalisierung führen dazu, dass auch nationales, europäisches (und internationales) Recht auf vielfältige neue Art und Weise tätig werden müssen, um potenziellen Bedrohungen zu begegnen. Im Folgenden werden die bereits vorhandenen Rechtsquellen ausgeführt:

a) EU-Ebene:

EU-NIS-RL: *Richtlinie (EU) 2016/1148 des Europäischen Parlaments und des Rates vom 6. 7. 2016 über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (NIS-Richtlinie):*

- Die NIS-Richtlinie resultiert aus der ungenügenden Prävention von Unternehmen vor Cyberangriffen.
- Die NIS-Richtlinie verpflichtet Unternehmen, die wesentliche Dienstleistungen in lebens-

wichtigen Bereichen wie Energie, Verkehr und Bankwesen erbringen, sowie Anbieter digitaler Dienste wie Suchmaschinen, CloudComputing-Dienste oder Online-Marktplätze, ihre informationstechnologischen Systeme zu schützen und größere Vorfälle im Bereich der Cybersicherheit den nationalen Behörden zu melden.

- Die NIS-Richtlinie musste bis Ende 2018 verpflichtend in Wasserversorgungswerken, öffentlichen Transportunternehmen, Krankenhäusern, Flughäfen, Banken oder auch Atomkraftwerken umgesetzt werden. Die Meldung schwerer Hackerangriffe ist zudem für digitale Dienste wie Google, den Internetversandhandel Amazon und diverse Cloud-Computing-Dienste vorgeschrieben. In erster Linie soll die NIS-Richtlinie Problemfeldern wie der Industriespionage, dem Hacking und der Zerstörung digitaler Infrastrukturen entgegenwirken.

Direkt anwendbar:

Cyber Security Act: *VO (EU) 2019/881 des Europäischen Parlaments und des Rates vom 17. 4. 2019 über die ENISA (Agentur der Europäischen Union für Cybersicherheit) und über die Zertifizierung der Cybersicherheit von Informations- und Kommunikationstechnik und zur Aufhebung der VO (EU) 526/2013 (Rechtsakt zur Cybersicherheit):*

- Stärkung der ENISA (Agentur der Europäischen Union für Cybersicherheit), Als Kompetenzzentrum wird sie hauptsächlich beratend und unterstützend tätig, soll aber auch die Umsetzung der Unionspolitik und des Unionsrechts auf dem Gebiet der Cybersicherheit fördern (durch Stellungnahmen, Leitlinien und Beratung bzw Vorgabe von Verfahren zu Themen wie Risikomanagement, Meldung von Sicherheitsvorfällen und Informationsaustausch). Die Verordnung regelt Ziele, Aufgaben und organisatorische Aspekte der ENISA, erteilt ihr ein dauerhaftes Mandat und erweitert die Kompetenzen und Ressourcen.
- Weiters bildet die VO einen Rahmen für EU-weite Zertifizierungen für Produkte, Dienstleistungen und Prozesse der Informations- und Kommunikationstechnologien. Zertifizierungen stärken das Vertrauen in Produkte und Dienstleistungen, die für den digitalen Binnenmarkt von zentraler Bedeutung sind. Bisherige aufwändige und kostenintensive Verfahren sollen nun abgelöst werden durch eine EU-weit einheitliche Cybersicherheitszertifizierung. Damit sollen Unternehmen ihre Produkte und Dienstleistungen ohne Hindernisse am Europäischen Markt anbieten können. Den Rahmen für diese Cybersicherheitszertifizierung soll die ENISA aufbauen und pflegen.

DSGVO *(Datenschutz-Grundverordnung): Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. 4. 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG:*

- EU-weiter einheitliche Rechtsrahmen für die Verarbeitung und Speicherung personenbezogener Daten.

Beschluss *(GASP) 2020/651 des Rates vom 14. Mai 2020 zur Änderung des Beschlusses (GASP) 2019/797 über restriktive Maßnahmen gegen Cyberangriffe, die die Union oder ihre Mitgliedsstaaten bedrohen:*

- Enthält eine Liste von natürlichen oder juristischen Personen, Organisationen oder Einrichtungen, die für Cyberangriffe des geschilderten Ausmaßes oder versuchte Angriffe verantwortlich sind, diese in irgendeiner Form unterstützen oder mit entsprechenden Tätern in Verbindung stehen (Anhang I zur Verordnung). Sämtliche Gelder und wirtschaftlichen Ressourcen, die sich im Eigentum oder Besitz der in Anhang I Genannten befinden oder von diesen gehalten oder kontrolliert werden, sind eingefroren. Es ist verboten, den in Anhang I Aufgeführten unmittelbar oder mittelbar Gelder oder wirtschaftliche Ressourcen zur Verfügung zu stellen oder zugute kommen zu lassen.

Empfehlung *(EU) 2019/534 der Kom v 26. 3. 2019 Cybersicherheit der 5G-Netze:*

- Gewährleistung der Cybersicherheit von 5G-Netzen durch Maßnahmen zur Bewertung der Sicherheitsrisiken, erforderliche Sicherheitsmaßnahmen durch die Mitgliedsstaaten, gemeinsame Entwicklung einer koordinierten Risikobewertung auf Unionsebene sowie Bestimmung möglicher gemeinsamer Maßnahmen, die zur Minderung der Cybersicherheitsrisiken im Zusammenhang mit Infrastrukturen (EU-Kooperationsgruppe).

Übereinkommen (+ Zusatzprotokoll) über Computerkriminalität, *SEV Nr. 185, BGBl. III Nr. 140/2012:*

- Bildet den Rechtsrahmen für die Bekämpfung von über das Internet oder über andere Computernetze begangenen Straftaten (insbesondere Computerbetrug, Kinderpornografie, Verstöße gegen die Netzsicherheit und Verletzungen des Urheberrechts);
- Harmonisierung der Strafrechtsvorschriften im Bereich der Cyberkriminalität;
- Bereitstellung von Strafverfahrensinstrumenten für die Untersuchung und Verfolgung von Angriffen auf Informationssysteme sowie anderer Straftaten, die mit Hilfe eines Computersystems begangen werden, und von elektronischen Beweismitteln in Bezug auf diese Straftaten;
- Förderung eines schnellen und wirksamen Systems der internationalen Zusammenarbeit.

Richtlinie 2013/40/EU *des Europäischen Parlaments und des Rates vom 12. August 2013 über Angriffe auf Informationssysteme und zur Ersetzung des Rahmenbeschlusses 2005/222/JI des Rates:*

- Normiert die Mindestvorschriften zur Festlegung von Straftaten und Strafen bei Angriffen auf Informationssysteme. Diese Richtlinie soll überdies die Verhinderung derartiger Straftaten erleichtern und die Zusammenarbeit zwischen Justizbehörden und anderen zuständigen Behörden verbessern.

Richtlinie 2002/58/EG *des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation):*

- Dient der Harmonisierung der Vorschriften der Mitgliedsstaaten, die erforderlich sind, um einen gleichwertigen Schutz der Grundrechte und Grundfreiheiten, insbesondere des Rechts auf Privatsphäre, in Bezug auf die Verarbeitung personenbezogener Daten im Bereich der elektronischen Kommunikation sowie den freien Verkehr dieser Daten und von elektronischen Kommunikationsgeräten und -diensten in der Gemeinschaft zu gewährleisten.

b) Österreich

Netz- und Informationssystemsicherheitsgesetz – NIS-G: *Bundesgesetz zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen, BGBl. I Nr. 111/2018:*

- Es handelt sich um die nationale Umsetzung der NIS-RL.
- Soll ein hohes Sicherheitsniveau von Netz- und Informationssystemen von Betreibern wesentlicher Dienste (in den Sektoren Energie, Verkehr, Bankwesen, Finanzmarktinfrastrukturen, Gesundheitswesen, Trinkwasserversorgung und Digitale Infrastruktur), Anbietern digitaler Dienste (ab einer gewissen Größe) und Einrichtungen der öffentlichen Verwaltung schaffen.
- Schwerpunkte:
  - Festlegung von Aufgaben und Behördenzuständigkeiten sowie Befugnissen zur Gewährleistung eines hohen Sicherheitsniveaus von Netz- und Informationssystemen;
  - Festlegung einer nationalen Strategie für die Sicherheit von Netz- und Informationssystemen;
  - Regelung von Verpflichtungen für die ermittelten Betreiber wesentlicher Dienste, die digitalen Diensteanbieter und Einrichtungen des Bundes (angemessene Sicherheitsvorkehrungen für ihre Netz- und Informationssysteme; Meldung von Sicherheitsvorfällen an die zuständigen Stellen);
  - Überprüfung der Sicherheitsvorkehrungen und der Einhaltung der Meldepflicht;
  - Einrichtung von Computer-Notfallteams (bzw. CSIRTs – Computer Security Incident Response Teams (auch: CERTs – Computer Emergency Response Teams) und Festlegung ihrer Aufgaben;
  - Regelung von Strukturen und Aufgaben im Falle einer Cyberkrise (d.h. eines oder mehrerer Sicherheitsvorfälle mit gegenwärtiger und unmittelbarer Gefahr für die Aufrechterhaltung wichtiger gesellschaftlicher Funktionen und schwerwiegenden Auswirkungen auf die Gesundheit, die Sicherheit oder das wirtschaftliche und soziale Wohl großer Teile der Bevölkerung oder das effektive Funktionieren von staatlichen Einrichtungen);
  - Festlegung von Sanktionen bei Nichteinhaltung der Pflichten des NISG;

- Netz- und Informationssystemsicherheitsverordnung – NISV:
- definiert konkret, was unter „wesentliche Dienste“ und „Sicherheitsvorfälle“ allgemein und jeweils in den einzelnen Sektoren zu verstehen ist und welche Sicherheitsvorkehrungen zu treffen sind.
- Diese Sicherheitsmaßnahmen umfassen Themen wie z.B. Risikomanagement, Umgang mit Dienstleistern, Lieferanten und Dritten, Sicherheitsarchitektur, Identitäts- und Zugriffsmanagement, aber auch das Erkennen und Bewältigen von Vorfällen und das Krisenmanagement.

Telekom-Netzsicherheitsverordnung 2020 (TK-NSiV 2020):

- Verordnung der Rundfunk und Telekom Regulierungs-GmbH (RTR-GmbH) über Verpflichtungen von Betreibern elektronischer Kommunikationsnetze und Anbietern elektronischer Kommunikationsdienste iZm Mindestsicherheitsmaßnahmen unter Berücksichtigung von 5G-Netzen sowie mit Informationspflichten bei Sicherheitsvorfällen
- Informationspflichten von Betreibern elektronischer Kommunikationsnetze und Anbietern elektronischer Kommunikationsdienste bei Sicherheitsvorfällen iZm elektronischen Kommunikationsnetzen und -diensten, die zu beträchtlichen Auswirkungen auf den Netzbetrieb oder die Dienstebereitstellung führen.
- Weiters geregelt werden:
  - Vorgehen der Regulierungsbehörden
  - Rahmenbedingungen einer Erstattung von Mitteilungen in Bezug auf Sicherheitsvorfälle ohne beträchtliche Auswirkungen auf Netzbetrieb oder Dienstebereitstellung;
  - Anforderungen an die Mindestsicherheitsmaßnahmen, die die Betreiber elektronischer Kommunikationsnetze und Anbieter elektronischer Kommunikationsdienste zur Gewährleistung einer angemessenen Beherrschung der Risiken für elektronische Kommunikationsnetze und -dienste und Aufrechterhaltung des diesbezüglich geeigneten Sicherheitsniveaus ergreifen müssen (unter besonderer Berücksichtigung der Sicherheit von 5G-Netzen).
  - Die Verordnung gilt für alle im Bundesgebiet betriebenen öffentlichen elektronischen Kommunikationsnetze mit Ausnahme von Rundfunknetzen und für alle im Bundesgebiet öffentlich angebotenen elektronischen Kommunikationsdienste mit Ausnahme von Übertragungsdiensten in Rundfunknetzen.

4.5.2 WAS IST – WAS KOMMT – WAS FEHLT

Im Folgenden soll in aller Kürze aufgezeigt werden, welche Normen, die in Zusammenhang mit den hier skizzierten digitalen Herausforderungen stehen, bereits existieren, welche (vor allem auf europäischer Ebene) in Entwicklung sind – und wo noch Handlungsbedarf besteht. Dies ist keinesfalls als abgeschlossene Darstellung zu verstehen, sondern lediglich als eine erste Übersicht.

AKTUELLE RECHTSLAGE – WICHTIGSTE RECHTSVORSCHRIFTEN	IN ENTWICKLUNG	HANDLUNGSBEDARF – OFFENE FRAGEN
EU: NIS-Richtlinie Cyber Security Act DSGVO Empfehlung der Komm. zur Sicherheit der 5G-Netze Übereinkommen (+ZP) über Computerkriminalität **Österreich:** NIS-G, NIS-VO StGB Telekom-NetzsicherheitsVO	**EU:** Überarbeitung der NIS-RL[2] E-Privacy-VO[3]	Ausbildung des Sicherheitsbeauftragten bei kleineren Betrieben Frage, wer bei transnationaler Vernetzung wofür Verantwortung trägt Standards für Datensicherheit (Security by Default & Design) Cloud Security: Gibt es rechtliche Standards für Cloud Security, reichen diese aus, Garantien der Privatsphäre ausreichend? Inwieweit ist die Auslagerung unternehmenskritischer Daten möglich/sicher? 5G Netzentwicklung: Ist Gesetzgeber auf die kriminellen Möglichkeiten, die durch 5G Umstieg entstehen, vorbereitet? Neue Arten von Delikten, zB Social Engineering (Trickbetrug, welcher die modernen Formen der Kommunikation nutzt), Angriff mit KI, Angriff mit Quantencomputern Reichen bestehende Haftungssysteme? Soll es Zugangsbeschränkungen zu bestimmten Technologien geben? Ist neue Software von bestehenden Normen ausreichend umfasst (PHG)?

TABELLE 1: Aktuelle relevante Rechtsdokumente im Bereich digitale Zukunft der Kriminalität und offene Fragen (Eigene Zusammenstellung)

2 Die EU-Kommission beabsichtigt, die Richtlinie über Maßnahmen zur Gewährleistung eines hohen gemeinsamen Sicherheitsniveaus von Netz- und Informationssystemen in der Union (sog. NIS-Richtlinie) zu überarbeiten, und hat hierzu am 07.07.2020 eine öffentliche Konsultation eingeleitet, über die sich Bürgerinnen und Bürger, öffentliche und private Organisationen sowie andere Interessengruppen einbringen können. Die Möglichkeit einer breiten Beteiligung besteht bis 02.10.2020. Am 16. Dezember 2020 hat die Kommission einen Vorschlag für eine Richtlinie „über Maßnahmen für ein hohes gemeinsames Maß an Cybersicherheit in der gesamten Union“, die sogenannte NIS 2, vorgelegt.

3 Die E-Privacy-Verordnung soll einen europaweit einheitlichen Rechtsrahmen für die Verarbeitung von Daten in elektronischen Kommunikationsdiensten (Stärkung der Privatsphäre von Bürgern) schaffen. Nach vier Jahren zähen Verhandlungen einigten sich die Mitgliedsstaaten im EU-Ministerrat unter der portugiesischen Ratspräsidentschaft im ersten Quartal 2021 auf eine erste Version der E-Privacy Verordnung. Der Erstentwurf sah sich auf mehreren Ebenen mit harter Kritik durch Datenschützer*innen konfrontiert.

5 UMWELTVERBRECHEN – KAMPF GEGEN DEN KLIMAWANDEL

5.1 UMWELTKRIMINALITÄT – UNTERSCHÄTZT, UNTERFORSCHT?

Die Klimakrise ist im europäischen und auch österreichischen Diskurs-Mainstream angekommen. Spätestens durch die Protestbewegung „Fridays for Future“ (FFF), initiiert von der Schwedin Greta Thunberg, wurde das Bewusstsein für die Zerstörung des globalen Klimas erneut geschärft. Bis auf Absichtserklärungen und flammende Appelle progressiver Politiker*innen und NGOs konnten zwar noch keine bleibenden Ergebnisse erzielt werden, doch die Bevölkerungen der Welt werden sich des immensen Risikos bewusst, dem sie sich und ihre Kinder aussetzen, sollte nicht bald ein radikales Umdenken in unserem Umgang mit der Natur stattfinden. Die ernsthafte Verfolgung von Verbrechen gegen die Natur und unser Klima sowie die angemessene Sanktionierung umweltschädlichen Verhaltens wird eine der zentralen Herausforderungen für Strafverfolgungsbehörden und Gesetzgeber der Zukunft sein.

Das Thema ist nicht neu. Bereits die beginnende Grünbewegung in den späten 1970ern sowie die bereits Jahrzehnte aktiven Organisationen wie Greenpeace warnen vor dem Raubbau, den die Menschen an der Natur betreiben, und die Gesetzgebung hat bereits seit Jahrzehnten Umweltkriminalität als Kategorie im Strafrecht etabliert. Nach wie vor wird die Umweltkriminalität oft als „opferloses Verbrechen“ angesehen, da die Folgen dieser Taten oft erst Jahre oder Jahrzehnte später sichtbar werden und während des Aktes selbst niemand zu Schaden kommt. Doch die langfristigen Schäden am Ökosystem werden transformative Folgen für nachfolgende Generationen haben, was die Einordnung als „opferlos“ unhaltbar macht.

Wenngleich das informelle europäische „EnviCrimeNet“ (ein 2011 gegründetes Netzwerk für Ermittler*innen im Bereich Umweltkriminalität in den EU-Mitgliedsstaaten) betont, dass keine universell akzeptierte Definition von „Umweltverbrechen“ existiert (Environmental Crime Network, 2015, S. 4), so kann man doch zumindest den Umfang dessen, was als Umweltkriminalität geahndet wird, festsetzen: Im österreichischen Bundeskriminalamt residiert ein eigenes Referat (Bundesministerium für Inneres, 2018), welches sich dem Thema widmet. Das Innenministerium definiert den Umfang wie folgt: „Umweltkriminalität umfasst Boden-, Luft-, Wasserverunreinigungen, Zerstörung von Habitaten und geschützten Lebensräumen, illegales Entnehmen und Töten von geschützten Arten sowie illegale Abfallverschiebungen und -deponierungen“. Das Hauptproblem bei der Bearbeitung dieser Art der Kriminalität sieht das EnviCrimeNet in der fehlenden Zugänglichkeit zu Daten, was es erschwert, die reale Dimension, aber auch die Auswirkungen adäquat darzustellen (Environmental Crime Network, 2015, S. 5). Darüber hinaus kritisieren sowohl EnviCrimeNet als auch der frühere Leiter des Referats Umweltkriminalität im Bundeskriminalamt, Karl Frauenberger, dass eine „funktionierende und praktikable Kooperation auf nationaler Ebene zwischen den relevanten Vollzugsbehörden im Bereich Umweltkriminalität basierend auf strategischen Grundsätzen und Zielen (…) nicht vorhanden [ist]“ (Frauenberger, 2017, S. 20).

Im internationalen Kontext sind die profitabelsten Umweltverbrechen der illegale Wildtierhandel, der illegale Holzhandel sowie der illegale Fischhandel (ebda., S. 6). Diese Verbrechen

sind zum einen eher sekundär als Klimaverbrechen, nichtsdestotrotz ist es interessant zu sehen, dass laut Schätzungen des EnviCrimeNet diese drei Tatbestände zu den zwölf profitabelsten Geschäftszweigen des organisierten transnationalen Verbrechens zählen.

Für den Kampf gegen den Klimawandel werden vor allem Boden-, Luft- und Wasserverunreinigung sowie die Zerstörung von Habitaten und geschützten Lebensräumen eine Rolle spielen. Es ist nicht unwahrscheinlich, dass neue Kriminalitätsformen entstehen, die durch eine Veränderung unseres Umgangs mit der Natur vormals legale Aktivitäten illegalisieren.

5.2 WIE WIRD SICH UMWELTKRIMINALITÄT VERÄNDERN?

Viele der jetzt bereits sanktionierbaren Umweltverbrechen werden auch in Zukunft eine Rolle spielen, es wird jedoch darauf ankommen, ob eine rein moralisch-ethische Verpflichtung der Bevölkerung, aber vor allem der Wirtschaftsunternehmen, ausreichen wird, um dem Klimawandel angemessen zu begegnen. Es ist davon auszugehen, dass in Zeiten knapper werdender Ressourcen die adäquate Umsetzung von Boden-, Luft- und Wasserschutzgesetzen nicht einfach angenommen werden kann. Hier geht es zum einen um die umweltschonende Entsorgung von Industrieabfallprodukten, aber auch um einen schonenden Umgang mit Ressourcen allgemein. Mit zunehmender Strenge dieser Gesetze – und sie werden verschärft werden müssen, um supranationale Zielvorgaben erreichen zu können – werden auch die Verstöße zunehmen. Hier ist eine aufmerksame Politik gefordert, die gemeinsam mit den Strafverfolgungsbehörden aktiv und frühzeitig mit gebotener Strenge gegen Umweltverbrechen vorgeht.

Ein zentrales internationales Abkommen zur Bekämpfung des Klimawandels ist das Pariser Abkommen von 2015. Dieses sieht unter anderem die Reduktion von CO2-Emissionen vor, jedoch – wie so vielen Abkommen im Bereich Klimaschutz – fehlt ein effektiver Sanktionsmechanismus bei Nichteinhaltung. Auf EU-Ebene existiert zwar theoretisch die Möglichkeit, bei Nichteinhaltung der Reduktionspflicht ein Vertragsverletzungsverfahren einzuleiten, was in weiterer Folge zur Möglichkeit von Strafzahlungen durch den Mitgliedsstaat führt (Baresch, Goers, Holzleitner & Steinmüller, 2017, S. 12 f.). Die Frage, ob es in der Zukunft zu einem Strafverfahren führen könnte, wenn einzelne Unternehmen die ihnen zugeteilten Grenzwerte für Emissionsausstoß überschreiten, wird sicher einer der zentralen Punkte in der Evolution von Umweltverbrechen sein.

Für Privatpersonen könnte das sommerliche Grillen zu einem potenziell teuren Vergnügen werden: Die Gefahr großflächiger Brände auf Grund zunehmender Trockenheit durch unreglementiertes Grillen wird immer mehr steigen. Dies könnte über kurz oder lang dazu führen, dass Grillen in bestimmten Gebieten vollständig untersagt wird und in eigens dazu verwendeten Bereichen nur unter strengen Auflagen möglich sein wird.

Durch die Erderwärmung sinkt außerdem der Grundwasserpegel in Österreich. Diese nichtregenerative Wasserquelle ist jedoch zentral für viele Aspekte unseres Lebens und wird ausgiebig genutzt. Hier wird sich die Frage stellen, ob bestimmte Formen des Grundwassergebrauchs in Zukunft sanktioniert werden müssen, um eine weitere Abnahme des Pegels zu verhindern. Zu diesen in Zukunft möglicherweise unter Strafe gestellten Formen des Wassermissbrauchs zählt klassischerweise der private Swimmingpool. In den USA gibt es bereits Gesetze in besonders trockenen Gebieten, die das Befüllen der privaten Wasserbecken ab einem gewissen Grundwasserpegel bzw. einer besonders lange andauernden Hitzeperiode untersagen und Zuwiderhandeln unter Strafe stellen. Die Erfahrung aus den USA zeigt auch, dass ein Appellieren an die Solidarität und Vernunft in Hitzezeiten wenig nützt und lediglich sichtbare Sanktionen von Fehlverhalten zu einer Veränderung geführt haben.

Ein weiterer Bereich, der zukünftig unsere Aufmerksamkeit auch in Hinblick auf kriminelle Aktivitäten erfordern wird, ist jener der Abfallentsorgung. Die illegale Entsorgung von potenziellen Altlasten könnte weiter zunehmen, vor allem die Ableitung in Flüsse oder andere Gewässer.

Damit verknüpft, als in der Zukunft massiv relevanter werdendes Spezialgebiet, ist der Lithium-Ionen-Akku, der in großer Zahl in modernen Elektroautos, aber auch E-Scootern und E-Bikes verbaut wird, ein zunehmendes Problem. Werden diese Akkus im normalen Müll entsorgt, besteht ein enormes Explosionsrisiko. Für Li-Ion-Akkus sind spezielle Sammelstellen notwendig, damit sie sachgemäß zerlegt und wiederverwertet bzw. anschließend entsorgt werden können. Die unsachgemäße Entsorgung von solchen potenziell hochgefährlichen Altstoffen wird ein weiter zunehmendes Problem unserer Industriegesellschaften darstellen. Auch hier besteht die Möglichkeit, dass dies in Zukunft unter Strafe gestellt werden wird. Gleichzeitig wird es jedoch notwendig sein, das Bewusstsein in der Bevölkerung zu schärfen, dass die meisten ihrer modernen Geräte genau solche Akkus enthalten. Die sachgemäße Entsorgung sollte in jedem Verkaufsgespräch angesprochen werden. Hinzu kommt, dass der Staat möglichst niederschwellige Entsorgungsmöglichkeiten für diese Akkus schafft.

Auf einem globalen Level wird außerdem die Rationierung von Allgemeinressourcen wie Wasser eine zunehmende Herausforderung darstellen. Der Klimawandel und die Austrocknung bereits jetzt wasserknapper Regionen werden zu einer steigenden Gefahr von Konflikten um diese Ressourcen führen. Es ist nicht unwahrscheinlich, dass es in absehbarer Zukunft kriegerische Auseinandersetzungen um Trinkwasser geben wird. Darüber hinaus wird auch Energie zunehmend zu einem knappen Gut. Der Diebstahl von Energie ist zwar in hochentwickelten postindustriellen Gesellschaften eher unwahrscheinlich, kann jedoch in Schwellenländern jederzeit zu einem Problem werden. Österreich und Europa würden von dieser Verknappung von Grundressourcen sekundär betroffen sein, zum Beispiel durch neue Flüchtlingswellen auf Grund von Wassermangel oder Konflikten um die Kontrolle dieser Ressourcen.

Allgemein ist zu sagen, dass viele der jetzt bereits bestehenden Kriminalitätsfelder im Bereich Umweltverbrechen in Zukunft weiterhin bestehen werden, jedoch an Intensität und damit auch an notwendiger Sanktionierung und Strafverfolgung zunehmen werden. Viele der Taten, die unter dem Überbegriff „Umweltkriminalität" zusammengefasst werden, waren in der Vergangenheit wenig mehr als Kavaliersdelikte und wurden erst durch die Quantität der Umweltbelastung zu einem ernstgenommenen Delikt. Dies muss sich in Zukunft massiv verändern, und die Sanktion ist neben der weiterhin dringend notwendigen Bewusstseinsbildung eine der wichtigsten Maßnahmen, um unser Klima und unsere Umwelt zu schützen.

5.3 UMWELT IM RECHT

Fact Box – relevante Rechtsquellen:

- **Verwaltungsgesetze:** Gewerbeordnung, Wasserrechtsgesetz, Abfallwirtschaftsgesetz, Emissionsschutzgesetz für Kesselanlagen, Immissionsschutzgesetz Luft, Forstgesetz, Naturschutzgesetze der Länder
- **Umweltdelikte im StGB:** §§181, 182, 183 befassen sich mit den oben erwähnten existierenden Delikten.
- **EU-Umweltstrafrechtsrichtlinie:** soll wirksame, angemessene und abschreckende strafrechtliche Sanktionen einführen. Trotz der Implementierung der Richtlinie durch alle Mitgliedsstaaten gibt es unterschiedlich hohe Sanktionen, bedingt durch unpräzise Vorgaben der RL.

Im Detail:

- Die wichtigsten Verwaltungsgesetze, die aus praktischer Sicht für die Verwaltungsakzessorietät (dienen dem Schutz der Umwelt) in Frage kommen, sind:
  - Gewerbeordnung
  - Wasserrechtsgesetz
  - Abfallwirtschaftsgesetz
  - Emissionsschutzgesetz für Kesselanlagen
  - Immissionsschutzgesetz Luft
  - Forstgesetz
  - Naturschutzgesetze der Länder
- Umweltdelikte im StGB:
  - Vorsätzliche und fahrlässige Beeinträchtigung der Umwelt (§§ 180, 181)
  - Schwere Beeinträchtigung durch Lärm (§ 181a)
  - Vorsätzliches und fahrlässiges umweltgefährdendes Behandeln und Verbringen von Abfällen (§§ 181b, 181c)

- Vorsätzliches und fahrlässiges umweltgefährdendes Betreiben von Anlagen (§§ 181d, 181e)
- Vorsätzliche und grob fahrlässige Schädigung des Tier- oder Pflanzenbestandes (geschützt sind wildlebende Tierarten, die in Anh IV lit a der RL 92/43/EWG zur Erhaltung der natürlichen Lebensräume sowie der wildlebenden Tiere und Pflanzen oder des Anh I der RL 2009/147/EG über die Erhaltung der wildlebenden Vogelarten aufgezählt sind sowie geschützte wildlebende Pflanzenarten, die in Anh IV lit b der RL 92/43/EWG zur Erhaltung der natürlichen Lebensräume sowie der wildlebenden Tiere und Pflanzen aufgezählt sind) (§§ 181 f, 181g)
- Vorsätzliche und grob fahrlässige Schädigung von Lebensräumen in geschützten Gebieten (§§ 181h, 181i)
- Andere (auch fahrlässige) Gefährdungen des Tier- oder Pflanzenbestandes (Ausnahme von der Verwaltungsakzessorietät) (§§ 182, 183), Auffangtatbestand
- Unerlaubter (auch fahrlässiger) Umgang mit Kernmaterial, radioaktiven Stoffen oder Strahleneinrichtungen (§§ 177b, 177c)
- Vorsätzlicher und grob fahrlässiger unerlaubter Umgang mit Stoffen, die zum Abbau der Ozonschicht beitragen (§§ 177d, 177e)
- Unerlaubter Handel mit geschützten wildlebenden Tier- oder Pflanzenarten, Teilen oder Erzeugnissen davon, mit Ausnahme der Fälle, in denen die Handlung eine unerhebliche Menge dieser Exemplare betrifft und unerhebliche Auswirkungen auf den Erhaltungszustand der Art hat (§ 7 ArtHG)

- EU-Umweltstrafrechtsrichtlinie: umgesetzt in Ö. 2012; diese sieht vor, dass die Mitgliedsstaaten wirksame, angemessene und abschreckende strafrechtliche Sanktionen einführen. Trotz der Implementierung der Richtlinie durch alle Mitgliedsstaaten gibt es unterschiedlich hohe Sanktionen, bedingt durch die unpräzise Vorgabe der RL.

Kurze Übersicht über aktuelle rechtliche Fragestellungen:

- Strafrechtstatbestände & Abhängigkeit von vorgelagertem Verwaltungsrecht:
  Nach StGB werden **nur wenige Fälle zur Anklage gebracht** – aufgrund von **Beweisschwierigkeiten** und **Abgrenzungsfragen** zu anderen Straftatbeständen sowie zum Verwaltungsstrafrecht –, der überwiegende Teil der Verfahren wird ohne Verurteilung eingestellt. So ist z.B. §180 StGB (vorsätzliche Beeinträchtigung der Umwelt) ohne Verletzung eines Verwaltungsrechts kein Umweltstrafrechtsdelikt. Dazu müssen nunmehr Grenzwerte eindeutiger formuliert werden, da diese in den meisten Paragrafen zu allgemein beschrieben sind. Dies führt dazu, dass jeder Einzelfall geprüft werden muss. Obwohl das Umweltministerium eine Liste mit Mengenangaben erarbeitet hat, kommt diese jedoch nicht zum Einsatz, da sie nicht von allen Staatsanwälten anerkannt wird.
- Strafrechtliche Verfolgung von Umweltdelikten als ultima ratio:
  Zunächst legen die Verwaltungsbehörden iSd Rechtssicherheit den Handlungsrahmen (oftmals per Bescheid im Zuge eines Genehmigungsverfahrens) fest. Wer sich an die

Bestimmungen des Verwaltungsrechts hält (umfasst sind sowohl nationale Rechtsvorschriften als auch unmittelbar anwendbares Europarecht), kann sich also nicht gerichtlich strafbar machen. Dadurch wird von den Verwaltungsbehörden mittelbar ein starker Einfluss auf das Strafrecht ausgeübt. Zum Teil können so auch **strafrechtliche Lücken** entstehen, z.B. durch ein Versäumnis einer Behörde, einen Bereich oder eine konkrete Tätigkeit ausreichend zu regeln, sei es mittels Rechtsvorschriften oder behördlichen Auftrags.

- **Breite Zuständigkeit unterschiedlicher Behörden und Dienststellen:** In den einzelnen Ländern finden sich unterschiedliche Verwaltungs- und Bekämpfungsorganisationen – je nach Kompetenz im Umweltverwaltungs- und Exekutivbereich.
- Problem bei Umweltschäden ist, dass es in der Regel **keine individuellen Opfer** gibt oder dass für jedes individuelle Opfer der Schaden relativ begrenzt ist.
- Ein Problem im Umweltbereich ist auch, dass eine Emission häufig in einem bestimmten Moment stattfindet, aber die Schäden erst viele Jahre später sichtbar werden. Diese lange Zeitspanne führt zu einem Problem, das im Englischen als „latency" bezeichnet wird. Eine **große Latenzzeit** ist problematisch: So ist es möglich, dass nach vielen Jahren eine juristische Person nicht mehr existiert und auch keinen Rechtsnachfolger hat. Möglicherweise kann auch eine Kausalität nicht mehr nachgewiesen werden oder Opfer (z.B. Krebskranke) nehmen an, dass ihre Gesundheitsschäden durch eine natürliche Ursache verursacht worden sind und erkennen nicht, dass jemand für diese Schäden haftbar ist.
- Zehn Empfehlungen der EU an Österreich: insb.
  - Erstellung einer nationalen Umweltstrategie
  - Erarbeitung von Statistiken
  - Spezialisierung der Justizbehörden, Stärkung der Fachdienststellen im Bundeskriminalamt sowie in den Landeskriminalämtern
  - Klare Grenze zwischen strafrechtlichen und verwaltungsbehördlichen Delikten
  - Einführung einer strafrechtlichen Verantwortlichkeit juristischer Personen, wie Stiftungen oder Vereine, mit verhältnismäßigen Verbandsstrafen
  - Kooperationsabkommen zwischen allen Verwaltungs- und Strafrechtsbehörden, um effektiv gegen Umweltkriminalität vorzugehen
- Plan im aktuellen Regierungsprogramm:
  - Evaluierung und ggf. Novellierung der derzeitigen Strafbestimmungen im Umweltstrafbereich
  - Bestrebung, staatsanwaltliche Ermittlungskompetenzen zu bündeln

6 ÜBERALTERUNG ALS CHANCE FÜR KRIMINELLE

6.1 SENIOR*INNEN ALS AM STÄRKSTEN WACHSENDE RISIKOGRUPPE

Österreichs Gesellschaft wird immer älter. Die durch medizinischen Fortschritt und generell sinkende Lebensrisiken stetig steigende Lebenserwartung, kombiniert mit einer relativ geringen Geburtenrate, wird in Österreich – sollte es nicht zu nachhaltigen Veränderungen der demografischen Umstände kommen – dazu führen, dass der Anteil der Menschen über 65 Jahren auf knapp 30 Prozent im Jahr 2080 steigen wird (academia-superior.at, 2019).

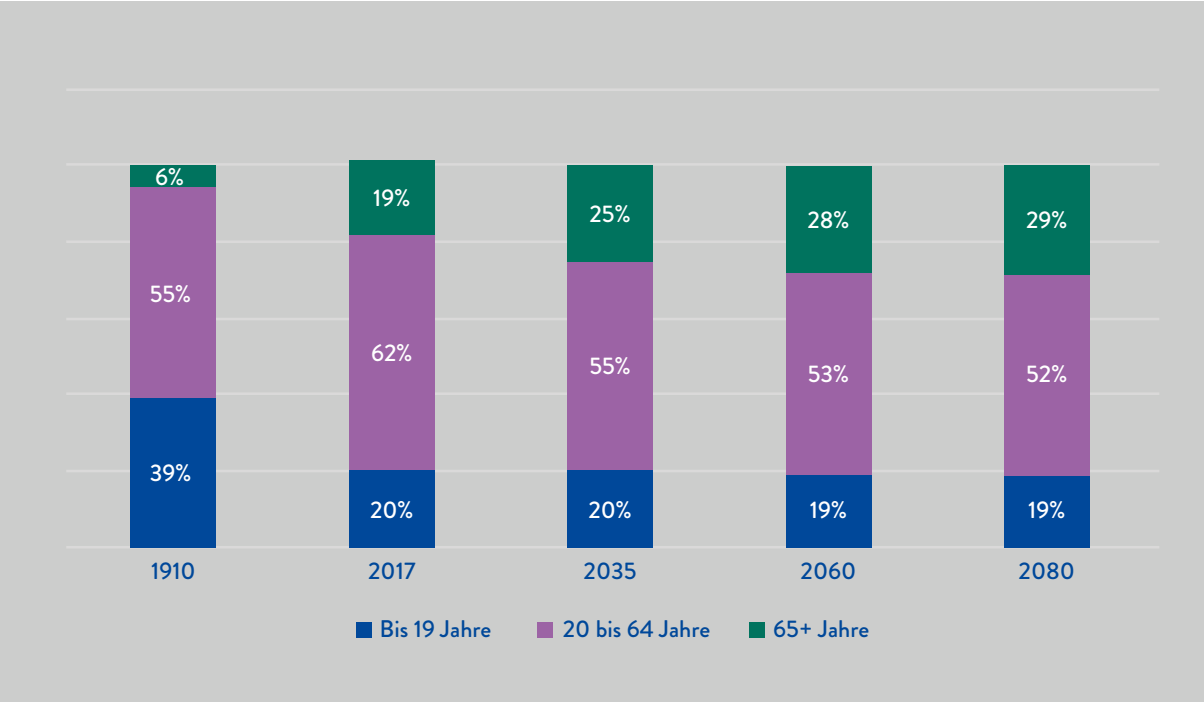

ABBILDUNG 9: Entwicklung der Altersstruktur in Österreich bis 2080. Quelle und Grafik: STATISTIK AUSTRIA, Bevölkerungs- und Erwerbsprognose 2018, academia-superior.at

Menschen in der nachberuflichen Lebensphase (Senior*innen) machen somit einen immer größer werdenden Teil der Bevölkerung in Österreich (und hochindustrialisierter Gesellschaften allgemein) aus. Zwar leben Senior*innen insgesamt sicherer als andere Altersgruppen, fühlen sich auch sicherer und sind tendenziell vorsichtiger (Bundesministerium für Familie, Senioren, Frauen und Jugend, 2019). Gleichzeitig wird diese Gruppe allerdings auch als besonders anfällig für einige Eigentumsdelikte wie Betrug und Diebstahl eingeschätzt. Die Gründe für die Anfälligkeit sind zum einen in einem Nachlassen der Gehirnaktivität in der Region, die für Frühwarnsysteme in Bezug auf die Vertrauenswürdigkeit zuständig ist, zu suchen (Der Spiegel, 2012). Zum anderen führt die nachlassende mentale Verfassung immer wieder dazu, dass ältere Menschen bei Druck schneller nachgeben, sich überfordern lassen oder bei hartnäckigen Versuchen eine eigentlich nicht gewollte Handlung doch zulassen. All diese Gründe führen dazu, dass ältere Menschen speziell anfällig sind für Betrug und Trickdiebstahl, wie zum Beispiel den Enkel- und Neffentrick, das Spiel mit falschen Identitäten allgemein oder den klassischen Taschendiebstahl.

Menschen in der nachberuflichen Lebensphase, oder Senior*innen (Alter 60+), bewegen sich immer mehr auch im digitalen Raum. Laut einer repräsentativen Studie des SPECTRA Marktforschungsinstituts aus 2017 nutzen drei Viertel der Österreicher*innen zwischen 50 und 65 Jahren das Internet. Ab 66 Jahren sinkt diese Zahl auf 37 Prozent. 56 Prozent der 50- bis 65-Jährigen haben ein Smartphone, aber nur 20 Prozent der über 65-Jährigen. Inklusive Laptop oder Notebook steigen diese Zahlen auf 68 bzw. 29 Prozent an. Durchschnittlich verbringen die Österreicher*innen im jüngeren Segment eine Stunde und 18 Minuten täglich im Internet, die ältere Gruppe lediglich 24 Minuten (Spectra Marktforschung, 2017).

Oftmals gestaltet sich das Navigieren durch den digitalen Raum gerade für die sogenannten „Silver Surfer" weniger einfach als für jüngere Menschen. Verschiedene Studien zeigen, dass sich Senior*innen nur mit großer Vorsicht im Internet bewegen und sich vor allem auf Dienste des „Internet 1.0" (E-Mail, Informationen) beschränken. Speziell die Möglichkeiten des „Internet 2.0" (Soziale Netzwerke, Streaming) sowie Transaktionen und Bankgeschäfte werden von ihnen weit weniger genutzt (Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVISI), 2016; ZEIT online, 2019; Telefónica Deutschland/Stiftung Digitale Chancen, 2017). Vor allem Sicherheitsbedenken und gefühlte Überforderung wirken vielfach abschreckend auf Senior*innen, die sich als Reaktion komplett gegen eine Nutzung entscheiden (Amann-Hechenberger et al., 2017, S. 51).

Auch wird von Seiten der Senior*innen mit der Angst vor Cyberkriminalität argumentiert, wenn das Nicht-Nutzen der Möglichkeiten des Internets begründet wird. Es gibt kaum belastbare Zahlen zu Menschen in der nachberuflichen Lebensphase, die Opfer von Internetkriminalität wurden. In einer Umfrage des deutschen BITKOM-Instituts gaben lediglich 5 Prozent der befragten Senior*innen an, bereits im Internet finanziell geschädigt worden zu sein (BITKOM-Institut, 2014, S. 5).

Im Rahmen der 60-Jahr-Feier des KFV 2019 wurde in Fokusgruppen mit Menschen in der nachberuflichen Lebensphase über ihre Erfahrungen und Sorgen im Umgang mit digitalen Medien und dem Verhalten im Cyberspace gesprochen. Im Rahmen dieses Projekts wurde dann auch versucht, das Profil einer so genannten „Silver Surferin" in Österreich zu erstellen:

- **Je älter, desto weniger im Internet aktiv:** in Österreich nur 27% der Ü65-Jährigen
- **Verbringt wenig Zeit im Internet:** in Österreich 24 Minuten pro Tag (Ü65)
- **Nutzt vor allem klassische Endgeräte:** in Österreich: nur 20% nutzen ein Tablet/Smartphone (Ü65)
- **Nutzt vor allem das „Internet 1.0":** E-Mail, Informationen, Nachrichten
- **Internet 2.0 und soziale Medien** werden **meist nur widerstrebend** genutzt
- **Online-Geldgeschäfte** werden sehr **negativ** gesehen
- **Angst vor Falschinformationen** ist hoch

Darüber hinaus konnte anhand der Gespräche und parallel dazu stattfindender grundlegender Forschungsarbeit ein Gefahren- und Fehlerraster entwickelt werden, das besonders auf Senior*innen zutrifft:

Gefahren	Fehler
• **Phishing-Mails**, die spezifisch auf Senior*innen abzielen (Begräbniseinladung, Anwaltsbrief, Lottogewinne etc.) • **Love-Scamming** (es wird eine romantische Beziehung vorgegaukelt, um sich Geld zu erschleichen) • **Enkel*innentrick** • **Unseriöse Online-Shops**, -Flohmärkte • **Falsche Spendenaufrufe**	• **Gutgläubigkeit:** Führt dazu, dass viele Dinge im Internet erst einmal geglaubt werden • **Fehlende digitale Medienkompetenz:** Mangelhaftes Unterscheiden zwischen seriösen und unseriösen Inhalten • **Mangelhafter Schutz des Endgerätes:** mangelnde Update-Frequenz, kein Virenschutz

ABBILDUNG 10: Spezifische Gefahren für Senior*innen im Internet (eigene Darstellung)

6.2 GRUPPENSPEZIFISCHE ZUKÜNFTIGE RISIKEN IM BEREICH EIGENTUMSKRIMINALITÄT

In der Zukunft wird es wahrscheinlich dazu kommen, dass ältere Menschen vor allem mit bereits in den vorangegangenen Kapiteln erwähnten Formen der Kriminalität, die nochmalig spezifisch auf diese Bevölkerungsgruppe zugeschnitten werden, konfrontiert sind.

So ist es beispielhaft sehr gut möglich, dass der Neffen- oder Enkeltrick in einer neuen, digitalen Form zur Anwendung kommt: In einem Deep Fake könnte die verwandte Person, die für das betrügerische Erschleichen von Geld oder anderen Zahlungsmitteln genutzt wird, beispielsweise lebensecht wirken. Ein Videoanruf mit einem gefälschten Gesicht oder ein Anruf mit gefälschter Stimme macht es noch einfacher, einen Verwandten in Not vorzugaukeln. Alles, was in einem ersten Schritt benötigt wird, ist ein Foto oder ein kurzes Stimmensample.

Mit ähnlicher Technologie wird es auch ein Leichtes sein, die Einsamkeit von älteren Menschen auszunutzen. Love Scamming mit simplen Fakes (Videos, Audio, aber auch ganze Gespräche mit einer relativ einfachen KI als Gegenüber) wird in der Zukunft wahrscheinlich mit höheren Erfolgschancen gegen Senior*innen eingesetzt werden. Es wird ihnen eine Beziehung oder Freundschaft suggeriert, um anschließend Geldbeträge zu erschleichen.

Ältere Menschen sind außerdem viel weniger geübt im Umgang mit neuer Technologie als

jüngere. Gleichzeitig steigt aber auch die Anzahl der Alltagsgeräte, die es nur noch hochtechnologisiert zu kaufen gibt. Heute bereits ist es schwierig, einen nicht-smarten Fernseher zu kaufen, oder ein nicht-smartes Mobiltelefon. In Zukunft werden viele weitere Geräte hinzukommen, die ältere Menschen in eine unerwünschte vernetzte Welt zwingen. Da diese ungeübten Menschen natürlich auch weniger Kompetenz in Bezug auf Schutzmaßnahmen besitzen, wird die digitale Infrastruktur von Menschen in der nachberuflichen Lebensphase zu einem einfachen Angriffsziel für Kriminelle. Der Diebstahl von persönlichen Daten, aber auch der Diebstahl von physischen Wertgegenständen, wird durch diese Entwicklungen weiter erleichtert werden.

Um diese stetig wachsende Opfergruppe zu schützen, wird es in Zukunft ein hohes Engagement der Zivilgesellschaft, aber auch relevanter Verbände und der Strafverfolgungsbehörden benötigen. Ein auf die Bedürfnisse von Senior*innen zugeschnittenes Programm, das sie befähigt, sich vorsichtig, aber bestimmt im digitalen Raum zu bewegen und diesen Menschen die Fallstricke aufzeigt, die auf sie lauern, wird notwendig sein, um es den Täter*innen nicht zu einfach zu machen. Anstrengungen in diese Richtung sind bereits vielfach vorhanden, speziell die Senior*innenverbände und auch die Polizei bemühen sich, möglichst viele ältere Menschen zu erreichen. Doch für die Zukunft ist zu erwarten, dass der Betrug an Senior*innen ein in Quantität und Qualität enorm ansteigender Kriminalitätszweig werden wird. Hier ist weiterhin Achtsamkeit geboten.

7 KRIMINALITÄT HEUTE UND MORGEN: MÖGLICHE ENTWICKLUNGEN DER HÄUFIGSTEN EIGENTUMSDELIKTE IN ÖSTERREICH

Schauen wir uns zum Abschluss noch die fünf häufigsten Formen der Eigentumskriminalität laut der Polizeilichen Kriminalstatistik in Österreich für das Jahr 2019 genauer an. Können wir hier Prognosen treffen, wie sich diese Delikte in Zukunft entwickeln werden?

Taschen- und Trickdiebstahl (17.218 Anzeigen im Jahr 2019)

TASCHEN- UND TRICKDIEBSTAHL

- Elektronischer Taschendiebstahl: NFC-Chips von Kredit- und EC-Karten können mittels versteckter Geräte kontaktlos ausgelesen werden, um eine Zahlung bis zu 50 Euro ohne Abfrage eines PINs oder einer Zwei-Wege-Authentifizierung zu tätigen.
- Die Zahl von Fake Shops, die entweder nicht oder falsch liefern, wird stark steigen.

Der klassische Diebstahl im öffentlichen Raum sinkt seit Jahren. Steigendes Bewusstsein, mehr Aufmerksamkeit und Polizeipräsenz führen zu einer gesunkenen Lukrativität. In der Zukunft könnte dieser jedoch vermehrt kontakt- und bargeldlos ablaufen: Durch ein billiges und simpel zu bedienendes Auslesegerät kann quasi im Vorbeigehen der NFC-Chip von Kredit- und EC-Karten ausgelesen werden. Ist dies erfolgreich, kann eine Zahlung bis zu 50 Euro ohne Abfrage eines PINs oder einer Zwei-Wege-Authentifizierung vorgenommen werden. Ein einfacher Trick, der in Zukunft massiv zunehmen wird. Die Geräte, die zum Lesen benötigt werden, werden kleiner, die Technologie ausgereifter, und dank künstlicher Intelligenz werden in absehbarer Zukunft auch keinerlei Programmierfähigkeiten mehr nötig sein, um das Gerät an die eigenen Bedürfnisse anzupassen.

Darüber hinaus wird auch beim Einkauf im Internet die Zahl von Fake Shops stark steigen, die entweder nicht oder falsch liefern. Da der Handel mit Informationen und persönlichen Daten ebenso zunehmend lukrativ werden wird, ist auch sehr gut vorstellbar, dass die Zahl jener Fake Shops, deren einziges Ziel das Abgreifen möglichst vollständiger persönlicher Datensätze ist, weiter zunehmen wird.

Einbruch in den Wohnraum (8.835 Anzeigen im Jahr 2019)

EINBRUCH IN DEN WOHNRAUM

Durch Digitalisierung und 5G wird der Anteil an Smart Homes, die über vernetzte Geräte, digitale Schlösser oder Alarmanlagen verfügen, stark ansteigen. Ein geübter Hacker oder eine KI können die Schwachstellen von vernetzten Geräten in Smart Homes ausnutzen, um beispielsweise die Alarmanlage abzuschalten oder ein ferngesteuertes Türschloss zu öffnen.

Die Zahl der Wohnungseinbrüche sinkt bereits seit Jahren. Besser gesicherte Wohnhäuser und umfassende Präventionskonzepte der Polizei führten unter anderem dazu, dass sich Einbrecher*innen davor scheuen.

In der Zukunft könnte der Wechsel von der Brechstange zum Laptop die entscheidende Entwicklung darstellen: Durch Digitalisierung und 5G wird der Anteil an Smart Homes, die über vernetzte Geräte, digitale Schlösser oder Alarmanlagen verfügen, stark ansteigen. Hier wird nun die Suche nach dem geöffneten Kellerfenster in den digitalen Raum verlagert, gesucht wird also ein smartes Gerät, das nicht gesichert ist und mit anderen, sicherheitsrelevanten Geräten im Haus verknüpft ist. Ein geübter Hacker oder eine KI können dann diese Schwachstelle ausnutzen, um beispielsweise die Alarmanlage abzuschalten oder ein ferngesteuertes Türschloss zu öffnen.

Trickbetrug (4.464 Anzeigen im Jahr 2019)

TRICKBETRUG

- Aufgrund der Digitalisierung des Trickbetrugs ist dieser eines der wenigen Delikte, die in den vergangenen Jahren in der Anzeigenstatistik gestiegen sind.
- Deep Fakes und künstliche Intelligenz können hier zu Game Changern werden: Der „Enkel-“ oder „Neffentrick“ wird für unbedarfte Menschen unmöglich zu erkennen.
- Die zunehmende Einsamkeit von Menschen im digitalisierten Individualismus macht es für eine gut programmierte KI leicht, mit Hilfe eines Lovescams Geld oder Sachleistungen zu erschleichen.

Der Trickbetrug ist eines der wenigen Delikte, die in den vergangenen Jahren in der Anzeigenstatistik verstärkt verzeichnet wurden. Grund dafür ist vor allem die Digitalisierung des Trickbetrugs, und diese wird sich auch in der Zukunft fortsetzen. Bereits in den vorangegangenen Kapiteln wurde aufgezeigt, wie Deep Fakes und künstliche Intelligenz hier zu Game Changern werden können: Der Enkel- oder Neffentrick wird für unbedarfte Menschen unmöglich zu erkennen sein, wenn es scheinbar tatsächlich die verwandte Person ist, die per Videochat um

Geld bittet. Und die zunehmende Einsamkeit von Menschen im digitalisierten Individualismus macht es für eine gut programmierte KI leicht, mit Hilfe eines Lovescams Geld oder Sachleistungen zu erschleichen.

Erpressung: (2.415 Anzeigen im Jahr 2018)

ERPRESSUNG

- DDoS-Attacke: 5G wird dazu führen, dass zum Beispiel ein Firmenserver duch einen Angriff mit viel größeren Datenanfragen in viel kürzerer Zeit mit viel geringerem Aufwand für den*die Täter*in überfordert werden kann.
- KI kann genutzt werden, um Angriffe zu automatisieren und Sicherheitslücken rascher zu finden.
- Aus gefälschten Videos von kompromittierenden Situationen, erzeugt mit Hilfe eines Deep-Fake-Programms ergeben sich auch bei Privatpersonen neue Angriffsflächen.

Erpressung wird nicht jedes Jahr gesondert in der Broschüre des Bundeskriminalamtes zur Polizeilichen Kriminalstatistik ausgewiesen, daher werden hier die Zahlen von 2018 herangezogen. Auch bei der Erpressung ist sehr stark davon auszugehen, dass sich diese vermehrt im digitalen Raum abspielen wird. So wird beispielsweise 5G dazu führen, dass ein Angriff auf Firmenserver mit viel größeren Datenanfragen in viel kürzerer Zeit mit viel geringerem Aufwand für den*die Täter*in diese Server überfordern kann (DDoS-Attacke). Ebenso kann eine KI genutzt werden, um die Angriffe zu automatisieren und Sicherheitslücken rascher zu finden. Bereits jetzt kommt es vor, dass potenziellen Opfern eine erste Attacke mit relativ geringer Schlagzahl angekündigt wird. Diese wird durchgeführt, ohne dass direkt Schaden erzeugt wird. Es wird jedoch bereits bei der Ankündigung mit einer zweiten, viel schwereren, Attacke gedroht, sollte nicht der gewünschte Betrag in der gewünschten (digitalen) Währung überwiesen werden. Hier werden 5G und die Weiterentwicklung von künstlicher Intelligenz maßgebliche Treiber der Kriminalitätsveränderung sein.

Auch bei Privatpersonen ergeben sich neue Angriffsflächen: Gefälschte Videos von kompromittierenden Situationen, erzeugt mit Hilfe eines Deep-Fake-Programms, werden in der Zukunft Menschen vor die Wahl stellen, die Veröffentlichung einer nicht oder nur schwer nachweisbaren Fälschung zuzulassen oder einen Erpressungsbetrag zu zahlen und so die Veröffentlichung zu verhindern. Bereits heute ist die Erpressung mit (echten) Nacktbildern oder erotischen Heimvideos ein zunehmender Trend, gerade bei jüngeren Menschen. Wenn es nun immer einfacher wird, Videos zu fälschen und der Nachweis der Fälschung immer schwieriger wird, so wird auch diese Methode der Erpressung an Quantität zunehmen.

Diebstahl von Kraftfahrzeugen (2.194 Anzeigen im Jahr 2019)

DIEBSTAHL VON KFZ

- Keyless Entry stellt einen wichtigen Angriffsvektor für den Diebstahl von Fahrzeugen dar.
- Das Fahrzeug selbst wird immer mehr zum smarten Kfz. Das bedeutet, dass das Auto selbst auch gehackt werden kann, sobald es mit einem Netz kommuniziert.

Auch der Kfz-Diebstahl ist eine seit Jahren sinkende Straftat, weil Autohersteller*innen und Nutzer*innen den Schutz ihrer Gefährte immer weiter verbessert haben. Doch auch hier ist in der Zukunft ein Wechsel des Tatwerkzeugs zu erwarten: Zum einen wird die Keyless-Entry-Technologie einen bedeutenden Angriffsvektor für den Diebstahl von Fahrzeugen darstellen. Bereits heute ist sie eine oft kritisierte Sicherheitslücke, da das Signal, das genutzt wird, um zwischen Transponder und Fahrzeug zu korrespondieren, mit einem simplen Signalverstärker auf mehrere 100 Meter ausgedehnt werden kann. Somit kann ein Duo von Autodieb*innen mit einem simplen und im Internet für wenig Geld erhältlichen Gerät ein Auto innerhalb weniger Sekunden entsperren. Währenddessen ist der*die Besitzer*in zu Hause, und der Transponder befindet sich auf dem Schlüsselbrett neben der Haustür, oder er/sie ist in einem Restaurant, und der Schlüssel befindet sich in der Jackentasche.

Darüber hinaus wird aber natürlich auch das Fahrzeug selbst immer mehr zum smarten Kfz. Das bedeutet, dass das Auto selbst auch gehackt werden kann, sobald es mit einem Netz kommuniziert.

8 VERZEICHNISSE

8.1 ABBILDUNGSVERZEICHNIS

8.2 TABELLENVERZEICHNIS

8.3 LITERATURVERZEICHNIS

academia-superior.at. (2019). *Österreichs Bevölkerung bis 2080*. Abgerufen am 20. August 2020 von https://www.academia-superior.at/oesterreichs-bevoelkerung-bis-2080

Amann-Hechenberger, B., Buchegger, B., Erharter, D., Felmer, V., Fitz, B., Jungwirth, B., Xharo, E. (2017). *Tablet & Smartphone: Seniorinnen und Senioren in der mobilen digitalen Welt. Forschungsbericht zum Projekt „mobi.senior.A“.* Wien. Abgerufen am 18. November 2019 von http://forschungsbericht.mobiseniora.at/forschungsbericht.pdf

Baresch, M., Goers, S., Holzleitner, M.-T. & Steinmüller, H. (2017). *Auswirkungen der Umsetzung des Pariser Klimagipfels und der Zero-Emission Society auf die energieintensive Industrie: Eine rechtliche und volkswirtschaftliche Evaluierung für Oberösterreich.* Linz. Abgerufen am 12. August 2020 von https://www.wko.at/branchen/ooe/industrie/Auswirkungen-COP21-auf-OOe-Endbericht-EI-JKU-Linz.pdf

BITKOM-Institut. (2014). *Senioren in der digitalen Welt.* Berlin. Abgerufen am 18. November 2019 von https://www.bitkom.org/sites/default/files/file/import/141212-BITKOM-Praesentation-Senioren-in-der-Digitalen-Welt-12-12-2014.pdf

Bocetta, S. (2020). *Will 5G Implementation Lead to an Increase in Ransomware Attacks?* Abgerufen am 13. 07 2020 von www.circleid.com/posts/20200312-will-5g-implementation-lead-to-an-increase-in-ransomware-attacks/

Bundesministerium Digitalisierung und Wirtschaftsstandort. (2019). *Mittelstandsbericht 2018.* Abgerufen am 08.. 10. 2019 von https://www.bmdw.gv.at/Themen/Wirtschaftsstandort-Oesterreich/KMU/Mittelstandsbericht.html

Bundesministerium für Familie, Senioren, Frauen und Jugend. (2019). *„Rate mal, wer dran ist!“ So schützen Sie sich vor Betrug und Trickdiebstahl.* Berlin.

Bundesministerium für Inneres. (2018). *EU-Ratspräsidentschaft 2018: Treffen von Ermittlern im Bereich Umweltkriminalität in Wien*. Abgerufen am 19. August 2020 von https://www.bmi.gv.at/news.aspx?id=4D54694D36655A6D78484D3D

Coakley, A. (2019). *Quantum computing: Is it really all it's cracked up to be?* Abgerufen am 28.07.2020 von DW.com: https://www.dw.com/en/quantum-computing-is-it-really-all-its-cracked-up-to-be/a-51118334

Der Spiegel. (2012). Wieso Senioren eher Betrügern auf den Leim gehen. *Der Spiegel (online).* Abgerufen am 12. August 2020 von https://www.spiegel.de/wissenschaft/mensch/senioren-faellt-es-schwer-luegner-am-gesicht-zu-erkennen-a-870834.html

derstandard.at. (2020). „Privacy Shield“ gekippt: Datenschützerin fordert Umstieg auf europäische Cloudanbieter. *der Standard.* Abgerufen am 28. 07 2020 von https://www.derstandard.at/story/2000118933858/privacy-shield-gekippt-datenschuetzerin-fordert-umstieg-auf-europaeische-cloudanbieter

Deutsche Telekom. (2019). *Was ist 5G? Grundwissen zum Netz der Zukunft.* Abgerufen am 02.07.2020 von https://www.telekom.com/de/konzern/details/was-ist-5g-grundwissen-zum-netz-der-zukunft-542352

Deutsches Institut für Vertrauen und Sicherheit im Internet (DIVISI). (2016). *DIVSI Ü60-Studie: Die digitalen Lebenswelten der über 60-Jährigen in Deutschland.* Hamburg. Abgerufen am 18. November 2019 von https://www.divsi.de/wp-content/uploads/2016/10/DIVSI-UE60-Studie.pdf

Environmental Crime Network. (2015). *Report on Environmental Crime.* Brüssel. Abgerufen am 19. August 2020 von http://www.envicrimenet.eu/images/docs/envicrimenet%20report%20on%20environmental%20crime.pdf

Europäische Kommission. (2019). *Member States publish a report on EU coordinated risk assessment of 5G networks security.* Brüssel. Abgerufen am 12. 07 2020 von https://ec.europa.eu/commission/presscorner/detail/en/IP_19_6049

Europäische Kommission. (2020). *Digital Economy and Society Index (DESI) 2020: Integration of digital technology.* Brüssel. Abgerufen am 14.07.2020 von https://ec.europa.eu/digital-single-market/en/integration-digital-technology

Europäische Kommission. (2020). *Quantum Technologies Flagship*. Abgerufen am 28.07.2020 von https://ec.europa.eu/digital-single-market/en/policies/quantum-technologies-flagship

Fanta, A. (2019). *EU-Staaten halten Staats-Hacking für größtes Risiko*. Abgerufen am 12.07.2020 von https://netzpolitik.org/2019/sicherheit-von-5g-netzen-eu-staaten-halten-staats-hacking-fuer-groesstes-risiko/

Fearn, N. (2019). *Why SMEs are at a higher risk to cyber crime*. Abgerufen am 28. Oktober 2019 von https://www.idgconnect.com/opinion/1502916/smes-risk-cyber-crime

Forum Mobilkommunikation (FMK). (2018). *Die nächste Mobilfunkgeneration: 5G.* Wien. Abgerufen am 10.07.2020 von https://www.fmk.at/site/assets/files/44752/fmk_factsheet_2018.pdf

Frauenberger, K. (2017). *Bekämpfung von Umweltkriminalität: Eine Analyse der Tätigkeit der österreichischen Verwaltung in diesem Bereich.* Masterarbeit, FH Campus Wien, Wien. Abgerufen am 19. August 2020 von https://pub.fh-campuswien.ac.at/obvfcwhsacc/download/pdf/2063599?originalFilename=true

Gangl, K. & Sonntag, A. (2020). *Digitale Kompetenzen in österreichischen KMUs.* Institut für Höhere Studien (IHS). Wien: Institut für Höhere Studien (IHS). Abgerufen am 02.07.2020 von https://www.bmdw.gv.at/Services/Publikationen/Studie-Digitale-Kompetenzen-in-österreichischen-KMUs.html

Graff, N. (2019). *5Gute Fragen zum 5Giganetz*. Abgerufen am 10.07.2020 von A1.net: https://www.a1.net/BusinessChange/pd/5g-fragen/

Greiner, W. (2019). *Mobilfunk bleibt auch mit 5G angreifbar*. Abgerufen am 13.07.2020 von https://www.lanline.de/news/mobilfunk-bleibt-auch-mit-5g-angreifbar.233845.html

Huang, S. (2017). *Cyber Criminals' Exploitation of Artificial Intelligence.* International Risk Assessment and Horizon Scanning Symposium 2017. IRAHSS 2017.

Informationszentrum Mobilfunk. (kein Datum). *Wissenswertes zu 5G.* Abgerufen am 08.07.2020 von https://www.informationszentrum-mobilfunk.de/technik/funktionsweise/5g

IONOS.at. (2020). *Deepfakes: Fälschungen der nächsten Generation*. Abgerufen am 18. August 2020 von https://www.ionos.at/digitalguide/online-marketing/social-media/deepfakes/

IT-daily.net. (2019). *Der neue 5G-Standard - Ein Paradies für Hacker*. Abgerufen am 13.07.2020 von https://www.it-daily.net/it-sicherheit/cyber-defence/22637-der-neue-5g-standard-ein-paradies-fuer-hacker

IT-Daily.net. (2020). *5G - welche Gefahren drohen durch den Mobilfunkstandard?* Abgerufen am 13.07.2020 von https://www.it-daily.net/it-sicherheit/mobile-security/23698-5g-welche-gefahren-drohen-durch-den-mobilfunkstandard

Kapilavai, S. & Schreier, J. (2019). *Die Rolle von Small Cells im 5G-Netz*. Abgerufen am 10.07.2020 von https://www.bandbreite.io/die-rolle-von-small-cells-im-5g-netz-a-855020/

KPMG Advisory GmbH. (2020). *Cloud Monitor: im Fokus der Digitalisierung.* Wien. Abgerufen am 22.07.2020 von https://home.kpmg/at/de/home/insights/2020/06/cloud-monitor-studie-2020.html

Krempl, S. (2019). Die Wahnsinns-Maschinen: Wo uns die neuen Super-Computer helfen können. *Focus*. Abgerufen am 28.07.2020 von https://www.focus.de/digital/dldaily/eine-ganz-neue-auf-der-quantenphysik-aufbauende-computergeneration-soll-komplexe-molekuele-wie-penicillin-simulieren-und-damit-etwa-die-medizin-oder-die-biotechnologie-sprunghaft-voranbringen-koennen-doch-die-welt-der-kleinen-teilchen-ist-eigensinnig-und-laesst-sich-noch-kaum-fuer-nuetzliche-rechenaufgaben-domestizieren-der-grosse-wettlauf-zum-magischen-quantencomputer_id_10173613.html

Lassnig, M., Stabauer, P., Güntner, G., Breitfuß, G., Mauthner, K., Stummer, M., Meilinger, A. (2016). *Industrie 4.0 in Österreich: Kenntnisstand und Einstellung zur digitalen Transformation durch Industrie 4.0 und neue Geschäftsmodelle in österreichischen Unternehmen.* Wien: Bundesministerium für Verkehr, Innovation und Technologie. Abgerufen am 02.07.2020 von https://www.bmk.gv.at/dam/jcr:a9580834-ae72-4176-911b-13a406e31ac1/industrie_4_0_in_oesterreich.pdf

Mell, P. & Grance, T. (2011). *The NIST Definition of Cloud Computing: Recommendations of the National Institute of Standards and Technology.* Gaithersburg, MD: National Institute of Standards and Technology (NIST). Abgerufen am 14.07.2020 von https://nvlpubs.nist.gov/nistpubs/Legacy/SP/nistspecialpublication800-145.pdf

Mey, S. (2019). *Ab 2020 wird 5G in Österreich ausgebaut: Chancen und Potenziale des neuen Standards*. Abgerufen am 03.07.2020 von https://www.derbrutkasten.com/5g-magenta-a1-drei-2020/

Prosser, D. (2019). *Cyber Criminals Target Poorly Protected Small Businesses.* Abgerufen am 28. Oktober 2019 von https://www.forbes.com/sites/davidprosser/2019/04/17/cyber-criminals-target-poorly-protected-small-businesses/#143d4de87177

Sauermann, M. (2019). *Studie: Mittelstand unterschätzt Gefahren von Cyberkriminalität*. Abgerufen am 28. Oktober 2019 von https://www.zdnet.de/88368347/studie-mittelstand-unterschaetzt-gefahren-von-cyberkriminalitaet/

Shamiulla, A. M. (November 2019). Role of Artificial Intelligence in Cyber Security. *International Journal of Innovative Technology and Exploring Engineering, 9*(1), S. 4628-4630.

Spectra Marktforschung. (2017). *Spectra Digi-Monitor Österreich (Teil 1).* Wien. Abgerufen am 18. November 2019 von https://www.spectra.at/fileadmin/news/2017/Spectra_Digi-Monitor_Teil1.pdf

Telefónica Deutschland/Stiftung Digitale Chancen. (2017). *Digital mobil im Alter: So nutzen Senioren das Internet. Zentrale Befunde einer Studie.* Berlin/München. Abgerufen am 18. November 2019 von https://www.telefonica.de/file/public/1016/2017-Digital-mobil-im-Alter-So-nutzen-Senioren-das-Internet-Zentrale-Befunde-einer-Studie.pdf

Verein Industrie 4.0. (2019). *Cyber-Security Leitfaden für Produktionsbetriebe: Schutz vor Cyberattacken - Mehr Wertschöpfung mit Security.* Wien. Abgerufen am 02.07.2020 von https://plattformindustrie40.at/wp-content/uploads/2020/05/WEB_Industrie4.0_Ergebnispapier_CyberSecurity_2019.pdf

Vogt, A. (2019). *Das Internet der Dinge im deutschen Mittelstand: Bedeutung, Anwendungsfelder und Stand der Umsetzung.* München: Deutsche Telekom. Abgerufen am 02.07.2020 von https://iot.telekom.com/resource/blob/data/183656/e16e24c291368e1f6a75362f7f9d0fc0/das-internet-der-dinge-im-deutschen-mittelstand.pdf

Wallden, P. & Kashefi, E. (April 2019). Cyber Security in the Quantum Era. *Communications of the ACM, 62*(4), 120-129.

Wenzel, S. (2020). *Was unterscheidet schwache KI & starke KI?* Abgerufen am 29.07.2020 von epicinsights: https://epic-insights.com/blog/schwache-ki/

Weyrauch, R. & Schmitz, P. (2019). *Quanten-Computing und die IT-Sicherheit.* Abgerufen am 28.07.2020 von Security Insider: https://www.security-insider.de/quanten-computing-und-die-it-sicherheit-a-838784/

Wirtschaftskammer Österreich. (2017). *Wirtschaftskraft KMU 2018.* Wien: Wirtschaftskammer Österreich. Abgerufen am 22.10.2019 von https://news.wko.at/news/oesterreich/wirtschaftskraft-kmu2018.pdf

Wirtschaftskammer Österreich. (2019). *Klein- und Mittelbetriebe in Österreich*. Abgerufen am 08.10.2019 von https://www.wko.at/service/zahlen-daten-fakten/KMU-definition.html

ZEIT online. (24.07.2019). *Bertelsmann-Studie: Ältere Menschen fühlen sich online unsicher*. Abgerufen am 18.11.2019 von https://www.zeit.de/digital/2019-07/bertelsmann-studie-senioren-internetnutzung-unterstuetzung

9 IMPRESSUM

KFV (KURATORIUM FÜR VERKEHRSSICHERHEIT)
SCHLEIERGASSE 18
1100 WIEN
T +43-(0)5 77 0 77-DW ODER -0
F +43-(0)5 77 0 77-1186
E-MAIL KFV@KFV.AT
WWW.KFV.AT

MEDIENINHABER UND HERAUSGEBER
Kuratorium für Verkehrssicherheit

VERLAGSORT
Wien

REDAKTION
Dr. Georg Plattner
Mag. Andrea Feymann

GRAFIK
Catharina Ballan
Patricia Jeßner, BA (eigene Darstellung)

COVER-FOTO
iStock (504397959)

SAFETY FIRST!

ISBN (PRINT) 978-3-903808-01-0

ISBN (PDF) 978-3-903808-00-3