ÖSTERREICHISCHE
FMA · FINANZMARKTAUFSICHT

DIGITALISIERUNG AM ÖSTERREICHISCHEN FINANZMARKT 2021

INHALTSVERZEICHNIS

Einleitung 5
Call for Input 6
Struktur des Berichts 7
Executive Summary 8
1 Strategien 10
1.1 Erwartete Zukunftsszenarien 10
1.2 Treiber der Digitalisierung 11
1.3 Digitalisierungsstrategie 12
1.4 Chancen der Digitalisierung 13
1.5 Digitaler Wettbewerb 15
1.6 Kooperation mit FinTechs / InsurTechs 16
1.7 Herausforderungen bei der Umsetzung 18
1.8 Gefragtes IT-Know-how 19
1.9 Hindernisse der Digitalisierung 22
1.10 Auswirkungen der COVID-19-Pandemie 23
1.11 Fazit und Handlungsfelder der FMA 24
1.12 Konsultation zu den Strategien 28
2 Produktgestaltung 29
2.1 Bankprodukte 29
2.1.1 Technologiegetriebene Produktinnovationen 29
2.1.2 Neue Produktarten 30
2.2 Versicherungsprodukte 31
2.2.1 Dunkelverarbeitung 31
2.2.2 Nutzung von Big Data 32
2.2.3 Verhaltensbasierte Produkte 32
2.2.4 Situative Versicherungen 33
2.2.5 Parametrische Versicherungen 34
2.2.6 Community based insurance 34
2.2.7 Sharing Economy basierte Produkte 35
2.2.8 Cyberversicherung 36
2.2.9 Kryptoassets-Polizzen 37
2.3 Fazit und Handlungsfelder der FMA 38
2.4 Konsultation zur Produktgestaltung 39

3 Vertrieb / Kundenschnittstelle 40
3.1 Trends bei den verschiedenen Kommunikationskanälen 40
3.2 Digitale Kommunikation in den Geschäftsprozessen 46
3.3 Automatisiertes Marketing 47
3.4 Vergleichsportale 48
3.5 Digitale Vertriebsplattformen 50
3.6 Fazit und Handlungsfelder für die FMA 51
3.7 Konsultation zum Vertrieb 52
4 Asset Management 53
4.1 IT-Systeme im Asset Management 53
4.1.1 Recherche 53
4.1.2 Front Office 54
4.1.3 Mid/Back Office 54
4.1.4 Softwareunterstützung der Asset Management Prozesse 55
4.2 Neue Anlageformen und Krypto-Assets 56
4.3 Fazit und Handlungsfelder für die FMA 58
4.4 Konsultation zum Asset Management 60
5 IT-Infrastruktur 61
5.1 IT-Systemlandschaft am österreichischen Finanzmarkt 61
5.2 Life-Cycle der eingesetzten IT-Systeme 63
5.3 Konzentrationen bei den genutzten Applikationen 67
5.4 Fazit und Handlungsfelder der FMA 69
5.5 Konsultation zum Einsatz von IT-Systemen 70
6 IT-Verflechtungen 71
6.1 IT-Dienstleisterlandschaft 71
6.2 Abhängigkeitsnetze pro Sektor 74
6.3 Konzentration der wichtigsten Dienstleister 77
6.4 Zertifizierungen von IT-Dienstleistern 78
6.5 Fazit und Handlungsfelder der FMA 80
6.6 Konsultation zu den IT-Verflechtungen 81
7 Digitale Technologien 82
7.1 Cloud Services 82
7.2 Blockchain 86
7.3 Robotic Process Automation 87
7.4 Big Data Analytics 88

7.5 Machine Learning 89
7.6 Automatisierte Datenschnittstellen 90
7.7 Natural Language Processing 91
7.8 Einsatzgebiete digitaler Technologien 92
7.9 Konsultation zu den digitalen Technologien 94
8 IKT-bezogene Vorfälle 95
8.1 Cybervorfälle 95
8.1.1 Anzahl der Cybervorfälle 96
8.1.2 Häufigste Angriffsarten 97
8.1.3 Finanzielle Verluste 99
8.2 Andere schwerwiegende Betriebs- oder Sicherheitsvorfälle 100
8.2.1 Ursachen 100
8.2.2 Auswirkungen 101
9 Post-COVID-19 bezogene IKT-Risiken 102
9.1 Verwendung persönlicher Geräte 102
9.2 Zulässigkeit persönlicher Applikationen 104
9.3 Wiedereinsetzung nicht überwachter IT-Systeme 106
9.4 Schulungen zu Social Engineering 106
10 FMA-Cyber Maturity Level Assessment 108
11 FMA-Cloud Maturity Level Assessment 115
11.1 Fazit und Handlungsfelder der FMA 120
11.2 Konsultation zu den Cyber-Risiken 121
12 Abkürzungsverzeichnis 122

EINLEITUNG

Die Digitalisierung ändert die Rahmenbedingungen am Finanzmarkt, bringt neue Auslegungsfragen und Risiken für beaufsichtigte Unternehmen und stellt die vorhandenen Aufsichtstools auf den Prüfstand.

Die FMA hat deshalb im Jahr 2021 ihre Analyse zur Digitalisierung am österreichischen Finanzmarkt fortgeführt. Mit diesem Bericht wollen wir einen Zwischenstand präsentieren, der konkret den Stand der Digitalisierung am österreichischen Finanzmarkt und die Einsatzbereiche digitaler Technologien darstellt. Wir wollen außerdem in komprimierter Form eine Einschätzung über Treiber, Trends und mögliche künftige Entwicklungen bieten. Damit schaffen wir auch für uns, die FMA, eine bessere Grundlage, um bei der Digitalisierung am Ball zu bleiben und Entwicklungen richtig einzuschätzen.

Im Zentrum der Aufmerksamkeit der FMA stehen dabei die Risiken. Deshalb beleuchten wir in diesem Bericht die Digitalisierung des österreichischen Finanzmarktes vor allem aus einer Risikosicht. Dabei gehen wir strikt nach dem Prinzip der Technologieneutralität vor: Die FMA beaufsichtigt keine Technologien, sondern hat primär Risiken im Blick. Gleiche Risiken verlangen gleich hohe Aufsichtsanforderungen, egal, ob sie aus digitalen oder analogen Geschäftsmodellen oder Prozessen entstehen. Die dem vorliegenden Bericht zugrundeliegende Studie hilft der FMA, die Risiken der Digitalisierung adäquat und frühzeitig einschätzen zu können.

Um neue Erkenntnisse zu Chancen, Trends und Risiken der Digitalisierung erlangen zu können, haben wir als Grundlage für diesen Bericht eine umfangreiche Erhebung am österreichischen Finanzmarkt durchgeführt. Wir haben dazu im Sommer 2021 von den beaufsichtigten Unternehmen aus allen[1] Sektoren des Marktes Rückmeldungen erhalten. Dabei konnten wir in fast allen Sektoren des Finanzmarkts eine beinahe vollständige Marktabdeckung erreichen:

Sektroteilnehmer:

- 32 Versicherungsunternehmen (VU)[2]
- 8 Pensionskassen (PK)
- 8 Betriebliche Vorsorgekassen (BVK)
- 49 (explizit) bzw. 440 (implizit) Kreditinstitute (KI)
- 6 Zahlungsinstitute (ZI)

[1] Aufgrund der geringen Anzahl der Teilnehmer aus den Sektoren Marktinfrastrukturen und virtuelle Asset Provider wurden die Ergebnisse in diesen beiden Sektoren in den vorliegenden Bericht nicht aufgenommen, um keine Rückschlüsse auf individuelle Unternehmen zu ermöglichen.

[2] Versicherungsunternehmen, die unter Solvency II fallen.

- 79 Wertpapierdienstleister und Wertpapierfirmen (WPF)
  dh 64 WPF und 15 WPDLU
- 23 Verwaltungsgesellschaften (KAG, ImmoKAG, AIFM)
- 2 virtuelle Asset Provider (VASP)
- 3 Marktinfrastrukturen (MI)

Wir glauben, mit dieser enorm hohen Marktabdeckung auch 2021 die umfassendste und gleichzeitig detaillierteste Daten- und Informationsbasis geschaffen zu haben, die es derzeit zum Thema Digitalisierung am österreichischen Finanzmarkt gibt.

CALL FOR INPUT

Der vorliegende Bericht soll auch dafür genutzt werden, eine breitere Diskussion zur Digitalisierung des österreichischen Finanzmarktes anzustoßen und den Dialog am österreichischen Finanzmarkt zu den Implikationen der Digitalisierung in den Finanzdienstleistungen zu intensivieren. Dafür ist uns Ihr Input besonders wichtig.

Wir laden Sie, unsere Stakeholder – beaufsichtigte Unternehmen, die Investoren, Sparer, Versicherungsnehmer und die Verbraucherinnen und Verbraucher, öffentliche Institutionen und die interessierte Öffentlichkeit – ein, die in diesem Bericht skizzierten Erkenntnisse und Schlussfolgerungen kritisch zu hinterfragen und um Ihre Sichtweisen, Erfahrungen und Lösungsansätze anzureichern. Am Ende jedes Kapitels dieses Berichtes haben wir dazu als Orientierungshilfe auch einige Fragen an Sie formuliert.
Bis 28.2.2022 können Sie dazu formlos Ihren Input zum Bericht an digitalisierung@fma.gv.at übermitteln. Wir werden Ihren Input gerne aufnehmen und bei der strategischen Planung der FMA bzw. bei der Festlegung der Aufsichtsschwerpunkte berücksichtigen.

STRUKTUR DES BERICHTS

Der Bericht ist in die folgenden Teile gegliedert:

- **Strategien** der beaufsichtigten Unternehmen in Bezug auf die Digitalisierung (Kapitel 1),
- **neue Geschäftsmodelle:** neue Ökosysteme, neue digitalisierungsgetriebene Produkte, neue Kundenschnittstellen und der Einsatz digitaler Technologien in den einzelnen Geschäftsprozessen (Kapitel 2 bis 4),
- **neue digitale Technologien:** Verbreitung der am Finanzmarkt eingesetzten Technologien, die damit verbundenen Chancen und Risiken und Praxisbeispiele (Kapitel 7),
- **neue Risiken:** Anpassungen in der IT-Infrastruktur und Cyber-Risiken (Kapitel 5 bis 11 exkl. Kapitel 7).

Aufgrund der Erkenntnisse der Recherche zu internationalen, europäischen und nationalen Initiativen iZm der Digitalisierung am Finanzmarkt und der Ergebnisse der Erhebung in den einzelnen Sektoren sowie aufgrund sonstiger Wahrnehmungen aus der Aufsichtstätigkeit wurden mögliche Implikationen der Digitalisierung in den einzelnen Sektoren für die Aufsichtstätigkeit der FMA identifiziert und mögliche Handlungsoptionen für die FMA abgeleitet.

Hinweis:

Im vorliegenden Bericht wird aufgrund der leichteren Lesbarkeit durchgängig die männliche Form verwendet. Diese Bezeichnungen sind als geschlechtsneutral zu betrachten. Es wird ausdrücklich darauf hingewiesen, dass sich alle personenbezogenen Formulierungen grundsätzlich gleichermaßen auf Frauen und Männer beziehen. Die rechtlichen Grundlagen bleiben durch diesen Bericht unberührt. Über die gesetzlichen Bestimmungen hinausgehende Rechte und Pflichten können aus diesem Dokument nicht abgeleitet werden. Trotz sorgfältiger Aufbereitung und Recherche übernimmt die FMA keine Haftung für die Richtigkeit und Vollständigkeit der Daten und Inhalte in diesem Bericht.

EXECUTIVE SUMMARY

Zusammenfassend können aus der Studie folgende wesentliche Fakten und Trends für den österreichischen Finanzmarkt abgeleitet werden:

1. **Strategien / Governance:** Der Bedarf an externer Unterstützung im IKT-Bereich in Form von Beratung, Auslagerungen und Ad-hoc-Aufträgen wird zunehmen; die Abgrenzung zwischen den für das Kerngeschäft relevanten Prozessen und Dienstleistungen und dem Bezug sonstiger Dienstleistungen (bloße Delegationen) wird komplexer. IT-Skills werden für die Schlüsselfunktionen neben den eigentlichen Fachkompetenzen bedeutsamer.
   Seit 2018 haben sich die Erwartungen der beaufsichtigten Unternehmen in Bezug auf BigTech und FinTech-StartUps verändert: Dass BigTech-Unternehmen in ihre Märkte eintreten, halten die etablierten Finanzmarktteilnehmer derzeit für deutlich weniger wahrscheinlich als noch 2018. Dagegen steigt die Bedeutung von FinTech-/InsurTech-StartUps, was sich nicht nur durch deren erhöhte Wahrnehmung als Konkurrenz, sondern auch durch die intensivierte Kooperation äußert.
2. **Produkte / Neue Geschäftsmodelle:** Die Produktlandschaft passt sich sukzessive an die neuen digitalen Möglichkeiten an. Im Vordergrund stehen technologiegetriebene Innovationen, bei denen die herkömmlichen Produkte und Dienstleistungen auf die neuen Technologien umgestellt werden. Neue Produktarten werden seit 2018 zwar in einem stärkeren Ausmaß, aber in der Regel noch immer nur partiell bzw. experimentell lanciert.
3. **Vertrieb:** Kundenkontakt erfolgt zunehmend über digitale Kanäle (z.B. Social Media, Chats, Videokonferenzen) direkt von den beaufsichtigten Unternehmen aus, insbesondere im pre-sales-Bereich. Konventionelle Wege des Vertriebs verlieren durch den Einsatz von digitalen Vertriebsplattformen, Vergleichsportalen und Robo advice zunehmend an Bedeutung. Insbesondere bei der Nutzung von Videokonferenzen und sozialen Medien lässt sich seit 2018 eine starke Steigerung erkennen; ersteres wurde durch die COVID-19-Pandemie intensiviert und letzteres unter anderem durch Konkurrenzdruck in der Neukundenakquise verstärkt.
4. **Technologien:** Trotz der zunehmenden Verbreitung von Kryptoassets investieren die beaufsichtigten Unternehmen derzeit kaum in dieses Segment. Das gilt sowohl für den Eigenbestand als auch für die Kundengelder. Wegen offener regulatorischer Fragen hat sich die Blockchaintechnologie bislang noch nicht als Basis für neue Produkte bzw. Dienstleistungen etablieren können. Dies könnte sich mittelfristig durch neue Regelungen wie die MICA ändern. Der Vergleich mit 2018 zeigt jedenfalls eine zunehmende Bedeutung von Cloudservices.

5. **IT-Applikationen:** Der Trend geht in Richtung konsolidierter, durch Updates möglichst lang einsetzbarer, Standardsoftware. Dadurch kann sich langfristig die Vielfalt der Anbieter reduzieren und eine Konzentration auf wenige große Softwareentwickler stattfinden.
6. **Vernetzung / IKT-Sicherheit:** Der Grad der Vernetzung des Finanzsektors mit Dienstleistern steigt durch die Digitalisierung. Das IT-Risiko beaufsichtigter Unternehmen verlagert sich daher zunehmend an die Schnittstelle zu Dritten (Kooperationspartner, IT-Dienstleister). Gleichzeitig steigt aber auch die Qualität der eigenen IT-Sicherheitsmaßnahmen der beaufsichtigten Unternehmen. Dies zeigen auch die von der FMA entwickelten Cyber und Cloud Maturity Level Assessments, die erstmalig einen Einblick in die Cyber-Resilienz des österreichischen Finanzmarktes erlauben. Im Hinblick auf die sich laufend weiterentwickelnden Cyberbedrohungen und die steigenden digitalen Kundenansprüche erfordert die IKT-Sicherheit laufende Anpassungen der Sicherheitsmaßnahmen.

Die FMA führt Digitalisierungsstudien durch, weil die verstärkte Verwendung neuer Informations- und Kommunikationstechnologien und die dadurch bedingten Veränderungen in den Geschäftsmodellen, in der Produktlandschaft und in der Interaktion mit den Kunden für die Aufsichtstätigkeit von großer Bedeutung sind.

Aus den Ergebnissen der vorliegenden Digitalisierungsstudie können die folgenden für die Aufsichtstätigkeit besonders relevanten Themenbereiche abgeleitet werden:

- die externe Erbringung von IKT-Leistungen, insbesondere im Wege von Auslagerungen, und die damit verbundenen Risiken,
- die Identifizierung von neuen Ansteckungskanälen und Konzentrationsrisiken,
- die Interaktionen zwischen beaufsichtigten und nichtbeaufsichtigten Marktteilnehmern sowie die genaue Abgrenzung des Umfangs konzessionspflichtiger Geschäfte insbesondere in Gruppenstrukturen,
- die Anforderungen an Vorstände und Schlüsselfunktionen bei Anwendung von digitalen Geschäftsmodellen,
- die gleichwertige Sicherung der Kundeninteressen für digitale, wie für traditionelle Vertriebs- und Kommunikationsformen,
- das Monitoring der weiteren Entwicklung von Krypto-Assets als Veranlagungsinstrument und
- die Intensivierung der Überwachung von Cyber-Risiken und Ableitung von Aufsichtsschritten.

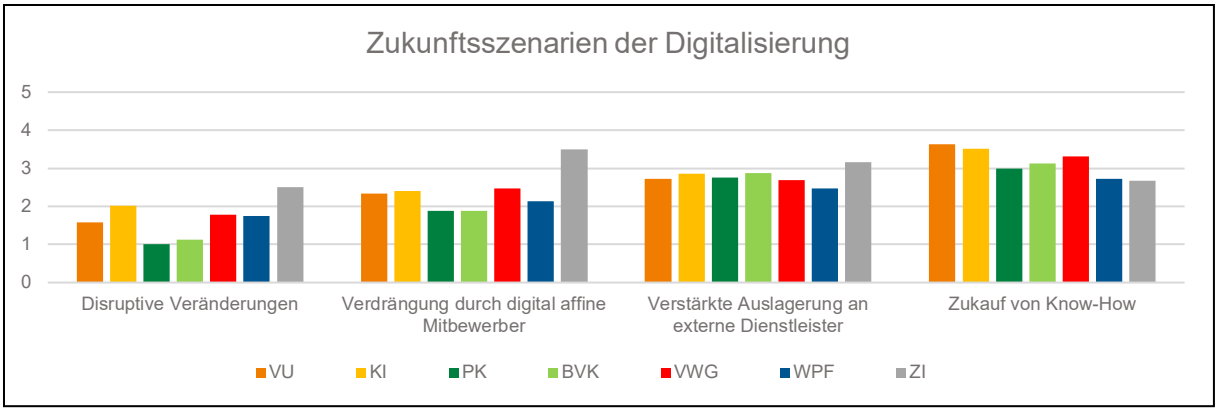
Die Ergebnisse der Studie zeigen, dass die bisher von der FMA gesetzten Maßnahmen in die richtige Richtung gehen. Konkrete weitere strategische und operationale Schritte werden unter Berücksichtigung des Feedbacks der teilnehmenden Unternehmen sowie anderer Stakeholder gesetzt werden.

1 STRATEGIEN

1.1 ERWARTETE ZUKUNFTSSZENARIEN

Die Unternehmen am österreichischen Finanzmarkt erwarten im Aggregat eine kontinuierliche Fortsetzung bisheriger Trends in der Digitalisierung. Es wird dabei ein verstärkter Bedarf an externer Unterstützung in Form von Beratung, Auslagerungen und Ad-hoc-Aufträgen antizipiert. Je digitaler das Geschäftsmodell, desto höher sind allerdings die Erwartungen einer disruptiven Entwicklung.

Die Erwartungen des österreichischen Finanzmarkts hinsichtlich möglicher Zukunftsszenarien haben sich seit der letzten FMA-Digitalisierungsstudie im Jahr 2018 nicht nennenswert verschoben,[3] wie auch die Einschätzungen der beaufsichtigten Unternehmen anhand einer Zahlenskala von 5 („sehr wahrscheinlich“) bis 1 („sehr unwahrscheinlich“) in der folgenden Graphik verdeutlichen:



Die Prognosen zwischen den Sektoren sind dabei großteils homogen:

- Als wahrscheinlichstes Zukunftsszenario wird insgesamt ein verstärkter Bedarf an externer Unterstützung in Form von Beratung, Auslagerungen und Ad-hoc-Aufträgen antizipiert.

  Die Tendenzen zur Beauftragung von externen Dienstleistern unterscheiden sich hier jedoch stark von Unternehmen zu Unternehmen. Digitalisierungsgetriebene Auslagerungen schätzen immer noch deutlich weniger als die Hälfte der Beaufsichtigten als „sehr wahrscheinlich“ oder „eher wahrscheinlich“ ein. Derartige Auslagerungen können zwar die Effizienz steigern, haben aber gleichzeitig Implikationen für die Fähigkeit, komplexe Dienstleistungen In-House zu erbringen, und für die Themen IT-Sicherheit sowie Konzentrationsrisiken.

[3] *FMA, Digitalisierung am österreichischen Finanzmarkt – Stand, Ausblick, Call for Input, Juni 2019.*

- Revolutionäre bzw. disruptive Veränderungen werden von Zahlungsinstituten (ZI) und Providern virtueller Assets (VASP) als überdurchschnittlich wahrscheinlich gesehen, was die vergleichsweise hohe Dynamik in diesen relativ jungen und digitalisierungsbasierten Marktsegmenten widerspiegelt. Pensionskassen (PK) und Vorsorgekassen (BVK) schließen dagegen Disruption und Verdrängungseffekte besonders kategorisch aus, was sich direkt aus den entsprechenden Geschäftsmodellen dieser Unternehmen erklären lässt.

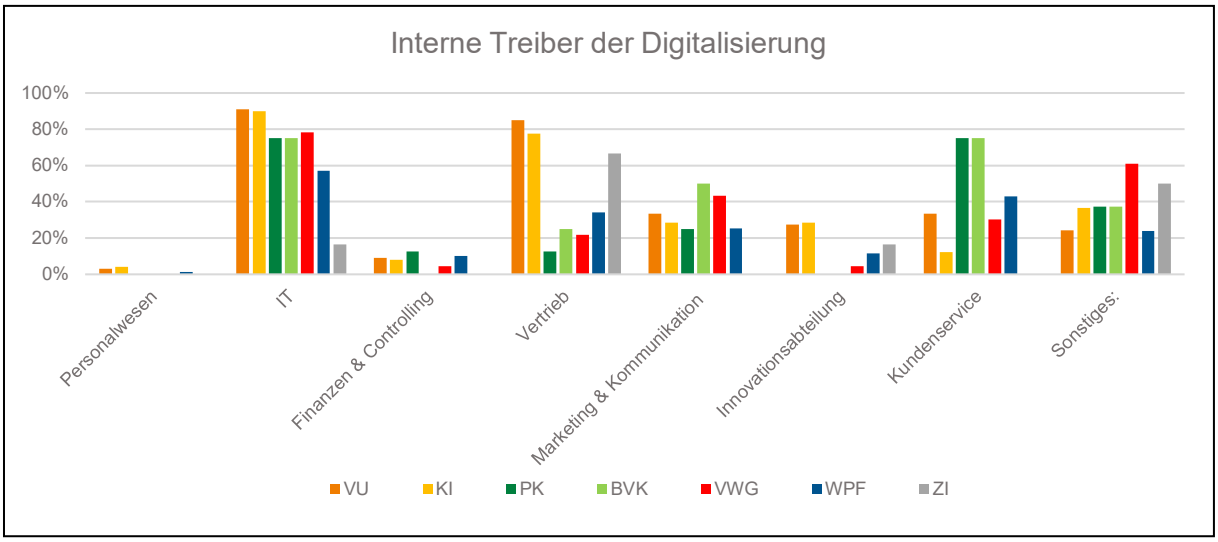
1.2 TREIBER DER DIGITALISIERUNG

Haupttreiber der Digitalisierung in den Unternehmen selbst ist in fast allen Branchen nach wie vor die **IT-Abteilung.** Das weist darauf hin, dass internes technisches Know-How trotz häufig bestehender Auslagerungen ein wichtiger Bestandteil digitaler Innovation ist und die IT-Abteilungen in vielen Unternehmen eine über die bloße technische Administration hinausgehende Rolle einnehmen.

Gleichzeitig werden **Bereiche mit einer direkten Kundenschnittstelle** (Vertrieb, Kundenservice, Marketing und Kommunikation) als wichtiger Antrieb für die Digitalisierung wahrgenommen. Der Fokus der Unternehmen auf dieses Gebiet zeigt einen gewissen Konkurrenzdruck beim digitalen Kontakt zu den Kunden auf. Sowohl beim Marketing der Produkte und Dienstleistungen als auch bei der Festigung bestehender Kundenbeziehungen spielen moderne Kommunikationskanäle eine entscheidende Rolle.

- Der wichtigste unternehmensinterne Treiber der Digitalisierung ist in fast allen Finanzsektoren die **IT** (VU 91%, KI 90%, BVK 75%, Verwaltungsgesellschaften [KAG, ImmoKAG, AIFM] 78% und WPF/WPDLU 57%). Bis auf Zahlungsinstitute gaben in jedem Sektor mehr als 50% der Unternehmen an, dass die IT-Abteilung ein interner Haupttreiber der Digitalisierung sei.
- Gleichzeitig werden **Vertrieb und Kundenservice** als wichtiger Antrieb für die Digitalisierung wahrgenommen. Etwa 80% der VU und KI haben den Vertrieb idZ als Kernelement genannt, bei PK und BVK nimmt diesen Platz geschäftsmodellbedingt das Kundenservice mit je rund 75% ein. Da die Kundenkommunikation bzw. die Erbringung von Beratungsleistungen in den einzelnen Sektoren besonderen aufsichtsrechtlichen Regelungen unterworfen ist, ist es für die FMA essentiell, mit diesen Entwicklungen Schritt zu halten, um ihrem Aufsichtsauftrag gerecht zu bleiben.

- Finanzen & Controlling sowie Personalwesen haben als Digitalisierungstreiber hingegen nur minimalen Zuspruch erhalten. Personal- und Finanzabteilungen werden somit etwa bei Innovationen zur Effizienzsteigerung im administrativen Bereich offenbar weniger als treibende Kraft gesehen.
- In der Zwischenzeit verfügen über 20% der KI und VU über eine eigene **Abteilung für digitale Innovation**; diese Zahl ist seit der FMA-Digitalisierungsstudie 2018 gewachsen.



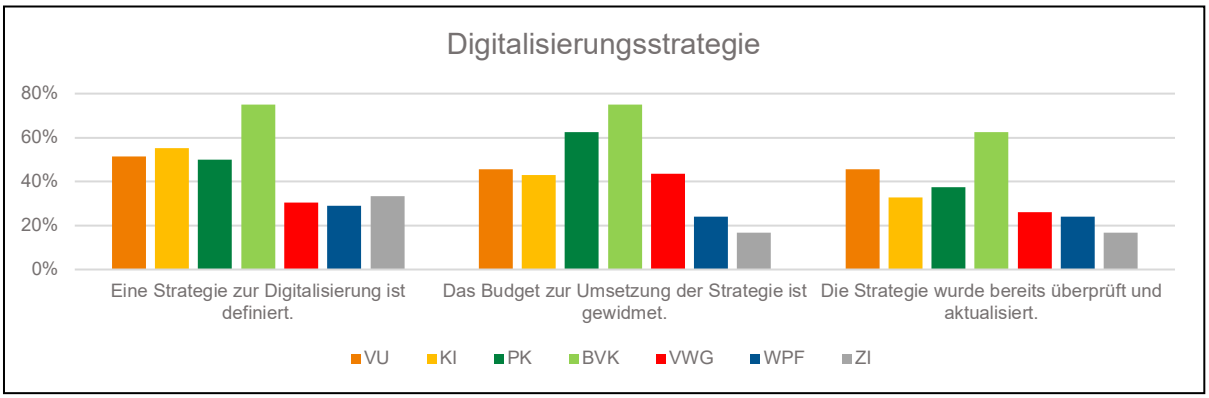
1.3 DIGITALISIERUNGSSTRATEGIE

Nahezu alle beaufsichtigten Unternehmen haben in der Zwischenzeit zumindest teilweise die Digitalisierung in ihre Strategie integriert. Vor drei Jahren zeigte sich noch ein vollkommen gegensätzliches Bild: Bei lediglich 20% der Unternehmen war Digitalisierung Teil der Strategie. Fortschritt im Bereich Digitalisierung hat sich somit über die vergangenen Jahre zu einem essentiellen Ziel der beaufsichtigten Unternehmen in Österreich entwickelt.

Zwischen den einzelnen Finanzsektoren bestehen jedoch große Unterschiede:

- So haben etwa nur etwas mehr als ¼ (29%) der WPF eine explizite Digitalisierungsstrategie vollständig definiert. Weiters haben etwa 2/3 der VWG und der ZI Digitalisierung erst teilweise in ihre Strategie integriert.
- Die größten Fortschritte haben dagegen die PK und BVK verzeichnet, die 2018 im Hinblick auf die strukturellen Unterschiede ihrer Geschäftsmodelle der Ausrichtung ihrer Strategie an die

Digitalisierung noch keine so große Bedeutung beigemessen haben. So haben etwa ¾ (75%) der BVK eine explizite und vollständige Digitalisierungsstrategie definiert.



Über die Branchen hinweg betrachtet, hat fast die Hälfte (44%) der beaufsichtigten Unternehmen und somit doppelt so viele wie 2018, ihr Zielbild und die Digitalisierungsstrategie vollständig mit messbaren Zielen und Budget unterlegt (24% der WPF, 63% der PK, 45% der VU, 43% der KI, 43 % der VWG, 17% der ZI und 75% der BVK).

Von den übrigen Unternehmen haben mittlerweile fast alle zumindest implizit bzw. in Teilbereichen eine Digitalisierungsstrategie definiert bzw. dieses Budget gewidmet.

Bezüglich Digitalisierungsstrategien lässt sich kein klarer Zusammenhang mit den anderen Fragestellungen herstellen; eine solche Strategie scheint somit nicht zwingend Voraussetzung für Innovation und Digitalisierung zu sein, wenngleich eine solche - wenn vorhanden - ein klares Symbol für das Engagement des Managements in dieser Thematik darstellt.

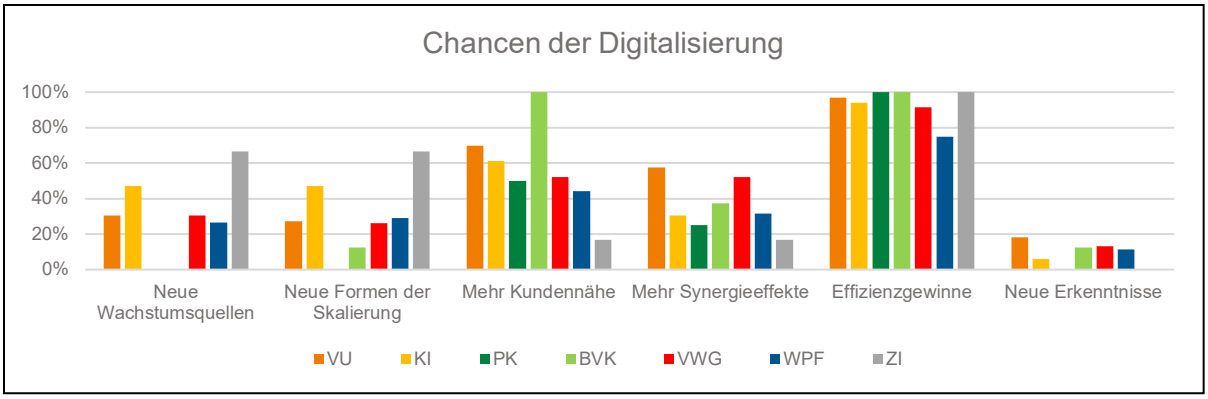
1.4 CHANCEN DER DIGITALISIERUNG

Effizienzgewinne und mehr Kundennähe werden praktisch über alle Sektoren hinweg als größte Chancen der Digitalisierung gesehen.

Insgesamt sehen die beaufsichtigten Unternehmen unterschiedliche Einsatzmöglichkeiten für digitale Technologien und fokussieren sich dabei am stärksten auf die Effizienzerhöhung in bestehenden Prozessen. Der unternehmensinterne Fokus überwiegt aktuell auch bzgl. der Potentiale der Digitalisierung. Es werden dabei eher inkrementelle als revolutionäre Verbesserungen erwartet:

- Alle Sektoren sehen **Effizienzgewinne** als bedeutendes Potential der Digitalisierung. Die Bandbreite der Einschätzungen liegt zwischen 100% (PK, BVK, ZI) und 75% (WPF).
- **Neue Wachstumsquellen** und **Formen der Skalierung** werden jeweils immerhin von 47% der KI erhofft, auf die anderen Sektoren trifft dies jedoch nur zu etwa 30% (VU, VWG, WPF) oder gar nicht (PK, BVK, MI) zu. Eine Ausnahme stellt der Sektor der ZI dar, die hier deutlich über 50% lagen. Neue Erkenntnisse (zB im Bereich Big Data Analytics) erwarten sich unabhängig vom Finanzmarktsektor nur einzelne Unternehmen.
- Die Möglichkeit, über digitale Medien **mehr Nähe zum Kunden** zu erreichen, wird als bedeutender Vorteil eingestuft. Konsistent mit der Einschätzung von Vertrieb und Kundenbetreuung als Treiber der Digitalisierung stufen mehr als 50% der beaufsichtigten Unternehmen dies als wichtige Chance ein, bei VU sind es rund 70% und bei BVK sogar 100%.
- Obwohl bei den internen Treibern der Digitalisierung vor allem Abteilungen mit Kundenkontakt prominent gereiht wurden, werden bis zu einem gewissen Grad auch Synergieeffekte als noch bedeutendere Chancen wahrgenommen.

Die folgende Graphik liefert einen Überblick über die Ergebnisse pro Sektor:

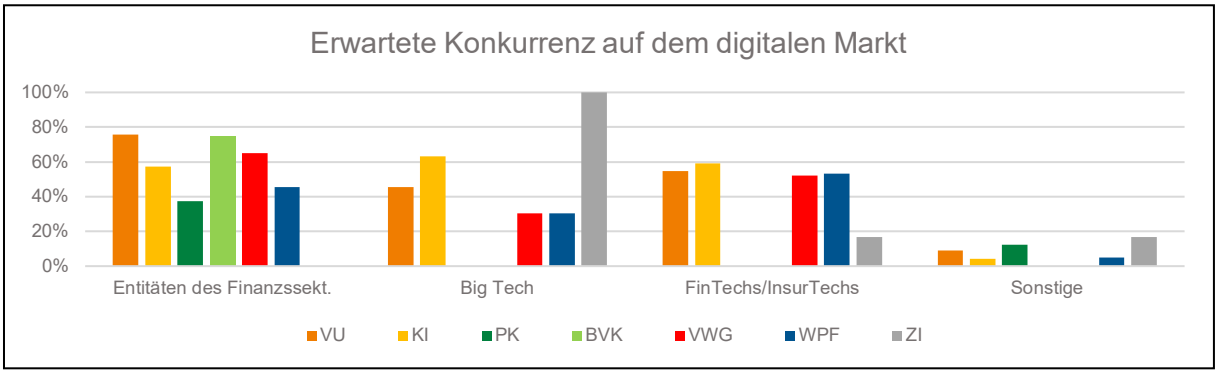


Das Gesamtbild und die oben hervorgehobenen Beobachtungen sind den Ergebnissen der Studie im Jahr 2018 relativ ähnlich. In einzelnen Sektoren hat es jedoch gewisse Verschiebungen gegeben, so wurde im Bankensektor damals die Chance auf mehr Kundennähe als relevanter eingestuft als jene für Effizienzgewinne.

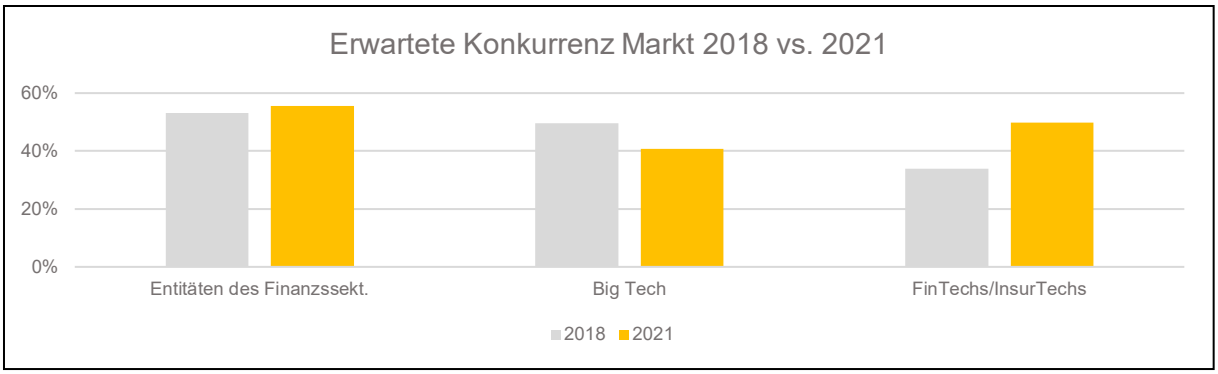
1.5 DIGITALER WETTBEWERB

Als größte Konkurrenten werden von den meisten beaufsichtigten Unternehmen nach wie vor andere etablierte Finanzmarktteilnehmer gesehen. Dabei zeigen sich allerdings starke sektorspezifische Unterschiede. Diese lassen sich auf ökonomische und regulatorische Unterschiede in den Geschäftsfeldern zurückführen, welche den Markteintritt von unterschiedlichen Konkurrenten aus Sicht der Unternehmen mehr oder weniger wahrscheinlich machen.

Während ZI, VASP und KI das Konkurrenzpotential von BigTech am höchsten einschätzen, erwarten die VU und VWG die stärkste Konkurrenz von anderen etablierten Unternehmen in ihrem Sektor. Nur die WPF nehmen FinTechs als größte Konkurrenz wahr. PK und BVK sehen ob ihres Geschäftsmodells allgemein wenig Konkurrenz auf dem digitalen Markt und sehen nur andere PK bzw. BVK als potentielle Mitbewerber.



Gesamtheitlich betrachtet haben sich die Erwartungen der Unternehmen seit 2018 insbesondere in Bezug auf BigTech- und FinTech-StartUps verändert:



Dass BigTech-Unternehmen aggressiv in ihre Märkte eintreten, halten die beaufsichtigten Unternehmen derzeit für deutlich weniger wahrscheinlich als noch 2018. Dies könnte daran liegen, dass sich dieses Szenario - abgesehen von einigen Experimenten - noch nicht verstärkt realisiert hat. In diesem Zusammenhang analysierte die Bank für Internationalen Zahlungsausgleich[4] die Möglichkeit der künftigen Einnahme einer marktbeherrschenden Stellung durch BigTechs, die sich vor allem auf Basis deren Datensätze aus E-Commerce und sozialen Medien ergeben könnte. Auch die Bereitschaft der Kunden, bei BigTechs auch Versicherungsprodukte zu kaufen, scheint gerade in der Corona-Krise extrem gestiegen zu sein.[5]

Im Gegensatz dazu werden von den beaufsichtigten Unternehmen zunehmend FinTech-/InsurTech-StartUps als potentielle Konkurrenten wahrgenommen.

Gleichzeitig wächst die Anzahl der Kooperationen mit diesen Akteuren. Beides weist auf eine stärkere Bedeutung von StartUps für den Finanzmarkt hin. Dieser Eindruck wird auch dadurch gestützt, dass einige Unternehmen, die ursprünglich als „StartUp“ charakterisiert wurden, Konzessionen für Finanzdienstleistungen erhalten und am Markt reussiert haben.

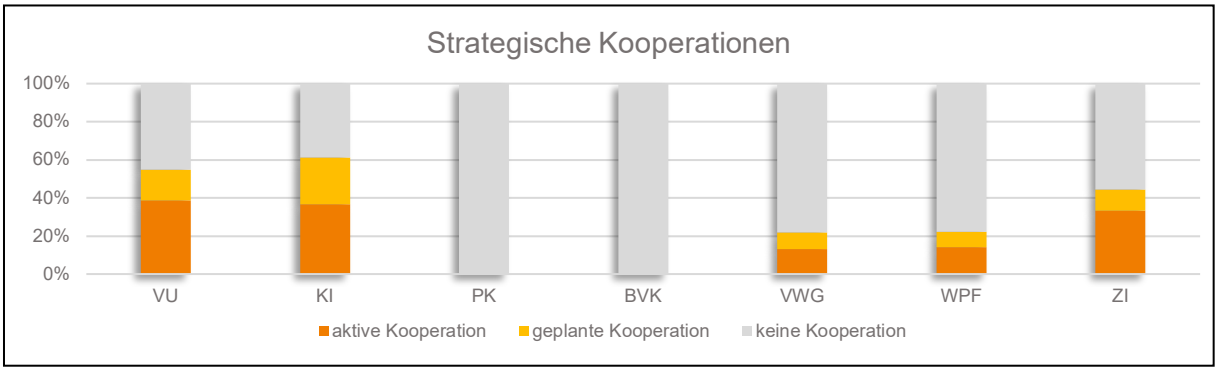
1.6 KOOPERATION MIT FINTECHS / INSURTECHS

Der Trend, mit FinTech-/InsurTech-StartUps Kooperationen einzugehen, setzt sich stetig fort. Dadurch konnten sich diese Unternehmen in einigen digitalen Nischen etablieren.

- Vor allem VASP, VU, KI und ZI kooperieren mit FinTechs/InsurTechs. Dies korreliert mit der Sorge der ZI, VASP, Banken und Versicherer, dass Google, Amazon & Co als digitale Quereinsteiger mit neuen Produkten und Dienstleistungen in den Finanzmarkt eintreten könnten.
- PK, BVK und MI sind dagegen bislang keine strategischen Kooperationen mit FinTechs eingegangen.

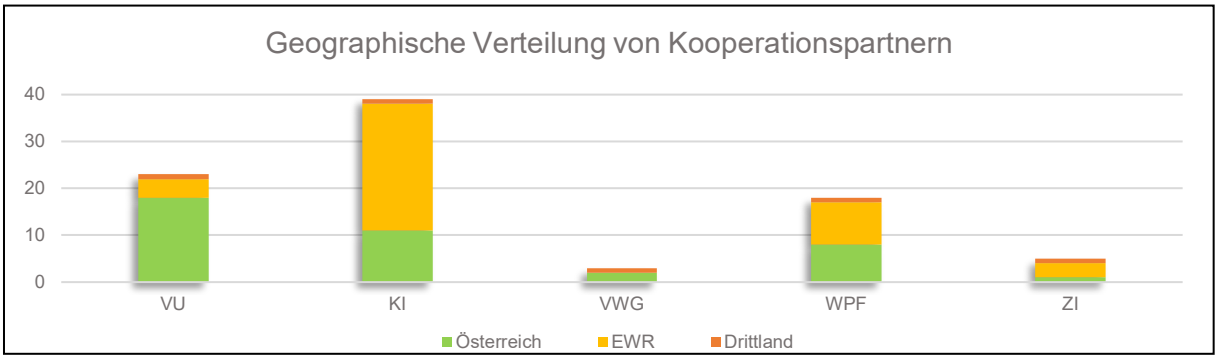
Ungeachtet der Sorge einiger beaufsichtigter Unternehmen, dass FinTechs/InsurTechs künftig zu Konkurrenten werden könnten, geht der österreichische Finanzmarkt davon aus, dass die Zahl der Kooperationen voraussichtlich auch in den nächsten drei Jahren steigen wird. Bis 2024 will jeweils mehr als die Hälfte der KI und VU zumindest mit einem FinTech/InsurTech kooperieren.

[4] Vgl. BIZ-Bulletin 45, https://www.bis.org/publ/bisbull45.pdf.
[5] Mehr als 50 % der Kunden wären demnach zu einem Kauf von Versicherungspolicen bei Google & Co. bereit. Siehe World Insurance Report 2021, https://worldinsurancereport.com.



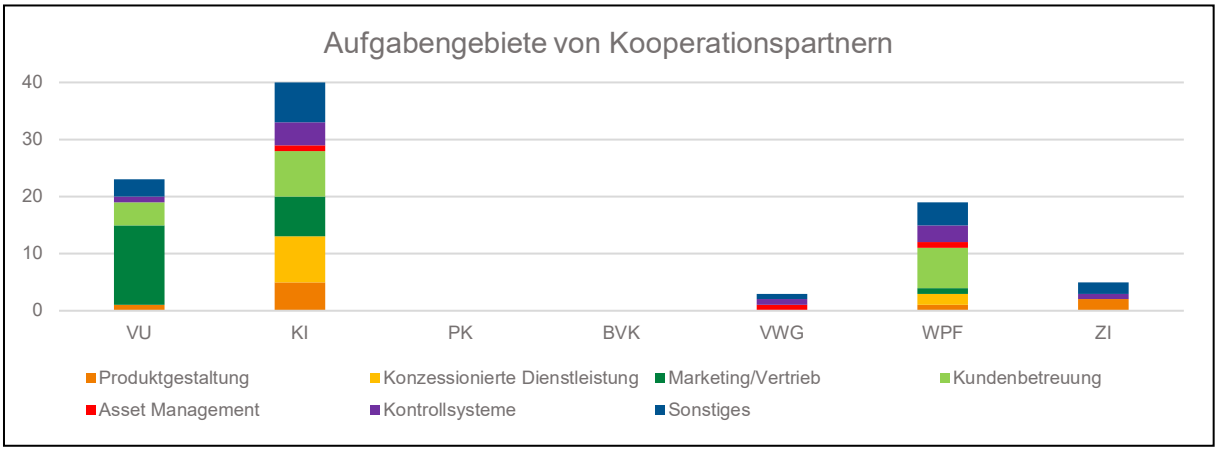
Betrachtet man die geographische Verteilung der Kooperationen mit StartUps, zeigt sich ein Unterschied zwischen den Sektoren:

- Während VU in erster Linie mit österreichischen Unternehmen kooperieren,
- arbeiten KI und WPF (sowie in weit geringerem Ausmaß VWG, VASP und ZI) überwiegend mit ausländischen StartUps, zumeist aus anderen EWR-Ländern, zusammen.



Hinsichtlich der Aufgabengebiete, in welchen Kooperationen mit StartUps zum Einsatz kommen, ist festzuhalten, dass

- bei VU Prozesse und Tools iZm Kundenbetreuung und Vertrieb im Fokus stehen,
- während in anderen Sektoren eine größere Vielfalt an Kooperationsfeldern zu beobachten ist: Neben kundenbezogenen Themen werden StartUps in diesen Sektoren auch teilweise zB in die konzessionierte Dienstleistung selbst und in Kontrollsysteme integriert.

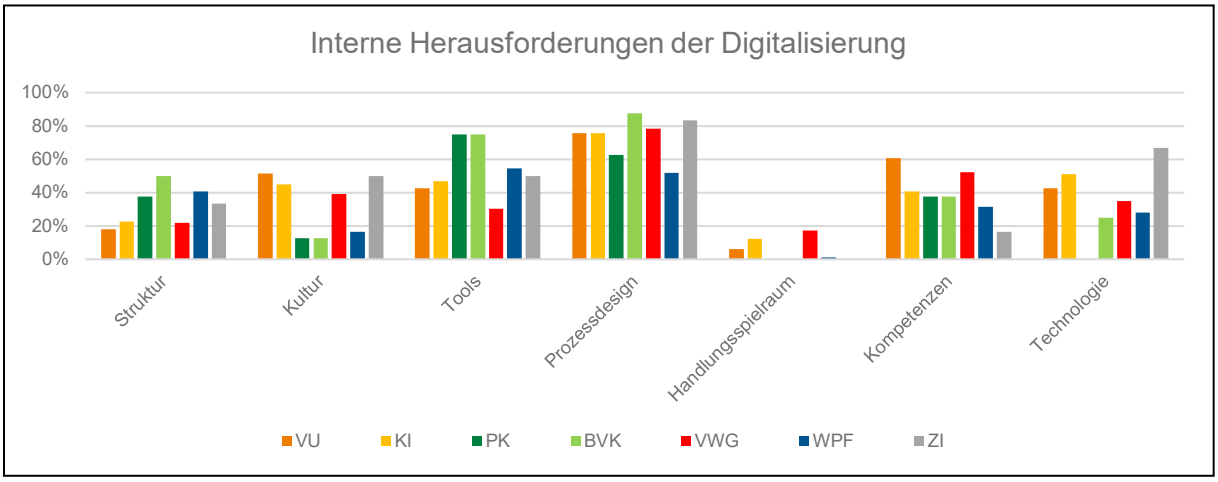


Insgesamt etablieren sich StartUps als Teil des österreichischen Finanzmarktes. Dabei sind Kooperationen mit konzessionierten Unternehmen ein logischer Schritt, um regulatorische Know-How-basierte bzw. finanzielle Einstiegshürden zu überwinden. Gleichzeitig bringen diese neuen Akteure Technologien und kreative, digitale Herangehensweisen in den Markt ein.
Somit stellt die Szene der FinTechs/InsurTechs ein weiteres aufsichtsrelevantes Feld für die FMA dar, die für gewisse Kooperationsmodelle bereits eine entsprechende Sandbox betreibt.

1.7 HERAUSFORDERUNGEN BEI DER UMSETZUNG

Die zunehmende Digitalisierung traditioneller Geschäftsmodelle bringt aber auch zahlreiche Herausforderungen mit sich und ist mit internen und externen Hindernissen verbunden. Welche Hindernisse identifiziert werden, hängt dabei nicht nur von der Branche, sondern auch stark vom individuellen Unternehmen ab und diktiert in weiterer Folge, wie die Digitalisierung weiter vorangetrieben wird:

- Die größte Herausforderung bei zunehmend digitalen bzw. hybriden Arbeitsabläufen wird relativ einheitlich im **Prozessdesign** erblickt. Dies ist auch insofern nachvollziehbar, da eine softwaregestützte Umsetzung eines Arbeitsablaufes oft eine hochgradig formalisierte Definition und Beschreibung desselben erfordert, die mitunter noch nicht vorhanden war.
- Adäquate **personelle sowie technische Ressourcen** (Kompetenzen und Tools) werden praktisch über alle Sektoren hinweg als wichtige Herausforderungen bei digitalen Unterfangen im Unternehmen angesehen.
- Etwa die Hälfte der Versicherungen (52%), Zahlungsinstitute (50%) und Banken (45%) sehen die nötige Anpassung der **Unternehmenskultur** als besondere Herausforderung an.
- Der Handlungsspielraum in Unternehmen wird dabei allgemein nicht als Problem gesehen.

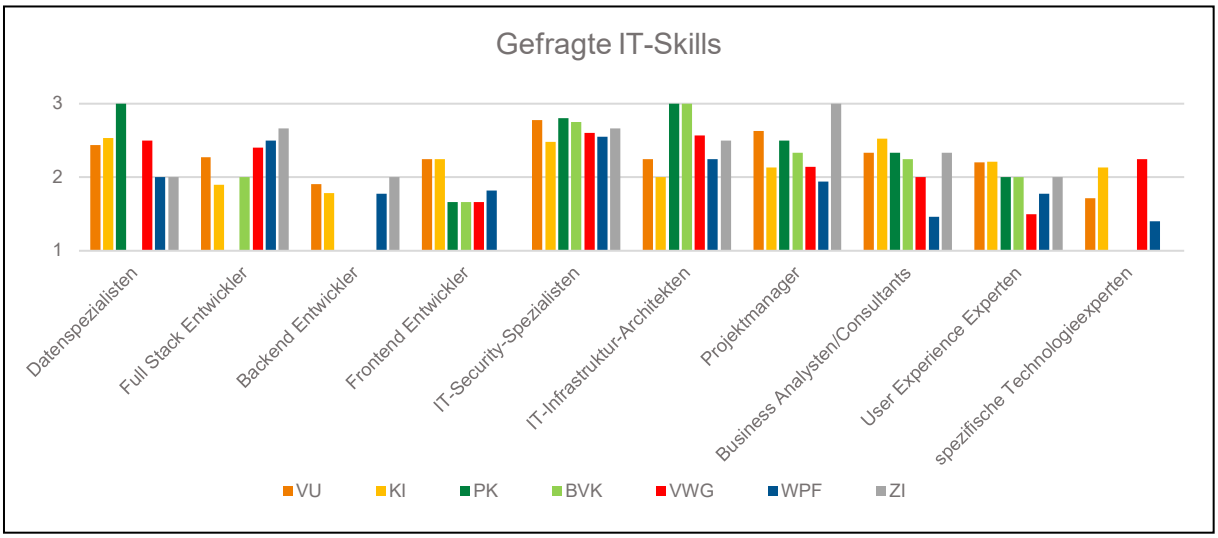


1.8 GEFRAGTES IT-KNOW-HOW

Durch die voranschreitende Digitalisierung können neue Chancen und Möglichkeiten entstehen, welche gerade vor dem Hintergrund des steigenden Konkurrenzdrucks spezialisierte IT-Kompetenzen erfordern. Die Digitalisierungsstudie zeigt, dass dabei Bedarf an einem breiten Feld an Disziplinen herrscht. Mit gewissen sektorspezifischen Unterschieden lassen sich folgende Trends auf dem Finanzmarkt erkennen:

- Alle Branchen sind vorrangig an einem Ausbau von Kapazitäten im Bereich der **IT-Sicherheit** interessiert.
- Tendenziell wird Management- bzw. Analystenstellen mit Technikaffinität aktuell eine höhere Relevanz zugeschrieben als dem Tätigkeitsbereich der reinen Softwareentwicklung.
- Im Hinblick auf IT-Entwicklung selbst geht hervor, dass einer Erweiterung von **Generalisten** (Full Stack-Entwickler) im Vergleich zum Ausbau von Know-How im Bereich Frontend- bzw. Backend-Entwickler größere Bedeutung beigemessen wird.
- Ein Ausbau von Know-How betreffend die Strukturierung und Analyse von Daten ist insbesondere bei VU, KI, PK, VWG und MI geplant.

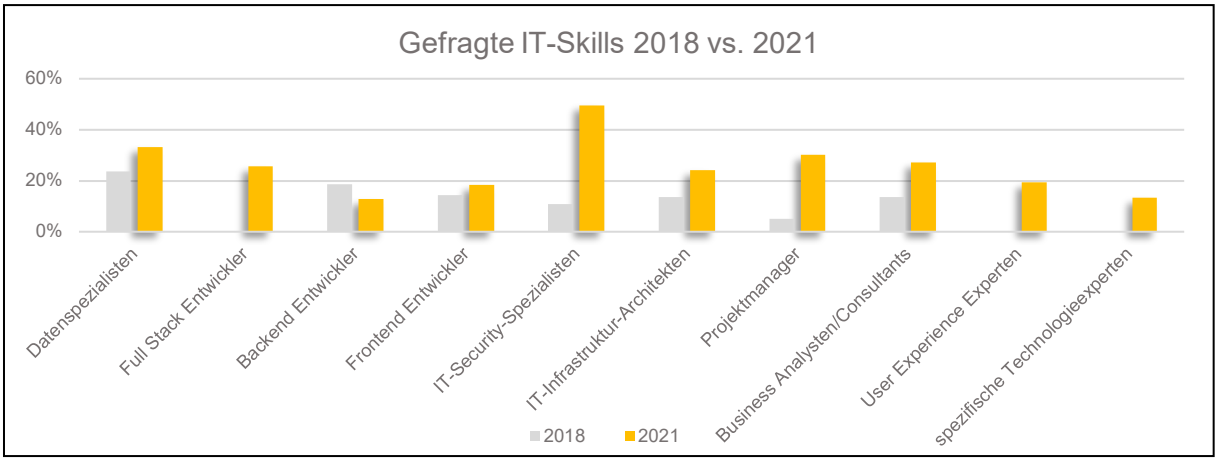
In der folgenden Graphik sind die Ergebnisse gereiht von 1 (wenig relevant) bis 3 (sehr relevant):



Im Vergleich zu 2018 zeigt sich bereits auf den ersten Blick, dass die beaufsichtigten Unternehmen ihre IT-Kompetenzen noch stärker ausbauen wollen. Außerdem haben sich einige Prioritäten deutlich verschoben:

- Standen 2018 noch die rein technischen Fähigkeiten im Fokus,
- steigt nun besonders markant der **Bedarf nach Projektmanagern und Analysten**, welche entsprechendes technisches Verständnis haben, um digitale Unterfangen zu leiten und zu unterstützen.
- Am stärksten ausgefallen ist die Gewichtung im Hinblick auf das Themenfeld **IT-Security**, welches 2018 noch von moderater Bedeutung war und nun, von rund 50% der Unternehmen als relevant betrachtet, mit Abstand den Spitzenplatz belegt.

Es folgt der entsprechende graphische Überblick für diesen Vergleich, wobei beachtet werden muss, dass die Felder *Full Stack-Entwickler, User Experience-Experten* und *spezifische Technologieexperten* in der Erhebung 2018 nicht vorhanden waren und somit hierfür keine Daten vorliegen:



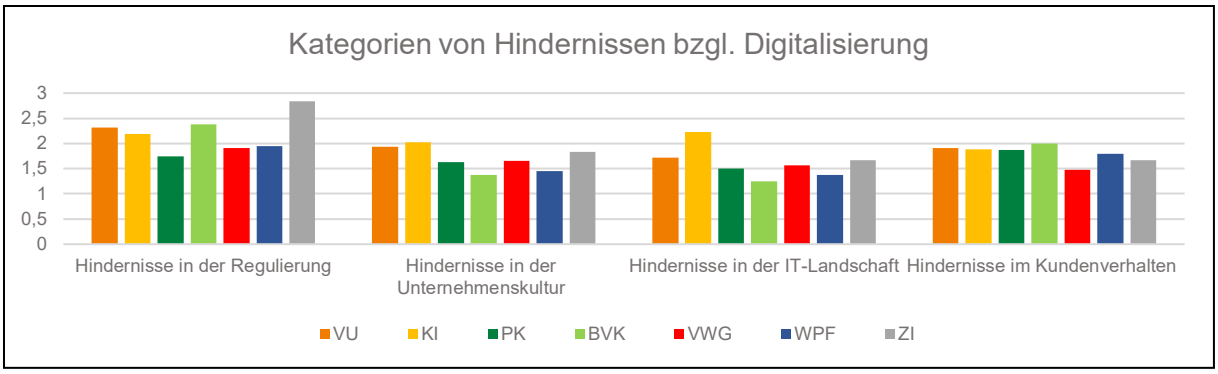
- Von Seiten der Aufsicht sticht hier vor allem der enorm gestiegene Bedarf nach IT-Security Skills ins Auge. Dies zeigt eine **stark gestiegene Awareness für die zunehmende Bedrohung durch Cyberattacken bei den beaufsichtigten Unternehmen** auf. Die Kehrseite dürfte jedoch auch ein gewisser Mangel an ausreichend qualifizierten Kräften am Arbeitsmarkt sein, die es den Unternehmen schwieriger machen könnte, Vorhaben in Bezug auf die IT-Sicherheit zeitnah umzusetzen, zumal entsprechend qualifiziertes Personal auch in anderen Sparten gesucht wird. [6]
- Außerdem zeigt sich, dass viele Unternehmen ihre I**n-House-Fähigkeiten** zumindest in einigen Bereichen stärken wollen. Dies kann ein gewisses Maß an Unabhängigkeit von externen Dienstleistern sichern und hilft, Konzentrationsrisiken vorzubeugen. Da Finanzmarktteilnehmer jedoch auch mit exakt diesen Unternehmen um Fachkräfte konkurrieren müssen, wird die Nachfrage nach entsprechenden Berufsgruppen wohl auch in Zukunft höher als das Angebot des Arbeitsmarktes bleiben und es schwierig machen, solche Stellen zu füllen.

[6] *Zu dieser Problematik siehe etwa auch Der Standard, 6.4.2021, Firmen fehlen mehr als 24.000 IT-Fachkräfte - Digitalisierung - derStandard.at › Karriere*

1.9 HINDERNISSE DER DIGITALISIERUNG

Die Relevanz der verschiedenen Kategorien von Hindernissen in Bezug auf Digitalisierung wurde von den beaufsichtigten Unternehmen aufgrund eines Rankings von 1 (nicht relevant) bis 3 (sehr relevant) eingestuft:

- Die größten Hindernisse werden in den meisten Sektoren in der **Regulierung** gesehen. Besonders ausgeprägt ist dies bei ZI, MI, BVK und VU. Hauptfaktoren sind hier insb. Vorgaben zu eigenhändigen Unterschriften, der Vorrang der Papierform, teils schwer erfüllbare Vorgaben in Bezug auf elektronische Übermittlung sowie das zu späte Erkennen von Digitalisierungstrends.
- Relevant sind aber auch Hindernisse, welche ihren Ursprung im **Kundenverhalten** haben. Hierbei berichten die Unternehmen vor allem über die inadäquate digitale Kompetenz von Kunden, welche ein Hemmnis für digitale Lösungen darstellt, sowie eine eher abwartende Haltung von Kundengruppen digitalisierten Prozessen gegenüber.
- Bis auf den Bankensektor und die VASP wird den Hindernissen für die Digitalisierung in der **Unternehmenskultur** eine größere Bedeutung beigemessen als den Hindernissen in Bezug auf die interne IT-Landschaft (genannt werden hier veraltete IT-Landschaft, unzureichende finanzielle Mittel für Forschung und Entwicklung sowie geringe Flexibilität etc.).



Sektorspezifisch werden überdies folgende Digitalisierungshindernisse genannt:

- **VU** sehen im Rahmen des Digitalisierungsfortschrittes zudem Erschwernisse in den umfangreichen Informationspflichten, wie beispielweise im Online-Vertrieb, sowie im Fachkräftemangel im Digitalisierungsumfeld.
- Für **KI** stellt der fehlende Schwerpunkt im Geschäftsfeld „Wertpapier“ bei modernen Kernbanksystemen ein Hindernis dar.

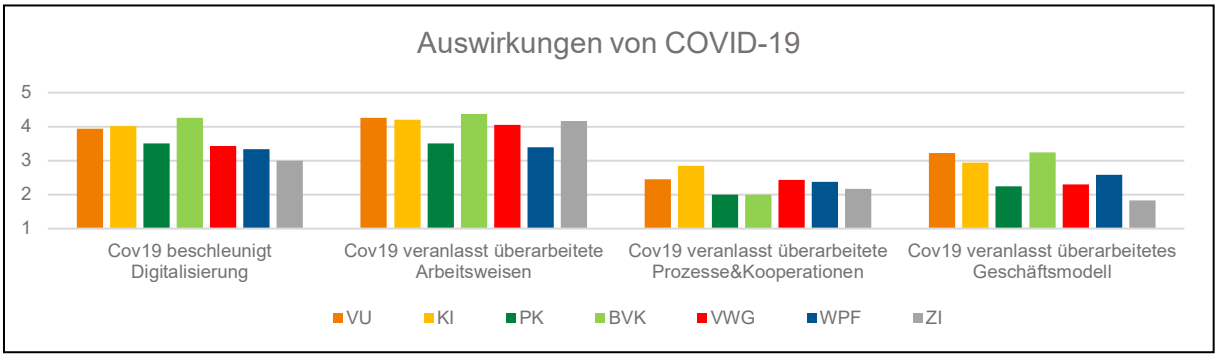
- **BVK** äußern sich im Rahmen der Erhebung zum fehlenden regulatorischen Vorrang der elektronischen Form gegenüber der Papierform und sehen in diesem Bereich ggf. Handlungsbedarf.
- **VWG** sehen in den hohen Anforderungen den IT-Geschäftspartnern gegenüber ein Hindernis, welches Digitalisierungsbemühungen entgegensteht.
- **WPF** berichten über fehlende Flexibilität bei Geschäftspartnern.

1.10 AUSWIRKUNGEN DER COVID-19-PANDEMIE

Der plötzliche Ausbruch der COVID-19-Pandemie und die damit einhergehenden Einschränkungen der physischen Mobilität haben auch im Finanzsektor zu großen Umstellungen geführt. Einerseits ist bei vielen Geschäftsmodellen Kundenkontakt standardmäßig vorgesehen, andererseits basierten die Prozesse bei den beaufsichtigten Unternehmen überwiegend auf physisch am Arbeitsplatz tätigem Personal. Dass die Auswirkungen von Schutzmaßnahmen, Lock-Downs, Quarantänen und Krankheitsfällen nicht noch deutlich größer ausgefallen sind, ist zu einem guten Maß der Digitalisierung am österreichischen Finanzmarkt zuzuschreiben.

Die beaufsichtigten Unternehmen identifizieren folgende Auswirkungen der COVID-19-Pandemie:

1. Die wichtigste Implikation der COVID-19-Pandemie in Bezug auf die Digitalisierung sieht der österreichische Finanzmarkt darin, dass die geänderten Rahmenbedingungen Anlass dazu geben, unternehmensinterne **Arbeitsweisen** langfristig neu zu bewerten. Beispielsweise könnten permanente digitale Arbeitsplätze geschaffen werden. Damit verbunden wären die mögliche Flexibilisierung von Arbeitszeiten oder die Reduktion von Arbeitsräumen.
2. COVID-19 hat in allen Finanzmarktsektoren als **Treiber der Digitalisierung** zu einer allgemeinen Beschleunigung des Einsatzes digitaler Technologien geführt.
3. Demgegenüber sehen sich die beaufsichtigten Unternehmen durch COVID-19 weniger veranlasst, künftige Arbeitsprozesse und Kooperationen langfristig neu zu bewerten. Überlegungen zu **Ausweitungen von Auslagerungen und Kooperationen** mit externen Dienstleistern werden somit auf Grundlage anderer Beweggründe vorgenommen.
4. Eine weitere mögliche Folge von COVID-19 ist die Neubewertung des konzessionierten **Geschäftsmodells**. Die beaufsichtigten Unternehmen – und hier vor allem VU, BVK und KI – beschäftigen sich mit potentiellen Anpassungen digitaler Dienstleistungen oder mit der Adaption von Kommunikations- und Vertriebsstrategien.



Aus Sicht der Aufsicht hat sich durch COVID-19 die bereits bestehende Entwicklung in Richtung elektronischer Kundenkommunikation beschleunigt, wodurch diesbezügliche regulatorische Themen zusätzlich an Relevanz gewonnen haben.

Außerdem stellen die verstärkte Nutzung digitaler Medien und Kommunikationsmittel sowie der breite Einsatz von remote work („Fernarbeit“) Themen dar, die in den IT-Sicherheitskonzepten der Unternehmen berücksichtigt werden müssen.

Zuletzt haben sich durch COVID-19 auch die Arbeitsweisen der FMA selbst weiterentwickelt, um den Umstieg auf Homeoffice zu bewältigen, auch ohne physische Treffen die Nähe zum Finanzmarkt nicht zu verlieren und weiterhin Aufsichtsaktivitäten durchführen zu können.

1.11 FAZIT UND HANDLUNGSFELDER DER FMA

Die Digitalisierungsstudie 2021 und der Vergleich mit den Ergebnissen im Jahr 2018 bestätigen eine **technologiegetriebene Transformation des österreichischen Finanzmarktes**. Dessen sind sich auch die Unternehmen des österreichischen Finanzmarktes bewusst und integrieren deshalb zunehmend digitalisierungsbetriebene Agenden in ihre Planung und Strategie.

Dementsprechend zeigen die Antworten im Kapitel „Strategie“ einen zunehmenden, unterschiedlich stark ausgeprägten, aber insgesamt deutlich erkennbaren Wandel von einer abwartenden Haltung zu einer aktiven Reflexion digitaler Themen durch die Entscheidungsträger der beaufsichtigten Unternehmen.

Diese Entwicklung wird vor allem durch die folgenden Erkenntnisse der Erhebung untermauert:

- Vorhaben zur weiteren Auslagerung und dem Bezug von Beratungsleistungen zu digitalen Themen setzen sich der Einschätzung der Unternehmen nach weiter fort (siehe Abschnitt Erwartete Zukunftsszenarien).
- Viele Ansätze zu effizienteren digitalisierten Prozessen und verbesserter Kundennähe durch neue Kommunikationsmethoden werden bereits praktisch genutzt, dennoch wird das

Verbesserungspotential in diesen Bereichen weiterhin als hoch eingestuft (siehe Abschnitt Chancen der Digitalisierung).

- Zusätzlich zum Konkurrenzdruck durch andere konzessionierte Unternehmen stuft ein Teil der Akteure des Finanzmarktes StartUps als mögliche zukünftige Konkurrenten ein (siehe Abschnitt Digitaler Wettbewerb).
- Die Unternehmen suchen zunehmend qualifizierte Mitarbeiter mit digitalen Fähigkeiten, wobei die Nachfrage nach Spezialisten für IT-Sicherheit mit Abstand am stärksten gestiegen ist (siehe Abschnitt Gesuchtes IT-Know-How).
- Die Anzahl der Kooperationen mit StartUps steigt stetig, außerdem wird in einigen Sektoren auch auf grenzüberschreitende Zusammenarbeit gesetzt (siehe Abschnitt Strategische Kooperationen).
- Die allgemeine Entwicklung in Richtung Digitalisierung wurde durch COVID-19 noch beschleunigt (siehe Abschnitt Auswirkung von COVID-19).

Die FMA hat bereits verschiedene Schritte gesetzt, um diese Entwicklungen zu begleiten und in ihren Aufsichtsansatz zu integrieren. Die in der vorliegenden Studie erhobenen Trends lassen erkennen, dass künftig insbesondere folgende strategische Bereiche zu adressieren sind:

Digitale Transformation am österreichischen Finanzmarkt aktiv begleiten; die Spielregeln klar kommunizieren:

- Die Struktur der Wertschöpfungskette wandelt sich, (Teil-)Leistungen werden zunehmend von Dienstleistern bzw. Kooperationspartnern erbracht. Durch diese vernetzten Abhängigkeiten können für Unternehmen diverse Risiken, wie etwa Konzentrationsrisiken und Unterbrechungen der digitalen Wertschöpfungskette, entstehen.
- Die Einbindung von StartUps sowie neue Geschäftsmodelle und Plattformen können außerdem Implikationen für Vertriebspraktiken und den gesamten konzessionierten Geschäftsbetrieb mit sich bringen.

Neue Verflechtungen in die laufende Aufsicht und Risikoklassifizierung einfließen lassen:

- Die Geschäftsmodelle beaufsichtigter Unternehmen ändern sich durch die Kooperation mit FinTechs/InsurTechs. Die FMA muss sich auf eine höhere Komplexität einstellen und diese neuen Verflechtungen in ihre Risikosicht auf Unternehmen und den Finanzmarkt als Ganzes einfließen lassen.

- Die Abhängigkeit von externen Dienstleistern sowie die zuliefernden Strukturen und die Konzentrationsrisiken sind dementsprechend auch in Zukunft in zunehmendem Maße von der Aufsicht zu berücksichtigen.

Die Kontaktstelle FinTech und die Sandbox laufend den Anforderungen des Marktes und der Regulierung anpassen:

- Mit FinTechs und InsurTechs drängen außerdem neue, innovative Anbieter auf den österreichischen Finanzmarkt; sie bieten aber auch den etablierten, beaufsichtigten Unternehmen neue Möglichkeiten. Durch derartige Kooperationen entlang der ganzen Wertschöpfungskette können Geschäftsmodelle modernisiert und effizienter gestaltet werden. FinTech-/InsurTech-Geschäftsmodelle können auch von nicht konzessionierten und beaufsichtigten Unternehmen angeboten werden. Die Abgrenzung ist häufig nicht leicht zu treffen, daher sieht die FMA es als ihre Aufgabe an, FinTechs/InsurTechs bei der Klärung zu unterstützen. Als zentrale Anlaufstelle für aufsichtsrechtlich relevante Fragen hat die FMA die **Kontaktstelle FinTech** etabliert, die ihr Informationsangebot laufend den Anforderungen des Marktes und der Regulierung anpassen muss.
    - Am 01.09.2020 trat § 23a FMABG unter der Überschrift „Regulatory Sandbox in der FMA“ in Kraft und verpflichtet die FMA zur Einrichtung einer solchen:
    - In der Sandbox sollen konzessionswerbende FinTechs, aber auch bereits konzessionierte Unternehmen mit ihren Finanzinnovationen in einem intensiven Dialog mit der FMA auf die Aufsicht vorbereitet werden. Die aufsichtsrechtlichen Implikationen von FinTech-Modellen können mit einer Konzession unter Auflagen getestet werden.
    - Sandbox bedeutet Aufsicht: Die Sandbox richtet sich an Teilnehmer, die bereits eine Konzession haben oder eine solche im Laufe des Sandboxverfahrens erlangen möchten. Eine Kooperation mit technischen Dienstleistern ist möglich, diese können aber nicht alleine Sandbox-Teilnehmer sein.
    - Es gibt keine Befreiung von regulatorischen Anforderungen und keine „Konzession light“, aber es kommt der Grundsatz der Proportionalität zur Anwendung.
    - In der Testphase können sogar zusätzliche Auflagen und Einschränkungen auferlegt werden, unter denen Dienstleistungen an Kunden erbracht werden dürfen.
    - In der Kontaktstelle FinTech (als Innovation Hub) kann zuvor Konzessions-, Registrierungs- oder Prospektpflicht abgeklärt werden.
    - Die maximale Verweildauer in der Sandbox beträgt 2 Jahre.

Die Sandbox der FMA hat ihre Arbeit rechtzeitig aufgenommen und es wird bereichsübergreifend an der Lösung der sich aufgrund der neuartigen Geschäftsmodelle ergebenden Herausforderungen

gearbeitet. Es haben bereits drei Unternehmen einen Antrag auf Aufnahme in die Sandbox gestellt (für diesen ist eine anwaltliche Vertretung nicht erforderlich). Die eingereichten Geschäftsmodelle beschäftigen sich insbesondere mit Dienstleistungen in Bezug auf Krypto-Assets/tokenisierten Wertpapieren bzw. neuartigen Formen der Wertpapierveranlagung für Kleinanleger.

Aufbau von Allgemeinbildung in den Bereichen Finanzen (financial literacy) und digitale Technologien (digital literacy) fördern und fordern:

- Disruptive Entwicklungen durch technologische und strukturelle Entwicklungen können weiterhin nicht ausgeschlossen werden. Zwar halten die beaufsichtigten Unternehmen selbst revolutionäre Veränderungen für eher unwahrscheinlich, dennoch wurden etwa StartUps noch 2018 deutlich weniger häufig als wichtige Akteure wahrgenommen; ebenfalls ist die Awareness für Cyber-Risiken deutlich gestiegen und neue Technologien werden rascher adaptiert als vor einigen Jahren. Dies unterstreicht die Notwendigkeit für die FMA, weiterhin mit Awareness und Verständnis für neue Trends Schritt zu halten, um Veränderungen auf den Finanzmärkten antizipieren zu können.

1.12 KONSULTATION ZU DEN STRATEGIEN

- Wie schätzen Sie die Auswirkungen der Digitalisierung auf den Finanzmarkt ein?
- Teilen Sie die Einschätzung der Finanzmarktteilnehmer, dass disruptive Veränderungen (dh eine Ablösung des Grundprinzips des Kerngeschäfts) innerhalb der nächsten drei Jahre am Finanzmarkt unwahrscheinlich scheinen?
- In welchen Bereichen werden disruptive Entwicklungen aus Ihrer Sicht mittel- bis langfristig erwartet?
- Was sind aus Ihrer Sicht die entscheidenden Erfolgsfaktoren für die am Finanzmarkt tätigen Unternehmen, um den digitalen Wandel optimal für die Weiterentwicklung des eigenen Geschäftsmodells nutzen zu können?
- In welchen Bereichen bestehen aus Ihrer Sicht Hindernisse der Digitalisierung?
- Wie schätzen Sie die Implikationen des Eintritts neuer digitaler Mitbewerber in den Finanzmarkt ein? In welchen Geschäftsbereichen kommt gemäß Ihrer Einschätzung den neuen Playern innerhalb der nächsten drei Jahre wesentliche Bedeutung zu? Welche Entwicklungen bzgl. des Verhältnisses der etablierten zu den neuen Playern erwarten Sie?
- Entsprechen die von der FMA identifizierten Risiken und Chancen Ihren Sichtweisen bzw. welche wesentlichen Abweichungen ergeben sich aus Ihren Erfahrungen?
- Was ist Ihre Erwartungshaltung hinsichtlich der Rolle der Aufsicht bei der digitalen Transformation des österreichischen Finanzmarktes?

2 PRODUKTGESTALTUNG

Die Digitalisierung stellt sich als Katalysator neuer Produkte und Dienstleistungen dar. Das Kundenverhalten ändert sich hinsichtlich des Zugangs zu Dienstleistungen, der jederzeit, von jedem Ort und über verschiedene Kanäle gegeben sein muss. Die zunehmende Vernetzung von Geräten, Haushalten und Infrastrukturen stellen außerdem neue Ansprüche auf das Design von Produkten und Dienstleistungen.

2.1 BANKPRODUKTE

Die Ergebnisse der Digitalisierungsumfrage der FMA zeigen, dass Banken in Österreich die Digitalisierung als sehr relevantes Thema einstufen und entsprechend bereit sind, Maßnahmen zu setzen, um diese Entwicklung für sich zu nutzen. Dabei scheint gleichzeitig die Chance gesehen zu werden, von neuen technischen Möglichkeiten zu profitieren, als auch das Risiko erkannt zu werden, in diesem Punkt hinter der Konkurrenz zurückzubleiben. Dieser zweite Aspekt wird zusätzlich dadurch betont, dass man erwartet, in Zukunft nicht nur im Wettbewerb mit anderen Kreditinstituten zu stehen. Die befragten Banken sehen weiterhin, dass große Technologiekonzerne (wie zB Google, Amazon) sowie Finanzdienstleister versuchen könnten, den Markt mit ihren eigenen Produkten zu erschließen.[7] Der größte Einfluss der Digitalisierung auf die Produktgestaltung wird im besseren Kundenverständnis durch mehr Daten und Interaktionspunkte sowie in der Effizienzsteigerung auf Basis von Automatisierungen und Ressourceneinsparungen gesehen.

2.1.1 TECHNOLOGIEGETRIEBENE PRODUKTINNOVATIONEN

Internet of Things	■ Das Internet of Things ermöglicht eine Verknüpfung klassischer Bankdienstleistungen mit bestehenden **digitalen Sprachassistenten**. Derartige Produkte sind (zumindest in Österreich) noch nicht weit verbreitet und derzeit erst in einfachen Funktionen verfügbar. ■ Ein wesentlicher derzeit beobachteter technologischer Trend ist die **sprachgesteuerte Interaktion ohne manuelle Eingabe** („Luftzeitalter“).[8] Es ist daher davon auszugehen, dass sich die Digitalisierung in diesem Bereich auch auf Produktebene widerspiegeln wird.
Künstliche Intelligenz	■ Automatische Bilderkennung.

[7] *Siehe weiterführend Bank für Internationalen Zahlungsausgleich, Juli 2021, https://www.bis.org/publ/bppdf/bispap117.pdf.*
[8] *Erste Bank, 6.7.2017, https://www.erstegroup.com/de/news-media/news-views/2017/07/06/kuenstliche-intelligenz-spracherkennung-fintech; https://www.santander.com/csgs/Satellite/CFWCSancomQP01/en_GB/Corporate/Press-room/Santander-News/2018/04/12/Santander-launches-the-first-blockchain-based-international-money-transfer-service-across-four-countries-.html.*

	■ **Online-Kontoeröffnung:** In Zusammenarbeit mit externen Anbietern kann per Video-Chat („Kontoeröffnung von der Couch aus“) eine Identifizierung von Neukunden erfolgen.[9] ■ **Fotoüberweisung**: Einige Banken bieten in Kooperation mit einem FinTech die Überweisung durch Abfotografieren der relevanten Daten an.
Maschinelles Lernen	■ Banken nützen maschinelles Lernen vor allem iZm mit der Personalisierung und Verbesserung ihrer Produkte.
Blockchain-basierte Anwendungen	■ Auf Produktebene sind diese derzeit nicht weit verbreitet; aus Kundensicht sind Krypto-Assets das prominenteste Beispiel für Blockchain-basierte Anwendungen. ■ Einzelne Banken haben bereits Blockchain-basierte Projekte gestartet, u.a. Begebung von Schuldscheindarlehen.[10]

2.1.2 NEUE PRODUKTARTEN

Durch neue Technologien entstehen aber auch neue Nischen und Produkte (fast alle österreichischen Banken bieten zB Sofortüberweisung mittels Geldtransfer über das Smartphone [Zoin], ein Produkt der Payment Services Austria, an: Nach Registrierung der Zoin-App kann eine digitale Wallet genutzt werden und Geld direkt an Handykontakte gesendet werden (auch bankübergreifend).[11]

Durch das Inkrafttreten des ZaDiG 2018 werden nunmehr zwei neuartige Produkte klaren Regelungen unterworfen:

- Kontoinformationsdienstleistungen, die eine umfassende und konsolidierte Darstellung von Zahlungskonten ermöglichen;
- sowie Zahlungsauslösedienstleistungen, mit denen Zahlungen über Drittanbieter ausgelöst werden können.

Diese beiden innovativen Dienstleistungen bzw. Produkte werden in Zukunft sowohl von Banken als auch von Drittanbietern angeboten werden. Drittanbieter, die derartige Dienste anbieten wollen, sind von der FMA zu konzessionieren bzw. im Falle von Kontoinformationsdienstleistern zu registrieren.

Darüber hinaus hat sich im Bereich der Vermögensverwaltung ein Trend abgezeichnet. Sogenannte Robo-Advisor-Tools, welche zu einem Abschluss einer Vermögensverwaltung führen, ermöglichen

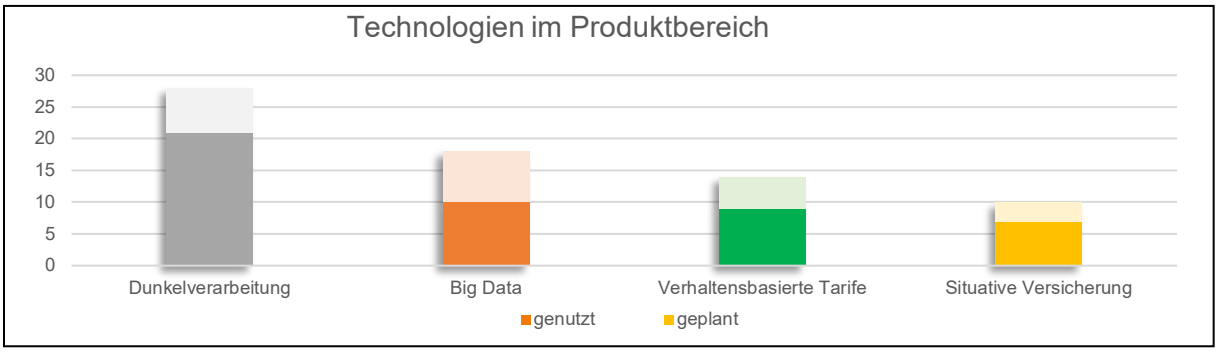
[9] *Der Standard, 23.1.2017, https://derstandard.at/2000051355606/Per-Selfie-zum-Konto-Banken-machen-mit-Video-Identifizierung-ernst.*
[10] *Vgl. dazu https://www.erstegroup.com/de/schuldscheindarlehen.*
[11] *Der Standard, 20.9.2017, Zoin: Sofortüberweisung als Feature zum Geldtransfer über Smartphones, https://derstandard.at/2000064349794/Zoin-Sofortueberweisung-als-Feature-zum-Geldtransfer-ueber-Smartphones.*

den Einstieg in diese Produktart bereits mit niedrigen Investitionssummen (ab 5.000 Euro) und eine laufende Zuzahlung in kleinen Beträgen (ab 100 Euro monatlich) werden ermöglicht.

2.2 VERSICHERUNGSPRODUKTE

Der Einsatz digitaler Technologien beeinflusst auch die Produktlandschaft. So werden zum einen die herkömmlichen Versicherungsprodukte auf die neuen Technologien umgestellt. Zum anderen ergeben sich durch die Technologien selbst neue Versicherungsprodukte, die teilweise noch experimentell lanciert werden.

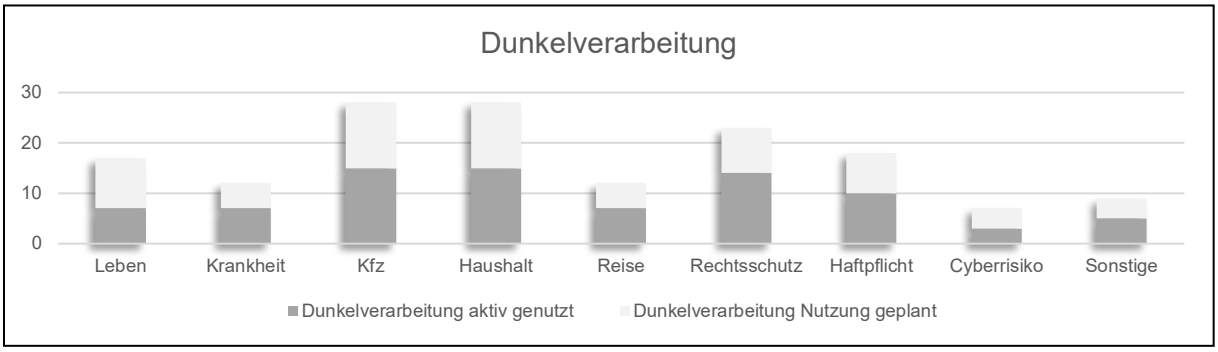
Die von den österreichischen VU idZ am häufigsten eingesetzte Technologien sind die Dunkelverarbeitung (85%) und Big Data Analysen (55%). Auch verhaltensbasierte Tarife (42%) sowie situative Versicherungen (30%) werden von VU angeboten oder befinden sich in Planung.



2.2.1 DUNKELVERARBEITUNG

Dunkelverarbeitung bezeichnet den vollautomatischen Ablauf von Geschäftsprozessen, mit dem der Prozessablauf effizienter gestaltet und die Bearbeitungsqualität standardisierter Vorgänge ohne Erforderlichkeit von Benutzerinteraktion gesteigert werden kann. In allen abgefragten Versicherungssparten finden Dunkelverarbeitungsprozesse bereits Anwendung und sollen in den nächsten drei Jahren noch weiter ausgebaut werden.

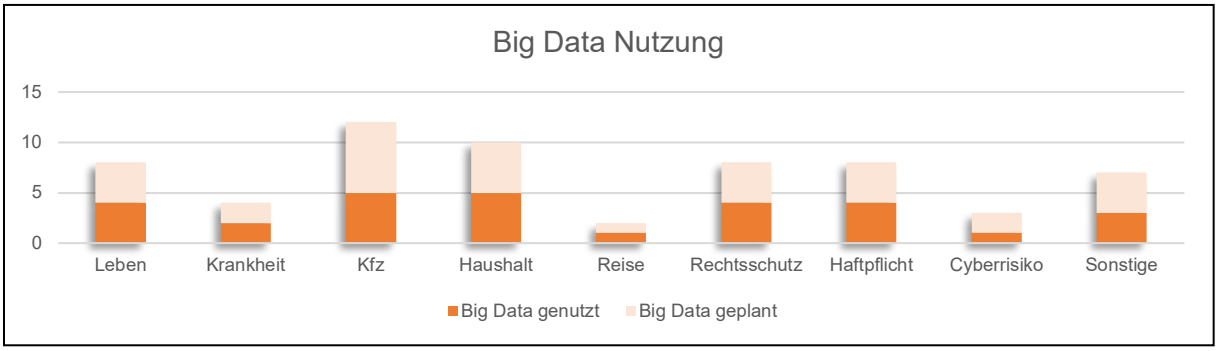
- Dunkelverarbeitungssysteme werden am häufigsten in der Kfz- und der Haushaltsversicherung (jeweils 15 VU), Rechtschutz- und Krankenversicherung eingesetzt.
- Aber auch die Hälfte der Haftpflichtversicherer und ein Drittel der Lebensversicherer nutzen bereits die Dunkelverarbeitung zur Optimierung standardisierter Prozesse.



2.2.2 NUTZUNG VON BIG DATA

Durch die Auswertung großer Datenmengen können Risiken in Echtzeit und auf Grundlage des individuellen Verhaltens bewertet werden. Das Schätzen von Risiken wird zukünftig immer exakter und folglich die Prämienbemessung viel individueller. Big Data gewinnt somit auch im Versicherungssektor immer mehr an Bedeutung.

- In allen abgefragten Versicherungssparten wird Big Data von den VU bereits genutzt. Allen voran in den Bereichen Kfz, Haushalt, Rechtschutz, Leben und Haftpflicht.
- Eine entsprechende Ausweitung der Nutzung bis 2024 ist bei zahlreichen VU in Planung.

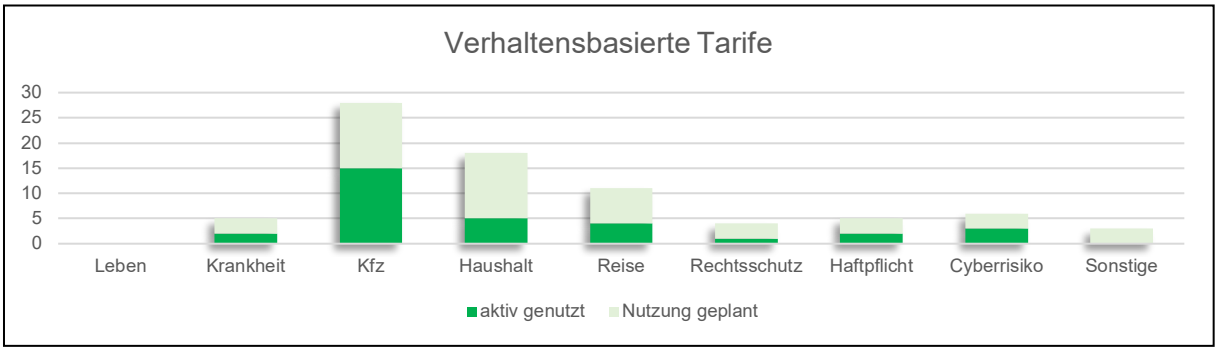


2.2.3 VERHALTENSBASIERTE PRODUKTE

Big Data Anwendungen ermöglichen auch die Implementierung von verhaltensbasierten Produkten:

- **Smart Homes:** Für die Kalkulation in der Haushaltsversicherung werden detaillierte Verhaltens-, Umwelt- oder Schadendaten genutzt, die miteinander in Beziehung gesetzt werden und validere Schlussfolgerungen als bloße Pauschaldaten erlauben.
- **Usage Driven Insurance:** Versicherungen richten ihr Angebot auf das Nutzungsverhalten, etwa Fahrverhalten und die gefahrenen Kilometer des Versicherten aus (Telematik-Tarife).

- **Pay as you live:** Versicherer können ihre Kunden durch zusätzliche Angebote (zB Fitnessarmbänder, welche Informationen über die tägliche Bewegung bereitstellen) aktiv unterstützen, gesundheitsbewusst zu leben, und so ihre Präsenz stärken.



- Verhaltensbasierte Tarife werden in Österreich bislang vor allem in der **Kfz-Versicherung** eingesetzt. Bereits die Hälfte der VU (15 VU) bietet verhaltensbasierte Tarife in dieser Sparte an. Weitere 40% (13 VU) planen zudem solche Tarife auszubauen bzw. in ihr Produktportfolio aufzunehmen.
- Auch in der **Haushaltsversicherung** werden verhaltensbasierte Tarife als Zukunftsthema gesehen. Insbesondere durch die aktuellen Entwicklungen rund um Smart Homes und die damit verbundenen Datenquellen planen 40% der VU (13 VU) die Nutzung bzw. den Ausbau ihrer Produkte in diesem Bereich.
- In der **Reise-Versicherung** sehen VU gewisse Zukunftspotentiale. In diesem Bereich ist eine Verdreifachung der Anbieter von Versicherungslösungen bis 2024 geplant (4 VU derzeit, bei 7 VU Tarifausbau in Planung).

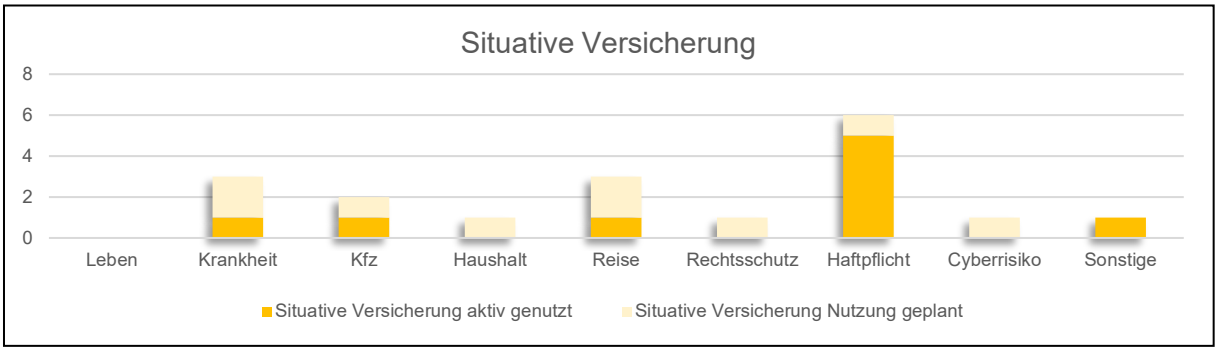
2.2.4 SITUATIVE VERSICHERUNGEN

Bei Versicherungen „on demand“ können Kunden Versicherungsschutz für bestimmte, in der Smart-Phone-App erfasste Fälle jederzeit ein- und ausschalten und somit die Vertragsdauer selbst bestimmen. Dadurch wird sich die Produktlandschaft der VU von Standardtarifen und -modulen hin zu einem stärker individualisierbaren und situativen Versicherungsschutz entwickeln.

Situative Versicherungen werden in Österreich bislang noch von vergleichsweise wenigen VU angeboten. Als Hauptanwendungsfelder für dieses neuartige Versicherungsformat dienen die Sparten Reise, Krankheit, Unfall und Haftpflicht.

- In der Sparte Haftpflicht bieten derzeit 12% der VU (1 weiteres VU in Planung) situative Versicherungslösungen an. In den Sparten Krankheit, Reise und Kfz kann bislang bei je einem VU eine situative Versicherung abgeschlossen werden.

- Beispiele für derzeitige Angebote sind kurzfristige Reise-Krankenversicherungen, kurzfristige Veranstalterhaftpflichtversicherungen sowie die Möglichkeit zur befristeten Erweiterung der örtlichen Geltung von Versicherungsleistungen im Kundenportal.



2.2.5 PARAMETRISCHE VERSICHERUNGEN

Bei parametrischen Versicherungen werden die Vertragsbestimmungen auf Basis einer Blockchain technisch so abgebildet, dass Vertragsklauseln teilweise oder vollständig selbständig ausführbar sind. Eine Prüfung, ob und in welcher Höhe dem Versicherten tatsächlich ein Schaden entstanden ist, wird dadurch obsolet, denn die vereinbarte Summe wird automatisch dann fällig, sobald ein bestimmter parametrischer Trigger erreicht ist. Als Trigger dienen etwa Niederschlagsmenge, Pegelstand oder Wind- oder Erdbebenstärke an einer vereinbarten Messstation. Damit könnten künftig auch bislang nicht versicherungsfähige Unternehmensrisiken versichert werden (zB Betriebsunterbrechungen ohne vorangegangenen Sachschaden, Cyber-Risiken, Produktrückrufe sowie Risiken durch Wetterschäden oder Energiepreise).

Chancen	■ Schadensprüfung nicht notwendig ■ hohes Automatisierungspotential, effizienter Risikotransfer ■ neue versicherungsfähige Bereiche (zB immaterielle Güter) ■ niedrige Verwaltungskosten und geringe Schadenregulierungskosten ■ eine bessere Sichtbarkeit von Betrug und eine einfachere Preisgestaltung
Risiken	■ Die Datenverfügbarkeit stellt eine enorme Herausforderung dar. Technische Fortschritte (Fernerkundung, Big Data) können hier eine Verbesserung bringen.

2.2.6 COMMUNITY BASED INSURANCE

Gemeinschaftlich basierte Versicherungen führen wieder an den Ursprung des Versicherungswesens zurück, wo sich bestimmte gemeinschaftliche Gruppen wie Familien oder Dorfgemeinschaften

gegenseitig in Schadensfällen unterstützt haben. Neu hinzu kommt, dass solche Arten von Versicherungen im Zeitalter von Computer und Handy andere Durchführungswege ermöglichen.
Mit Hilfe der digitalen Möglichkeiten (P2P) können Personen zu kleinen Gruppen zusammengeschlossen werden. Schäden unterhalb eines Selbstbehalts werden innerhalb eines solchen Kollektivs geteilt. Erst bei größeren Schadensummen greift der Schutz des Versicherungsvertrages.

Chancen	■ Zugang zu Versicherungsschutz könnte durch moderne Technologien und das „Internet of Things“ erleichtert werden. ■ Der Schadensfrei-Bonus schafft positive Anreize gegen Versicherungsbetrug und spart Kosten.
Risiken	■ Antiselektion der Versicherungsrisiken ■ regulatorischer „Graubereich" ■ kompetente und finanziell solide Trägerunternehmen müssen vorhanden sein

2.2.7 SHARING ECONOMY BASIERTE PRODUKTE

Der Begriff Sharing Economy ist ein Sammelbegriff für Unternehmen, Geschäftsmodelle, Plattformen und Praktiken, die eine geteilte Nutzung von ganz oder teilweise ungenutzten Ressourcen ermöglichen. Sachen oder Dienstleistungen über Sharing-Economy-Plattformen zu nutzen, ist zwar kein neuer Trend, Novum bezieht sich auf die Art der Dienstleistungserbringung, dh die Nutzung digitaler Plattformen, welche das Matching von Angebot und Nachfrage aufgrund der dahinterstehenden Technologie besonders rasch ermöglichen.[12]
Die steigende Bedeutung von Geschäftsmodellen der Sharing Economy kann dazu führen, dass Versicherungsleistungen verstärkt an die Nutzung und weniger an die Eigentumsverhältnisse von Gütern geknüpft werden.

Chancen	■ Neue Versicherungsprodukte
Risiken	■ Zweckentfremdung und als Folge andere Risikoprofile ■ Unklar, in welcher Form Kunden und Sharing-Plattformen Risiken tragen ■ Komplexe versicherungsrechtliche Fragen ■ Schadenabwicklungsprozesse könnten komplexer werden

[12] *Vgl. etwa Squaring risk in the sharing age: How the collaborative economy is reshaping insurance products, Lloyds und Deloitte (2018); kritisch im Hinblick auf US health insurance betreff sogenannte health sharing ministries It Looks Like Health Insurance, but It's Not. 'Just Trust God,' Buyers Are Told. - The New York Times (nytimes.com).*

2.2.8 CYBERVERSICHERUNG

Die Kehrseite der Digitalisierung ist der Anstieg von Cyber-Risiken. Auch bei einem gewissenhaften Cyberrisikomanagement können Cybervorfälle nicht vollkommen ausgeschlossen werden. Diesem Potential, das auch Betreuungsleistungen zum Schutz vor bzw. zur Behandlung von Cybervorfällen umfasst, stehen beispielsweise aufgrund eingeschränkt verfügbarer Datengrundlagen zur Berechnung der Prämien und durch vermehrte, sich verändernde Cyberangriffe, die auch durch das COVID-19-Umfeld bedingt sind, neue Herausforderungen gegenüber. Auch Kumulrisiken, die zB durch eine Cyberattacke, die gleichzeitig bei vielen Versicherten schlagend werden, sind zu beachten.[13]

Cyberversicherungen sind keine standardisierten Produkte, es gibt hierzu auch keinen eigenen Versicherungszweig. Der jeweilige Deckungsumfang einer Cyberversicherung kann unterschiedlich ausgeprägt sein. Cyberrisiken sind oft über Haftpflicht- oder Rechtsschutzversicherungen abgedeckt.[14]

Chancen	■ Risikobewusstsein ■ Großes Potential auch durch das Zurverfügungstellen von Schutz vor Cyberattacken und der Betreuung nach einer erfolgreichen Cyberattacke: Die Verlagerungen ins Home-Office, die Professionalisierung der Angreifer und die darüber erfolgenden täglichen Berichterstattungen erhöhen das Bewusstsein bezüglich möglicher Auswirkungen schlagend werdender Risiken. Zudem treiben auch Datenschutzvorgaben die Nachfrage nach Cyberversicherungen. Insgesamt wird die globale Marktgröße des Cyberversicherungsmarktes für 2019 auf rd. 5 Mrd. USD geschätzt und für 2026 auf rd. 29 Mrd. USD projiziert.[15]
Risiken	■ Schwierige Kalkulation der Prämie wegen geringer Erfahrungswerte mit Schadensfällen und das sich schnell ändernde Umfeld

In Österreich bieten 11 VU einen expliziten Cyberrisikoschutz an.[16] Knapp drei Viertel dieser Anbieter nehmen Rückversicherungen in Anspruch und reduzieren dadurch ihre Risiken.

Die von den österreichischen VU verrechneten Cyberversicherungsprämien belaufen sich 2020 auf rd. 3,4 Mio. Euro. Im Vergleich zu 2019 haben sie sich mehr als verdoppelt. Trotz dieses hohen Anstiegs ist der Anteil des Cyberversicherungsmarkts am Gesamtprämienvolumen 2020 iHv 19 Mrd. Euro gering.

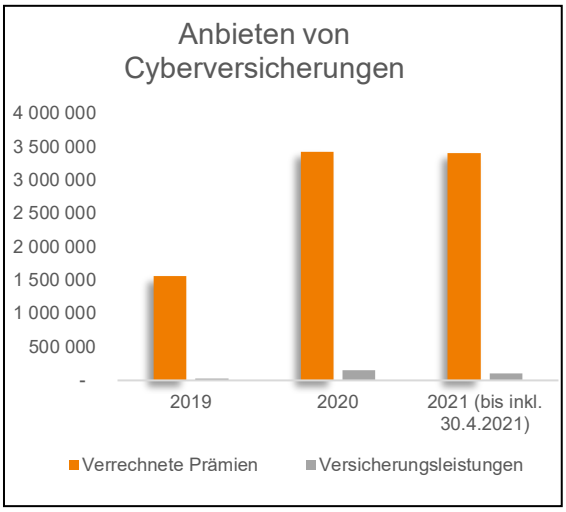
---

[13] Die Prämien und der Deckungsumfang werden aktuell von VU aufgrund gestiegener Cybervorfälle bzw. eines besseren Verständnises der Risikoprofile reevaluiert. Vgl. Insurance Business America, ‚Dysfunctional' cyber insurance market puts pressure on brokers, 8.3.2021; United States Government Accountability Office, Report to Congressional Committees, Cyber Insurance – Insurers and policyholders face challenges in an evolving market, May 2021.

[14] Dazu auch EIOPA, EIOPA Strategy on cyber underwriting, 2020.

[15] Allied Market Research, Cyber Insurance Market Outlook - 2026, abgefragt am 7.9.2021.

[16] Vgl. dazu zB VersicherungsJournal.at, „Dramatische Marktverhärtung" in der Cyberversicherung, 2.9.2021.



Die Cyberversicherungsleistungen sind von 2019 auf 2020 zwar pro Versicherungsfall um die Hälfte gestiegen; sie befinden sich aktuell aber auf einem überschaubaren Niveau und lagen 2020 bei rd. 148.000 Euro.

Die Prämiensumme, die insgesamt auf mit beaufsichtigten Unternehmen abgeschlossenen Cyberversicherungen entfällt, belief sich 2020 auf rd. 42 Mio. Euro. Diese kann zum Großteil dem KI-Sektor zugeordnet werden.

- Die Prämiensumme 2020 ist im Vergleich zum Vorjahr um insgesamt rd. 6% gestiegen; für 2021 wird eine Erhöhung um 8% erwartet.
- Im Vergleich dazu beliefen sich die erhaltenen Versicherungsleistungen 2020 auf 5 Mio. Euro.

2.2.9 KRYPTOASSETS-POLIZZEN

Angesichts von Hacker-Angriffen und einer sukzessiven Regulierung der Krypto-Assets steigt der Bedarf nach Absicherung.[17] Insofern wächst global die Nachfrage nach Versicherungen gegen „Kryptowährungsbetrug“. Insbesondere Versicherer aus den USA und Japan bringen seit einigen Jahren Krypto-Assets-Polizzen auf den Markt.

Chancen	■ Neue Versicherungsprodukte ■ Steigerung des Risikobewusstseins ■ Bessere Risikobewertung und Abschätzung
Risiken	■ Risiken, die aus „Kryptowährungen“ entstehen, sind sehr schwer abzuschätzen[18]

[17] *Vgl. etwa den Diebstahl von einer halben Mrd. Dollar bei der japanischen Börse Coincheck, BBC, 27.1.2018, Coincheck: World's biggest ever digital currency 'theft' - BBC News; siehe auch den Vorfall vom August 2021 Hackers return $260 mln to cryptocurrency platform after massive theft | Reuters.*

[18] *Vgl. ENISA Opinion Paper on Cryptocurrencies in the EU (europa.eu) wie bspw: AML issues, tax issues, illicit activities, energy used causing impact on climate change.*

2.3 FAZIT UND HANDLUNGSFELDER DER FMA

Digitale Transformation braucht stabiles Fundament und Rechtssicherheit:

- Rechtsunsicherheiten hinsichtlich der aufsichtsrechtlichen Einordnung und der Möglichkeiten der digitalen Transformation in der Produktgestaltung müssen weiter identifiziert und beseitigt werden. Dies betrifft auch
  - die Abwägung zwischen den Kosten für eine weitergehende Prämiendifferenzierung und dem damit erzielbaren Nutzen der Vermeidung einer Antiselektion;
  - die Beurteilung, welchen Freiraum auf Dauer die Regulierung für ein Fortschreiten des individuellen versicherungstechnischen Äquivalenzprinzips und eine damit verbundene, immer feinere Prämiendifferenzierung lässt.

Technologieneutralität schließt Regulierung nicht aus:

- Die Aufsicht steht grundsätzlich neutral gegenüber Innovation und technologischen Entwicklungen. Dies schließt jedoch nicht die Erlassung neuer Regelwerke für bestimmte Innovationen aus (etwa iZm den „ethischen“ Grenzen der Digitalisierung).

Produktinnovationen erfordern Transparenz:

- Die Digitalisierung bringt nicht nur innovative, sondern teilweise auch komplexere Produkte mit sich. Um dem gesteigerten Informationsbedürfnis von Kunden zu begegnen und Kunden auf Informationspflichten für Anbieter und sensible Themenbereiche aufmerksam zu machen, muss die FMA ihre Verbraucherinformationen weiter forcieren.

Rechts- bzw. sozialpolitischen Diskurs bei drohender finanzieller Exklusion anstoßen:

- Im Versicherungsbereich können zunehmend individuell berechenbare Prämien das Versicherungsprinzip des Risikoausgleichs in der großen Zahl gefährden: Gute Risiken könnten sich günstiger, schlechte Risiken hingegen nur noch teurer versichern. Im Extremfall könnten individuell risikoadjustierte Prämien prohibitiv hoch ausfallen.
- Daraus ergibt sich die Frage, inwiefern künftig die Gefahr besteht, dass sich schlechte Risiken nicht mehr versichern können – und damit ein partielles Marktversagen droht (Auswirkungen auf die finanzielle Inklusion und Exklusion).

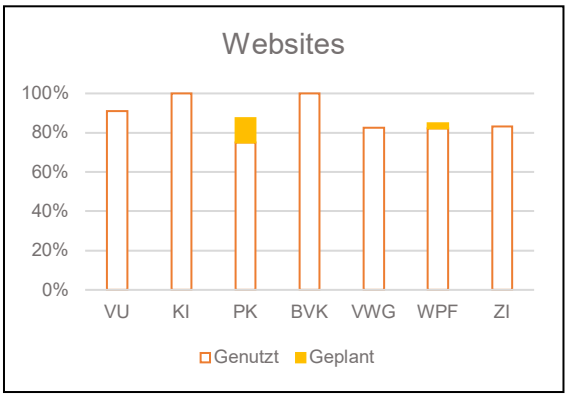
2.4 KONSULTATION ZUR PRODUKTGESTALTUNG

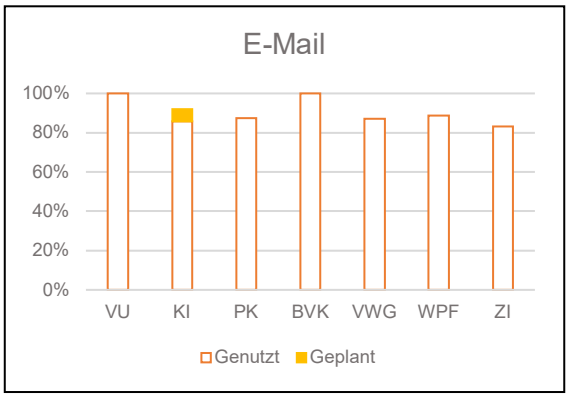
- Welche Aufgaben soll aus Ihrer Sicht die FMA im Rahmen des Anleger-, Versicherten- und Gläubigerschutzes bezüglich „digitaler“ Finanzprodukte wahrnehmen?
- Welche konkreten regulatorischen Vorgaben sind durch die Digitalisierung des Finanzsektors noch notwendig?
- Welche Hindernisse, die die Entwicklung von neuen digitalen Finanzprodukten erschweren, bestehen aus Ihrer Sicht in Österreich?
- Teilen Sie die Einschätzung der FMA zu den mit den Auswirkungen auf das Bank- bzw. Versicherungsgeschäft verbundenen Chancen und Risiken?
- Welche konkreten positiven, aber auch negativen Entwicklungen bezüglich „digitaler“ Finanzprodukte sind aus Ihrer Sicht zu beobachten?

3 VERTRIEB / KUNDENSCHNITTSTELLE

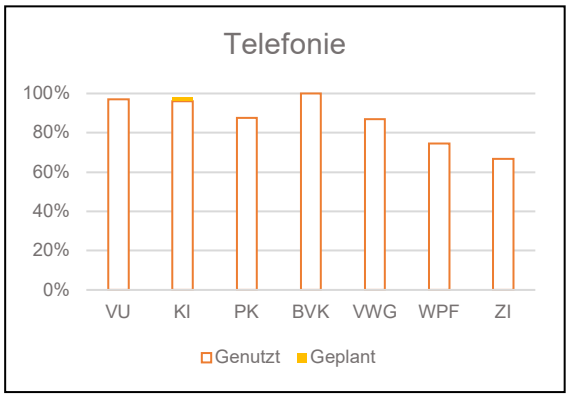
3.1 TRENDS BEI DEN VERSCHIEDENEN KOMMUNIKATIONSKANÄLEN

Wie iZm den Strategien dargestellt, ist die Verbesserung sowie Intensivierung des Kundenkontaktes einer der Haupttreiber der Digitalisierung am österreichischen Finanzmarkt. Im Wettbewerb um Vertragsabschlüsse ist es ein Vorteil, Kunden über möglichst viele potentielle Kanäle ansprechen zu können, während eine elektronische Kundenbetreuung die Effizienz erhöhen und zu verstärkter Kundenbindung beitragen soll. Dementsprechend haben viele beaufsichtigte Unternehmen in den Ausbau ihrer digitalen Kommunikationskanäle investiert. Letztendlich hat auch die Pandemie die Digitalisierung beschleunigt. Die diesbezüglichen Trends lassen sich wie folgt zusammenfassen:
Klassische Kommunikationskanäle wie Websites, E-Mail und Telefon gehören unverändert zum Standardreportoire aller Finanzmarktsektoren.

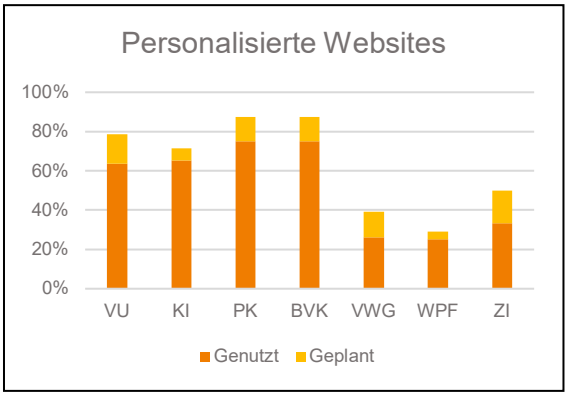


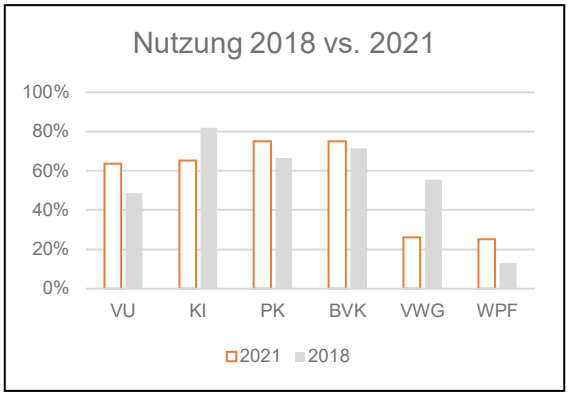


Ausnahmen ergeben sich nur aus den Geschäftsmodellen der Unternehmen.
In einigen Fällen (so etwa im Fall von VASP) werden diese Kanäle bewusst nicht genutzt.



Personalisierte Websites (zB Kundenportale) zeigen bereits eine insgesamt hohe Verbreitung und sollen in den nächsten drei Jahren in allen Sektoren noch stärker zum Einsatz kommen:

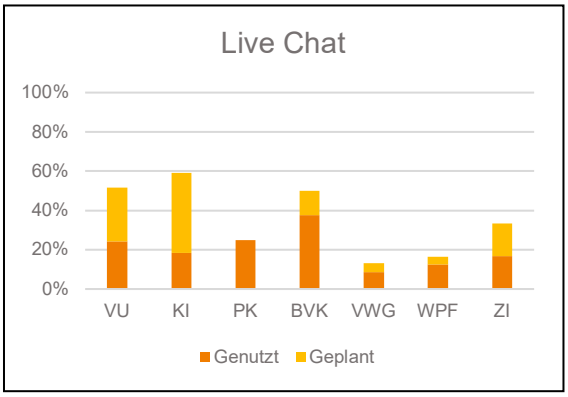


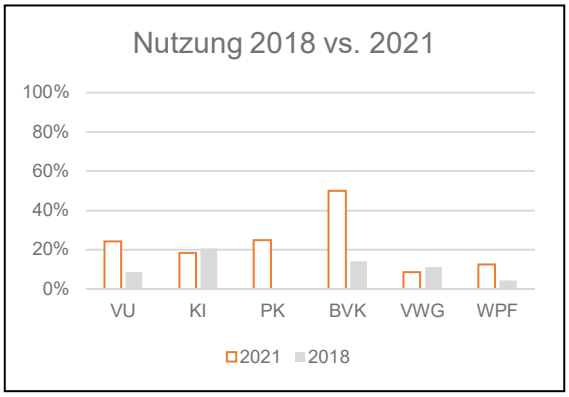


Die Nutzung und der allgemeine Trend bei der Nutzung von Kundenportalen variiert stark nach Finanzmarktsektor. Deutlich gestiegen ist die Verbreitung von personalisierten Websites bei VU (aktuell 64%) und BVK (100%). Digitale Kundenportale können zu einer erhöhten Interaktion des Kunden mit dem Unternehmen führen. Die Möglichkeit, jederzeit in seinen Vertrag und dessen Wertentwicklung einzusehen oder Änderungen unmittelbar durchzuführen, könnte die Attraktivität für Kunden erhöhen. Rückläufige Trends zeigen sich bei KI und VWG, was allerdings zum Teil auf die Erweiterung des Teilnehmerkreises der Digitalisierungsstudie 2021 in diesen beiden Sektoren um Sonderinstitute zurückzuführen sein wird.

Dabei ist zu bedenken, dass es sich bei der Einrichtung von Kundenportalen um eine vergleichsweise aufwändige Kommunikationsmöglichkeit handelt. Eine solche Lösung muss intern oder extern von Softwareentwicklern implementiert werden und an die Website und IT-Infrastruktur des Unternehmens angepasst werden. Sie muss aus der Perspektive der IT-Sicherheit gut abgesichert sein, da sie eine potentielle Angriffsfläche darstellt und muss laufend gewartet und instandgehalten werden. Da ein Portal nicht bei jedem Geschäftsmodell gut einsetzbar ist, ist es insofern gut erklärbar, dass sich dieses Werkzeug nicht bei allen Unternehmen durchsetzen wird bzw. in Einzelfällen dahingehende Prototypen auch wieder eingestellt werden.

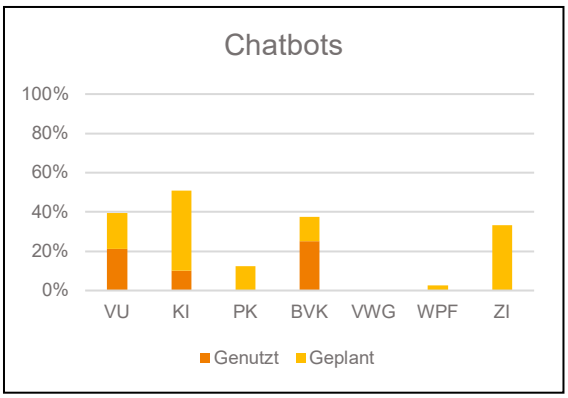
Livechat-Lösungen, bei welchen in Echtzeit Textnachrichten mit Kunden ausgetauscht werden, sind in den letzten drei Jahren stärker eingesetzt worden und sollen auch in den nächsten drei Jahren weiter ausgebaut werden. 2024 will sie etwa die Hälfte der VU, KI und BVK nutzen.

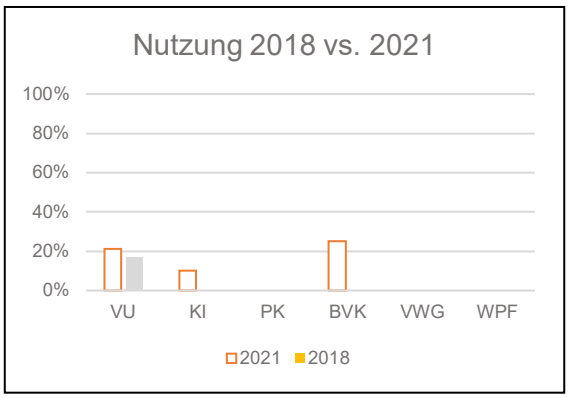




Diese Möglichkeit wurde 2018 nur von wenigen Unternehmen genutzt und hat sich seither insbesondere bei einer gewissen Zahl von VU, PK und BVK etabliert. Vor allem VU und KI planen dabei einen starken weiteren Ausbau in den nächsten drei Jahren. Diese Angabe wurde insbesondere bei VU und KI auch vor drei Jahren bereits vermehrt getätigt. Dass es hierzu bei vielen Unternehmen Pläne gibt, diese im Zuge von COVID-19 aber offenbar nur bei wenigen bereits umgesetzt wurden, kann darauf hinweisen, dass in Livechat-Tools zwar ein Mehrwert gesehen wird, diesen jedoch nicht eine so hohe Umsetzungspriorität wie anderen Technologien eingeräumt wird.

Chatbots waren 2018 nur im Versicherungssektor im Einsatz. Mit der Livechat-Möglichkeit wächst aber auch das Potential, die Kundenkommunikation mittels Chatbots automatisiert zu unterstützen:





Nach einer in Österreich, Deutschland und der Schweiz 2021 durchgeführten Studie zum Thema Chatbots [19] gaben 63 % der Befragten an, bereits mit einem Chatbot interagiert zu haben. Dabei wird lieber geschrieben als gesprochen, dh deutlich häufiger erfolgte die Interaktion mit einem Chatbot als mit einem Voicebot. Als positiv aus Sicht der Benutzer wird die Erreichbarkeit und die schnelle, unkomplizierte Hilfe gesehen. Die bisherigen Erfahrungen der Nutzer mit Bots sind überwiegend

[19] *https://page.aiaibot.com/de/chatbot-studie*.

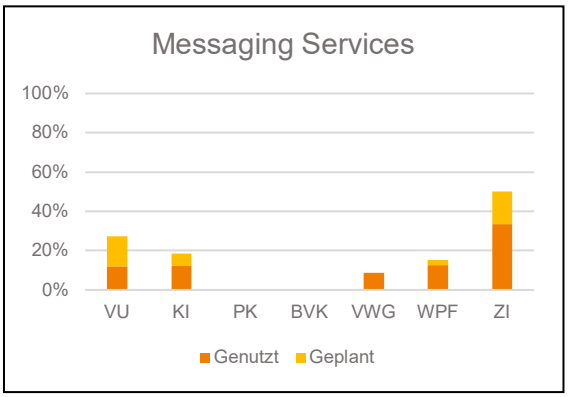
positiv. Jeder Fünfte kann sich vorstellen, einen kompletten Vertragsabschluss – von der Beratung bis hin zum Kauf – via Chatbot abzuwickeln.

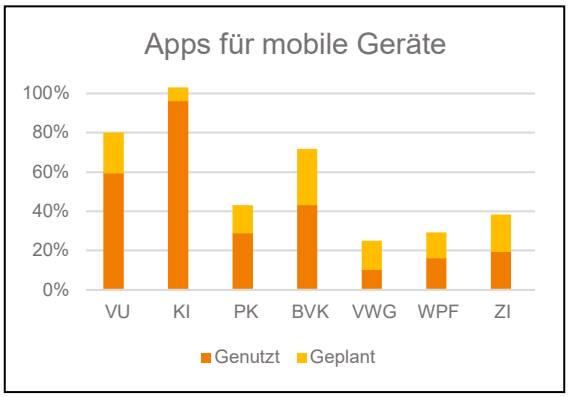
Wie bei den Livechat-Tools selbst planen auch bei Chatbots insbesondere VU und KI, diese künftig stärker einzusetzen. Daraus lassen sich einige Schlussfolgerungen ziehen:

- In Chatbots wird ein gewisses Potential gesehen, die Übernahme in den Betrieb läuft jedoch nicht so schnell wie ursprünglich geplant.
- Wie bei den Livechat-Tools selbst, von deren Einsatz ein Chatbot abhängt, scheint die Umsetzung nicht die höchste Priorität zu haben.
- Die meisten Unternehmen, die den Einsatz von Livechat-Tools planen, planen gleichzeitig die Automatisierung mittels Chatbot. Der Mehrwert von Chatprogrammen hängt somit stark von deren Automatisierbarkeit ab.

Beim Einsatz von Chatbots in der Kundenberatung können sich außerdem rechtliche Herausforderungen ergeben. Aufgrund der Einschränkungen der Technologie selbst und diesem zusätzlichen Aspekt werden zukünftige Umsetzungen in diesem Feld wohl davon abhängen, welchen Unternehmen es gelingt, klar abgrenzbare und definierbare Anwendungsfälle für den Bot zu finden.

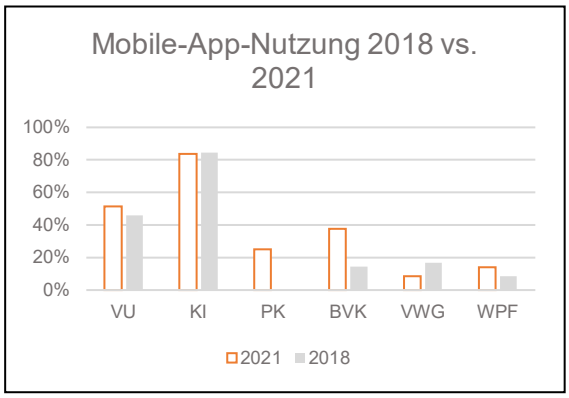
Kommunikation über mobile Geräte mittels **Messaging Services** oder anderer Apps wurde insbesondere von VU und KI bereits 2018 relativ breit eingesetzt. Insbesondere PK und BVK haben seitdem nachgezogen:





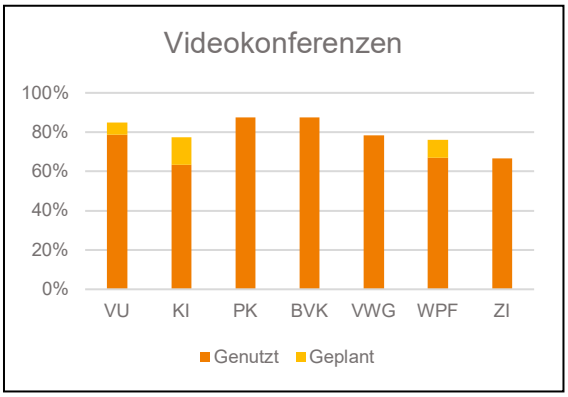
Da die Nutzung von Apps auch in Zeiten von COVID-19 bei VU und KI nicht merklich zugenommen hat, kann angenommen werden, dass bereits die meisten der Unternehmen dieser Sektoren, die einen Mehrwert in diesen Kommunikationskanälen sehen, sie bereits einsetzen.

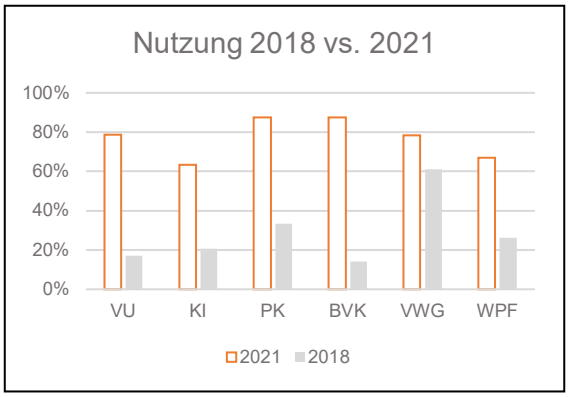
PK und BVK sind noch nicht an diesem Peak angelangt, sodass die Nutzung von Messaging Services und mobilen Apps hier in Zukunft vermutlich noch zunehmen wird.



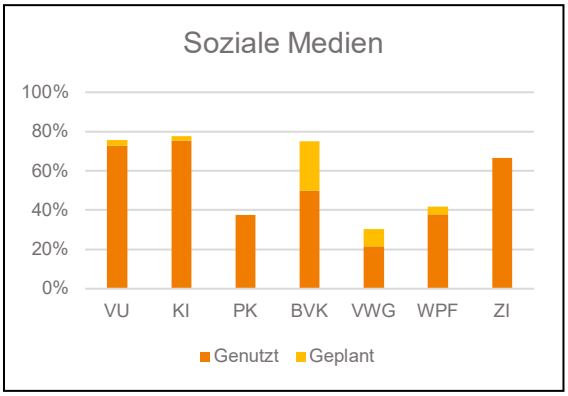
Bei VWG und WPF zeigt sich hingegen noch kein klarer Trend. Zwar planen einige Unternehmen diese Werkzeuge aufzugreifen, andererseits hat sich in dieser Hinsicht in den letzten drei Jahren wenig bewegt. Kurz- und mittelfristig gesehen werden mobile Kommunikationskanäle von diesen Sektoren also vermutlich nicht flächendeckend erschlossen werden.

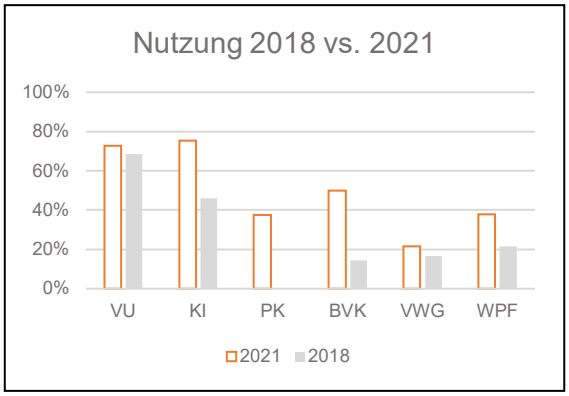
Videokonferenzen haben in den letzten drei Jahren in allen Sparten den stärksten Aufwärtstrend erfahren. Im Zuge der Lockdowns haben sie in vielen Fällen den direkten Kundenkontakt abgelöst. Während die anderen Kommunikationskanäle oft neue Ansätze sind, die zusätzlich gewählt werden, um bestimmte Kundensegmente besser anzusprechen oder Prozesse effizienter zu gestalten, wurden Videokonferenzen eingesetzt, um das Tagesgeschäft am Laufen zu halten. Nachdem sich diese Tools für interne und externe Kommunikation etabliert haben, ist anzunehmen, dass sie auch weiterhin in ähnlichem Ausmaß genutzt werden.





Soziale Medien nehmen ebenfalls klar eine größere Rolle in der Kundenkommunikation ein als noch vor drei Jahren:

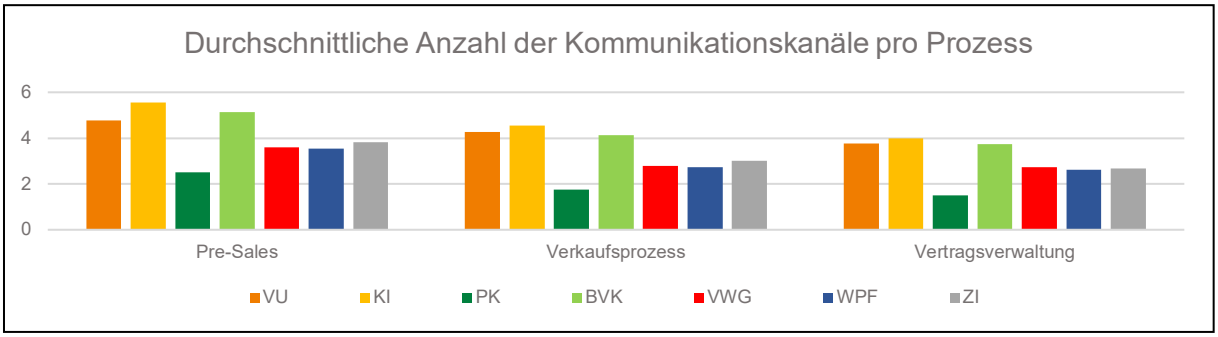




- Mit Ausnahme des Versicherungssektors, welcher bereits 2018 stark Gebrauch von sozialen Medien machte, ist die Nutzung dieser Netzwerke durch Unternehmen deutlich gestiegen. Abgesehen von Plänen bei BVK und VWG scheint dabei bereits ein gewisser Sättigungseffekt eingetreten zu sein und der Nutzungsgrad mittelfristig auf hohem Niveau zu stagnieren.
- Dabei werden soziale Medien speziell für die Akquise von Neukunden genutzt (siehe Abschnitt 3.2). Ein Treiber der stark gestiegenen Präsenz der Unternehmen in den entsprechenden Netzwerken kann möglicherweise auf einen gewissen Konkurrenzdruck zurückzuführen sein. Die Präsenz in sozialen Medien gehört heutzutage für viele Unternehmen zum Standard. Kein Unternehmen möchte es sich leisten, als eines von wenigen nicht vertreten zu sein, zumal der Aufwand für die Wartung entsprechender Social-Media Accounts in der Regel überschaubar ist.

3.2 DIGITALE KOMMUNIKATION IN DEN GESCHÄFTSPROZESSEN

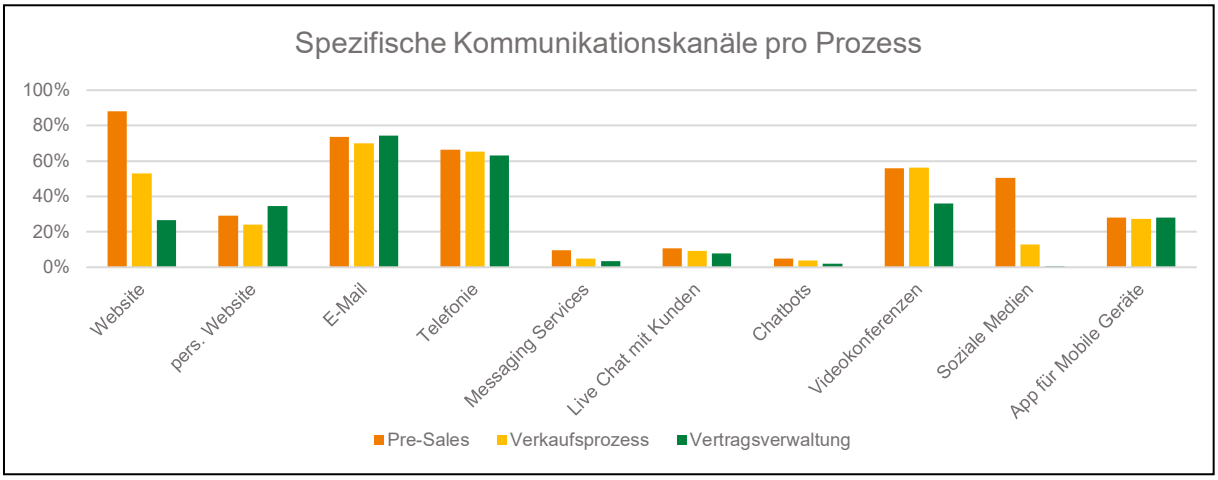
Allgemein setzen Unternehmen mehr **Kommunikationsmedien im Bereich Pre-Sales als beim Verkaufsprozess selbst ein**, Schlusslicht ist die Vertragsverwaltung. Dies kann auf einen gewissen Konkurrenzdruck bei der Neukundenakquise hindeuten, allerdings differieren die Kommunikationsmedien auch in Hinblick auf ihre inheränten Eigenschaften voneinander und sind für unterschiedliche Zwecke unterschiedlich gut geeignet.



Im Einsatzgebiet der Kommunikationskanäle zeigen sich klare, mit den technischen Eigenschaften der Kommunikationsmedien einhergehende Unterschiede.

- Insbesondere Websites und soziale Medien sind geeignet, schnell eine begrenzte Menge an Information an einen weiten Adressatenkreis zu bringen, was sie für den Einsatz im Pre-Sales Bereich prädestiniert.
- Personalisierte Websites (Kundenportale) sind hingegen insbesondere für die Verwaltung bestehender Vertragsverhältnisse geeignet.

Die folgende Graphik zeigt die anteilige Nutzung der Kommunikationskanäle pro Prozess aggregiert für alle Finanzmarktsegmente:

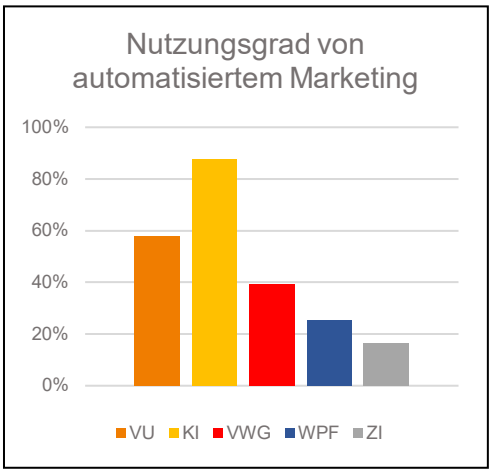


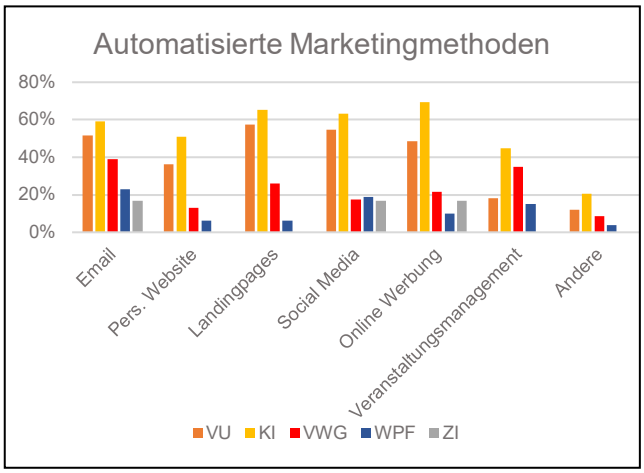
Insgesamt setzen die Unternehmen mehr Kanäle für Pre-Sales bzw. Marketing ein als für den Kontakt mit bestehenden Kunden, dafür sind diese meistens weniger aufwändig zu betreiben.
Für die FMA ist insbesondere der Verkaufsprozess relevant, da hier je nach Finanzmarktsegment spezielle aufsichtsrechtliche Regelungen für den Kundenkontakt einzuhalten sind.
Trotz unterschiedlicher Gewichtungen sind praktisch alle abgefragten Kanäle in allen Prozessen im Einsatz, was die Notwendigkeit für die Aufsicht unterstreicht, mit neuen Technologien Schritt zu halten und die bestehenden Regelungen in einem dynamischen Kontext anzuwenden.

3.3 AUTOMATISIERTES MARKETING

Softwaregestützte Methoden zur Automatisierung von Marketing- und Vertriebsprozessen werden unter den beaufsichtigten Unternehmen immer häufiger eingesetzt. Angefangen bei E-Mail-Newslettern bis hin zu Anzeigekampagnen in Suchmaschinen und sozialen Medien existieren bereits zahlreiche Möglichkeiten, um die Reichweite des eigenen Marketings – und somit die Zahl potentieller Neukunden – zu vergrößern und den Werbeprozess effizienter zu gestalten. Konkret befragt wurden die Unternehmen nach der Nutzung automatisierter Marketingprozesse in folgenden Kategorien (aufgrund der Geschäftsmodelle, die nicht auf direktes Privatkundenmarketing aufbauen, wurden in den Sektoren PK, BVK und MI hierzu keine Daten erhoben):

- E-Mail Kampagnen (automatisierte Newsletter etc.)
- Personalisierte Website (personalisierte Angebote im Kundenportal)
- Personalisierte Landingpages basierend auf Kundenverhalten
- Social Media (gezielte Werbung basierend auf Kundendaten)
- Online Werbung (Kampagnen in Suchmaschinen etc.)
- Veranstaltungsmanagement (automatisierte Einladungen/Erinnerungen)





Automatisiertes Marketing wird allen voran von KI (88%), gefolgt von VU (58%) und VWG (39%) eingesetzt. Auch WPF (25%) und ZI (17%) wenden diese Form des Marketings teilweise an.

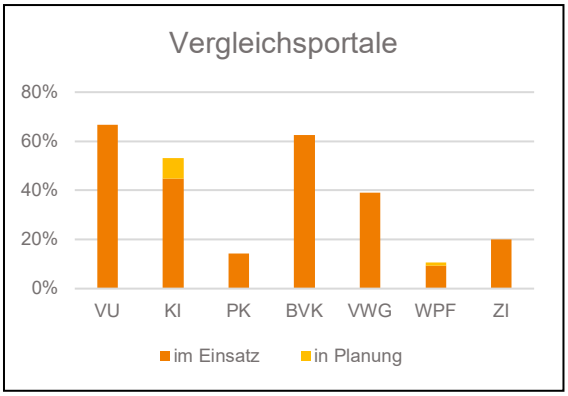
Ähnlich wie im Bereich der Pre-Sales Kommunikationskanäle, sind in den Unternehmen diverse Methoden parallel im Einsatz, um eine möglichst große Reichweite zu erzielen. Die häufigsten automationsunterstützten Marketingmethoden stellen hierbei **Online Werbung** (zB Google-Ads im Rahmen von Werbekampagnen), **Landingpages** (Webpages mit Kampagnenbezug), **Social Media** (zB Werbung ggf. mit Trackingmöglichkeiten via Youtube, Instagram, Facebook o.Ä.) und **E-Mail** (zB Newsletter, Erstinformationen zu Produktneuheiten, Geburtstagswünsche).

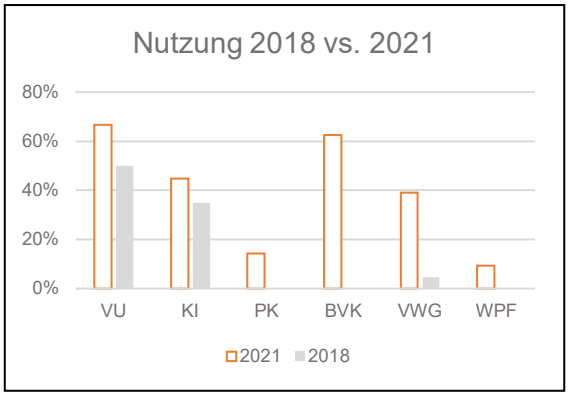
Etwas weniger wird auf **personalisierte Webseiten** (zB zur direkten Ansprache des Kunden mit Bonusaktionen) bzw. **Veranstaltungsmanagement** (zB jährliche Kundenevents) abgestellt. Abgesehen von den vorgegebenen Auswahlkategorien wurden InGame-Ads, Prämienrechner mit Online-Abschluss sowie Geburtstags- bzw. Terminerinnerungs-SMS als Maßnahmen im Rahmen der Befragung angeführt, um eine größere Reichweite zu erzielen sowie Kundenbindung zu erzeugen.

Aufgrund der bereits recht ausgeprägten Verbreitung dieser Methoden unter KI, ist zu erwarten, dass insbesondere VU und VWG in den nächsten Jahren die Möglichkeiten des automatisierten Marketings weiter ausbauen. Insbesondere im Pre-Sales Bereich herrscht ein erkennbarer Konkurrenzdruck innerhalb der Branchen, worin ein starker Anreiz besteht, neue Marketingmethoden aufzugreifen, sobald diese bei den Peers eine gewisse Verbreitung aufweisen.

3.4 VERGLEICHSPORTALE

Vergleichsportale haben stark an Bedeutung gewonnen: während 2018 im Grunde nur VU und KI ihre Produkte listen ließen, setzten sich Vergleichsportale über die letzten Jahre praktisch in allen Sektoren als Pre-Sales-Instrument durch.

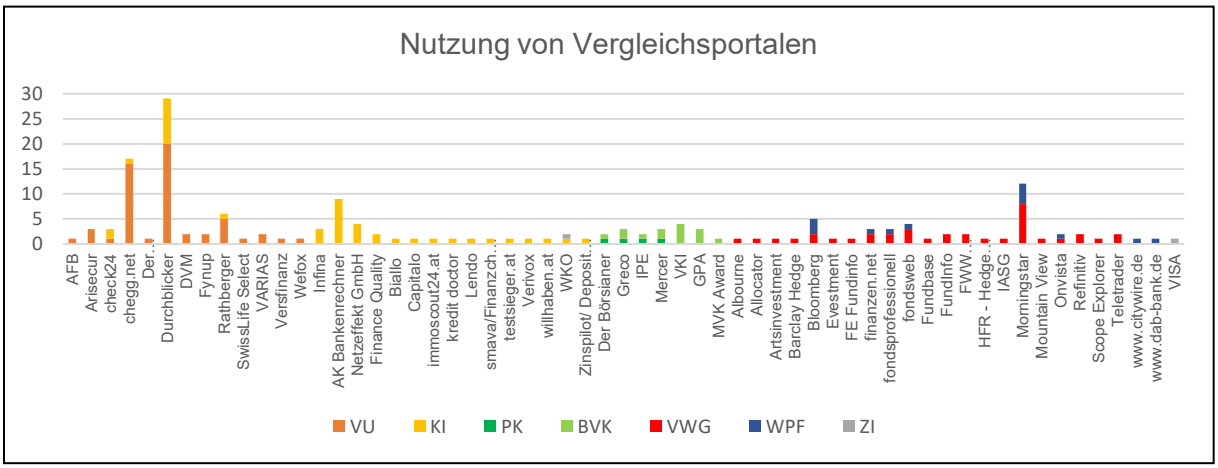




Die starke Konkurrenz der Unternehmen im Bereich Pre-Sales ist hier möglicherweise ein essentieller Faktor. Potentielle Kunden sowie auch Dienstleister können sich über Vergleichsportale

mit geringem zeitlichen Aufwand selbst über Dienstleistungen und Produkte informieren und stehen im Zuge dessen oftmals bereits nahe an einem Geschäftsabschluss. Der Druck, die eigenen Produkte in Vergleichsportalen zu listen, ist im Fall, wenn konkurrierende Unternehmen dies bereits tun, entsprechend groß.

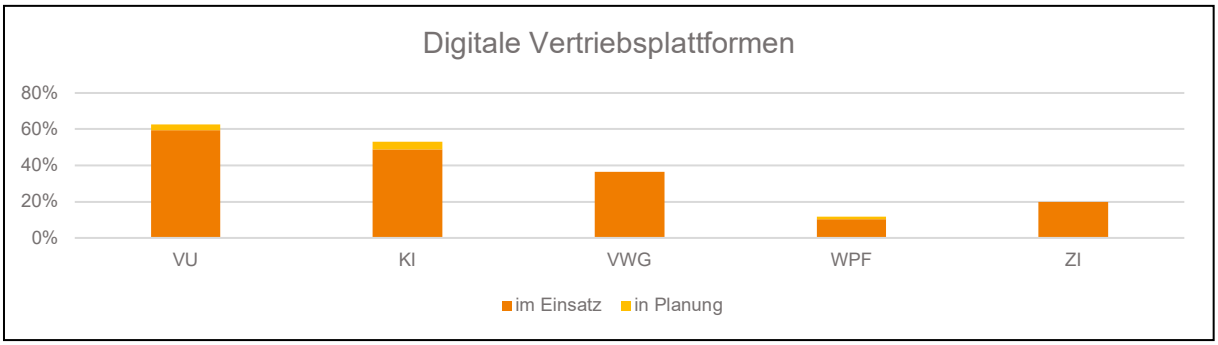
- VU setzen im Bereich der Vergleichsportale insbesondere auf „Durchblicker.at“, „chegg.net“ und „Rathberger“.
- KI sind ebenfalls vorwiegend über „Durchblicker.at“ und den Bankenrechner der Arbeiterkammer Österreich in Vergleichsportale eingebunden.
- PK und BVK werden auf Vergleichsportalen des VKI, des GPA sowie „Greco“ oder „Mercer“ gelistet.
- In den Sektoren der VWG und WPF spielen Finanzinformationsunternehmen wie Morningstar und Bloomberg im Rahmen von Vergleichsmöglichkeiten die größte Rolle.



Die FMA hat bereits 2020 im Versicherungssektor die Praktiken der einzelnen Vergleichsportale am österreichischen Versicherungsmarkt analysiert und eine Informationsbroschüre herausgegeben, in der sie praktische Hinweise gibt, was bei der Nutzung von Vergleichsportalen im Hinblick auf Aktualität der Inhalte, Unabhängigkeit der Portale, Provision der Vermittler, Ranking der Produktauswahl und Beratung zu beachten ist. Eine Checkliste enthält Hinweise darauf, worauf vor Vertragsabschluss geachtet werden sollte.

3.5 DIGITALE VERTRIEBSPLATTFORMEN

Die Digitalisierung erleichtert und fördert die Nutzung von digitalen Vertriebsplattformen. Digitale Vertriebsplattformen werden ähnlich oft genutzt wie Vergleichsportale (VU 59%, KI 49%, VWG 36%, WPF 10%, ZI 20%). Aufgrund der konzeptuellen Nähe zu den Vergleichsportalen kann hier eine ähnliche Entwicklung angenommen werden: Einerseits verdeutlicht dies das Voranschreiten der digitalen Entwicklung, insbesondere im Vertriebsprozess, andererseits unterstreichen diese Entwicklungen auch die wachsende Bedeutung von Kooperationen und Partnerschaften zwischen beaufsichtigten Unternehmen und digitalen Dienstleistern.



Die beaufsichtigten Unternehmen nutzen dabei zahlreiche unterschiedliche Vertriebsplattformen. Über alle Sektoren hinweg entfällt jedoch der mit Abstand größte Nutzeranteil auf „Durchblicker.at“ sowie die unternehmenseigenen Webpages/Kundenportale. Am häufigsten werden folgende Vertriebsplattformen genutzt:

VU	■ Durchblicker
	■ Arisecur
	■ chegg.net
	■ Clark
	■ fynup
	■ Klickmal
	■ Together
KI	■ Durchblicker
	■ Google
	■ immoscout24
	■ Bing
	■ Netzeffekt GmbH
VWG	■ Clearstream
	■ Cominvest

Derzeit liegt der prozentuelle Anteil des Absatzes über Vergleichsportale und Vertriebsplattformen bei den meisten Unternehmen im einstelligen Prozentbereich oder darunter. Hier kann jedoch in

den nächsten Jahren ein weiteres Wachstum erwartet werden. Mit steigender Nutzung von Vergleichsportalen steigt implizit auch der Bedarf an Fairness und Transparenz dieser Anbieter. Die regulatorischen Anforderungen, welche in den einzelnen Segmenten des Finanzmarktes gelten, sollen auch bei diesen (vergleichsweise neuen) Vertriebsformen bedacht werden.

3.6 FAZIT UND HANDLUNGSFELDER FÜR DIE FMA

Die FMA muss aufsichtsrechtliche Implikationen auch bezogen auf bislang wenig bzw. nur in einigen Sektoren verwendeten digitalen Technologien (Vergleichsportale, soziale Medien, Chatbot) beurteilen können:

Aus den Umfrageergebnissen lassen sich drei grobe Gruppen an Technologien ableiten:

- **Etablierte Kommunikationsmittel** (zB Website, Telefonie, E-Mail, Videokonferenzen, App für mobile Geräte) werden bereits von einer breiten Mehrheit der Beaufsichtigten genutzt.
- **Wachstumsgruppen** (zB soziale Medien, Vergleichsportale) haben bereits eine gewisse Verbreitung am Finanzmarkt erlangt und sollen künftig noch stärker genutzt werden. Dadurch scheint es, als ob diese Kommunikationswege bald zum Standard gehören werden.
- **Randgruppen** (zB Live Chat, Chatbots) kommen kaum bzw. nur in einigen Sektoren zum Einsatz. Einige Unternehmen planen die Einführung dieser Technologien, wodurch sie in absehbarer Zeit vermutlich eine bedeutendere Rolle spielen werden.

Digitale Transformation braucht stabiles Fundament und Rechtssicherheit

- Rechtsunsicherheiten hinsichtlich der aufsichtsrechtlichen Einordnung und der Möglichkeiten der praktischen Umsetzung betreffen insbesondere
  - die Frage der Zustimmungserfordernisse im Rahmen des elektronischen Vertragsabschlusses und der elektronischen Kommunikation,
  - die Beurteilung der Möglichkeiten einer Einflussnahme auf die Reihung in einem Vergleichsportal (zB im Hinblick auf potentielle Interessenkonflikte; die FMA hat bereits 2020 die Praktiken der Vergleichsportale im österreichischen Versicherungssektor analysiert und festgestellt, dass der Detaillierungsgrad der vom Nutzer abgefragten Informationen sehr unterschiedlich ist),
  - die Beurteilung, welche Technologien die Anforderungen an einen dauerhaften Datenträger erfüllen oder welche Anforderungen an voll- und teilautomatisierte Beratungssysteme und Beratungsalgorithmen gestellt werden.

Die FMA sollte deshalb in diesen Bereichen auf mehr Rechtssicherheit hinwirken und ggf. ihre Standpunkte bzw. Erwartungshaltung kommunizieren, um Rechtsrisiken möglichst zu minimieren und ein Level-playing-field zu schaffen.

3.7 KONSULTATION ZUM VERTRIEB

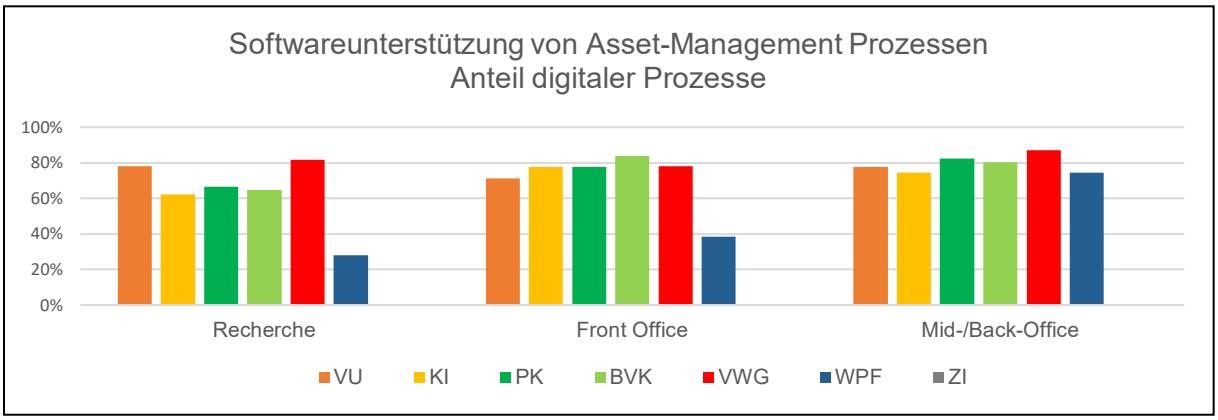
- Welche Aufgaben soll die FMA im Rahmen des Anleger-, Versicherten- und Gläubigerschutzes im Hinblick auf die Digitalisierung der Schnittstellen zu den Kunden wahrnehmen?
- In welcher Form sollen diese Aufgaben übernommen werden?
- Welche konkreten regulatorischen Vorgaben sind durch die Digitalisierung des Finanzsektors noch notwendig?
- Bestehen aus Ihrer Sicht in Österreich Hindernisse, welche die digitale Kommunikation erschweren?
- Welche konkreten positiven, aber auch negativen Entwicklungen bezüglich des „digitalen“ Vertriebs sind aus Ihrer Sicht zu beobachten?

4 ASSET MANAGEMENT

Die digitalen Informationstechnologien haben bereits sehr lange Eingang in das Asset Management gefunden. Die Digitalisierung im Asset Management betrifft sowohl die IT-Systeme der Marktteilnehmer als auch die Finanzinstrumente zB in Form neuer Anlageformen oder Anlageklassen. Um zu evaluieren, wie die Informationstechnologien in Aufsicht und Regulierung der beaufsichtigten Unternehmen berücksichtigt werden, wurde deren Einsatz anhand der einzelnen Prozessschritte in der Veranlagung untersucht und analysiert.

4.1 IT-SYSTEME IM ASSET MANAGEMENT

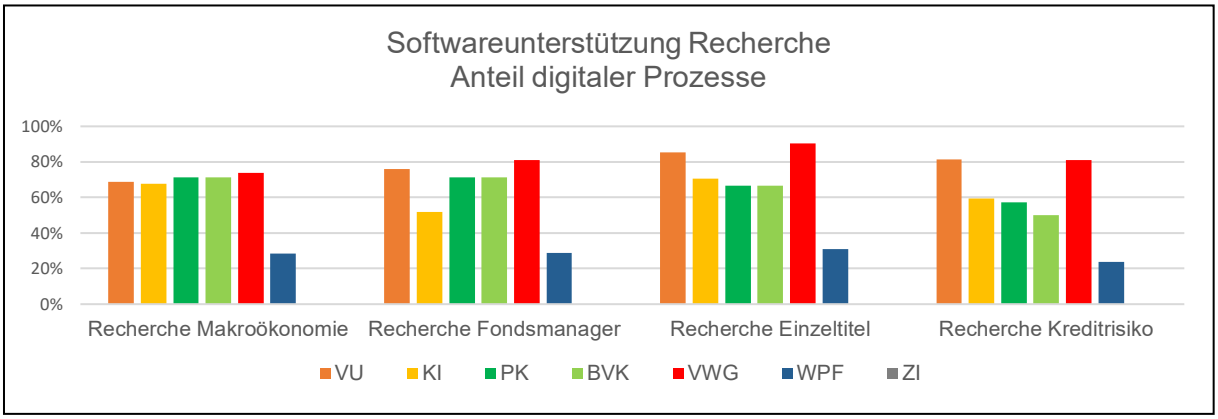
IT-Systeme kommen bei praktisch allen Prozessen im Asset Management zum Einsatz. Die unterschiedlichen Anteile an digitalen bzw. nicht digitalen Prozessen in den einzelnen Sektoren ist durch die branchenspezifischen Unterschiede der Geschäftsmodelle bedingt.



Insbesondere die Unternehmensgröße, die eingesetzten Ressourcen sowie der Grad der Zentralisierung der Veranlagung sind maßgeblich für den Digitalisierungsgrad in den Asset-Management-Prozessen. Auch die regulatorischen Anforderungen spielen dabei eine Rolle.

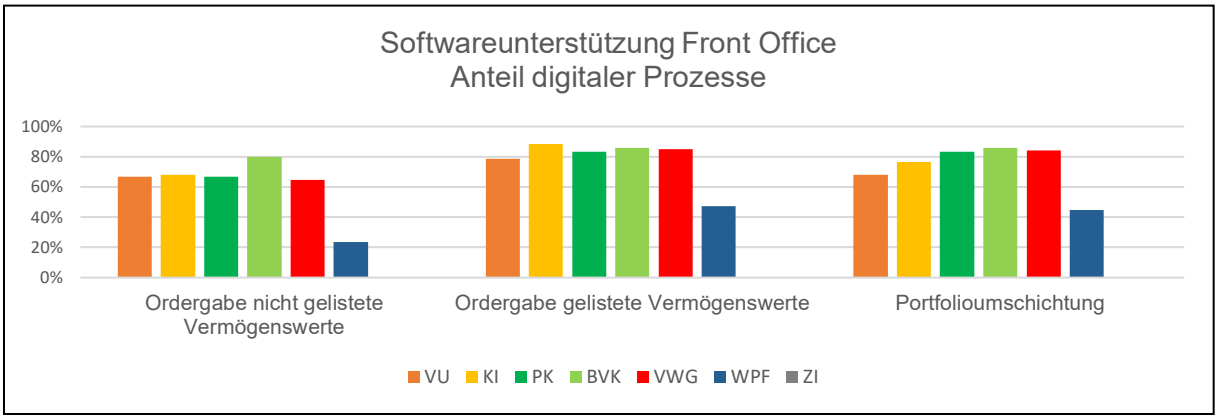
4.1.1 RECHERCHE

Vor jeder Investmententscheidung steht eine umfassende Daten-Analyse, zB hinsichtlich der Auswahl von externen Managern oder Einzeltitelinvestments. Ebenso ist iZm der laufenden Due Diligence eine Vielzahl von Informationen (zB Bilanzkennzahlen, Performances) zu evaluieren, zu dokumentieren und zu überwachen.



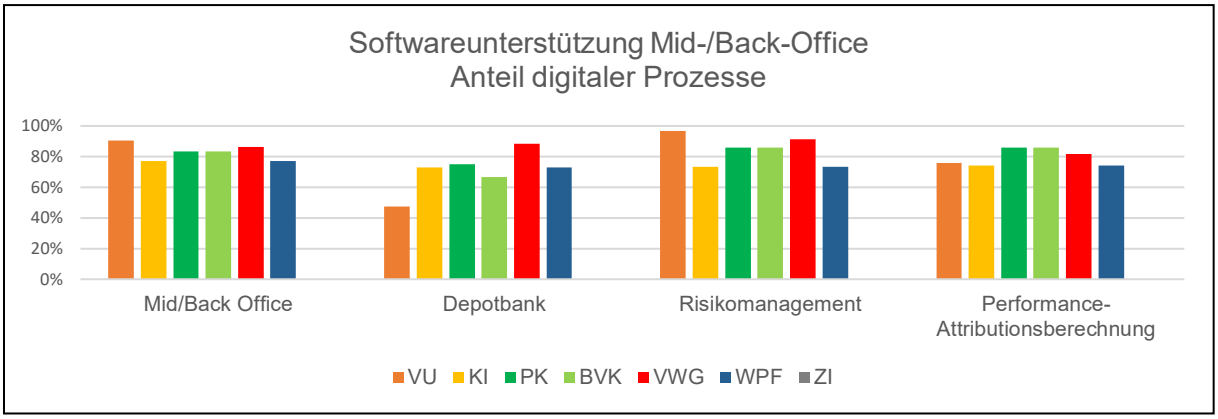
4.1.2 FRONT OFFICE

Nach Recherche im Rahmen der Due Diligence erfolgt die Umsetzung der Veranlagungsentscheidungen im Portfoliomanagement, wobei unterschiedliche Prozessschritte iZm dem Einsatz von IT-Systemen unterschieden werden können:

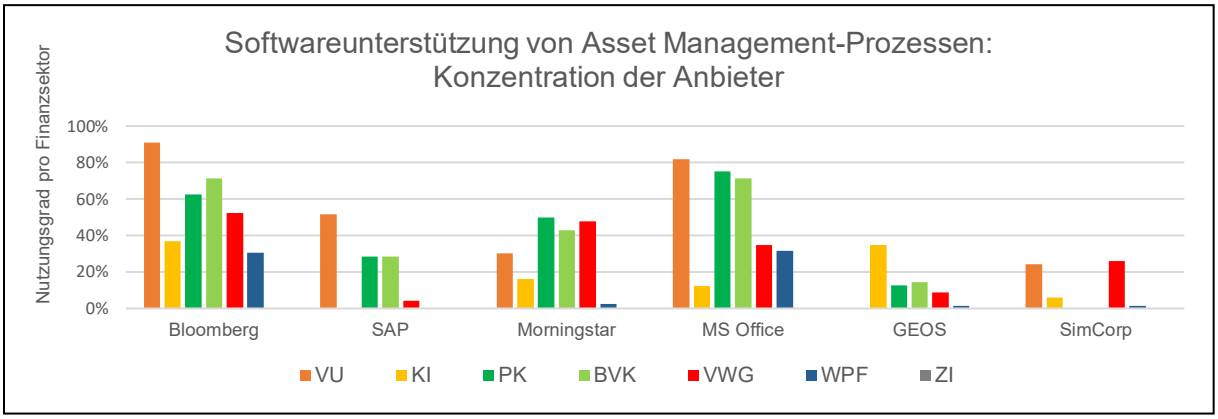


4.1.3 MID/BACK OFFICE

Nach erfolgter Investmententscheidung und Ordergabe, werden die Wertpapieraufträge abgewickelt und verbucht bzw. die Dokumentation iZm nicht gelisteten Vermögenswerten entsprechend aufbewahrt. Zu den Mid- und Back-Office Funktionen gehören auch die Schnittstelle zur Depotbank, das laufende Risikomanagement und die Performanceattributions-Analyse.



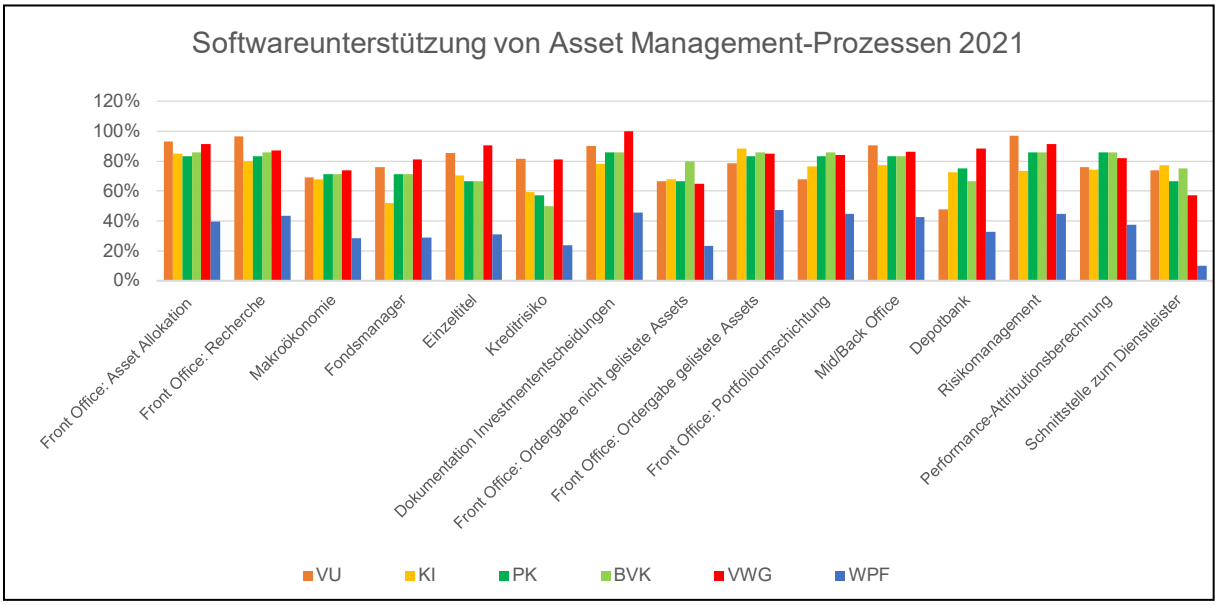
Insgesamt kommen folgende Informations- und Bestandsverwaltungs-Systeme am häufigsten im Asset Management zum Einsatz: Bloomberg, SAP, Morningstar, MS Office, GEOS (SDS) und SimCorp:



4.1.4 SOFTWAREUNTERSTÜTZUNG DER ASSET MANAGEMENT PROZESSE

Der Vergleich der erhobenen Nutzungsdaten von Softwarelösungen in Asset-Management Prozessen der beaufsichtigten Unternehmen mit jenen aus 2018 zeigt, dass der Anteil der Softwareunterstützung je nach Unternehmenskategorie und Anwendungsbereich in etwa auf demselben Niveau stagniert bzw. sogar leicht rückläufig ist.

- VU haben die Softwareunterstützung der Asset-Management Prozesse in einigen Bereichen (Recherche, Dokumentation, Ordergabe nicht gelistete Vermögenswerte, Depotbank und Performance-Attribut) anteilsmäßig etwas erhöht, während diese in den übrigen Prozessteilen in etwa auf gleichem Niveau geblieben sind.
- KI haben Softwareunterstützung in den meisten Teilprozessen ausgebaut und die vergleichsweise größte Steigerung realisiert.
- Im Bereich der PK hat der Anteil der softwareunterstützten Prozesse mit Ausnahme der Teilprozesse „Dokumentation Investmententscheidungen“ und „Depotbank“ etwas abgenommen.
- Bei VWG und BVK war der Anteil 2018 bereits hoch, eine weitere Steigerung ist nur vereinzelt festzustellen, beispielsweise im Bereich Dokumentation. Tendenziell sind die meisten Bereiche leicht rückläufig. Hier ist jedoch auch eine Veränderung in der Zusammensetzung und der Anzahl der Befragten im Vergleich zu 2018 zu berücksichtigen.
- Bei WPF hat die Softwareunterstützung in der überwiegenden Anzahl (Ausnahmen „Kreditrisiko“ und Ordergabe nicht gelistete Vermögenswerte) der Teilprozesse verhältnismäßig ebenfalls abgenommen.



4.2 NEUE ANLAGEFORMEN UND KRYPTO-ASSETS

Angesichts der Dynamik im Bereich der Krypto-Assets und unter Berücksichtigung von Einflussfaktoren wie steigendem Kostendruck, Niedrigzinsumfeld und der Suche nach renditebringenden Investments stellt sich die Frage, inwieweit neue Anlageformen zum Einsatz kommen. Die aktuelle Studie zeigt, dass die beaufsichtigten Unternehmen beim Einsatz von Blockchain-Technologie und Dienstleistungen in virtuellen Währungen nach wie vor zurückhaltend sind:

In % des Gesamtportfolios		*VU*	*KI*	*PK*	*BVK*	*VWG*	*WPF*
Beteiligung an FinTech	Eigen aktuell	<0,1 - <1	0,02 – 0,2	-	-	-	-
	Geplant	-	-	-	-	-	-
	Fremd aktuell	0,0005 – <1	0,17	-	-	-	-
	Geplant	-	-	-	0,015	-	-
Krypt-Assets	Eigen aktuell	-	0 – 0,036	-	-	-	-
	Geplant	-	-	-	-	-	-
	Fremd aktuell	-	-	-	-	-	-
	Geplant	-	0,012	-	-	0,0157	0,001 - 2

- Kein VU erbringt Dienstleistungen in virtuellen Währungen. Aus Veranlagungssicht planen fünf VU eine geringe Beteiligung an FinTech/InsurTech, drei davon halten bereits Beteiligungen im Ausmaß von jedenfalls unter 1% des Gesamtportfolios im Eigenbestand und planen keine nennenswerte Erhöhung. Indirekte Investments in Krypto-Assets über Fonds nehmen mit 0,0003% ebenfalls nur einen vernachlässigbaren Anteil ein und konzentrieren sich großteils auf ETFs, die nicht in Blockchain-Technologie selbst investieren, sondern bloß Zugang zu diesem Ökosystem gewähren.
- Lediglich ein befragtes KI ist aktuell indirekt in Krypto-Assets investiert (iHv 0,012% des Portfolios) und plant Investments in diesem Bereich auszuweiten (0,036-0,055%). Drei KI halten Beteiligungen an FinTech/InsurTech iHv rund 0,02-0,2% des Gesamtportfolios.
- Die PK sind in diesem Bereich noch zurückhaltender: Keine der PK erbringt Dienstleistungen iZm virtuellen Währungen oder plant direkte Investments in neue Anlageformen. Indirekte Fondinvestments in Assets im Krypto-Umfeld sind gering und beschränken sich auf Hardware und Software-Provider im Blockchain-Umfeld.
- Virtuelle Währungen werden zurzeit auch in BVK nicht aktiv eingesetzt. Eine BVK ist aktuell mit einem Anteil von 0,015% des Portfolios indirekt in FinTech/InsurTech investiert.
- Eines der beaufsichtigten VWG ist derzeit in Krypto-Assets (rund 0,015% des Gesamtportfolios, in Fremdbestand) investiert. Auch in dieser Sparte werden keinerlei Dienstleistungen iZm virtuellen Währungen erbracht.
- Eine WPF plant eine geringe (0-1% des Portfolios) Beteiligung an Krypto-Assets, zwei WPF sind in geringem Ausmaß in Krypto-Assets investiert. Eine weiterere plant ein Investment im FinTech/InsurTech in Fremdbestand (Kundengelder).
- Zwei WPF erbringen Dienstleistungen in virtuellen Währungen. Darüber hinaus hält ein Unternehmen eine Beteiligung an Krypto-Assets im Ausmaß von 0,5% des Portfolios.

4.3 FAZIT UND HANDLUNGSFELDER FÜR DIE FMA

Im Umfeld einer starken IT-Durchdringung gewinnen Automatisierungsprozesse an Bedeutung:

- Grundsätzlich gibt es bei den beaufsichtigten Unternehmen im Bereich Asset Management eine starke Durchdringung von IT-Systemen. Bei VU, VWG, WPF und BVK ist diese besonders stark ausgeprägt.
- Softwaregestützte Automatisierungsprozesse gewinnen dennoch zunehmend an Bedeutung. Im Hinblick auf den Kostendruck bei Asset Managern wird die Prozessautomatisierung mittels Robotic Process Automation (RPA) auch für Vermögensverwalter immer attraktiver. Die größten Effizienzpotentiale für RPA liegen nach wie vor im Middle- und Back-Office.

Monitoring des Ausbaus alternativer Techniken:

Eine starke Tendenz zum weiteren Ausbau von alternativen Techniken, wie AI, Deep Learning und Machine Learning lässt sich nicht feststellen. Diese Ergebnisse bedeuten grundsätzlich nicht, dass neue Technologien im Asset Management keine Rolle spielen, vielmehr werden spezielle Softwareanwendungen bereits entlang der Prozesskette eingesetzt.

Die manuelle Datenmanipulation stellt eine potentielle Fehlerquelle dar. Deshalb soll der Digitalisierungsgrad in die Beurteilung der Einhaltung des Prudent Person Prinzips in der Veranlagung Eingang finden:

- Wie die im Asset Management eingesetzten IT-Systeme in der unternehmensinternen IT-Landschaft verankert sind und ob bzw. von wem eine Prüfung vor Orderdurchführung durchgeführt wird, ist auch iZm den internen Veranlagungsgrenzen wichtig.
- Die elektronische Datenerfassung ist in der Regel ebenfalls Voraussetzung für die Erfassung der Vermögenswerte im Risikomanagement.

Die eingesetzten Finanzmarktdateninformationssysteme und die externen sowie unternehmens-internen Schnittstellen sind in einigen Sektoren in der Regel auch für die korrekte Berechnung des Eigenmittelerfordernisses maßgeblich.

- Ein Hauptproblem iZm der Bewertung der Vermögenswerte sind börsennotierte, jedoch oft wenig liquide Anleihen-Investments. Wenngleich der in den Finanzmarktdatensystemen ausgewiesene Marktwert nicht notwendigerweise den tatsächlich realisierbaren Veräußerungswert reflektiert, stützen sich auch alternative Bewertungsmethoden weitgehend auf Marktdaten (zB Zinssätze und -kurven, implizierte Volatilitäten).

- Da die Bewertung der Vermögenswerte direkt die Solvabilitätslage beeinflusst und Anleihen in einigen Sektoren die wichtigste Anlageklasse sind, sind die eingesetzten Finanzmarktdateninformationssysteme besonders wichtig[20]. Bei der aufsichtsbehördlichen Überprüfung sollen deshalb folgende Fragen in Erwägung gezogen werden:
  - Welche Finanzmarktdateninformationssysteme werden eingesetzt?
  - Wie sind die Software-Lizenzen definiert?
  - Wie und in welchen IT-Systemen werden alternative Bewertungsmethoden umgesetzt? Für welche Anlageklassen?
  - Welche Anpassungen in Bezug auf Marktdaten werden im Rahmen der Bewertung für die Solvenzbilanz „manuell" vorgenommen?
  - Wie sind die Schnittstellen mit externen Dienstleistern ausgestaltet?

Monitoring von Investments in neue Anlageformen:

- Eine der wesentlichen Fragestellungen zu neuen Anlageformen ist, wie diese bei Einstufung als Vermögenswerte bilanziell zuzuordnen sind. Indizien für eine Zuordnung zum Umlaufvermögen ist die hohe Volatilität virtueller Währungen, uU auch das umgehende Settlement.
- IZm der Veranlagung in Blockchain-Emissionen sollte Klarheit darüber herbeigeführt werden, inwiefern diese die Belegenheitsanforderungen erfüllen.
- Im Hinblick auf die häufig indirekte Form der Veranlagung über Investmentfonds ist zu klären, ob und wie institutionelle Investoren in Fonds mit neuen Anlageformen investieren und welche Investment-Prozesse und Risikomanagementanforderungen hierfür angewendet werden.
- Da in den Bewertungen von Wachstumsunternehmen oft die hohen Wachstumsraten eingepreist werden, können die gewählten Bewertungsansätze für FinTech-StartUps als Element zur Evaluierung der Veranlagung im Hinblick auf das Prudent Person Prinzip herangezogen werden.

[20] *Art. 10 der L2 VO (EU) 2015/35, 2017 wurden mehr als ein Viertel aller VU-Vermögenswerte zu alternativen Bewertungsmethoden bewertet.*

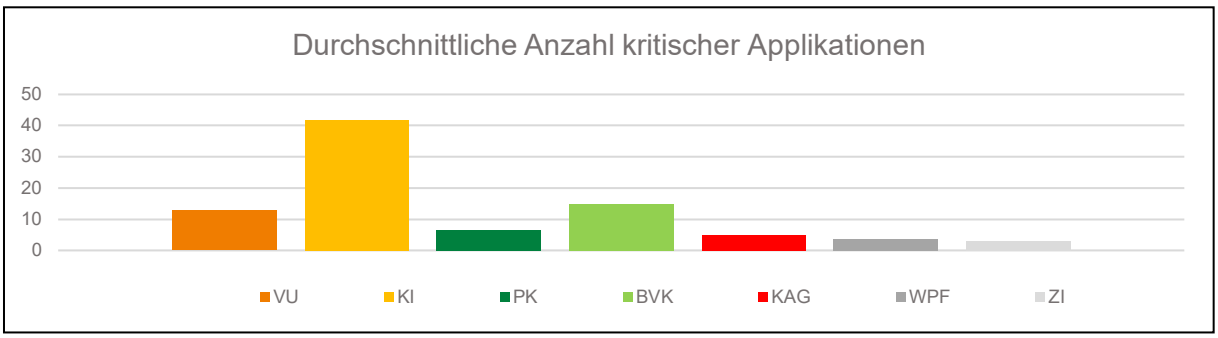
4.4 KONSULTATION ZUM ASSET MANAGEMENT

- Welche Aufgaben soll die FMA aus Ihrer Sicht bezüglich der Digitalisierung im Asset Management wahrnehmen?
- Welche konkreten regulatorischen Vorgaben sind durch die Digitalisierung des Finanzsektors noch notwendig?
- Welche Hindernisse bestehen in Österreich, um die Asset Management-Prozesse zu automatisieren und den Ausbau von alternativen Techniken, wie AI, Deep Learning und Machine Learning zu erleichtern?
- Welche konkreten positiven, aber auch negativen Entwicklungen bezüglich der Digitalisierung der Veranlagung sind zu beobachten?

5 IT-INFRASTRUKTUR

5.1 IT-SYSTEMLANDSCHAFT AM ÖSTERREICHISCHEN FINANZMARKT

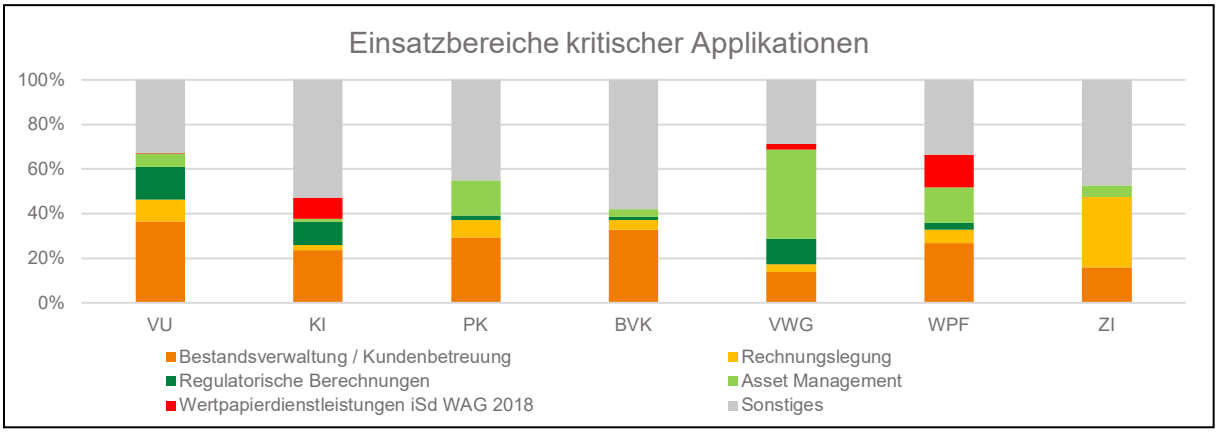
Die Akteure am österreichischen Finanzmarkt setzen zur Unterstützung ihrer kritischen Geschäftsprozesse **mehr als 3.000** (3.087) **IT-Applikationen** ein.
Mit durchschnittlich 42 Einzelsystemen sind allein im Bereich der Endanwender-Applikationen mit Abstand die meisten kritischen Applikationen **bei KI** im Einsatz, in großen Instituten werden teilweise sogar mehrere hundert Applikationen verwendet. Die den Applikationen zugrundeliegende Softwareinfrastruktur (zB Betriebssysteme, Virtualisierungslösungen) sowie Applikationen, welche für das Kerngeschäft nicht kritisch sind, werden nicht betrachtet.



Treiber für die Anzahl der eingesetzten Applikationen dürften dabei insbesondere das Geschäftsmodell und die IT-Strategie der Unternehmen sein:

- Einige der Finanzmarktsektoren wie etwa der Bankensektor decken hierbei entsprechend ihrem **Geschäftsmodell** inhärent ein vergleichbar breites Feld an Tätigkeiten ab, während andere stärker spezialisiert sind, wie es zB bei reinen Zahlungsdienstleistern oder VASP der Fall ist. Zusätzlich sind je nach Geschäftsfeld spezielle regulatorische Anforderungen abzudecken, wie die Prävention von Geldwäsche oder Terrorismusfinanzierung.
- Die **IT-Strategie** in Bezug auf die Systemlandschaft, egal ob geplant oder „gewachsen“, spiegelt sich ebenfalls in den Ergebnissen wider. Bei einigen Unternehmen sind Teile der Geschäftstätigkeit ausgelagert und somit ist die Zahl der In-House genutzten Anwendungen reduziert. Außerdem kann eine geringe Zahl an Anwendungen auf die Nutzung stark integrierter, multifunktionaler Anwendungen hindeuten, während andere Unternehmen ihre Prozesse mit zahlreichen kleineren Applikationen mit entsprechenden Schnittstellen zueinander unterstützen.

Der Unterschied in den Geschäftsmodellen spiegelt sich auch in den **Einsatzbereichen** der genutzten IT-Anwendungen wider:



- Systeme zur direkten **Bestandsverwaltung bzw. Kundenbetreuung** stellen je nach Sektor zwischen 37% (VU) und 14% (VWG) der kritischen Applikationen dar.
- Das **Asset Management** ist insb. bei VWG (40%) aber auch bei PK und WPF (je 16%) ein Bereich, in dem ein signifikanter Anteil der kritischen Softwarelösungen eingesetzt wird.
- Applikationen für **regulatorische Berechnungen** stellen insbesondere bei VU (15%), VWG (11%) und KI (10%) einen nennenswerten Anteil der kritischen Softwarelösungen dar.

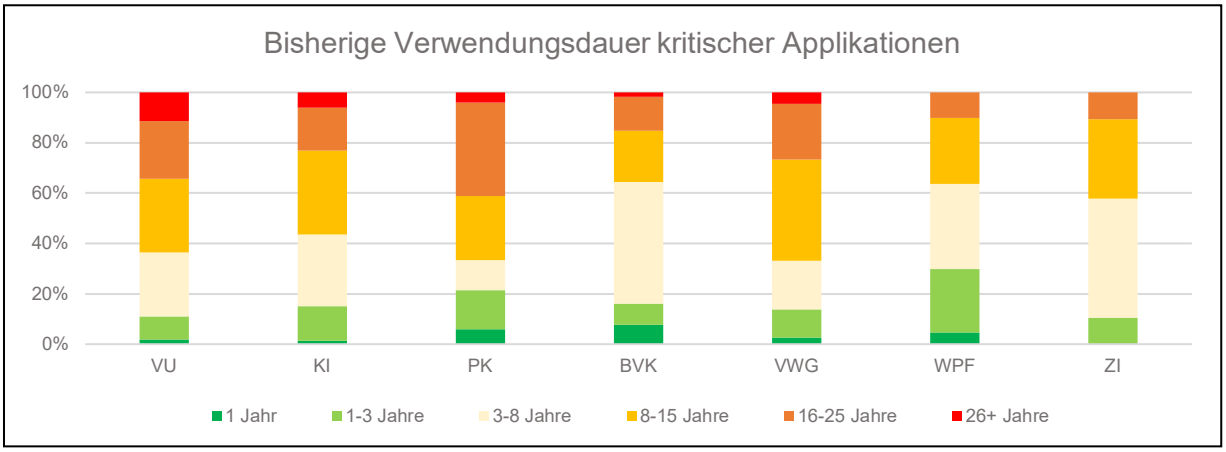
Unter „Sonstige“ Applikationen wurden von den Unternehmen etwa Kollaborationssysteme (parallele Bearbeitung von Dokumenten), Kommunikationssysteme, Geldwäscheprüfung/KYC, Fraudprüfung, Banktransaktionssysteme, Dokumentenverwaltungssysteme, Personalverwaltung subsumiert.

5.2 LIFE-CYCLE DER EINGESETZTEN IT-SYSTEME

Die Zukunftsfähigkeit der IT-Infrastruktur am österreichischen Finanzmarkt hängt von mehreren Faktoren ab. Einer davon ist die **Nutzungsdauer der eingesetzten IT-Systeme**. Eine veraltete IT-Landschaft

- ist Quelle von **operationalen Risiken** (Wartungslizenzen laufen aus, neue Anforderungen lassen sich zunehmend schwierig abbilden und mitunter nimmt durch Abgang bzw. Pensionierung von Kernmitarbeitern das vorhandene Know-How zu alter Software ab),
- kann besonders anfällig hinsichtlich von **Cyberrisiken** sein,
- bedingt **höhere Kosten** für deren Wartung, Weiterentwicklung und potentiellen Ersatz und
- erfordert teilweise relativ **aufwändige Softwareprojekte** zu deren Ablöse.

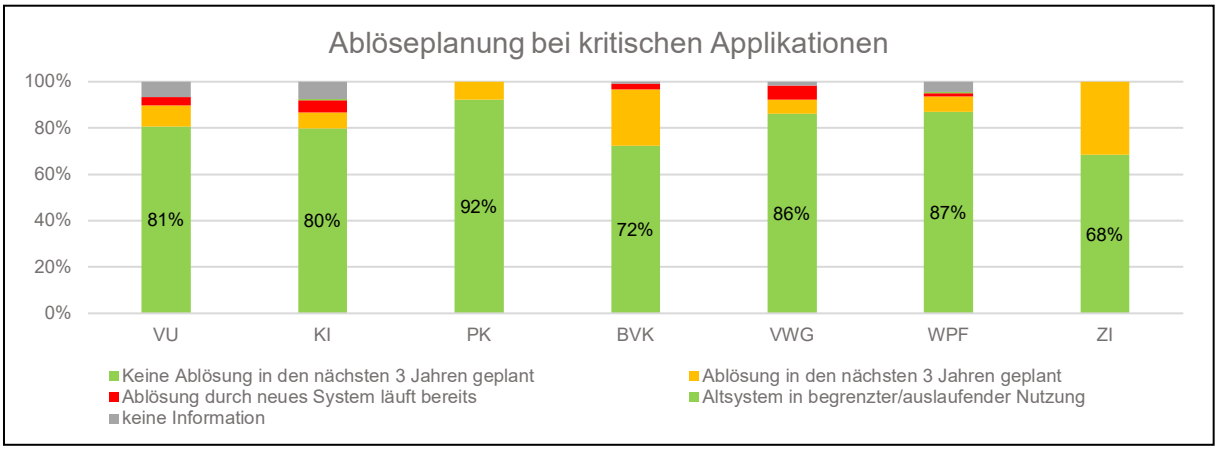
In den meisten Sektoren des Finanzmarktes werden IT-Anwendungen teilweise über Jahrzehnte hinweg genutzt.



- Bei **VU** sind rund 34% der Applikationen mindestens seit 16 Jahren, 11% sogar seit 26 Jahren im Einsatz.
- **KI** weisen mit 6% den zweithöchsten Anteil von Systemen im Bereich 26+ Jahre auf, 17% sind zwischen 16 und 25 Jahren im Einsatz.
- Bei **PK** zeigt sich einerseits mit 41% ein relativ hoher Anteil an Systemen, welche seit 16+ Jahren genutzt werden, andererseits wurden 22% der kritischen Applikationen erst in den letzten 3 Jahren in Betrieb genommen.
- Die Softwarelandschaft bei **BVK** wurde vergleichsweise häufiger erneuert, rund 64% der kritischen Applikationen sind 8 Jahre oder weniger im Einsatz.

- Bei **VWG** haben 27% der kritischen Applikationen eine Einsatzdauer von 16+ Jahren, während 19% der Applikationen eine Einsatzdauer von 3-8 Jahren haben.
- **VASP** stellen eine Sparte des Finanzmarktes dar, die insgesamt relativ jung ist, was sich auch in der Nutzungsdauer der Software widerspiegelt (75% seit 3 Jahren oder weniger genutzt).
- Die **WPF** haben mit 30% einen relativ hohen Anteil ihrer kritischen Applikationen in den letzten drei Jahren in Betrieb genommen, während nur 10% der Applikationen älter als 16 Jahre und keine älter als 26 Jahre sind.
- Von **ZI** werden Softwarelösungen mit einer durchschnittlich sehr ausgeglichenen Altersstruktur genutzt: lediglich je 11% der kritischen Applikationen sind länger als 16 oder kürzer als 3 Jahre im Einsatz.

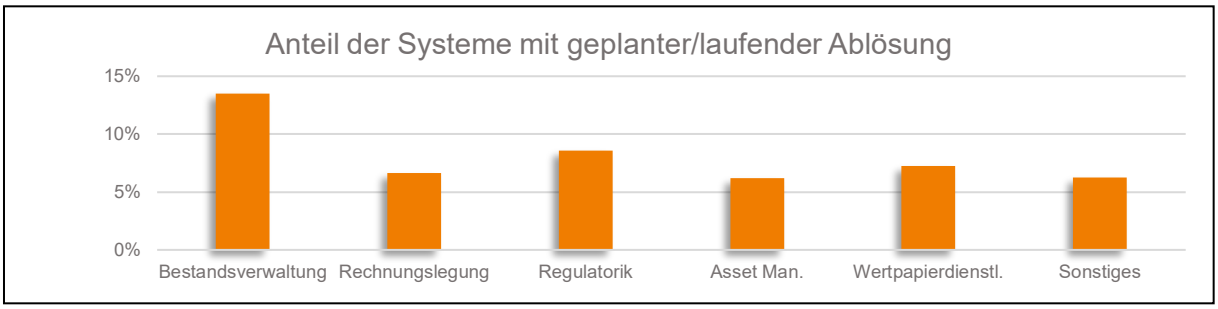
Der Life-Cycle-Status kritischer Applikationen darf jedoch nicht auf das reine Alter der eingesetzten Systeme reduziert werden. Die FMA hat deshalb auch die **Ablöseplanung der Unternehmen** für die einzelnen Systeme ermittelt. Hier ergibt sich ein deutlich homogeneres Bild zwischen den Sektoren und es zeigt sich eine **klare Tendenz, die vorhandenen Systeme auch in Zukunft einzusetzen**. In den meisten Finanzmarktsektoren ist für 80% oder mehr der kritischen Applikationen für mindestens die nächsten drei Jahre keine Ablösung geplant. Ausnahmen stellen lediglich die **BVK** und die **ZI** mit entsprechenden Quoten von 72% bzw. 68% dar.



Auf dieser Basis lässt sich ein **Vergleich zwischen in den letzten drei Jahren durchgeführter Einführung von Systemen** und in den nächsten drei Jahren geplanter Ablösung von Systemen anstellen und so ein grober Indikator dafür ableiten, wie stabil die Systemlandschaft ist und ob große Erneuerungen erfolgt oder geplant sind:

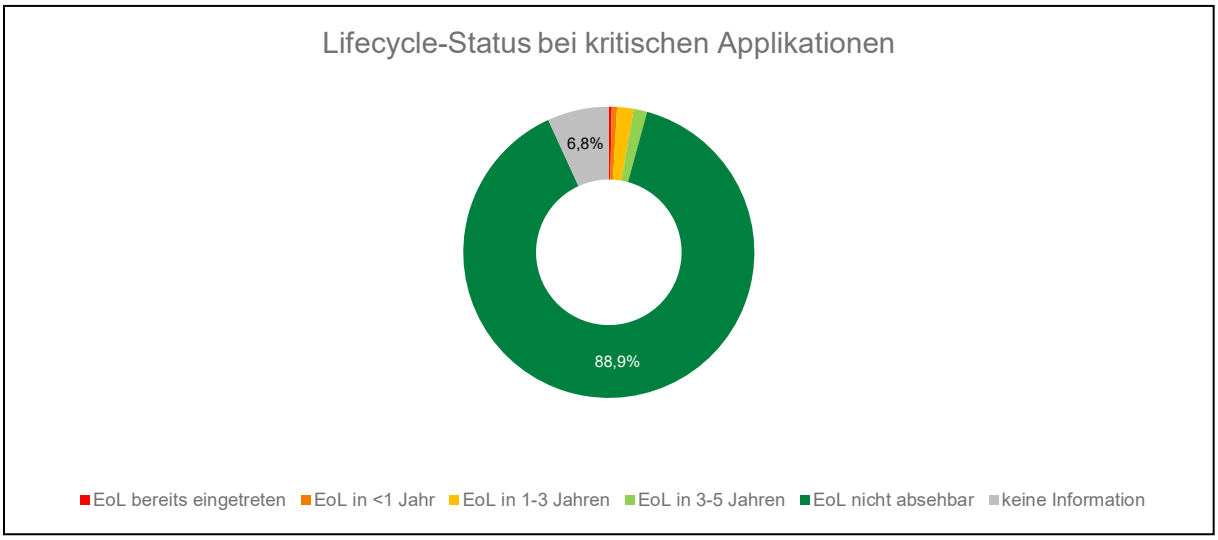
- Bei **VU, KI, VWG** und **MI** entspricht die Zahl der in den letzten drei Jahren neu eingeführten Anwendungen grob den geplanten Erneuerungen in den nächsten drei Jahren; dies ist ein Indikator für eine insgesamt relativ stabile IT-Landschaft in diesen Sektoren.
- **PK** und **WPF** planen in den nächsten Jahren deutlich weniger Erneuerungen von Systemen, als sie in den letzten Jahren bereits umgesetzt haben, was unter anderem ein Zeichen dafür ist, dass in diesen Sektoren verstärkt in neue Systeme investiert wurde, die sich nun für einen längeren Zeitraum in Betrieb befinden sollen.
- Parallel dazu haben **VASP** ihre ganze IT erst in den letzten Jahren aufgesetzt und planen derzeit keine Erneuerung dieser sehr jungen Applikationslandschaft.
- Umgekehrt sind bei **BVK** und **ZI** binnen drei Jahren signifikant mehr Erneuerungen geplant als im vergangenen Vergleichszeitraum durchgeführt wurden, was auf einen geplanten Modernisierungsprozess bei vielen Kernsysteme hindeutet.

Anteil kritischer Applikationen pro Einsatzbereich, bei dem eine Ablösung geplant oder laufend ist:



Im Durchschnitt befinden sich derzeit etwa 7% der kritischen Applikationen in geplanter oder laufender Ablösung. Nur im Bereich Bestandsverwaltung bzw. Kundenbetreuung wird eine Erneuerung bei rund 14% der Applikationen angestrebt. Dies kann im Gesamtkontext der Studienergebnisse daran liegen, dass besonders in diesem Gebiet die Integration mit neuen Konzepten (mobile Anwendungen, Kundenportale, …) ein wichtiger Treiber ist. Andere Anwendungsbereiche, wie zB Rechnungslegung, unterliegen hingegen deutlich stabileren Anforderungen.

Für die Beurteilung der Zukunftsfähigkeit der IT-Systeme ist schließlich das **End-of-Life** Datum (EoL) der kritischen Applikationen relevant. Dieses bezeichnet einen vom Hersteller/Lizenzgeber einer Anwendung genannten Zeitpunkt, ab welchem diese nicht mehr weiterentwickelt bzw. gewartet wird. Somit ist dies ein kritischer Indikator für die **IT-Sicherheit** und die **Adaptierbarkeit** von Applikationen für neue Anforderungen. Üblicherweise ist beides ab dem Eintritt des EoL nicht mehr gegeben, obgleich ein Weiterbetrieb in gewissen Fällen und unter Einbeziehung zusätzlicher Sicherheitsmaßnahmen erwogen werden kann.



- Insgesamt ist bei rund 89% der kritischen Applikationen explizit kein Ende des Supports absehbar. Dabei gibt es keine starken Abweichungen zwischen den Finanzmarktsektoren.
- Bei 0,3% der Applikationen ist EoL bereits eingetreten, bei 0,6% binnen einem Jahr zu erwarten.
- Zu 6,8% der Applikationen wurden keine Angaben zum EoL gemacht, hier bleibt also eine gewisse Unschärfe bestehen.

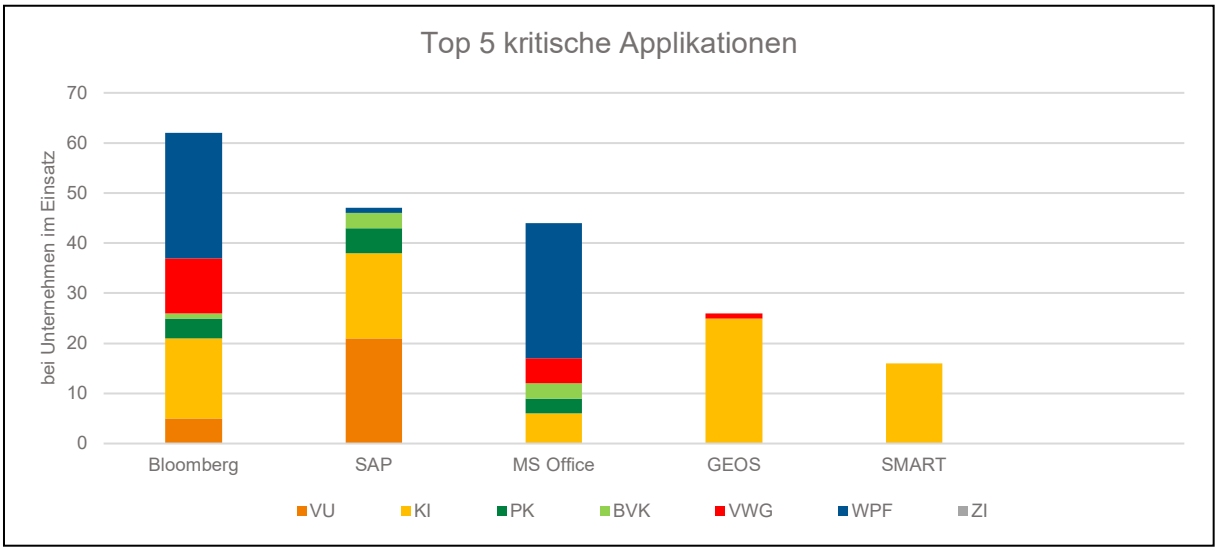
Die Betrachtung des End-of-Life Datums bei den eingesetzten kritischen IT-Applikationen ist wichtig, denn auch beim Einsatz relativ alter Anwendungen ist zu bedenken, dass wenn diese entsprechend gewartet und weiterentwickelt werden, sie auch über Jahrzehnte hinweg ihren Zweck erfüllen können.

Die Ablöseplanung und die Quote an Software, die aufgrund ihres EoL-Status als obsolet betrachtet werden kann, liefern **keine Anzeichen auf ein systemisches Problem** des Finanzsektors. In einigen Sektoren wurden in den letzten Jahren verstärkt Maßnahmen zur Erneuerung der Applikationen getroffen, teilweise sind solche gerade am Laufen. Insgesamt scheint die kontinuierliche Erneuerung und Wartung der Systeme mit deren Obsoleszenz Schritt zu halten.

5.3 KONZENTRATIONEN BEI DEN GENUTZTEN APPLIKATIONEN

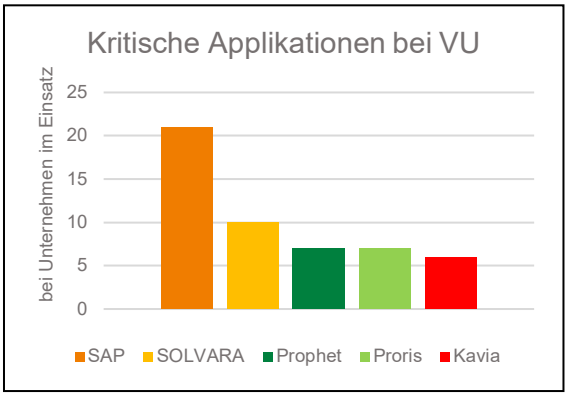
Auch im Hinblick auf die große Anzahl an maßgeblichen IT-Applikationen herrscht eine hohe Diversität der Systeme über den Markt, aber auch innerhalb der Unternehmen. Es sind sowohl Applikationen aus Eigenentwicklung, zunehmend aber auch Standardlösungen in Gebrauch.
Durch den Einsatz der Lösungen großer Anbieter wird die Softwarelandschaft zur Abdeckung von Standardprozessen insgesamt immer einheitlicher.
Der mögliche Verlust an Flexibilität bei nichtunternehmensspezifischen Anwendungen wird dabei oft in Kauf genommen, da Produkte externer Anbieter über vordefinierte Datenschnittstellen verfügen und mehrere Bereiche im Unternehmen abdecken. Dieser Trend zeigt sich auch im vermehrten Einsatz von Cloud Services.

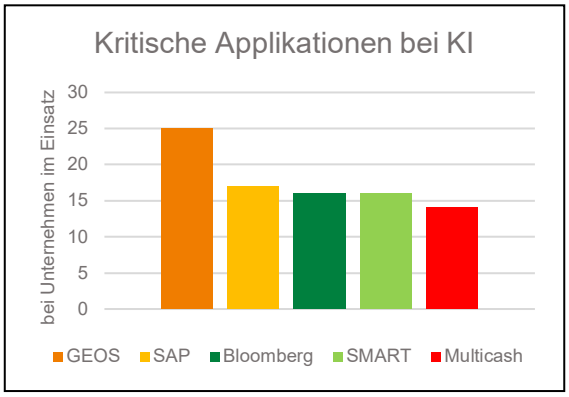
Um Konzentrationsrisiken zu erkennen und ein besseres Verständnis der IT-Landschaft des österreichischen Finanzmarktsektors zu erlangen, wurden jene Applikationen identifiziert, welche am häufigsten kritisch für die Aufrechterhaltung der Geschäftsprozesse der Unternehmen sind:

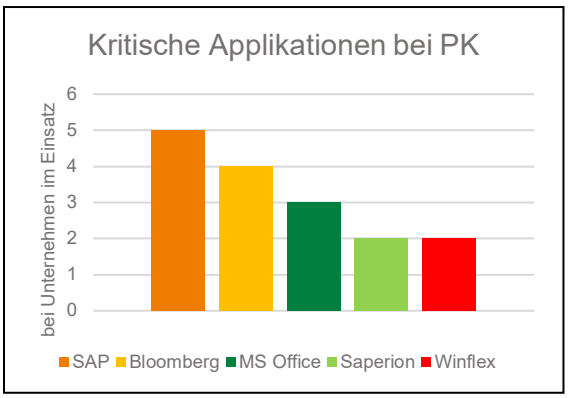


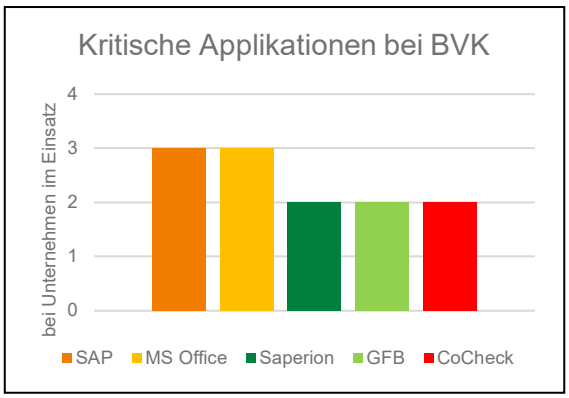
- Die Top-3 der häufigst in kritischen Geschäftsprozessen genutzten Applikationen stellen Bloomberg, SAP und Microsoft Office dar, diese sind in beinahe allen Finanzmarktsektoren verbreitet und werden dort insgesamt jeweils von 62, 48 und 42 Unternehmen eingesetzt.
- In diesem Ranking dominieren ab Platz 4 großteils KI-spezifische Anwendungen (GEOS und SMART in den Top-5).
- Bei der Interpretation der Ergebnisse ist zu bedenken, dass nur jene Nutzungen erfasst sind, bei welchen die Anwendung zur Aufrechterhaltung mindestens eines kritischen Geschäftsprozesses erforderlich ist.
- Nur relativ wenige Lösungen sind sektorenübergreifend relevant.
- Innerhalb der einzelnen Sektoren des Finanzmarktes gibt es jedoch fachspezifische Applikationen mit relativ hohen Marktanteilen. Für die FMA stellt diese Analyse gemeinsam mit der Analyse der Vernetzung mit IT-Dienstleistern eine wichtige Informationsquelle zum Thema Konzentrationsrisiken dar.

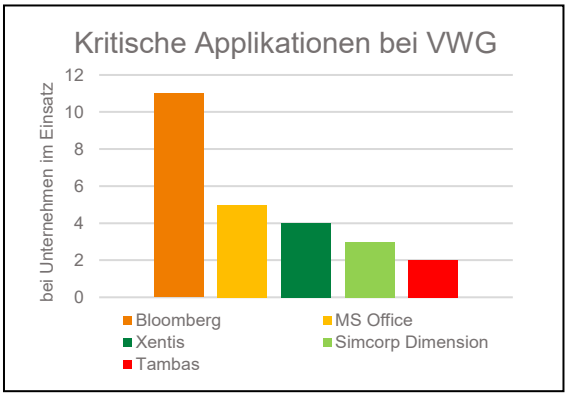
Die folgende Serie an Graphiken zeigt die wichtigsten Applikationen pro Finanzmarktsektor auf (aufgrund geringer Überschneidungen bzw. geringer Anzahl an Unternehmen werden für MI, VASP und ZI keine eigenen Diagramme dargestellt):

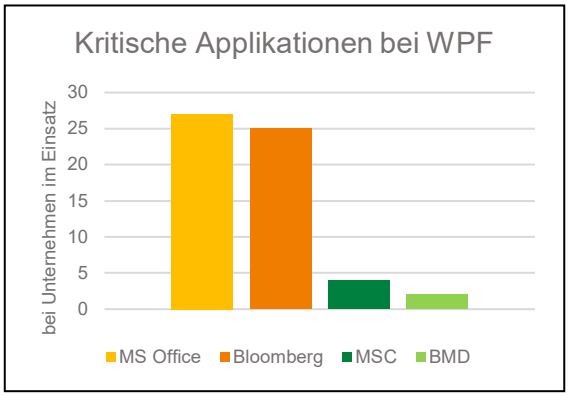












- **Bloomberg, SAP** und zu einem gewissen Grad auch **Microsoft Office** stellen kritische Applikationen in mehreren Finanzmarktsektoren dar.
- Die wichtigen Folgeplätze werden jeweils von **sektorspezifischer Software** belegt, welche sich mit einer Ausnahme (Saperion bei PK und BVK) auch jeweils nur in einem Sektor unter den Top-5 befindet.
- Neben Bloomberg, SAP und Microsoft Office gibt es mehrere spezifische Applikationen, welche in einzelnen Sektoren vergleichsweise weit verbreitet sind. Dies trifft besonders deutlich auf KI zu. Bei WPF ist dieser allgemeine Trend hingegen nicht erkennbar.

5.4 FAZIT UND HANDLUNGSFELDER DER FMA

Die Erkenntnisse der vorliegenden Studie bringen für die FMA folgende Implikationen mit sich:

- Die Akteure des österreichischen Finanzmarktes setzen **zahlreiche IT-Applikationen** zur Unterstützung ihrer kritischen Geschäftsprozesse ein. Allein im Bereich der Endanwender-Applikationen werden im Durchschnitt pro Unternehmen knapp 15 kritische Anwendungen verwendet, wobei sich die Angaben je nach Finanzsektor deutlich unterscheiden.
- Bezogen auf die Altersstruktur und Aktualität der eingesetzten Applikationen konnten keine Anzeichen identifiziert werden, welche auf ein systemisches Problem mit veralteter Software hindeuten würden. Kritische Applikationen bleiben **teilweise sogar jahrzehntelang im Einsatz, jedoch werden auch kontinuierlich Erneuerungen durchgeführt** und es sind insgesamt nur wenige Systeme mit absehbarem Support-Enddatum in Betrieb.
- Bloomberg, SAP und Microsoft sind wichtige Softwarelieferanten für den österreichischen Markt und müssen in etwaigen Abhängigkeitsanalysen bedacht werden. Für einzelne Sektoren sind aber auch zahlreiche kleinere Softwareprodukte von Bedeutung; zwar hat der Ausfall eines Lieferanten/Lizenzgebers nicht unmittelbar den gleichen Effekt wie beim Wegfall eines

kritischen Dienstleisters, dennoch besteht hier eine gewisse Abhängigkeit von Support und Updates.

Wie auch im Kapitel Strategie in Bezug auf strategische Kooperationen dargestellt, begünstigt die Digitalisierung eine zunehmende Vernetzung der Akteure. Die FMA muss diese Entwicklungen auch in Zukunft beobachten und begleiten, um ihrem Aufsichtsauftrag gerecht zu werden. Eine belastbare Datenlage zu in den Finanzmarktsektoren eingesetzten IT-Systemen hat sich für die Aufsicht zu einer relevanten Anforderung entwickelt:

- Konzentrationsrisiken bei einzelnen extern bezogenen Softwarelösungen sind sowohl im Falle der Einstellung von Produkten als auch im Sinne der IT-Sicherheit (siehe zB den Angriff über die Solar Winds Plattform 2020[21]) für die Finanzmarktstabilität relevant.
- Schlagworte wie „veraltete IT-Landschaften“ werden auch medial im Zusammenhang mit Themen der Digitalisierung freizügig gebraucht; eine gute Datenlage ermöglicht der FMA hier ein differenziertes Bild. Ein Überblick zu den tatsächlich eingesetzten Systemen hilft dabei, aktuelle Trends besser erfassen zu können und nicht rein von teilweise durch Marketing getriebenen Ankündigungen abhängig zu sein.

5.5 KONSULTATION ZUM EINSATZ VON IT-SYSTEMEN

- Welche Aufgaben soll die FMA iZm den am österreichischen Finanzmarkt genutzten IT-Systemen wahrnehmen? In welcher Form sollen diese Aufgaben übernommen werden?
- Welche konkreten regulatorischen Vorgaben sind iZm dem Einsatz von IT-Systemen im Finanzsektor notwendig?
- Welche positiven und negativen Aspekte für die IT-Sicherheit hat die zunehmende Konzentration des Finanzmarktes auf wenige IT-Anbieter?
- Sind die wesentlichen Vorteile und möglichen Nachteile agiler Vorgehensweisen erfasst?
- Welche konkreten positiven, aber auch negativen Entwicklungen bezüglich der IT-Systeme sind in den einzelnen Sektoren zu beobachten?

[21] *Highly Evasive Attacker Leverages SolarWinds Supply Chain to Compromise Multiple Global Victims With SUNBURST Backdoor | Mandiant.*

6 IT-VERFLECHTUNGEN

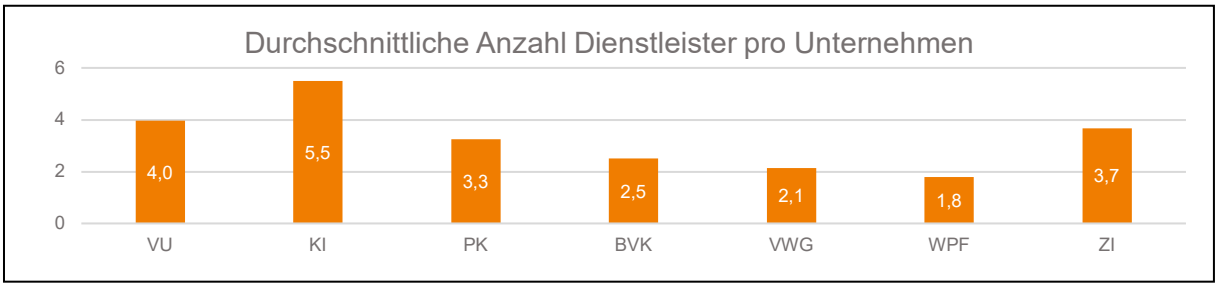
6.1 IT-DIENSTLEISTERLANDSCHAFT

Die Digitalisierung begünstigt auch die **fortschreitende Vernetzung wirtschaftstreibender Akteure**. Im Hinblick auf die stetig wachsende technische Komplexität gewinnt die **Erbringung kritischer Leistungen durch IT-Dienstleister** laufend an Bedeutung. Im Rahmen der vorliegenden Studie wurde daher die Nutzung von IT-Dienstleistern (DL) und IT-Subdienstleistern (SDL; Dienstleister von IT-Dienstleistern in 1. Ebene) erhoben. Die Abfrage war dabei eingeschränkt auf jene DL und SDL, welche **für die Erhaltung der kritischen Geschäftsprozesse nötig** sind. Dabei wurden die erhobenen Dienstleisterbeziehungen in die folgenden Kategorien gegliedert:

- Hardware (zB klassische Rechenzentrumsleistungen)
- Datenanbindung (zB Betreiber einer Datenleitung zwischen zwei Standorten)
- Netzwerkinfrastruktur (zB Wartung der Router und Switches)
- Betriebssysteme (zB Administration von Microsoft/Linux-Geräten)
- Datenbanken (zB Betrieb/Wartung von SQL-Datenbanken oder Datenbankservern)
- Middleware (zB Bereitstellung von Authentifizierungsservices oder APIs)
- Sicherheitsservices (zB Wartung von Firewalls)
- Applikationen (zB Hosting, Betrieb oder Administration von Endanwendersoftware)
- Sonstige

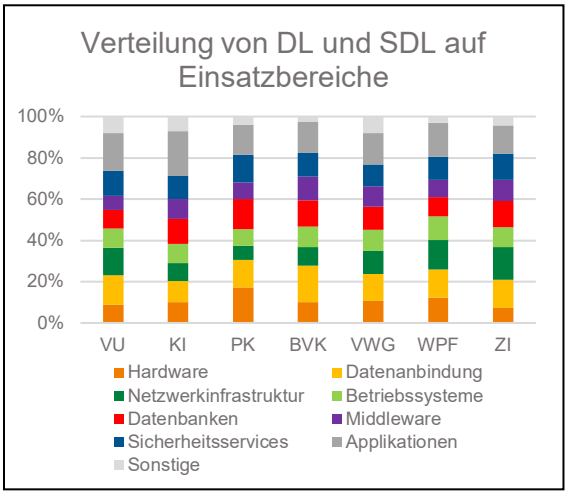
Zusätzlich wurde zwischen konzerninternen und konzernexternen Dienstleistern unterschieden.

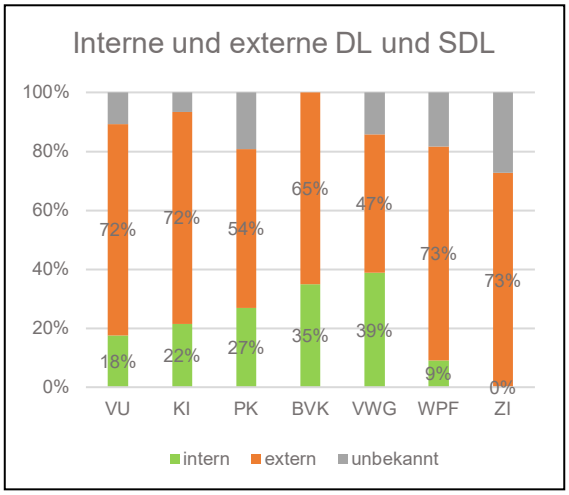
Am österreichischen Finanzmarkt bestehen rund 1.000 kritische Vernetzungen mit IT-Dienstleistern und Subdienstleistern (im Rahmen der Studie wurden 966 ermittelt).



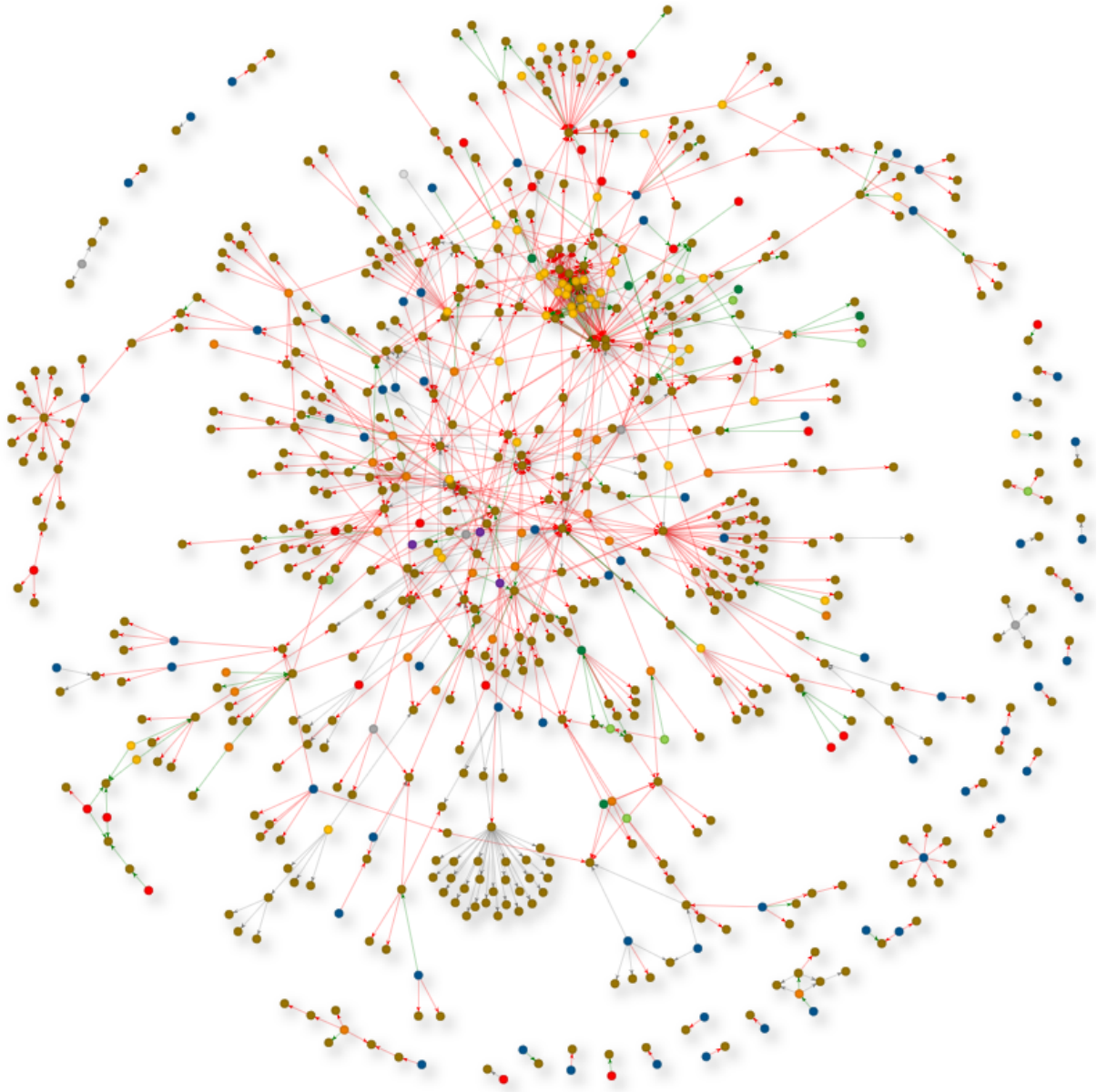
- Im Durchschnitt sind die Unternehmen aller Finanzmarktsektoren von mehreren DL/SDL abhängig.
- Die Spannweite reicht von 5,5 DL bei KI bis 1,8 DL bei WPF; Geschäftsmodell, Komplexität der IT-Landschaft und Auslagerungen stehen hier in engem Zusammenhang.
- Generell sind mehr direkte Dienstleister als Subdienstleister gemeldet worden; dies kann teilweise Informationslücken bei den SDL geschuldet sein. Bei einigen DL, welche gleichzeitig mehrere beaufsichtigte Unternehmen servicieren, konnten diese jedoch gut durch die Aggregation der entsprechenden SDL-Meldungen ergänzt werden.

Die Zahl der durchschnittlich eingesetzten DL und SDL variiert zwar zwischen den Sektoren des Finanzmarktes relativ stark; deren Verteilung auf Einsatzgebiete ist jedoch relativ vergleichbar.
Es gibt hier keine besonders starken Trends und Dienstleister werden in allen abgefragten Gebieten genutzt. Eine Mehrheit der DL und SDL ist hierbei in allen Sektoren konzernexterner Natur:





Die Vernetzung der IT-Dienstleisterlandschaft am österreichischen Finanzmarkt kann unter Berücksichtigung sämtlicher IT-Vernetzungen wie folgt visualisiert werden:



Diese Darstellung verdeutlicht folgende Eigenschaften des IT-Dienstleisternetzwerkes:

- Zwar gibt es eine Reihe kleinerer autarker Ketten und 1:1 Beziehungen, aber die Mehrheit der beteiligten Akteure formt ein großes Netzwerk.
- Es können zwar lokale Cluster beobachtet werden, in das IT-Dienstleisternetzwerk sind jedoch alle Bereiche des Finanzmarktes eingebunden; es liegt keine systemische Trennung zwischen den Dienstleistern der einzelnen Sektoren vor.
- Bei einigen Dienstleistern lassen sich klare Konzentrationen erkennen; ein Problem oder Ausfall würde sich auf zahlreiche Unternehmen auswirken.

- IT-Dienstleister, insbesondere jene, die eine zentrale Rolle spielen, nutzen zur Erbringung kritischer Aspekte ihrer Leistungen meist ebenfalls Subdienstleister.
- Obwohl nur eine Ebene an SDL erhoben wurde, ergaben sich teilweise sehr lange Abhängigkeitsketten, sodass ein Ausfall eines IT-Dienstleisters mitunter über mehrere Zwischenschritte unerwartete Auswirkungen auf beaufsichtigte Unternehmen haben kann.

6.2 ABHÄNGIGKEITSNETZE PRO SEKTOR

Die komplexe Landschaft an Verflechtungen zwischen beaufsichtigten Unternehmen und IT-Dienstleistern kann in unterschiedlichen Dimensionen detaillierter betrachtet werden. Im folgenden Abschnitt wurden die Subnetze der einzelnen Finanzmarktsektoren herausgelöst. Folgende Farbcodes wurden dabei gewählt:

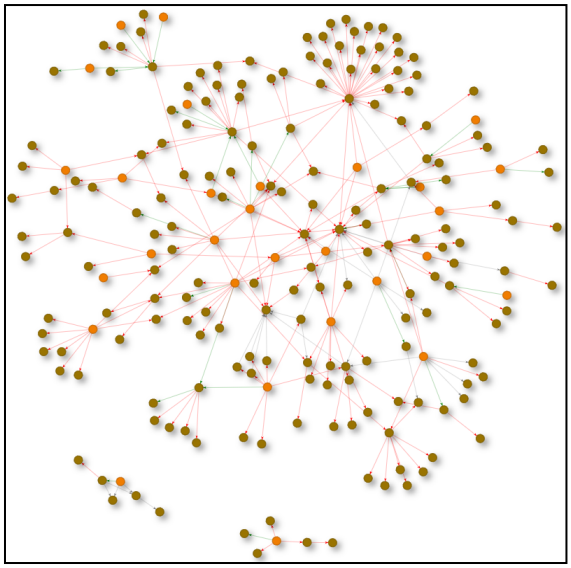
VU dunkles Orange	KI helles Orange	PK dunkles Grün	BVK helles Grün	VWG Rot	MI Violett	WPF Blau	ZI Grau

VASP wurden aufgrund der geringen Anzahl an verbundenen Dienstleistern exkludiert.

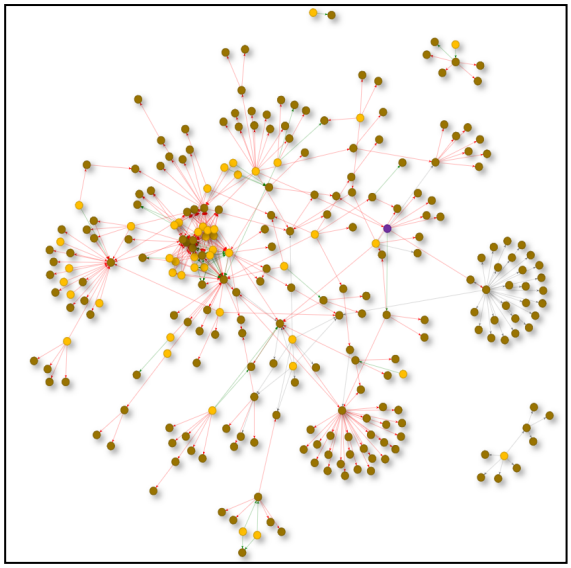
Reine IT-Dienstleister, welche keine beaufsichtigten Unternehmen der FMA darstellen, sind mit bronzefarbenen Knoten gekennzeichnet.

Die verbindenden Kanten zwischen den Knoten des Netzwerkes stellen die Dienstleistungsbeziehungen dar und sind im Falle **konzerninterner DL** grün und im Falle **konzernexterner DL** rot markiert.

VU

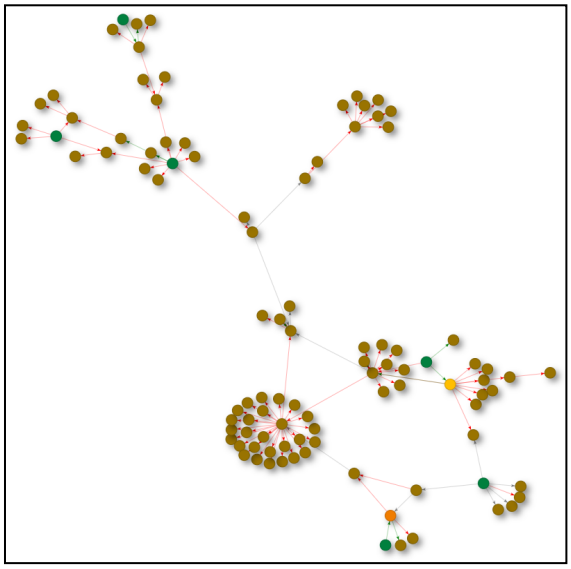


KI

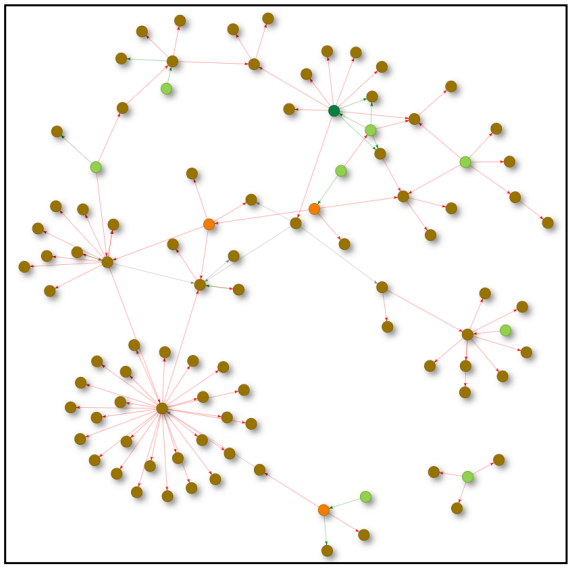


- Das Auslagerungsnetz bei **VU** ist insgesamt eher durch **viele kleine Cluster** (oft in Zusammenhang mit Konzernverbänden) denn Konzentration bei einzelnen DL geprägt. Über teils längere Abhängigkeitsketten sind jedoch die meisten Versicherer über einen oder mehrere SDL auch mit konzernfremden Unternehmen bzw. über externe Dienstleisterbeziehungen verknüpft.
- **KI** nutzen im Durchschnitt die meisten DL und SDL der Unternehmensgruppen. Dementsprechend vermag die sehr starke Verflechtung dieses Sektors wenig zu überraschen. Auffällig ist jedoch eine **kleine Zahl sehr großer Cluster**, die sich teilweise aus Konzernen erklären, teilweise jedoch auch aus grundsätzlich unabhängigen Banken bestehen, die parallel den gleichen externen DL nutzen. Außerdem wurde bei einigen DL eine sehr **große Zahl kritischer SDL** identifiziert, was einen möglichen Ausgangspunkt für weitere Fragestellungen darstellt (siehe Abschnitt 6.5 Fazit und Handlungsfelder der FMA).

PK



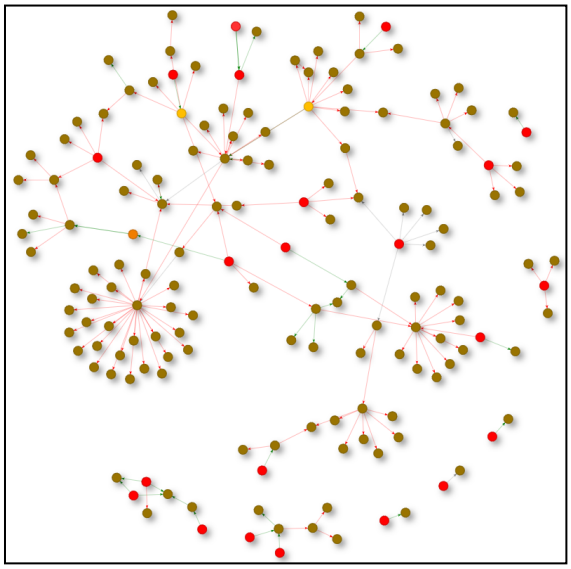
BVK



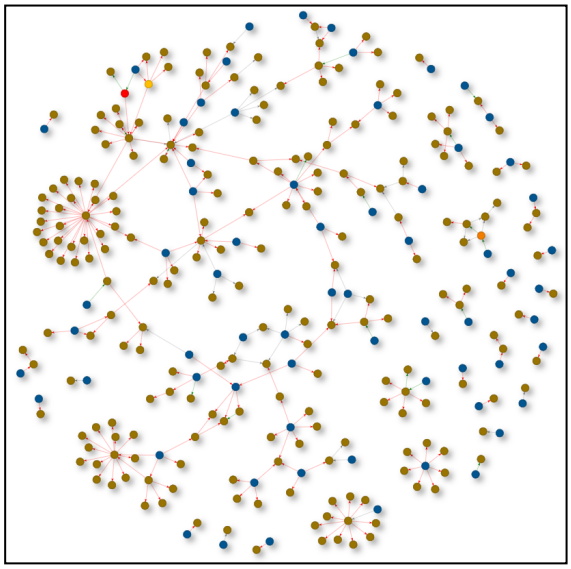
- **PK** sind untereinander **weniger stark über Dienstleister vernetzt** als andere Sektoren, die Nutzung desselben DL durch zwei PK bleibt die Ausnahme. Ein VU und ein KI sind ebenfalls als IT-DL in das Netzwerk der PK integriert. Trotz der schwächeren Vernetzung sind **alle PK über mehrere Sprünge über SDL verknüpft**, dies unterstreicht die rasch fortschreitende Verknüpfung der Akteure in Zeiten der Digitalisierung: selbst Unternehmen, die sonst unabhängig voneinander agieren, sind über einige Zwischenschritte wieder miteinander verbunden.

- Bei **BVK** kann ähnlich zu den PK ebenfalls eine zwar **vollständige, aber nicht besonders enge Verflechtung** über DL und SDL beobachtet werden. Mit drei VU und einer PK sind vergleichsweise viele sektorfremde Unternehmen des Finanzmarktes in die Dienstleistungsketten der BVK eingebunden.

VWG



WPF



- Die Dienstleisterbeziehungen von **VWG** sind **vergleichsweise heterogen**, tendieren aber dazu, **relativ distanziert** zu sein. Es gibt auch mehrere **kleine Cluster**, die nicht mit dem Rest des Netzes verbunden sind. Umgekehrt gibt es mehrere Fälle der parallelen Nutzung eines Dienstleisters durch zwei VWG. Zwei KI, ein VU und auch eine VWG selbst sind als DL von VWG eingebunden.
- **WPF** und ihre DL/SDL bilden ein **relativ loses Netzwerk mit vielen nicht-verbundenen Clustern**, die auch häufig aus 1:1 Beziehungen bestehen. Vergleicht man dieses Bild mit zB dem Netzwerk der VU oder KI, zeigt sich ein klarer struktureller Unterschied. Dies dürfte dem Geschäftsmodell und der Unternehmensgröße der WPF geschuldet sein. Bei genauerer Betrachtung fällt auf, dass viele insbesondere kleinere WPF auch kleinere Unternehmen als DL einsetzen und oft auch alle relevanten Leistungen von einem IT-Unternehmen erbringen lassen, statt dies auf mehrere aufzuteilen.
- Bis auf zwei **ZI**, die einen gemeinsamen Dienstleister nutzen, sind diese Unternehmen über ihre Auslagerungsketten **nicht direkt verbunden**, obwohl sie insgesamt relativ viele DL nutzen.

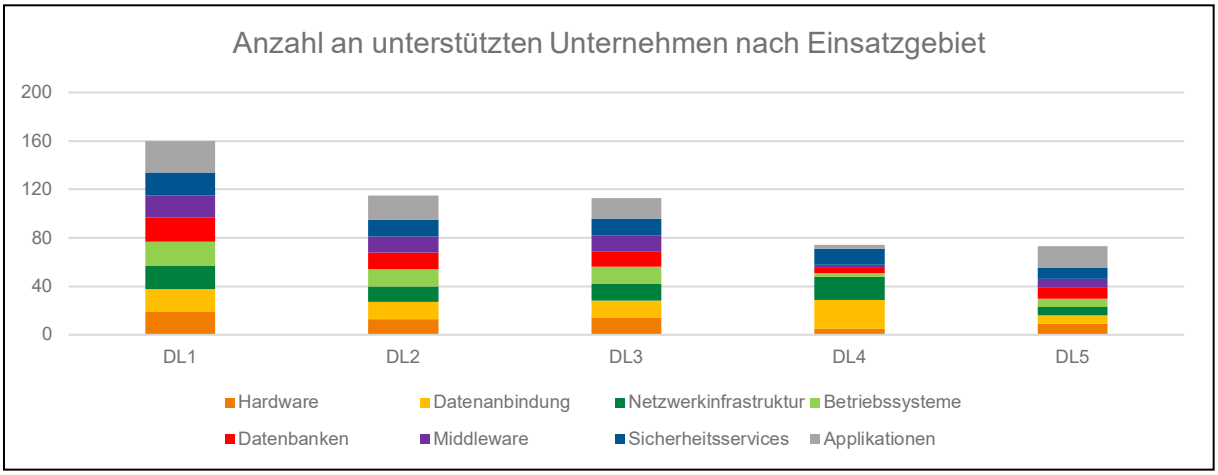
Insgesamt werden die sektoralen Unterschiede bei den Dienstleisterabhängigkeiten deutlich. Sowohl die durchschnittliche Anzahl an DL und SDL pro beaufsichtigtem Unternehmen als auch der Grad der Vernetzung und die Struktur der gebildeten Cluster stellen hier unterscheidbare Merkmale dar.

Ebenso deutlich wird, dass es in vielen Sektoren Dienstleister gibt, deren Ausfall mehrere Unternehmen treffen würde. Werden dazu auch Subdienstleistungen betrachtet, gibt es klare Konzentrationen in jedem Sektor. Die Darstellungen in diesem Abschnitt lassen dabei überdies die möglichen zusätzlichen Auswirkungen auf andere Finanzsegmente außer Acht.

6.3 KONZENTRATION DER WICHTIGSTEN DIENSTLEISTER

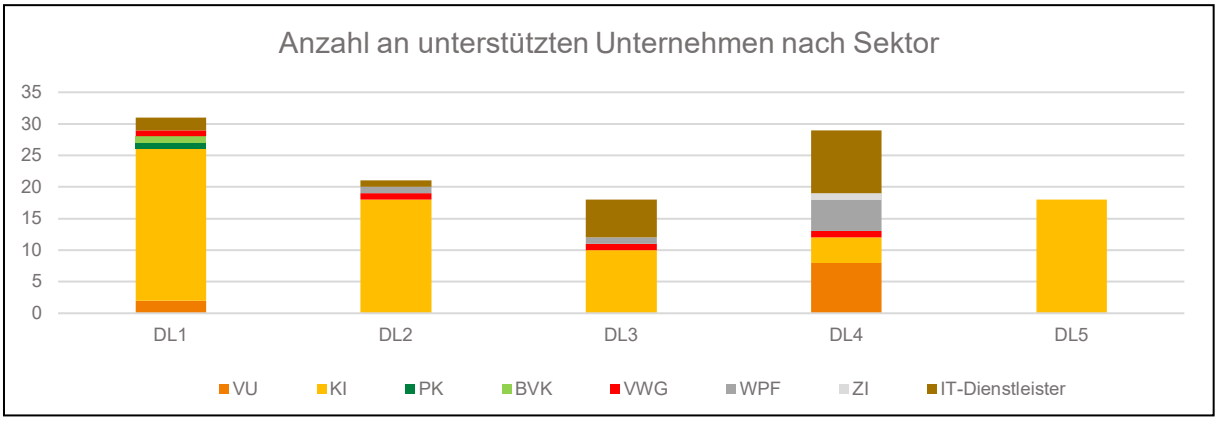
Die Rolle der einzelnen Technologieunternehmen für einzelne Finanzsektoren und den gesamten Markt lässt sich nicht rein auf Basis quantitativer Kriterien ermitteln. Eine Betrachtung in mehreren Dimensionen kann dennoch einen Einblick in die Stellung einiger zentraler Dienstleister liefern:

In Bezug auf die **Zahl der direkt erbrachten geschäftskritischen Dienstleistungen** für beaufsichtigte Unternehmen oder andere DL von beaufsichtigen Unternehmen lässt sich die Relevanz einzelner Akteure im Dienstleisternetzwerk anhand der folgenden Graphik erkennen (es sind hier die kaskadierende Anzahl an Unternehmen, für welche diese DL einen SDL darstellen, nicht inkludiert und auch keine Gewichtung nach Bilanzsummen hinterlegt):



- Diese **großen direkten Dienstleister sind eher Generalisten denn Spezialisten**. Abgesehen von einem Fokus von DL4 auf Datenanbindungen und Netzwerkinfrastruktur sowie einer generellen Tendenz zur verstärkten Betreuung auf Applikationsebene, werden alle Arten von Dienstleistungen in ähnlichem Ausmaß angeboten; oftmals auch für dasselbe Unternehmen in Form einer weitgehenden Gesamtauslagerung der IT.

In Bezug auf die **Zahl der durch kritische Dienstleistungen unterstützten Unternehmen** pro Sektor lässt sich bei den fünf wichtigsten Dienstleistern **ein sehr hoher Anteil an KI** feststellen:

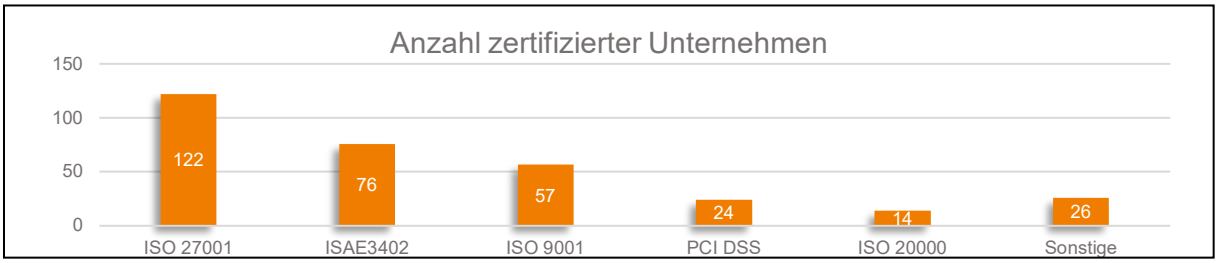


- DL5 ist ein reiner Bankensektordienstleister und lediglich bei DL4 stellen KI nicht die Mehrheit der unterstützten Unternehmen.
- Dieses Ergebnis ist konsistent mit den in Abschnitt 6.2 untersuchten sektoralen Netzwerken. **Der Bankensektor bildet bei direkten Auslagerungen die größten Cluster, während andere Sektoren meist erst über SDL stark vernetzt sind.** Dennoch fällt am Beispiel von DL4 auf, dass es durchaus, insbesondere im Feld spezialisierter IT-Dienstleistungen, nennenswerte sektorübergreifende Abhängigkeiten von DL gibt.
- Die Analyse der Abhängigkeiten ermöglicht außerdem **zentrale Subdienstleister** zu identifizieren. Bei den oben angeführten fünf DL macht zB DL1 Gebrauch von 11, DL3 von 10 und DL4 von 3 bekannten SDL. Weitere Verknüpfungen ergeben sich häufig jedoch erst nach mehreren Schritten in der Dienstleistungskette.
- Die Frage, inwieweit sich ein hypothetischer Ausfall eines Subdienstleisters über mehrere Stufen auswirken kann, wäre in weiterer Folge zu untersuchen.

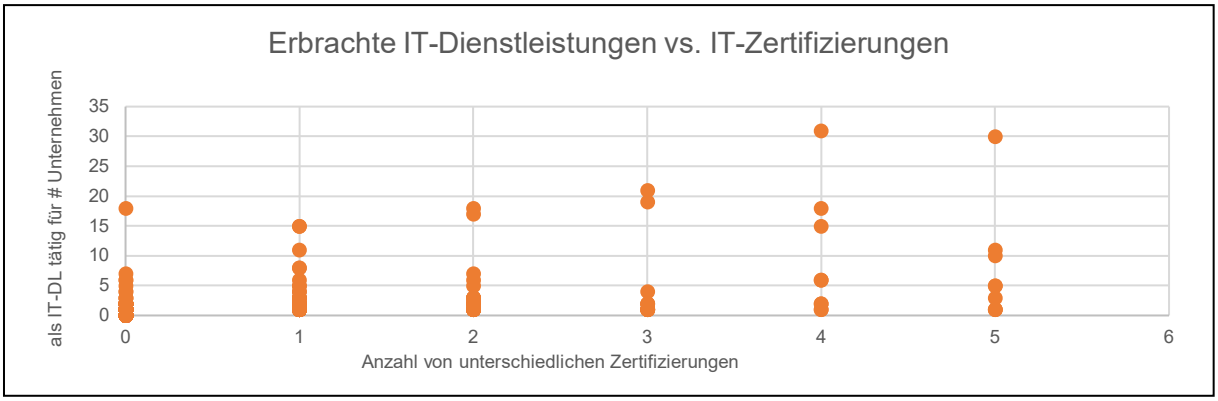
6.4 ZERTIFIZIERUNGEN VON IT-DIENSTLEISTERN

Im Rahmen der vorliegenden Studie wurden außerdem die den beaufsichtigten Unternehmen bekannten **IT-relevanten Zertifizierungen** ihrer Dienstleister erhoben. Da die DL und SDL selbst nicht befragt wurden, kann das Gesamtbild mitunter Lücken aufweisen. Dennoch sollte sich eine insgesamt repräsentative Übersicht ergeben, da Kenntnis über die Zertifizierungen kritischer DL von den Unternehmen als Teil der entsprechenden Risikoabwägung erwartet wird.

168 von 512 Unternehmen, welche Dienstleistungen erbringen, dh **ein Drittel der IT-Dienstleister** (diese Zahl inkudiert auch einige der beaufsichtigten Unternehmen, welche zusätzlich als IT-DL agieren) **verfügt über relevante Zertifizierungen**. Relativ viele der 168 zertifizierten Unternehmen verfügen dabei gleichzeitig über mehrere einschlägige Zertifikate:



Dabei lässt sich ein gewisser Zusammenhang zwischen der Anzahl der als IT-DL unterstützten Unternehmen und der Anzahl an gehaltenen IT-Zertifikaten feststellen:



- Auch wenn der Trend nicht streng linear ist, werden Zertifikate eher von größeren Dienstleistern gehalten.
- Insgesamt ist die Zahl an DL und SDL, die über keine Zertifizierungen verfügen, obwohl sie mehrere Unternehmen mit IT-Dienstleistungen versorgen, relativ hoch.
- Die Frage, ob und welche Zertifizierungen für die Erbringung einer gewissen Tätigkeit sinnvoll sind, hängt grundsätzlich vom Einzelfall ab. Dennoch stellt sich die Frage, was insgesamt die Gründe für diese relativ geringe Abdeckung auch bei an sich relativ gängigen Standards wie ISO 27001/9001 sind und ob den beaufsichtigten Unternehmen aktuelle Informationen zu den Zertifizierungen ihrer Dienstleister vorliegen.

6.5 FAZIT UND HANDLUNGSFELDER DER FMA

Die umfassenden Daten zeigen ein hohes Maß an Verflechtung zwischen den einzelnen Finanzmarktsektoren mit IT-Unternehmen, aber auch untereinander:

- Starke sektorale Unterschiede können beobachtet werden, aber ein überwiegender Teil der beaufsichtigten Unternehmen ist über DL und SDL, welche kritisch für die Geschäftsprozesse der Unternehmen sind, miteinander vernetzt.
- Bei den am stärksten konzentrierten Sektoren, insbesondere den KI, ist eine große Anzahl Marktteilnehmer direkt und ohne Zwischenschritte für die Erbringung ihrer Leistungen von einigen wenigen Dienstleistern abhängig.
- Die Informationen zu IT-DL und SDL ermöglichen ein besseres Verständnis der IT-Landschaft der beaufsichtigten Unternehmen und somit einen besser informierten und risikobasierten Ansatz in der laufenden Aufsicht.
- Reine IT-Unternehmen werden für den Finanzmarkt immer bedeutsamer; mit den vorliegenden Informationen kann die FMA zentrale österreichische Dienstleister identifizieren und diese zielgerichtet in ihrer Aufsichtstätigkeit berücksichtigen.
- Mit der EU-Regulierung zu DORA wird ein Aufsichtsregime für kritische IKT-Dienstleister angestrebt, was ebenfalls wieder nach einer umfassenden Dienstleisterlandkarte auf nationaler Basis verlangt.
- Kommt es zu schwerwiegenden Vorfällen bei IT-DL oder SDL, kann die FMA auf dieser Basis rasch einen Kreis betroffener Unternehmen und Dienstleistungskategorien ermitteln.

Zuletzt liefert die vorliegende Studie für die FMA auch den Ansatzpunkt für weitere aufsichtsrelevante Fragestellungen:

- Aufgrund der exponentiell mit jedem Schritt der Auslagerungskette steigenden Anzahl an von einem Subdienstleister abhängigen Unternehmen ist es wichtig, die Effekte bei Ausfall eines Dienstleisters auf alle potentiell Betroffenen einschätzen zu können.
- Die Anzahl der gemeldeten kritischen Subdienstleister pro IT-Dienstleistungsunternehmen variiert teilweise stark: Die möglichen Hintergründe wären zu ermitteln.
- Der heterogene Einsatz von Zertifizierungen bei IT-Dienstleistern betont die Frage, wann und für welche Unternehmen diese sinnvoll sind bzw. welche Aussage das Fehlen solcher Zertifikate bei zentralen IT-Unternehmen haben kann.

6.6 KONSULTATION ZU DEN IT-VERFLECHTUNGEN

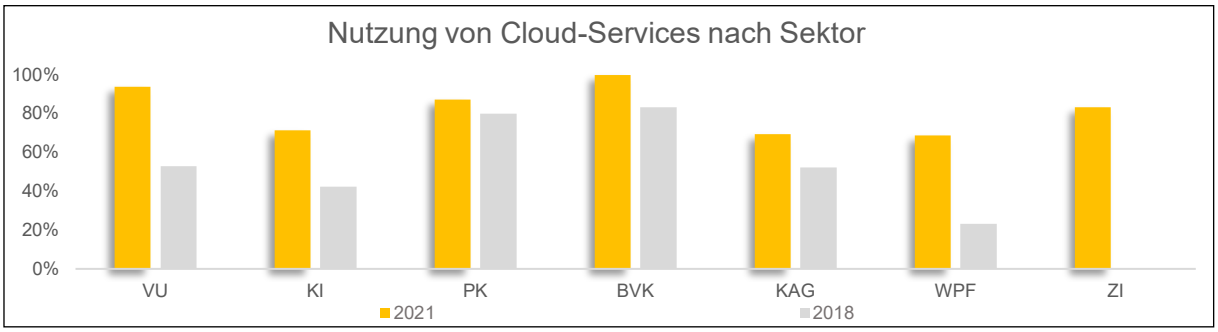
- Welche Aufgaben soll die FMA iZm den Verflechtungen zwischen den beaufsichtigten Unternehmen und den IT-Dienstleistern wahrnehmen?
- In welcher Form sollen diesen Aufgaben übernommen werden?
- Welche konkreten regulatorischen Vorgaben sind iZm den Verflechtungen am österreichischen Finanzmarkt notwendig?
- Welche konkreten positiven, aber auch negativen Entwicklungen bezüglich der Vernetzung mit IT-Dienstleistern sind in den einzelnen Sektoren zu beobachten?

7 DIGITALE TECHNOLOGIEN

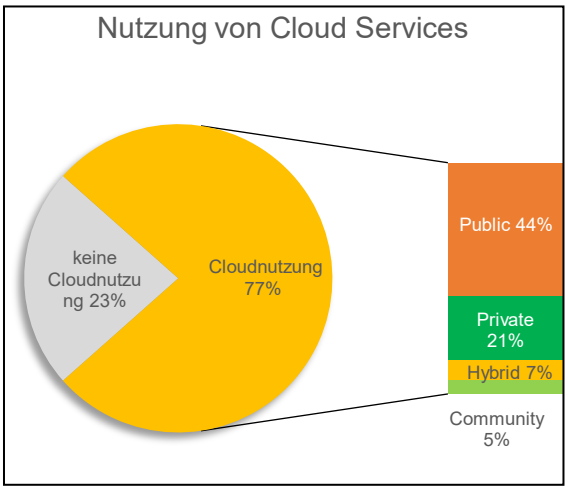
7.1 CLOUD SERVICES

Cloud Services bieten eine **Bereitstellung von IT-Infrastruktur und IT-Leistungen** wie etwa Speicherplatz, Rechenleistung oder Anwendungssoftware **als Service über das Internet**. Die Cloud Services werden dabei nicht von einem konkreten Rechner aus bereitgestellt. Vielmehr besteht die virtuelle Rechenwolke aus vielen verschiedenen, miteinander vernetzten Rechnern. Der Zugriff auf Cloud-Services erfolgt über ein Netzwerk. Der Nutzer greift auf den Ressourcenpool der Cloud zu und bekommt dynamisch jene Kapazitäten zugeteilt, die er gerade benötigt.

Cloud Services haben am österreichischen Finanzmarkt an Bedeutung gewonnen. Rund drei Viertel der beaufsichtigten Unternehmen nutzen bereits Cloud Dienstleistungen. Im Vergleich dazu hat 2018 ca. die Hälfte der Beaufsichtigten solche Services genutzt. Die Erwartungshaltung aus 2018, bei der eine Nutzung von Cloud Services durch mehr als 60% der Marktteilnehmer erwartet worden war, wurde somit klar übertroffen.



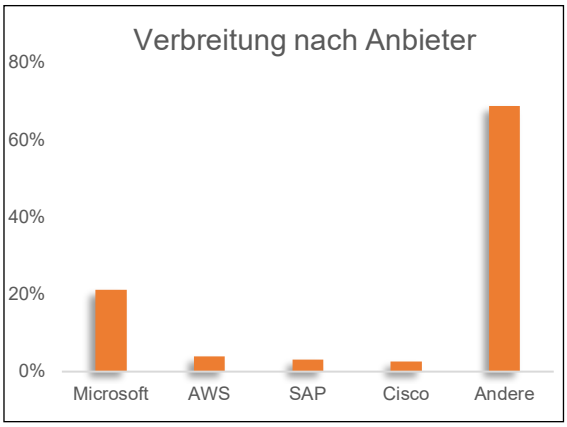
Am stärksten verbreitet sind Cloud Nutzungen in BVK. Jede BVK nimmt solche Dienstleistungen in Anspruch. Auch VU, PK und ZI nutzen Clouds intensiv. 94% der VU, 88% der PK und 83% der ZI greifen auf Cloud-Services zurück.



- Cloud Services werden von rd. drei Viertel der Beaufsichtigten genutzt.
- Rund drei Viertel der Cloud-nutzenden Unternehmen setzen mehr als eine Cloud-Lösung ein.
- Bei den Cloud-Bereitstellungsmodellen Public, Private, Hybride und Community dominiert die Nutzung von Public-Clouds.

Die bei den österreichischen Finanzdienstleistern am weitesten verbreiteten Anbieter im Verhältnis der Gesamtmenge der Cloudnutzer sind Microsoft, AWS, SAP und Cisco.

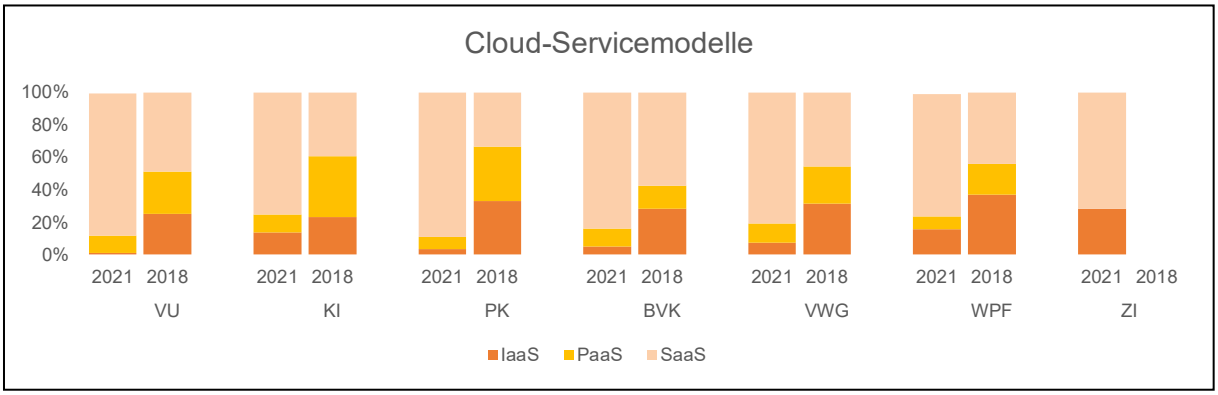
Von den österreichischen Anbietern sind zB das **ARZ** und **Fabasoft** vertreten.



Microsoft wird nach wie vor weit verbreitet als Cloud Dienstleister in Anspruch genommen. Neben MS Office 365 wird beispielsweise auch die Cloudplattform Azure genutzt. Der Anteil von Microsoft ist von 2018 mit einem Wert von 34% auf 21% im aktuellen Jahr zurückgegangen. Im Vergleich zur letzten Digitalisierungsstudie ist der Anteil der anderen Anbieter, die nicht unter die meistgenutzten vier Service Dienstleister fallen, von 60% auf 69% gestiegen.

Im Durchschnitt sind 80% aller von den beaufsichtigten Unternehmen genutzten Cloud-Dienste dem Servicemodell Software as a Service zuzurechnen.

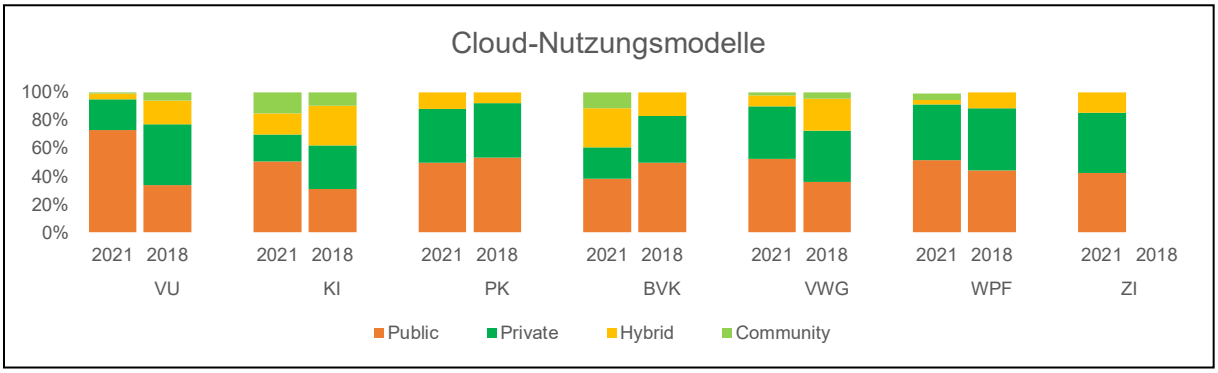
2018 belief sich der auf SaaS-Modelle entfallende Anteil auf rund 45%. Im gleichen Betrachtungszeitraum hat sich bei den IaaS-Servicemodellen der Anteil von 30% auf 14% vermindert. Auch bei PaaS ist die gleiche Tendenz nachverfolgbar – hier verlief die Entwicklung von 25% auf 7%.



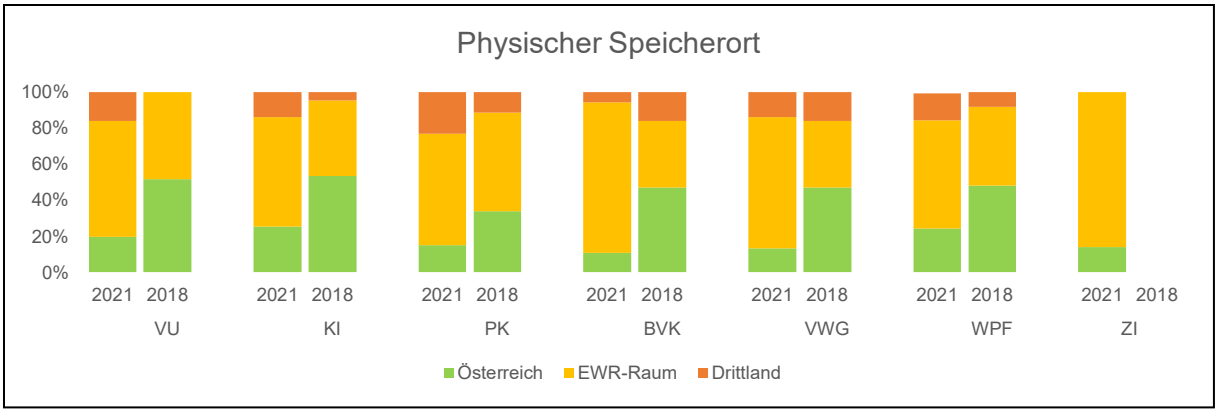
Die Hälfte der genutzten Cloud-Services sind Public Clouds zuzuordnen.

Die Inanspruchnahme von Public Clouds hat sich im Vergleich zu 2018 erhöht. Damals waren rd. 40% aller genutzten Cloud Services solche Public Clouds. Nunmehr entfällt rund die Hälfte der Cloud-Services auf dieses Nutzungsmodell.

Währenddessen hat sich der Anteil von Private Clouds leicht vermindert – konkret von rd. 38% auf 34%. Der gleiche Trend ist bezüglich der Hybriden Clouds, deren Anteil sich 2021 auf rd. ein Zehntel beläuft, festzustellen. Community Clouds haben eine stark untergeordnete Bedeutung mit rund 4% Nutzungsanteil.

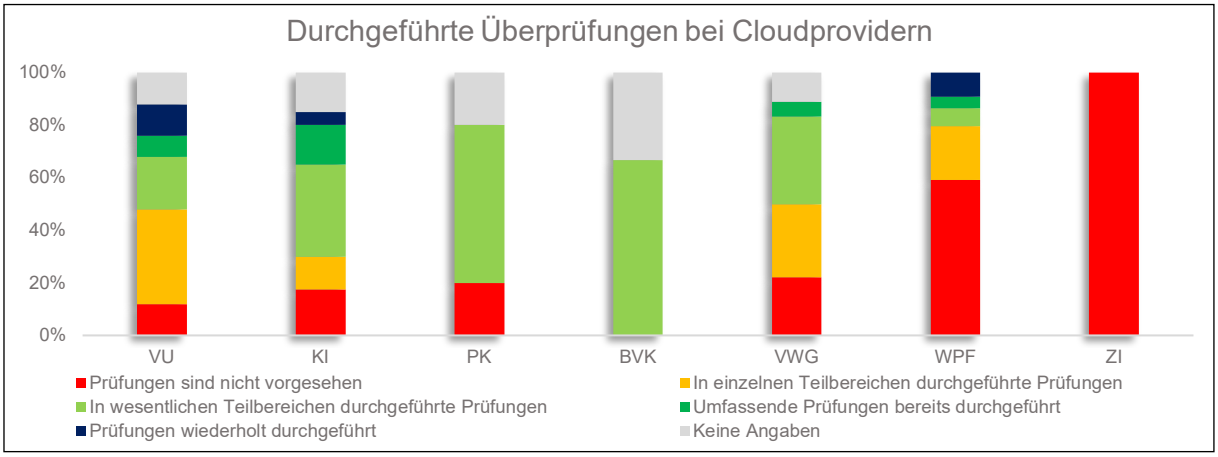


90% aller physischen Speicherorte der Cloud-Daten liegen in Österreich und in anderen EWR-Staaten. Im Vergleich zu 2018 hat sich der Anteil Österreichs von damals knapp 50% auf nunmehr rd. 15% vermindert.



Rund die Hälfte aller beaufsichtigten Unternehmen, die Cloud-Dienstleistungen nutzen, sieht keine Überprüfungen bei den Cloud-Dienstleistern vor.

In Anbetracht der vielschichtigen Risiken der Cloud Services ist es wichtig, dass die Nutzer von Clouds sich der potentiellen Gefahren bewusst sind. Die Digitalisierungsstudie zeigt, dass viele beaufsichtigte Unternehmen noch keine Überprüfung der Cloudlösung auf etwaige Defizite durchgeführt haben:



- Rund vier von zehn Unternehmen, welche Clouds nutzen, sehen keine Prüfungen der Cloud-Dienstleister vor. Sollten auch jene 10% aller Cloud-nutzenden Unternehmen, die zu dieser Frage keine Angabe übermittelt haben, von solchen Prüfungen absehen, ergibt sich im Ergebnis, dass die Hälfte aller Cloud-nutzenden Unternehmen von Vornherein keine Prüfungen der Cloud-Dienstleister plant. Vor allem in ZI, VASP und WPF sind Cloud-Serviceproviderprüfungen nicht vorgesehen.
- Rund 4% der Cloud-nutzenden Unternehmen haben bereits umfassende Prüfungen absolviert. Weitere 3% haben solche Prüfungen bereits wiederholt durchgeführt. Diese umfassenden Prüfungsaktivitäten entfallen zur Gänze auf VU, KI und – zu einem kleineren Teil – auf WPF und VWG.

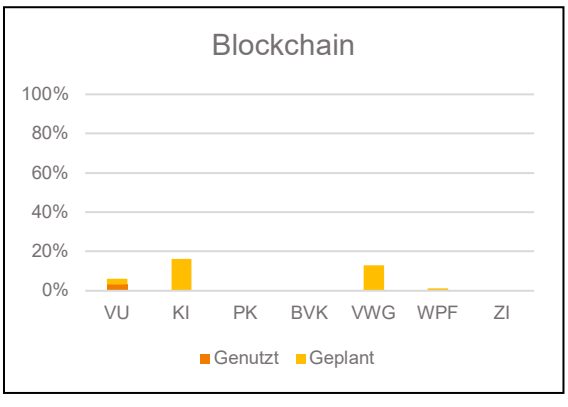
7.2 BLOCKCHAIN

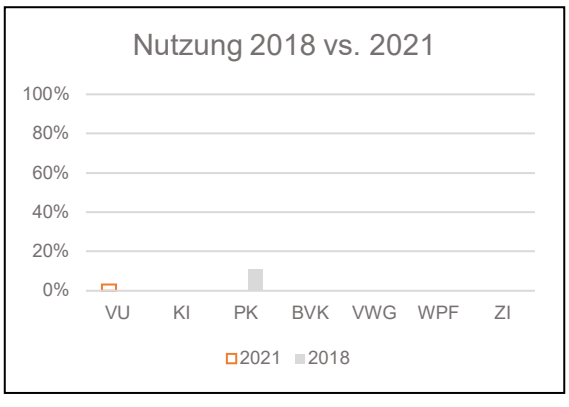
Eine Blockchain ist eine kryptographisch kodierte Datenbasis (Ledger) mit einer nicht manipulierbaren digitalen Logspeicherung auf einer Vielzahl von dezentralen Rechnern. Informationen unterschiedlichster Art (Buchungen, Kaufverträge) werden dabei im Netzwerk konsensual verifiziert. Die Blockchain ist aktuell die gebräuchlichste Ausprägung einer Distributed Ledger Technologie (DLT). Da die Begriffe meist synonym verwendet werden, wird auch hier in Folge Blockchain als generische Bezeichnung für die DLT gebraucht.

Chancen	■ vielseitig anwendbar ■ vor allem in verteilten, nicht-hierarchischen Systemen nutzbar ■ potentiell hohe Transparenz und Manipulationsresistenz durch konsensuale Verifikation ■ hohe Ausfallsicherheit durch verteilte Struktur
Risiken	■ relativ neue und teilweise schlecht verstandene Technologie ■ dezentrale Struktur verhindert inhärent Anwendungen mit zentraler Kontrolle ■ rein digitale Verarbeitbarkeit kann zu juristischen/technischen Risiken führen ■ alle in der Blockchain gespeicherten Daten sind zwischen den Teilnehmern öffentlich, was datenschutztechnische Implikationen haben kann

Aktuelle Entwicklungen:

Die Einschätzung im Zuge der letzten Digitalisierungserhebung 2018, wonach die Blockchain Technologie mittelfristig keine breiten Anwendungsfälle bei den beaufsichtigten Unternehmen finden würde, hat sich bestätigt. Einige beaufsichtigte Unternehmen planen zwar, Blockchain in den nächsten drei Jahren einzusetzen, diese Technologie kommt aber derzeit praktisch nicht zum Einsatz:





Das heißt natürlich nicht, dass Blockchain ein für die FMA oder den Finanzmarkt unrelevantes Thema ist, in der aufsichtsbehördlichen Wahrnehmung stehen aber vorranging Geschäftsmodelle iZm Token bzw. Kryptowährungen und ihren Anwendungen als Zahlungsmittel, Anlageobjekt etc.

im Fokus. Für die Technologie selbst haben sich nach wie vor keine anderen Anwendungsfälle bei den beaufsichtigten Unternehmen etabliert.

Dabei handelt es sich wohl eher um eine konzeptuelle als eine technische Hürde. Der Distributed Ledger ist, wie der Name impliziert, vor allem für dezentrale Systeme geeignet. Daher dürfte es einem etablierten Unternehmen entsprechend schwerfallen, technisch grundsätzlich mögliche und interessante Konzepte wie zB Peer-to-Peer Versicherung oder Smart Contracts in das bestehende Geschäftskonzept zu integrieren und diese zu monetarisieren.

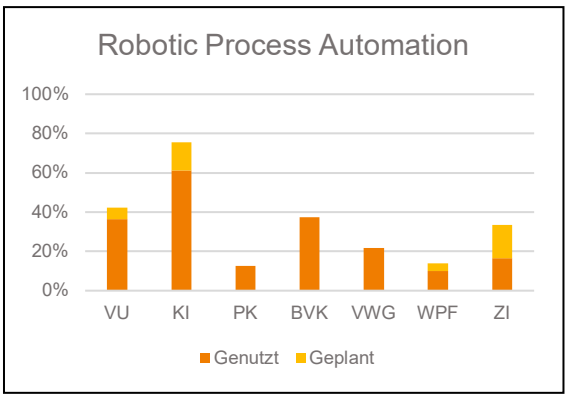
7.3 ROBOTIC PROCESS AUTOMATION

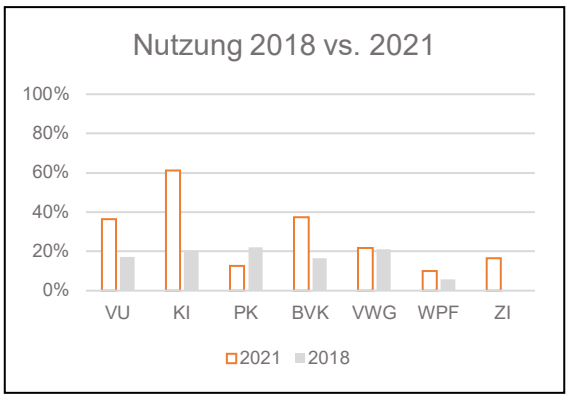
Robotic Process Automation (RPA) ist ein Sammelbegriff für „Bot"-Software, die zB durch die vordefinierte Ausführung von Tastatureingaben und Mausbewegungen, repetitive Tätigkeiten in Softwareanwendungen durchführen kann. Dabei ist typischerweise nur eine relativ einfache Entscheidungslogik hinterlegt, durch die Nutzung von Mauszeiger und Tastatur arbeitet das Programm auf dieselbe Weise wie es auch ein menschlicher Bearbeiter tun würde.

Chancen	■ leicht und kostengünstig implementierbar ■ erfordern in Bedienung und Anwendung oft keine IT-Kenntnisse ■ mit praktisch jeder Anwendung ohne deren Anpassung kompatibel
Risiken	■ bei einer Änderung an einem der mit RPA automatisierten Abläufe müssen mitunter alle darauf laufenden Bots angepasst werden ■ üblicherweise nicht für komplexe Entscheidungen geeignet ■ kann häufig nicht auf die einer Applikation zugrundeliegenden Daten zugreifen

Aktuelle Entwicklungen:

Die Nutzung von RPA ist in den letzten drei Jahren in den meisten Sektoren deutlich gestiegen und insbesondere bei KI schon weit verbreitet:





RPA ist eine Methode deren Anwendung meist als temporäre Hilfslösung oder Unterstützung bei Systemen, auf deren Geschäftslogik- und Datenbankebene man selbst keinen direkten Zugriff hat, erwogen wird. Die Möglichkeit zur raschen Implementierung scheint also bei der Nutzung von RPA den Ausschlag zu geben, um schnelle Effizienzgewinne zu erzielen.

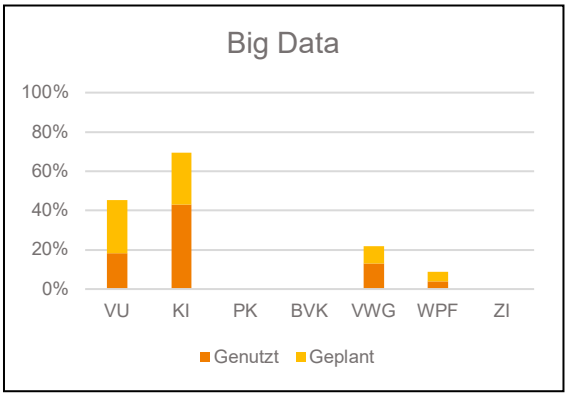
7.4 BIG DATA ANALYTICS

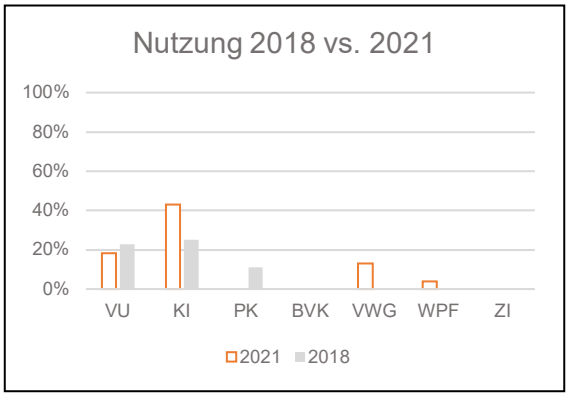
Big Data bezeichnet meist die automatisierte Verarbeitung großer Datenmengen (Volume) in engem Zeitrahmen (Velocity) aus unterschiedlichen Quellen (Variety). Im Finanzbereich gibt es zahlreiche mögliche Anwendungsfälle für diese Technologie (zB im Marketing, bei der Fraud Detection, bei der Erstellung mathematischer Modelle etc.).

Chancen	■ Durch die Analyse großer Datenmenge können genauere Modelle konstruiert werden ■ Durch neue Methoden für Data Analytics lassen sich individuelle Absicherungsbedarfe und Kaufwahrscheinlichkeiten genauer vorhersagen ■ Angebote können damit besser individualisiert werden ■ Big Data Anwendungen verbessern Analyseprozesse in der Prävention und Bekämpfung von Betrug, Geldwäsche und Terrorismusfinanzierung ■ Technologien wie Machine Learning sind nur mit großen Datenmengen realisierbar
Risiken	■ Mangelnde Datenqualität oder fehlerhafte Modelle können Ergebnisse verfälschen ■ Hohe Komplexität von Analysemodellen kann zu verschlechterter Transparenz und Nachvollziehbarkeit führen ■ Die Verarbeitung großer Datenmengen erfordert auch verstärkte Investition in Infrastruktur und Rechenleistung ■ Regelmäßig ablaufende Analysen großer Datenmengen lassen sich im Echtbetrieb aufgrund des Ressourcenaufwandes oft bei Bedarf nicht wiederholen

Aktuelle Entwicklungen:

Viele Unternehmen zeigen zwar Interesse an der Analyse großer Datenmengen, der konkrete Aufbau entsprechender Datenbanken und Analysesysteme scheint jedoch ein Hindernis darzustellen:





Über 40% der KI nutzen mittlerweile Big Data, in den anderen Bereichen stagniert die Verwendung dieser Technologie jedoch großteils. Insbesondere KI und VU planen oft die Einführung entsprechender Tools. Der vergleichsweise hohe Nutzungsgrad bei KI kann mitunter durch das Vorhandensein großer, strukturierter Datenmengen bei diesen Unternehmen erklärt werden, wohingegen andere Marktteilnehmer erst entsprechende Strukturen schaffen müssen.
Insgesamt existieren für Big Data insbesondere in Kombination mit Machine Learning potentiell zahlreiche wertvolle Anwendungsfälle. Ein mögliches Zukunftsszenario ist dementsprechend, dass Unternehmen mit einem Zugang zu großen Datenmengen daraus einen Wettbewerbsvorteil lukrieren können. Für die Aufsicht ist idZ wichtig, dass Kundeninteressen gewahrt bleiben.

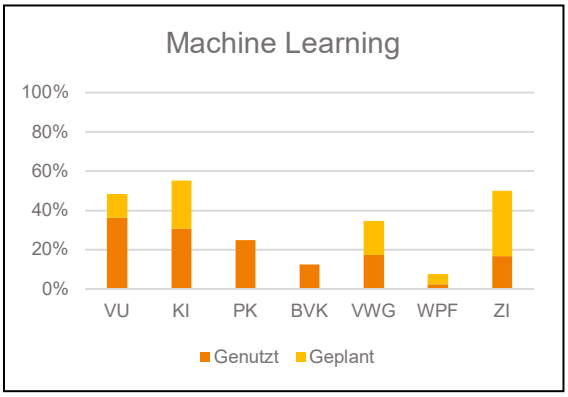
7.5 MACHINE LEARNING

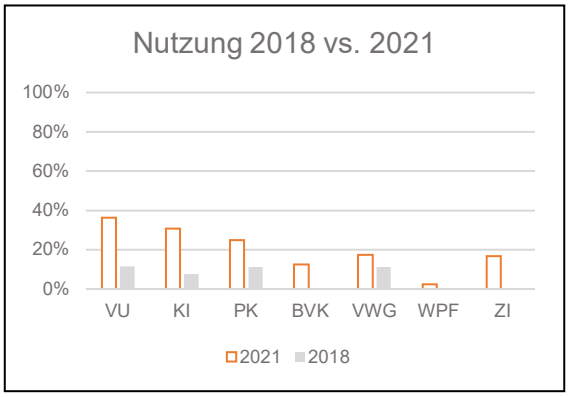
Ein Feld der Informatik, welches sich mit selbstlernenden Programmen beschäftigt. Dabei wird vom Programmierer kein Lösungsalgorithmus vorgegeben, die Software sucht selbst nach der passenden Vorgehensweise für ein Problem. Besonders geeignet ist dieses Verfahren zur Interpretation und Mustererkennung in großen Mengen spezifischer Daten.

Chancen	■ große Mengen Daten können automatisiert in kurzer Zeit verarbeitet werden ■ Sehr komplexe Tätigkeiten, die ansonsten einen Experten benötigen, können unterstützt oder übernommen werden. Ein richtig kalibriertes und angelerntes System kann sehr genau arbeiten und verbessert sich selbst laufend anhand neuer Daten ■ Es können potentiell neue, unbekannte Zusammenhänge erkannt werden
Risiken	■ Probleme mit der Datenqualität oder statistischen Methodik können zu ungenauen Ergebnissen führen ■ Komplexität und „Black Box“-Effekt können Transparenz schaden ■ Das System kann durch falsches Anlernen unbemerkt Stereotype entwickeln (zB Bilderkennung, Recruiting Tool)

Aktuelle Entwicklungen:

Der Nutzungsgrad von Machine Learning ist in den letzten drei Jahren deutlich gestiegen. Zwar konnten nicht alle Unternehmen, die dies planten, entsprechende Projekte umsetzen, aber bei über 20% der VU, KI und PK hat die Technologie bereits Anwendung gefunden:





Über Machine Learning können prädiktive Analysen ermöglicht werden und neue Zusammenhänge in Daten erkannt werden. Insgesamt bietet dieses Werkzeug großes Potential, ist aber anfällig auf methodische Fehler und Probleme in der Datenbasis. Je nach eingesetztem Algorithmus kann auch die Transparenz deutlich eingeschränkt werden.

Daraus ergeben sich einige Herausforderungen für die Aufsicht: Modelle müssen erklärbar bleiben und dürfen nicht unbeabsichtigt zu rechtlich bzw. ethisch problematischen Schlussfolgerungen führen.

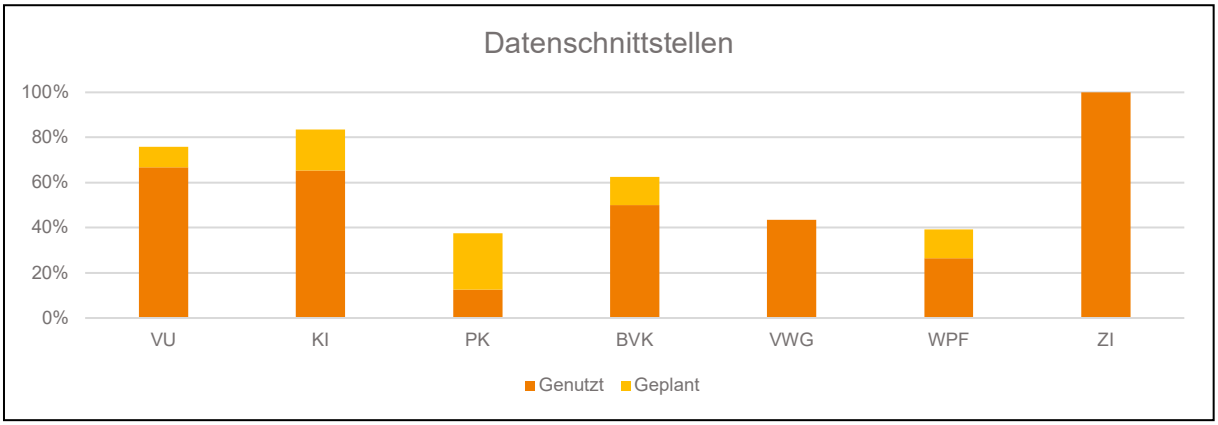
7.6 AUTOMATISIERTE DATENSCHNITTSTELLEN

Standardisierte Schnittstellen (APIs) ermöglichen den automatisierten Austausch von Daten mit Dritten über vordefinierte Formate und Transportkanäle. Auf diesem Weg ist es möglich, Daten von externen Anbietern auf regelmäßiger Basis in die eigenen Systeme und Berechnungen zu integrieren. Die möglichen Anwendungsfälle sind dabei weitreichend: Kapitalmarktdaten, Austausch von Bestandsdaten mit Vermittlern oder automatisierte Informationskanäle zu aktuellen IT-Risiken.

Chancen	■ Externe Datenprovider können Umsetzungen von Big Data Analytics und Machine Learning unterstützen ■ Ein externer Zulieferer kann verglichen mit rein interner Datensammlung oder manueller Datenübertragung kosteneffizienter sein ■ Korrekte Daten sind Grundlage für den Einsatz vieler komplexer IT-Systeme
Risiken	■ Jede Datenschnittstelle ist eine potentielle Angriffsfläche für externe Bedrohungen der IT-Sicherheit und muss entsprechend abgesichert werden ■ Bei personenbezogenen Daten ist die Wahrung des Datenschutzes mitunter eine zusätzliche Herausforderung ■ Zusätzliche Abhängigkeiten von externen Dienstleistern

Aktuelle Entwicklungen:

Viele beaufsichtigte Unternehmen nutzen bereits automatisierte Datenschnittstellen, bei VU, KI, BVK und ZI sind es jeweils 50% oder mehr. Das überrascht nicht, da moderne IT-Systeme immer mehr Aufgaben in Unternehmen übernehmen, dabei aber stets nur so gute Ergebnisse liefern können, wie es die ihnen zugeführten Daten ermöglichen. Für die FMA unterstreicht dieser Trend auch die wachsende Komplexität der von den Beaufsichtigten eingesetzten IT-Landschaften und die Notwendigkeit adäquater IT-Sicherheitsmaßnahmen sowie des Monitorings der eingesetzten Dienstleister.



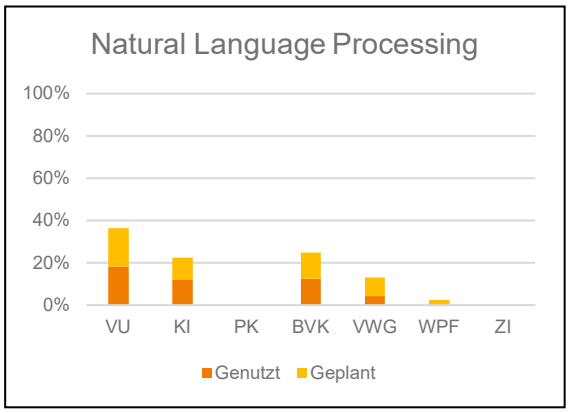
7.7 NATURAL LANGUAGE PROCESSING

Natural Language Processing beschreibt Techniken und Methoden zur maschinellen Verarbeitung natürlicher Sprache. Ziel ist eine direkte Kommunikation zwischen Mensch und Computer auf Basis der natürlichen Sprache (beispielsweise SIRI, ALEXA etc.).

Chancen	■ Effizienzgewinne durch möglichen Einsatz im Kundenverkehr ■ Umsetzung von Sprache in maschinelle Daten ermöglicht Schnittstellen zu den übrigen IT-Systemen des Unternehmens
Risiken	■ Technisch noch eher komplex; Mitunter Herausforderungen bei Datenschutz und Gefahr von Fehlinterpretationen beim Einsatz im Kundenverkehr

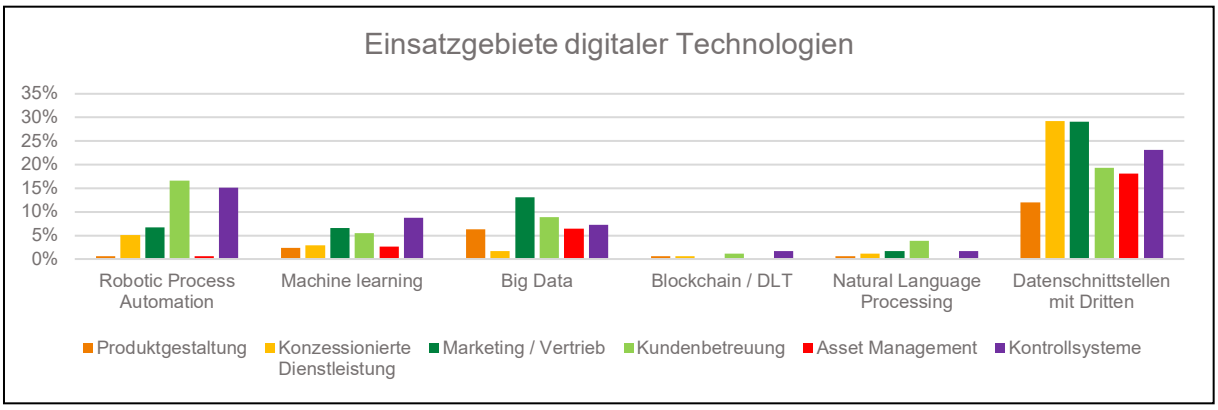
Aktuelle Entwicklungen:

Natural Language Processing ist bislang keine Technologie, welche große Verbreitung im österreichischen Finanzsektor gefunden hat. In keinem Segment des Marktes wird ein Nutzungsgrad von 20% erreicht, auch wenn eine Überschreitung dieser Marke bei VU, KI und BVK aufgrund geplanter Umsetzungen in den nächsten drei Jahren möglich scheint. Insofern ist dies eine der technologischen Entwicklungen, deren weitere Nutzung von der FMA vorerst abwartend beobachtet wird.



7.8 EINSATZGEBIETE DIGITALER TECHNOLOGIEN

Zusätzlich zu den Trends bei der Nutzung einzelner digitaler Technologien in den Sektoren des Finanzmarktes erlaubt die aktuelle Erhebung auch einen Einblick in die Nutzungsgebiete derselben. Dabei ergibt sich folgendes Bild:



Marketing/Vertrieb, Kundenbetreuung sowie regulatorische Kontrollsysteme (zB Risikomanagement, Compliance) sind **Haupteinsatzgebiete digitaler Technologien**. Dies deckt sich mit den sonstigen Erkenntnissen der vorliegenden Digitalisierungsstudie, wonach

- die Kundenschnittstelle am österreichischen Finanzmarkt grundsätzlich jener Ort ist, an welchem sich digitale Technologien am schnellsten etablieren;

- regulatorische Anforderungen sowie die Möglichkeit, etwa durch Fraud-Detection-Systeme eigene Kosten zu senken, den Einsatz neuer Analysemethoden bei den Kontrollsystemen treiben.

In Bezug auf die einzelnen Technologien selbst ergeben sich folgende Schlussfolgerungen:

- **Robotic Process Automation** wird primär in Kundenbetreuung und bei Kontrollsystemen eingesetzt, dort wohl zumeist für die Abarbeitung repetitiver Formulare, zB bei der Anlage und Übertragung von Datensätzen in den eigentlichen Analysesystemen.
- **Machine Learning** kommt im Marketing/Vertrieb und bei Kontrollsystemen zum Einsatz. Kundenanalysen, zB für Cross-Sales und fortschrittliche Fraud-Detection Systeme stellen hier zwei potentielle Anwendungsfälle dar.
- **Big Data Analytics** ist damit eng verknüpft und wird entsprechend in ähnlichen Feldern eingesetzt. Zudem wird diese Technologie von einigen Unternehmen im Asset Management genutzt.
- **Blockchain-Technologie** wird insgesamt kaum genutzt, hier ist die Identifikation konkreter Anwendungsfälle der Kern des Problems.
- **Natural Language Processing** ist ebenfalls noch nicht sehr häufig im produktiven Einsatz, der Trend geht aber hier, wie auch durch die Eigenschaften der Technologie indiziert, in Richtung Kundenbetreuung.
- **Datenschnittstellen** sind ein sehr vielseitiges Werkzeug und werden von vielen Unternehmen auch gleichzeitig in mehreren Bereichen eingesetzt, die starke Nutzung ist ein klarer Hinweis auf den steigenden Wert von Daten im Rahmen der Digitalisierung.

7.9 KONSULTATION ZU DEN DIGITALEN TECHNOLOGIEN

- Sollen entsprechend Ihren Erfahrungen bzw. Ihrer Einschätzung weitere digitale Technologien bzw. Einsatzmöglichkeiten in die Betrachtung der Implikationen der Digitalisierung auf den österreichischen Finanzmarkt einbezogen werden?
- Welche Rechtsunsicherheiten sind aus Ihrer Sicht mit dem Einsatz neuer digitaler Technologien verbunden?
- Teilen Sie die Einschätzung der FMA in Bezug auf die Chancen und Risiken der einzelnen Technologien?
- Welche weiteren wesentlichen Risiken könnten aus Ihrer Sicht für die einzelnen Sektoren künftig relevant sein?
- Was ist Ihre Erwartungshaltung hinsichtlich der Rolle der Aufsicht in den einzelnen Sektoren des Finanzmarkts?

8 IKT-BEZOGENE VORFÄLLE

Die intensivierte und vernetzte Nutzung digitaler Möglichkeiten, die auch durch die COVID-19-Pandemie getrieben wird, eröffnet neue Chancen, geht aber auch mit steigenden IKT-Risiken einher. So sind etwa die Cybercrime-Anzeigen in Österreich von 2019 auf 2020 um 26% gestiegen.[22] Der Angriff auf das Netzwerk des Bundesministeriums für Europäische und Internationale Angelegenheiten im Jahr 2020[23] wird von der Europäischen Agentur für Cybersicherheit, der ENISA, als einer der Hauptvorfälle weltweit im Zeitraum Januar 2019 bis April 2020 angeführt.[24] Dieses Beispiel verdeutlicht, dass sich auch Österreich im Betrachtungsradius von Cyberakteuren befindet und angemessene Sicherheitsmaßnahmen ergriffen werden müssen.

Zudem zählt der Finanzbereich nach wie vor zu den für Angreifer attraktiven Angriffszielen.[25] Dies liegt insbesondere an dem „inhärenten monetären Charakter" der Finanzdienstleistungsbranche, aber auch an den zunehmenden weltweiten Vernetzungen. Erfolgreiche Cyberangriffe können schnell um sich greifen und damit zu einer Gefahr für die Finanzmarktstabilität werden.

8.1 CYBERVORFÄLLE

Einheitliche sektorübergreifende Definitionen und Berichtspflichten zu IKT-bezogenen Vorfällen sind noch nicht definiert. Dies erschwert die Vergleichbarkeit innerhalb sowie zwischen den Sektoren und die Ableitung von Erkenntnissen.[26]

Während Zahlungsdienstleister schwerwiegende Betriebs- oder Sicherheitsvorfälle, die sich auf die finanziellen Interessen der Zahlungsdienstnutzer auswirken oder auswirken könnten, an die FMA melden müssen[27], sind solche Berichtspflichten in anderen Sektoren noch in Ausarbeitung bzw. sollen künftig vereinheitlicht werden. Der von der EK im September 2020 veröffentlichte Vorschlag für eine Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors (DORA)[28] umfasst auch IKT-bezogene Begriffsbestimmungen und ein sektorübergreifendes Berichtswesen zu

[22] *Bundesministerium für Inneres, Bundeskriminalamt, Cybercrime Report 2020, Lagebericht über die Entwicklung von Cybercrime, Wien 2021, 26.*
[23] *Bundeskanzleramt, Bericht Cybersicherheit für das Jahr 2020, Wien, 2021, 6.1 Der BMEIA-Vorfall und seine gesamtstaatlichen Konsequenzen.*
[24] *ENISA, Hauptvorfälle in der EU und weltweit – von Januar 2019 bis April 2020, 4.*
[25] *Vgl. zB FireEye Mandiant Services, M-Trends 2021, Special Report, 18.*
[26] *FMA, Digitalisierung am österreichischen Finanzmarkt, Juni 2019, VII. A. Definition von Cyberrisiken.*
[27] *Vgl. FMA, Meldung von schwerwiegenden Betriebs- oder Sicherheitsvorfällen nach § 86 ZaDiG 2018.*
[28] *Europäische Kommission, Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates über die Betriebsstabilität digitaler Systeme des Finanzsektors und zur Änderung der Verordnungen (EG) Nr. 1060/2009, (EU) Nr. 648/2012, (EU) Nr. 600/2014 und (EU) Nr. 909/2014, COM(2020) 595 final.*

IKT-bezogenen Vorfällen. Struktur und Inhalte der Meldevorgaben werden jedoch erst nach Inkrafttreten der Verordnung ausgearbeitet.

Die Erhebung der FMA zu IKT-bezogenen Vorfällen unterscheidet zwischen Cybervorfällen und anderen schwerwiegenden Betriebs- oder Sicherheitsvorfällen.

Die von der FMA gesammelten Daten zu Cybervorfällen basieren auf möglichen bzw. schlagend gewordenen nachteiligen Auswirkungen eines ungeplanten Einzelereignisses bzw. einer Serie von verbundenen Ereignissen auf Integrität, Verfügbarkeit, Vertraulichkeit, Kontinuität und bzw. oder Authentizität der bereitgestellten Finanzprodukte. Die Angaben waren dabei nach Angriffsarten aufzuschlüsseln.

8.1.1 ANZAHL DER CYBERVORFÄLLE

Von 2019 auf 2020 ist die **Anzahl der Cybervorfälle in beaufsichtigten Unternehmen deutlich stärker gestiegen als die allgemeine Zunahme** der Cybercrime-Anzeigen in Österreich. Auch wenn diese Zahlenangaben nicht unmittelbar vergleichbar sind, so stellen sie dennoch eine Indikation zur besonderen Exponiertheit von beaufsichtigten Unternehmen gegenüber Cyberangreifern dar.

Österreich	*Anzahl der Cybercrime Anzeigen*[29]	*Anzahl der Cybervorfälle bei Beaufsichtigungen*
2019 - 2020	+26%	+98%

Die Anzahl der Cybervorfälle in den beaufsichtigten Unternehmen hat sich von 2019 auf 2020 annähernd verdoppelt. Die Steigerung liegt damit deutlich über der Erhöhung der Cybercrime-Anzeigen in Österreich um 26% für den gleichen Zeitraum

Zwischen den Sektoren unterscheiden sich die Angaben zu Cybervorfällen teils massiv. Aktuell konzentrieren sich Cybervorfälle vor allem auf den KI-Sektor.[30]

[29] *Bundesministerium für Inneres, Bundeskriminalamt, Cybercrime Report 2020, Lagebericht über die Entwicklung von Cybercrime, Wien 2021, 26.*

[30] *Dies zeigt sich zB auch bei den der EZB gemeldeten Cybervorfällen. Diese sind von 2019 auf 2020 um 54% gestiegen, wobei jedoch keine wesentlichen Beeinträchtigungen bei der Erbringung der Bankdienstleistungen beobachtet worden sind. Vgl. EZB, Supervision Newsletter: IT and cyber risk: a constant challenge, 18.August 2021.*

8.1.2 HÄUFIGSTE ANGRIFFSARTEN

Phishing und Malware stellen seit 2019 die häufigsten Angriffsarten in den beaufsichtigten Unternehmen dar. 2020 sind knapp **90% der Cybervorfälle** diesen Angriffsarten zuzurechnen.

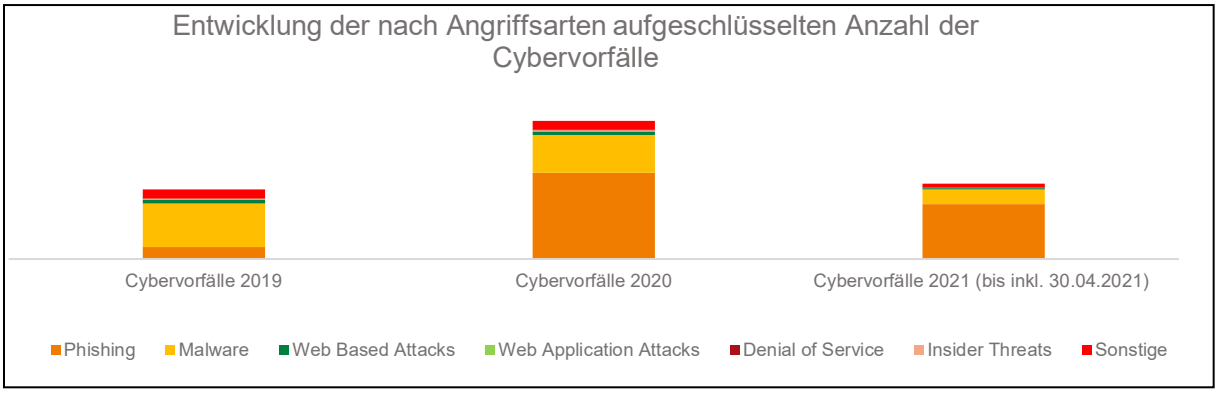
Top 5 Angriffsarten 2020

Rang 2020	*Angriffsart*	*Rang 2019*	*ENISA größte Bedrohungen 2019-2020*[31]
1.	Phishing	2.	3.
2.	Malware	1.	1.
3.	Sonstige	3.	-
4.	Web Based Attacks	4.	2.
5.	Denial of Service	11.	6.

Bei den Angriffsarten war 2020 Phishing mit großem Abstand am stärksten verbreitet. Malware nimmt Rang zwei ein und liegt deutlich vor den restlichen Angriffsarten.

Bei ENISA stellen 2019 bis 2020 Malware, Web Based Attacks und Phishing die größten drei Bedrohungen dar.[32] Denial of Service liegt bei ENISA auf dem sechsten Rang. Insgesamt ergibt sich ein kohärentes Bild, bei dem sich die Situation im Finanzsektor der österreichischen FI im Großen und Ganzen im Einklang mit der europäischen Lage befindet.

Im Vergleich dazu liegen bei den im Jahr 2020 der EZB gemeldeten Cybervorfällen Denial of Service-Attacken vor unberechtigten Zugriffen und Phishing; danach folgen böswillige Scripting Angriffe und Malware.[33]

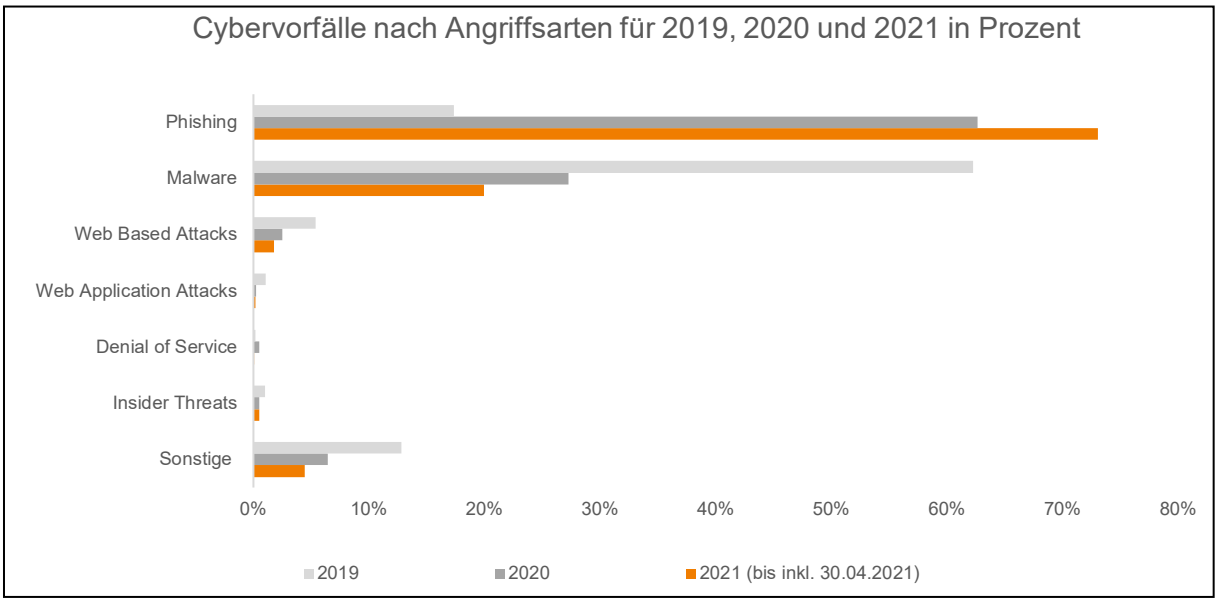


Auch von Jänner bis Ende April 2021 ist Phishing die häufigste Angriffsart.

[31] *ENISA: Das Jahr im Rückblick – Von Januar 2019 bis April 2020, ENISA Threat Landscape.*
[32] *ENISA: Das Jahr im Rückblick – Von Januar 2019 bis April 2020, ENISA Threat Landscape.*
[33] *EZB, Supervision Newsletter: IT and cyber risk: a constant challenge, 18. August 2021.*

In diesem Zeitraum sind fast ¾ aller Cybervorfälle dieser Kategorie zuzurechnen. Die Top-Positionierung ist auch durch die leichte Skalierbarkeit von Phishing-Attacken erklärbar. So können Phishing-E-Mails zB schnell an mehrere Empfänger geschickt werden.

2021 liegt Malware wiederum auf Rang zwei; auf den dahinterliegenden Plätzen befinden sich „Sonstige“, gefolgt von Web Based Attacks und Insider Threats.



Worin bestehen die häufigsten Angriffsarten?

Phishing	Persönliche Daten von Kunden oder Mitarbeitern (Beispiele sind Passwörter oder Kreditkartennummern) werden mittels gefälschter E-Mails oder Websites beschafft.
Malware	Schadsoftware wie Viren oder Trojaner ist hier subsumiert.
Web Based Attacks	Websysteme werden kompromittiert, um deren Nutzer umzuleiten oder Scripts – also eine Abfolge von Befehlen – zu starten, welche das Herunterladen von Schadsoftware initiieren.
Denial of Service	Systeme werden durch eine große Anzahl von Anfragen gezielt überlastet.
Web Application Attacks	Angriffe auf Webapplikationen des Unternehmens bzw. auf dahinterliegenden Datenbanken erfolgen.
Insider Threats	Datenpanne bzw. Datendiebstahl durch unternehmensinterne Verursacher.

8.1.3 FINANZIELLE VERLUSTE

Seit 2019 ist der größte Teil der Verluste **auf Phishingangriffe zurückzuführen**. Wie bei der Anzahl der Cybervorfälle unterscheiden sich auch die direkten und indirekten finanziellen Verluste, die im Zusammenhang mit Cybervorfällen stehen, innerhalb und zwischen den Sektoren deutlich. Die Hauptlast der ausgewiesenen Verluste **entfällt auf Kreditinstitute**.

- Insgesamt sind die mit Cybervorfällen verbundenen **direkten finanziellen Verluste** von 2019 auf 2020 um ~80% gesunken und belaufen sich 2020 auf knapp 600.000 Euro. Die Wertänderung ist im Wesentlichen auf den Verlustausweis eines Unternehmens 2019 zurückzuführen. Dies veranschaulicht auch, dass schlagend gewordene Cyberrisiken mit bedeutenden finanziellen Auswirkungen verbunden sein können.
- **Indirekte finanzielle Verluste** können direkte Verluste wesentlich übersteigen. Einige Unternehmen schätzen indirekte Verluste anhand der Anzahl erforderlicher Personentage. Andere Unternehmen orientieren sich an möglichen Reputationseinbußen, die ggf. auch Auswirkungen auf den Aktienkurs nach sich ziehen können. Insgesamt ist deshalb in diesem Bereich die Addition der Angaben nur stark eingeschränkt möglich.

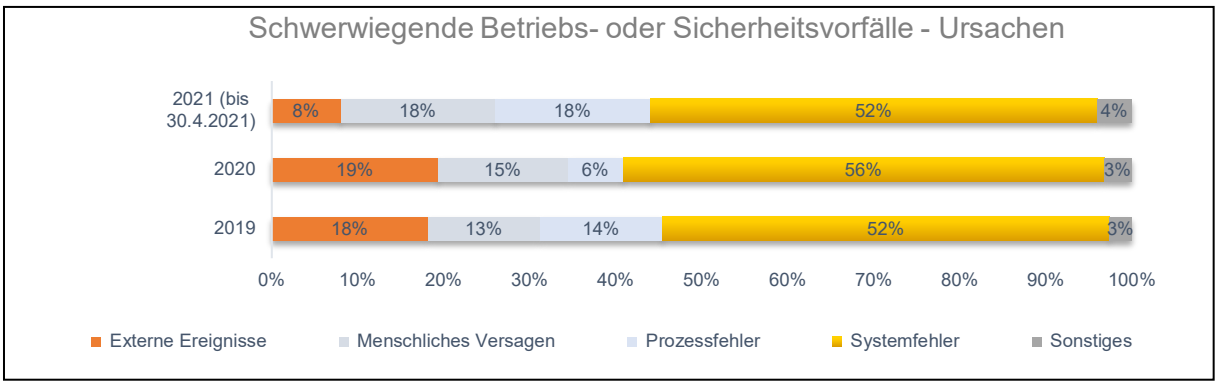
8.2 ANDERE SCHWERWIEGENDE BETRIEBS- ODER SICHERHEITSVORFÄLLE

IKT-bezogene Vorfälle, die nicht unter Cybervorfällen subsumiert werden, werden als andere schwerwiegende Betriebs- oder Sicherheitsvorfälle ausgewiesen.

Die beaufsichtigten Unternehmen waren von schwerwiegenden Betriebs- oder Sicherheitsvorfällen **in ca 2/3 aller Fälle indirekt durch einen Dienstleister** betroffen. Die meisten Vorfälle wurden von KI, gefolgt von VU, gemeldet. Die direkten und indirekten Kosten variieren je nach Vorfall stark und betreffen wiederum vor allem Kreditinstitute.

8.2.1 URSACHEN

Systemfehler sind die häufigste Ursache von anderen schwerwiegenden Betriebs- oder Sicherheitsvorfällen gemäß der ab 2019 vorliegenden Datensammlung.

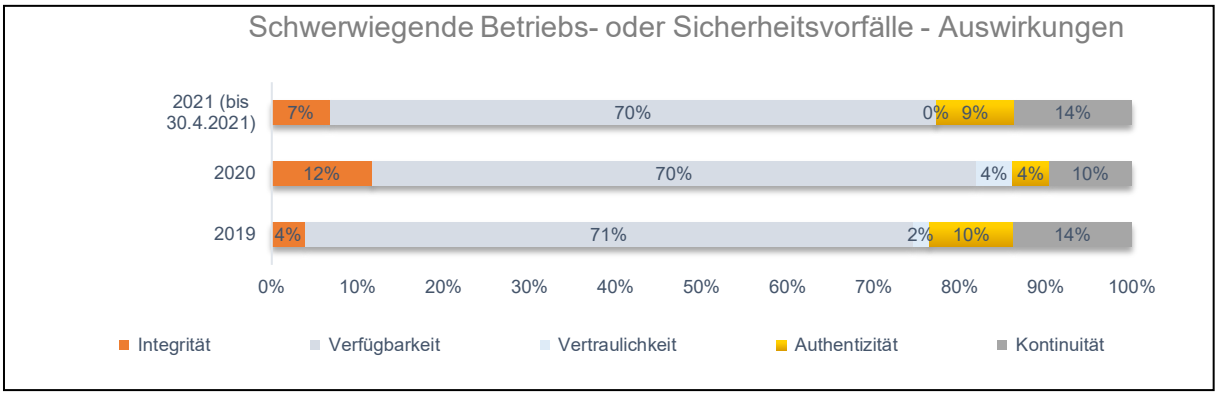


Schwerwiegende Betriebs- oder Sicherheitsvorfälle können durch Systemfehler, externe Ereignisse, Prozessfehler oder bzw. und durch menschliches Versagen bedingt sein. Systemfehler werden dabei von den FI am häufigsten als Quelle angegeben.

Während 2019 und 2020 rund ein Fünftel aller Angaben auf externe Ereignisse entfielen, beläuft sich der Vergleichswert für die ersten vier Monate 2021 auf knapp ein Zehntel.

8.2.2 AUSWIRKUNGEN

Schwerwiegende Betriebs- oder Sicherheitsvorfälle beeinträchtigen das Ziel der **Verfügbarkeit** am häufigsten.



Das Schutzziel der Verfügbarkeit, das ist die Eigenschaft, zugänglich und verwendbar zu sein, wurde seit 2019 mit Abstand am stärksten betroffen.

Rund **70%** aller Angaben zu den Auswirkungen entfallen seit 2019 auf diese Kategorie.

Im Gegensatz dazu haben solche Vorfälle Vertraulichkeitsziele am wenigsten beeinträchtigt.

Worauf können sich die Auswirkungen beziehen?[34]

Verfügbarkeit	Die Eigenschaft, zugänglich und verwendbar zu sein.
Vertraulichkeit	Informationen werden unbefugten Personen, Stellen oder Prozessen nicht zugänglich gemacht oder diesen nicht offengelegt.
Integrität	Korrektheit und Vollständigkeit.
Kontinuität	Die für die Erbringung der Finanzdienstleistungen erforderlichen Prozesse, Aufgaben und Vermögenswerte sind in vollem Umfang zugänglich und auf einem annehmbaren vordefinierten Niveau funktionsfähig.
Authentizität	Eine Quelle ist tatsächlich das, was sie zu sein vorgibt.

[34] *Die Angaben erfolgen in Anlehnung an EIOPA, Leitlinien zu Sicherheit und Governance im Bereich der Informations- und Kommunikationstechnologie, EIOPA-BoS-20/600 sowie an EBA, Leitlinien für die Meldung schwerwiegender Vorfälle gemäß der Richtlinie (EU) 2015/2366 (PSD 2), EBA/GL/2017/10.*

9 POST-COVID-19 BEZOGENE IKT-RISIKEN

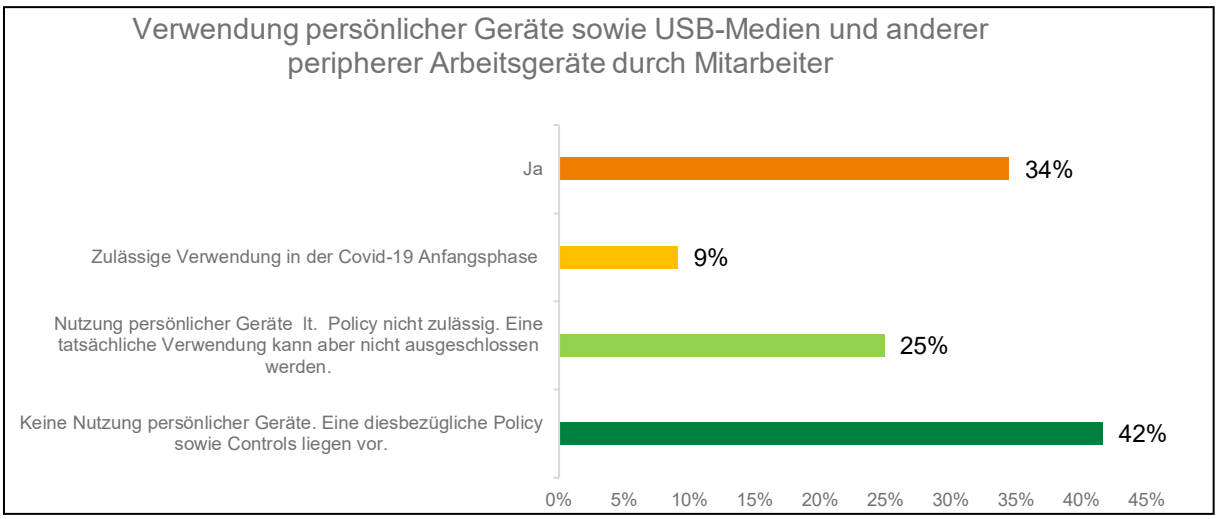
Die Risiken iZm der Rückkehr an den physischen Arbeitsplatz nach der COVID-19-Krise hat die FMA durch Analysen zur Verwendung persönlicher Geräte, zur Zulässigkeit persönlicher Applikationen (zB Telekonferenz-Software), zur Wiedereinsetzung nicht überwachter IT-Syteme sowie zu Social-Engineering-Schulungen analysiert.

Insgesamt scheinen beaufsichtigte Unternehmen angemessene Maßnahmen getroffen zu haben, um auch eine IKT-risikominimierende Rückkehr an den physischen Arbeitsplatz zu gewährleisten.

9.1 VERWENDUNG PERSÖNLICHER GERÄTE

Die COVID-19-Pandemie hat unerwartet rasche und umfangreiche Umstellungen auf Homeoffice bedingt. Dadurch wurde teilweise auch die Nutzung persönlicher Geräte (wie Computer oder Mobiltelefone) sowie von USB-Speichermedien oder anderer peripherer Geräte intensiviert. Ohne angemessene Sicherheitsmaßnahmen können infolgedessen neue Risiken durch unbekannte Angriffsziele und Schwachstellen entstehen. Diese ergeben sich durch die Nicht-Durchführung erforderlicher Updates oder durch nicht bzw. unzureichend geschützten Zugang zu den Geräten. Unter anderem besteht auch die Möglichkeit der Infiltrierung des Unternehmensnetzwerks mit Malware über solche persönlichen Geräte.

Ein Drittel der beaufsichtigten Unternehmen erlaubt die Verwendung persönlicher Geräte (zB von Computern oder Handys) sowie von USB-Speichermedien und anderen peripheren Geräten explizit und sieht dabei gleichzeitig Sicherheitsmaßnahmen vor.



Zwei Drittel der beaufsichtigten Unternehmen sehen dagegen eine Nutzung persönlicher Geräte nicht vor. Dieser Grundsatz ist in vier von zehn Unternehmen auch in einer Policy angeführt; zudem wird die Einhaltung des Verbots auch überprüft.

Ein Viertel der Unternehmen schließt solche Nutzungen zwar laut Policy aus, kann eine tatsächliche Verwendung aber nicht ausschließen. Beispiele sind die Nutzung von USB-Geräten oder die Möglichkeit, dass über verschlüsselte USB-Speicher Daten transferiert werden.

In der COVID-19-Anfangsphase war die Verwendung in knapp 10% der beaufsichtigten Unternehmen grundsätzlich in Verbindung mit weiteren Sicherheitsmaßnahmen erlaubt.

- Der Ausschluss persönlicher Geräte ist am stärksten in BVK (3/4 aller BVK) und mit 33% am wenigsten in VU verbreitet.
- Die Verwendung persönlicher Geräte sowie USB-Speichermedien oder anderer periphere Geräte für Arbeitszwecke ist in VU am häufigsten verbreitet – sie ist in rund der Hälfte der VU erlaubt.

Im Fall der Zulässigkeit persönlicher Geräte sind beispielsweise folgende technische und organisatorische Sicherheitsmaßnahmen – auch in Kombination – vorgesehen:

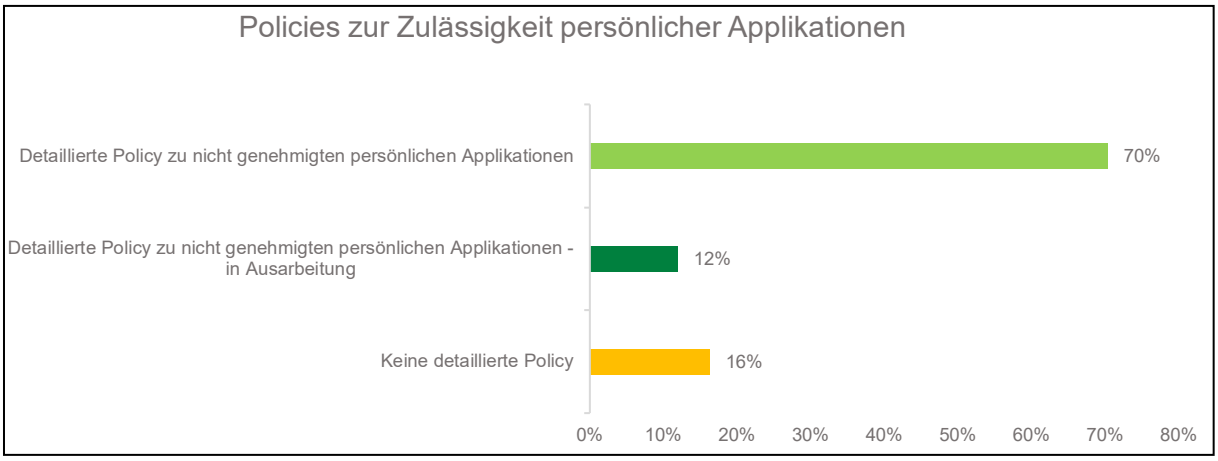
- MDM (Mobile Device Management): In einem MDM werden beispielsweise alle Geräte inventarisiert und können remote konfiguriert und gewartet werden. Auch Fernlöschungen sind möglich. Der Zugriff auf Apps und Webseiten kann geregelt, zB ausgeschlossen werden. Auch die Verwendung von sogenannten Containern, bei denen Unternehmensdaten von persönlichen Daten getrennt werden, kann umfasst sein
- Containerlösungen für Handys
- Technisches Unterbinden bzw. Kontrolle von USB-Nutzungen
- Aufspüren von Cyberbedrohungen durch künstliche Intelligenz
- Zwei- oder Multi-Faktor-Authentifizierung: Im Zuge der Authentifizierung sind zwei oder mehr Nachweise zur Identifizierung zu liefern. Nachweisfaktoren sind zB Wissen, Besitz, Inhärenz[35] oder der Ort des Benutzers
- Zugriff auf ein Netzwerk von außen über eine geschützte Verbindung, über ein Virtuelles Privates Netzwerk (VPN)
- Verschlüsselung von Verbindungen zwischen Geräten
- Nutzung von Virtualisierungen: Hier kann der Benutzer von seinem Gerät auf gewohnten Anwendungsflächen arbeiten

[35] *Gemeint sind biometrische Methoden, wie zB ein Fingerabdruck.*

- Installation von Fernwartungs-Software oder Überprüfung der Sicherheitssoftware bei persönlichen Endgeräten
- Unterbindung von Daten-Downloads auf privaten Rechnern
- Dienstanweisungen bzw. Richtlinien zum Einsatz persönlicher Geräte
- Schulungen zur Stärkung der Cybersicherheit

9.2 ZULÄSSIGKEIT PERSÖNLICHER APPLIKATIONEN

Telekonferenz-Software, persönliche Cloud-Sicherungen, Drucker- und sonstige Hardware-Driver, Videospiele sowie die Verwendung von Social Media können im Arbeitsumfeld mögliche Beispiele für nicht genehmigte Applikationen darstellen. Diese können im Fall der Nichterfüllung der IT-Sicherheitsvorgaben die Unternehmens-IT verwundbar machen.

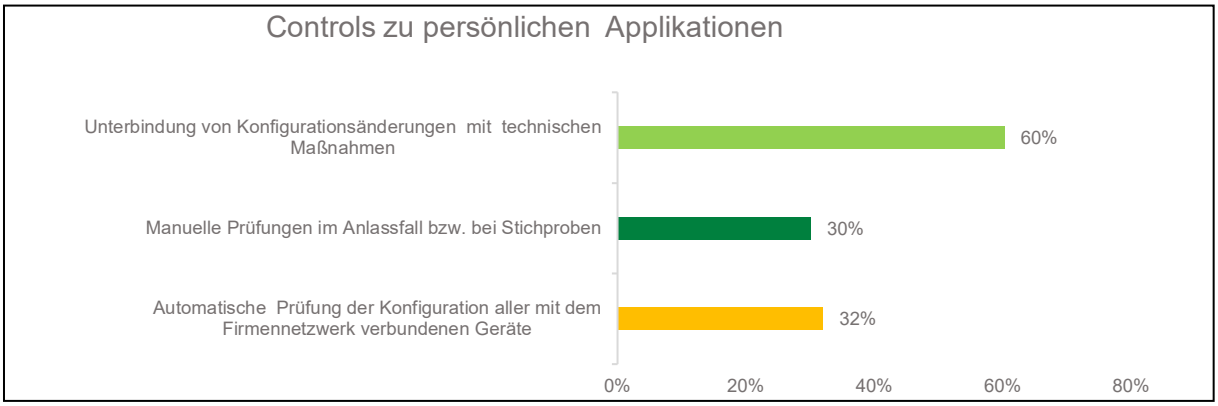


70% der beaufsichtigten Unternehmen haben eine detaillierte Policy zu nicht genehmigten persönlichen Anwendungen umgesetzt. In KI, VU, VWG und BVK sind solche Policies öfters als im Gesamtdurchschnitt vorhanden.

Während rd. 12% der FI solche Vorgaben aktuell ausarbeiten, geben 16% an, dass eine detaillierte Policy nicht explizit vorhanden ist. In den zuletzt genannten Fällen wird die Nutzung persönlicher Anwendungen beinahe durchgängig auf Basis von Richtlinien oder unternehmensinternen Standards untersagt oder durch ein Sicherheitssystem verhindert.

Etwa 16% der beaufsichtigten Unternehmen sehen zwar keine explizite Policy zu nicht genehmigten persönlichen Applikationen vor; beinahe alle diesen Unternehmen schließen jedoch solche Nutzungen über andere unternehmensinterne Vorgaben aus oder verhindern sie von Vornherein durch technische Maßnahmen.

Die beaufsichtigten Unternehmen setzen die folgenden Controls im Hinblick auf nicht genehmigte persönliche Applikationen:



60% der FI setzen technische Maßnahmen, um Konfigurationsänderungen an dienstlichen Geräten durch Benutzer zu unterbinden.

Ein Drittel aller FI prüft die Konfiguration aller Geräte, die mit dem Firmennetzwerk verbunden werden, automatisch.

Im Gegensatz dazu werden in 30% der FI Konfigurationen stichprobenmäßig oder im Anlassfall kontrolliert.

- Benutzerkontensteuerung
- Prinzip der geringsten Privilegien („Least Privilege“)
- Kontrollierte Nutzung von Administratorenrechten
- USB-Sperre
- Verhinderung von Downloads, Mailtransfers und Filetransfer von ausführbaren Dateien
- Zentrales Management der Versions- und der Patch-Stände
- Schwachstellenscans
- Port-Security
- Firewall
- Software-Sperrlisten („Blacklists“)
- Unterbindung der Ausführung unbekannter Applikationen („Application Whitelisting“)
- Jährliche Lizenzprüfung auf Basis der auf den Geräten gefundenen Software

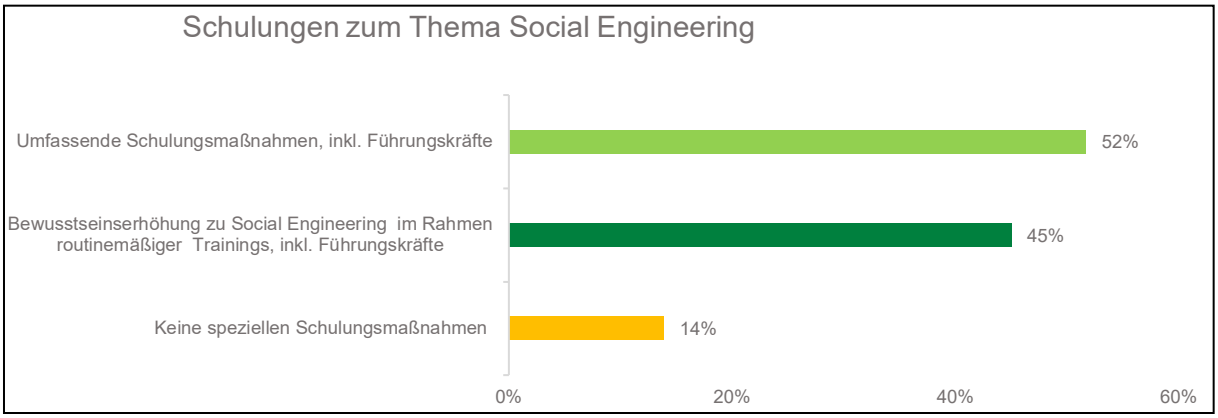
- Automatisierte Erfassung des Softwarestands auf Endgeräten und zentrale Speicherung
- Halbautomatisierte, zeitnahe Analyse von sicherheitsrelevanten Ereignissen (Security Information and Event Management, „SIEM“ / User and Entity Behavior Analytics, „UEBA“)
- Neuinstallation des Systems nach einem Incident

9.3 WIEDEREINSETZUNG NICHT ÜBERWACHTER IT-SYSTEME

Grundsätzlich waren bzw. sind während der COVID-19-Krise annähernd alle IT-Systeme in den beaufsichtigten Unternehmen online und überwacht. Lediglich in Ausnahmefällen waren einzelne Systeme offline bzw. zwar online, aber nicht überwacht. Beispielsweise konnte der Update-Status im Home-Office vereinzelt nicht überprüft werden. Auch in diesen Einzelfällen wurden vor der Rückkehr an den Arbeitsplatz Maßnahmen gesetzt, wie zB die Durchführung eines kompletten Antivirus-Scans oder Updates von Konfigurationen und Sicherheits-Patches.

9.4 SCHULUNGEN ZU SOCIAL ENGINEERING

Laut Europol haben sich Social Engineering Angriffe während der COVID-19-Krise sowohl hinsichtlich deren Anzahl als auch deren Sophistizierung signifikant erhöht.[36] Bei Social Engineering wird durch verschiedene Maßnahmen (zB Phishing) versucht, spezifische Informationen zu erhalten oder Personen zu bestimmten Handlungen zu bewegen. Als Sicherheitsmaßnahmen empfiehlt ENISA Bewusstseinskampagnen, Schulungen und auch zielgerichtete Penetrationstests.[37]

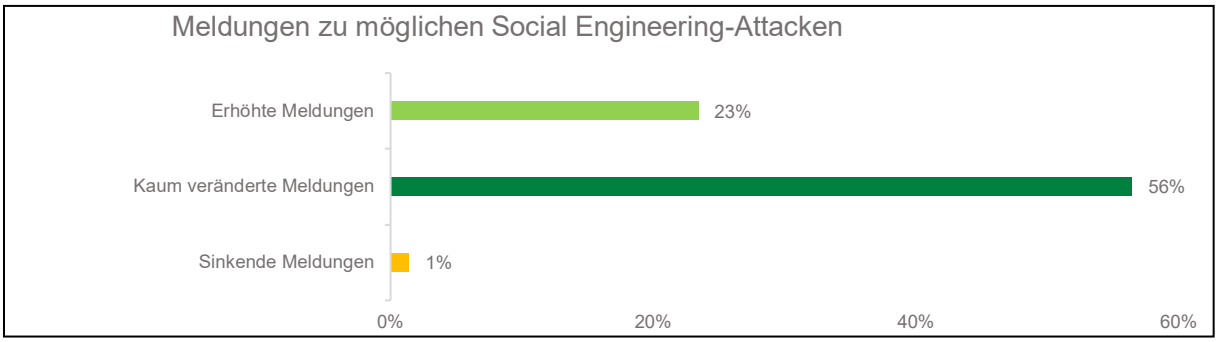


14% der beaufsichtigten Unternehmen haben keine speziellen Schulungsmaßnahmen zu Social Engineering durchgeführt.

[36] *Vgl. zB Europol, Internet Organised Crime Threat Assessment (IOCTA) 2020, 14.*
[37] *ENISA, What is „Social Engineering“? – Recommendations, abgefragt am 7.9.2021.*

Gut die Hälfte der beaufsichtigten Unternehmen hat demgegenüber umfassende Schulungen zu dieser Angriffsart – auch für Führungskräfte – vorgesehen. Zudem wurde das Bewusstsein zu Social Engineering im Rahmen routinemäßig stattfindender Trainings in 45% der Unternehmen erhöht.

Die meisten beaufsichtigten Unternehmen haben umfassende Schulungen oder Maßnahmen zur Bewusstseinserhöhung zum Thema Social Engineering unter Teilnahme von Führungskräften durchgeführt. Diese haben auch zu einem Anstieg der Meldungen möglicher Cyber-Attacken geführt.



Im Anschluss an Social Engineering Schulungen sind Meldungen zu möglichen Attacken in rd. einem Viertel der beaufsichtigten Unternehmen gestiegen.

Kaum veränderte Meldungen lagen in rd. 55% der Beaufsichtigten vor. In einem Prozent der Unternehmen waren sinkende Meldungen zu verzeichnen.

10 FMA-CYBER MATURITY LEVEL ASSESSMENT

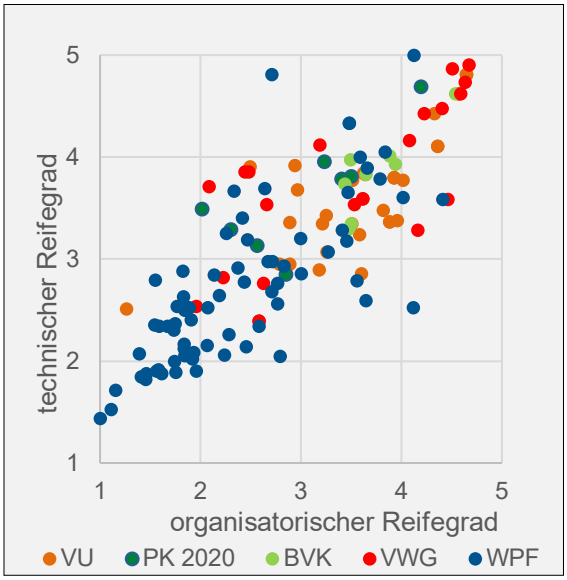
Das FMA-Cyber Maturity Level Assessment hat die FMA bereits 2019 entwickelt und erstmalig im Versicherungssektor und 2020 auch im Pensionskassensektor eingesetzt. Dieses Tool dient der FMA dazu, die Cyberresilienz der beaufsichtigten Unternehnehmen für Zwecke der Risikoeinstufung zu ermitteln und im Sinne der Prävention die Unternehmen auf neue regulatorische Vorgaben im Bereich der IKT-Sicherheit vorzubereiten (zB EIOPA-Leitlinien[38] bzw. Vorschlag der Europäischen Kommission über die Betriebsstabilität digitaler Systeme des Finanzsektors [DORA][39]). Im Rahmen der Digitalisierungsstudie 2021 wurden auch BVK, VWG, MI, WPF und VASP diesem Assessment unterzogen. Das ermöglicht einen ersten sektorübergreifenden Vergleich der Cyberrisikoreifegrade. Auf der fünfteiligen Reifegradskala, bei der ein höherer Reifegrad mit einer höheren Maturität einhergeht, hat der österreichische Finanzmarkt (der Bankensektor war hier nicht einbezogen) einen durchschnittlichen Gesamtreifegrad von 3,2 erzielt.

Mit einem durchschnittlichen Reifegrad von 3,2, hat der österreichische Finanzmarkt im Aggregat die wesentlichsten Vorkehrungen zur Sicherstellung einer angemessenen IKT-Sicherheit getroffen. Mit 3,8 bzw. 3,7 weisen BVK und VU die höchste Cybermaturität vor VWG, PK 2020 und WPF auf.

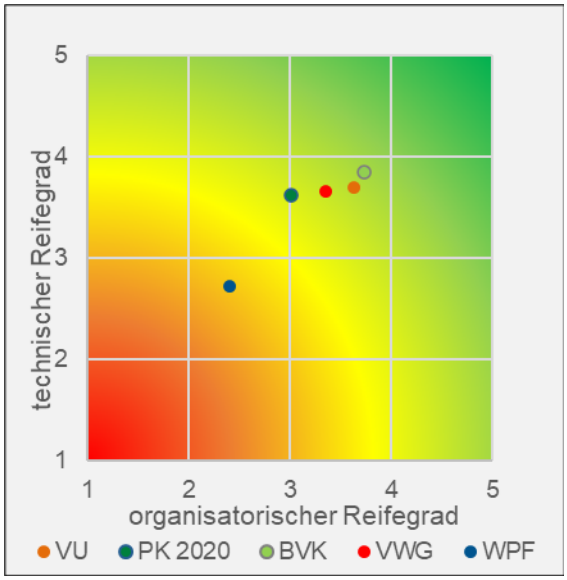
Übersicht	*VU*	*PK 2020*	*BVK*	*VWG*	*WPF*
Reifegrad gesamt	**3,7**	**3,3**	**3,8**	**3,5**	**2,6**
Reifegrad organisatorisch	3,6	3,0	3,7	3,4	2,4
Reifegrad technisch	3,7	3,6	3,8	3,7	2,7

[38] *EIOPA, Leitlinien zu Sicherheit und Governance im Bereich der Informations- und Kommunikationstechnologie, EIOPA-BoS-20/600.*
[39] *EK, Vorschlag für eine Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors, COM(2020) 595 final.*

Durchschnittliche Reifegrade pro Unternehmen



Durchschnittliche Reifegrade pro Sektor

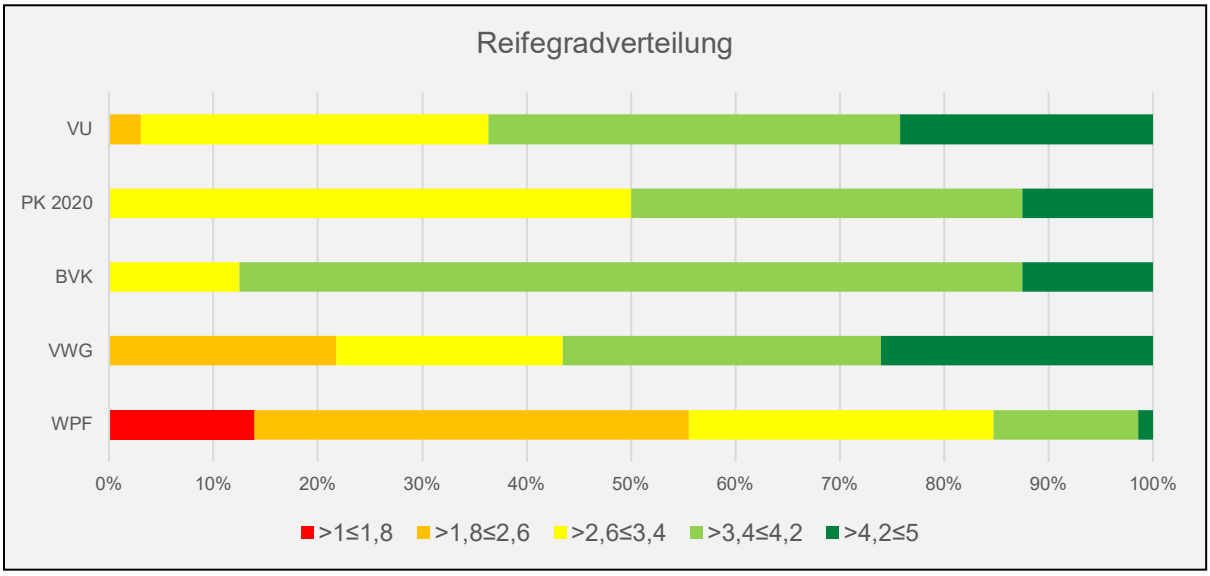


In der obigen Graphik ist auch gut erkennbar, dass von den Sektordurchschnittsreifegraden nicht auf die Cybermaturität einzelner Unternehmen geschlossen werden kann. Zu dieser Einschätzung sind Betrachtungen auf Einzelunternehmensebene jedenfalls erforderlich.

- Bei den im Ranking zweitplatzierten VU hat sich der durchschnittliche Maturitätsgrad vom ersten im Jahr 2019 in diesem Sektor durchgeführten Assessment mit einem Wert von 3,1 auf aktuell 3,7 erhöht. Bei der ersten Erhebung erreichten die organisatorischen Themenbereiche im Durchschnitt mit 2,9 geringere Reifegrade als die technischen Themen, die einen Vergleichswert von 3,3 aufwiesen. In den an das Assessment anschließenden bilateralen Gesprächen mit jedem einzelnen VU wurden die getroffenen Maßnahmen und Auffälligkeiten thematisiert. Nunmehr hat sich der durchschnittliche organisatorische Reifegrad mit 3,6 dem technischen Reifegrad von 3,7 angenähert und liegt mit diesem beinahe auf gleicher Ebene.
- In den PK wurde das Cyber Maturity Assessment bereits 2020 durchgeführt und ist hier zu Vergleichszwecken angeführt. Bei der Interpretation der Ergebnisse ist somit zu bedenken, dass PK in der Zwischenzeit schon weitere Maßnahmen gesetzt haben könnten.

Technische Vorkehrungen zur IKT-Sicherheit sind auf einem insgesamt höheren Niveau als organisatorische Maßnahmen.
Hohe technische Cyberreife kann beispielsweise auf IT-Auslagerungen beruhen, bei denen das Spezialwissen der IT-Dienstleister, jedenfalls in technischer Hinsicht, genutzt wird. Die Kehrseite kann, neben einer potentiell hohen Abhängigkeit von IT-Anbietern, ein reduziertes Bewusstsein zur Setzung organisatorischer Maßnahmen sein. Möglich ist auch, dass von den IT-Abteilungen Sicherheitsmaßnahmen gesetzt werden, die im Governance- bzw. Steuerungsbereich noch nicht zur Gänze berücksichtigt worden sind.

Die Reifegradverteilungen veranschaulichen nach dem Ampelsystem, welcher Unternehmensanteil des spezifischen Sektors welchen Reifegrad erlangt: Dunkelgrün zeigt zB den Anteil der Unternehmen des jeweiligen Sektors, die einen hohen Reifegrad (größer 4,2) erreicht.

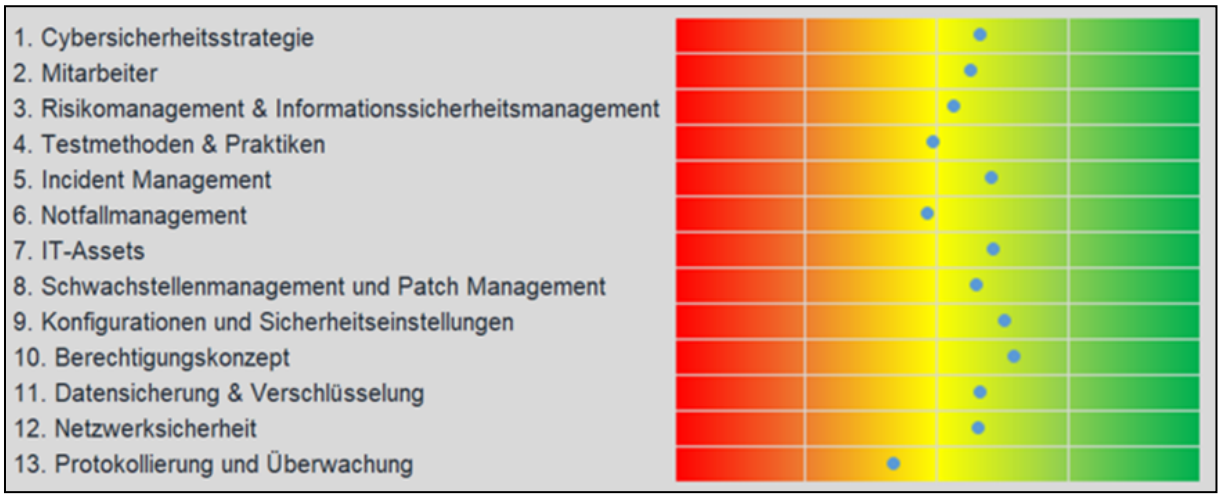


Während rund ein Viertel der VWG und VU im dunkelgrünen Bereich liegen, ist das im Unterschied dazu nur bei 1% der WPF und bei keinem VASP der Fall. In den roten und orangen Bandbreiten – mit Durchschnittsreifegraden kleiner gleich 2,6 – befinden sich aktuell vor allem VASP, WPF und auch VWG.

Die Korrelation zwischen den technischen und den organisatorischen Reifegraden beläuft sich auf durchschnittlich 0,8: Unternehmen mit einem höheren technischen Reifegrad haben tendenziell einen höheren organisatorischen Reifegrad. Unternehmen, die sich intensiv mit Cybersicherheitsthemen auseinandersetzen, scheinen dies ganzheitlich und nicht nur bezüglich der Setzung technischer Maßnahmen zu tun.

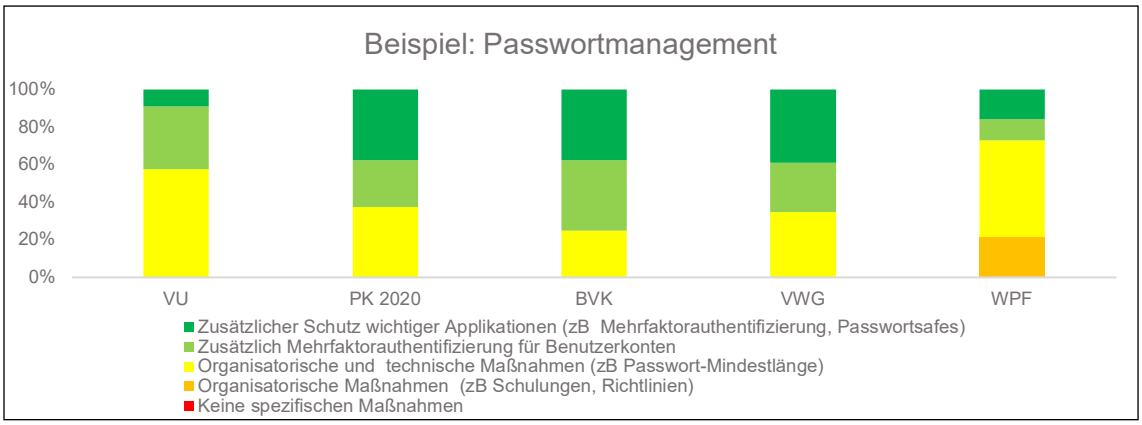
Bei einem Ranking der dreizehn Themenbereiche erreicht das „Berechtigungskonzept“ insgesamt den höchsten Reifegrad. Am schlechtesten schneidet „Protokollierung und Überwachung“ ab.

Die Gesamtdurchschnittsreifegrade pro Themenbereich:



Themenbereiche, deren Cyberreifegrad jeweils über dem Gesamtreifegraddurchschnitt liegt:

- Der Themenkomplex **Berechtigungskonzept** erreicht im Durchschnitt den höchsten Reifegrad. Insbesondere das Passwortmanagement zur Vermeidung schwacher Passwörter sowie Übersichten zu Benutzerberechtigungen und die Vergabe dieser nach dem Need-to-know-Prinzip werden weitgehend als Sicherheitsmaßnahmen eingesetzt.



- Hinter dem Berechtigungskonzept folgen die **Konfigurationen & Sicherheitseinstellungen** und **IT-Assets**. So sind etwa Virenscanner grundsätzlich installiert und deren Ergebnismeldungen werden meist zentral erfasst und nach einem vorgegebenen Prozess

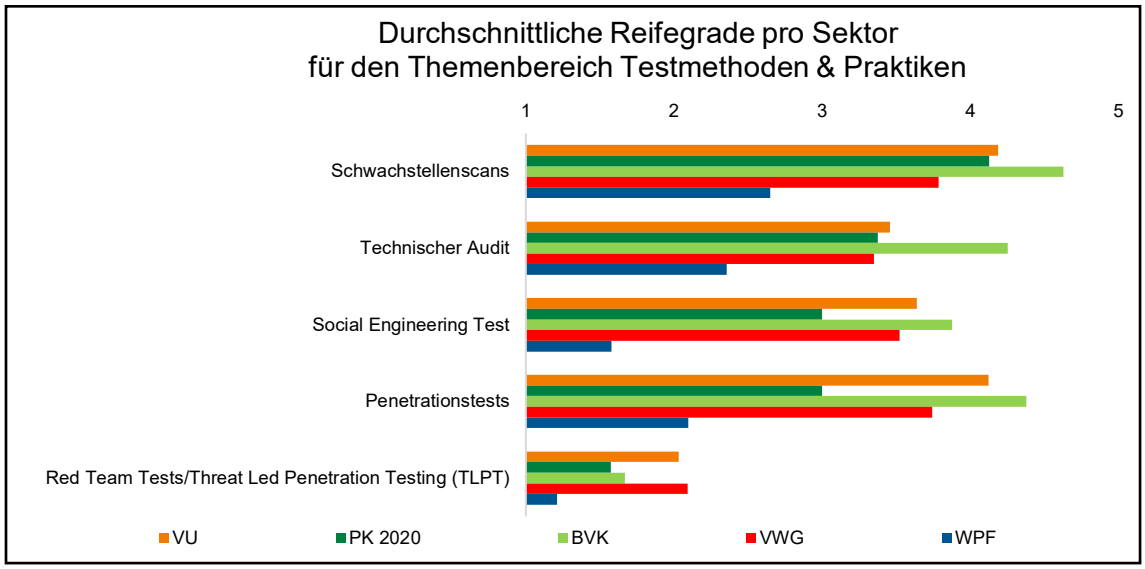
dokumentiert und behandelt. Auch Software-Whitelisting, durch welchen User nur vordefinierte Applikationen ausführen können, ist weit verbreitet.

- Bei der Kategorie **IT-Assets** stellen Inventare von Hardware- und Softwareassets eine wichtige Grundlage und Voraussetzung für Sicherheitsmaßnahmen, wie zB ein vollständiges Schwachstellenmanagement, dar. Diese Bestandsverzeichnisse werden teilweise teilautomatisiert geführt.
- **Incident Management** belegt im Ranking aller Themenbereiche Rang vier und erreicht gleichzeitig die höchste durchschnittliche organisatorische Cybermaturität. Prozesse, um IKT-bezogene Vorfälle zu managen, sind grundsätzlich definiert und auch Ursachenermittlungen und -beseitigungen sind jedenfalls für schwerwiegende Vorfälle implementiert.
- Bei der im Ranking folgenden Kategorie **Datensicherung & Verschlüsselung** sind Backups wichtiger Daten und Konfigurationen und deren vom Firmennetzwerk getrennte Aufbewahrung gängige Sicherheitsmaßnahmen.
- Bezüglich der **Cybersicherheitsstrategie** ist den Unternehmen insbesondere die Förderung des Bewusstseins hinsichtlich der Cybersicherheit wichtig. Dies erfolgt beispielsweise durch entsprechende Schulungen der Mitarbeiter.
- Es folgen die technischen Themenbereiche **Netzwerksicherheit** sowie **Schwachstellen- und Patch-Management**. Die systematische Absicherung des Zugriffs von außen auf das Firmennetzwerk sowie der Verbindungen aus dem Unternehmen in das Internet erzielt innerhalb des Themenbereichs Netzwerksicherheit den höchsten durchschnittlichen Reifegrad. Im Schwachstellenmanagement & Patch Management sind Verantwortliche für das Patch Management grundsätzlich definiert und Patches werden zumindest monatlich über eine Patch-Management-Software ausgerollt.
- **Mitarbeiter** ist der letzte Themenbereich, dessen Reifegraddurchschnitt für alle Sektoren knapp über dem durchschnittlichen Gesamtreifegrad für alle Kategorien in Höhe von 3,2 liegt. Hier schneidet die Definition von Rollen und Verantwortlichkeiten am besten ab. Auch Interessenskonflikte sind grundsätzlich evaluiert und ggf. adressiert bzw. mitigiert.

Ausbaufähige Bereiche:

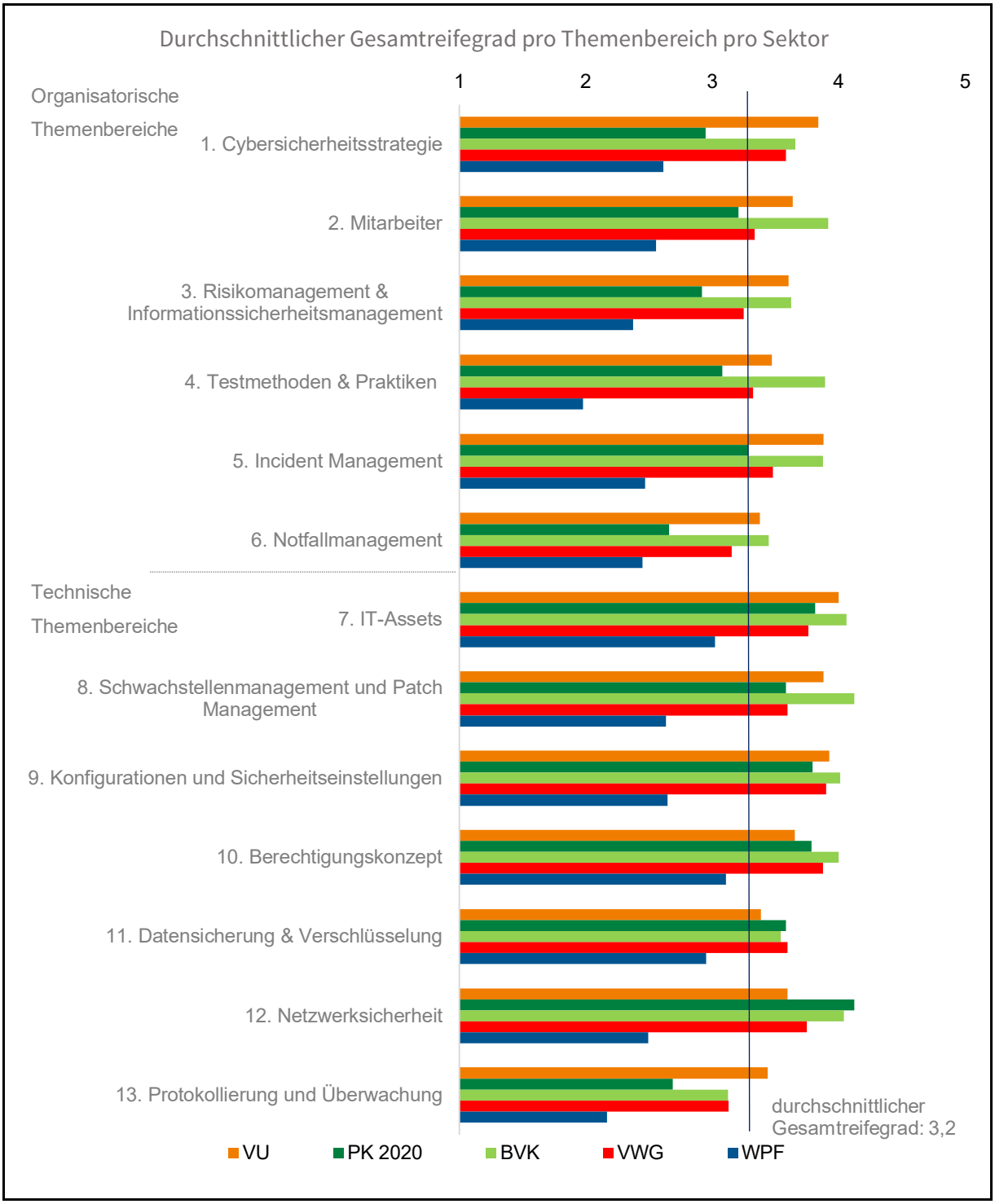
Aufholbedarf besteht insbesondere in den Themenkomplexen Risikomanagement und Informationssicherheitsmanagement, Testmethoden & Praktiken, Notfallmanagement sowie Protokollierung und Überwachung.

- Im Rahmen des **Risikomanagements und Informationssicherheitsmanagements** werden Agenden der Informationssicherheit im Durchschnitt jedenfalls von einer Organisationseinheit wahrgenommen, wobei die Einrichtung einer unabhängigen Funktion innerhalb des nächsten Jahres geplant ist. Insgesamt ist insbesondere der Informationsaustausch zum jeweiligen Cybersicherheitsrahmen mit Vertragspartnern verbesserungsfähig.
- Die Frage nach Red Team Tests / Threat Led Penetration Testing (TLPT), bei denen ein gezielter, kontrollierter Angriff auf die „Kronjuwelen" des Unternehmens mittels verschiedenster Methoden erfolgt, drückt den Reifegrad der Kategorie **Testmethoden und Praktiken** unter den Gesamtreifegraddurchschnitt. Allerdings erwartet die FMA die Durchführung solcher ressourcenintensiven Red Team Tests lediglich von signifikanten Unternehmen mit ausreichender Cybermaturität. Hinsichtlich der restlichen Testmethoden werden beispielsweise Schwachstellenscans in den Unternehmen grundsätzlich regelmäßig und anlassbezogen durchgeführt.



- Für **Notfallmanagement** errechnet sich die durchschnittlich niedrigste Cybermaturität aller organisatorischen Themenbereiche. Vor allem die Auswahl und die Umsetzung von Tests und komplexere Übungen zum Notfallmanagement sind ausbaufähig.
- Abweichend von den sonstigen überdurchschnittlich platzierten technischen Themenbereichen befindet sich die **Protokollierung und Überwachung** am unteren Ende des Cybermaturitätsspektrums. Sowohl die Sammlung als auch die Überwachung von Logdaten

zeigen insgesamt Optimierungsmöglichkeiten. Die Sammlung von Logdaten stellt eine wichtige Basis dar, um Auffälligkeiten bzw. Abweichungen vom üblichen Geschehen erkennen zu können. Eine strukturierte Sammlung relevanter Daten ist somit ein wichtiger Schritt für ein effektives Überwachungssystem.



11 FMA-CLOUD MATURITY LEVEL ASSESSMENT

Das FMA-Cloud Maturity Level Assessment ermöglicht einen sektorübergreifenden Vergleich der Cloudrisikoreifegrade.

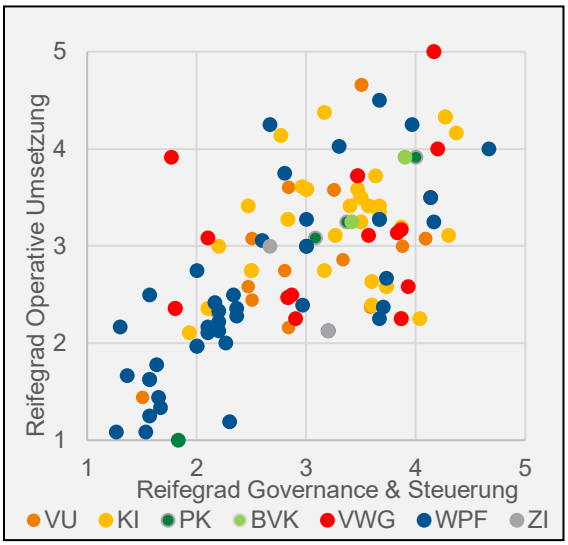
Entwicklung und Ziele des FMA-Cloud Maturity Level Assessments sind grundsätzlich analog zu jenen des Cyber Maturity Level Assessments.

Die Unternehmen am österreichischen Finanzmarkt konnten insgesamt einen durchschnittlichen Reifegrad von 3,1 erzielen. Die Vorkehrungen im Bereich Governance & Steuerung und Operative Umsetzung erzielen jeweils einen gleich hohen Reifegrad. Bei einem Ranking der Themenbereiche belegt Migration insgesamt den ersten Platz. Das größte Verbesserungspotential ergibt sich für die laufende Überwachung.

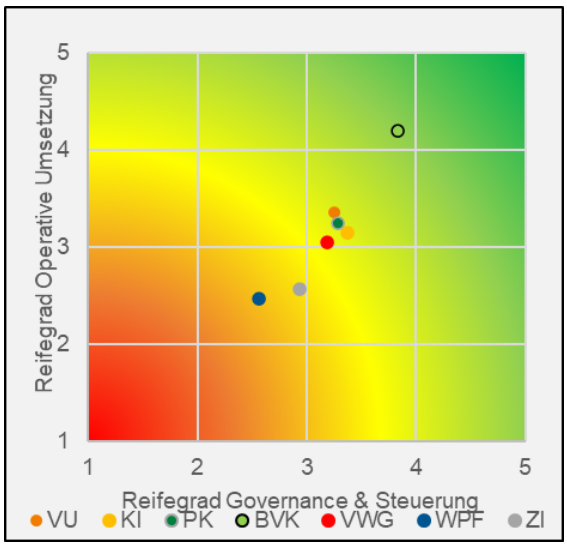
- Im FMA-Cloud Maturity Level Assessment 2021 erreichen BVK – wie auch beim FMA-Cyber Maturity Level Assessment – im Durchschnitt den höchsten Cloudmaturitätsgrad. Auf der fünfteiligen Reifegradskala, bei der ein höherer Reifegrad mit einer höheren Maturität einhergeht, beläuft sich der Reifegrad der BVK auf durchschnittlich 4,0. Dahinter liegen VU, MI, PK, KI und VWG. Mit etwas Abstand folgend dann ZI, VASP und WPF.
- In den VU wurde das Cloud Assessment erstmals 2019 durchgeführt. Damals ergab sich ein durchschnittlicher Cloudrisikoreifegrad in Höhe von 3,2, wobei der Reifegrad für die Themenbereiche Governance & Steuerung mit einem Durchschnittswert von 2,8 deutlich unter jenem für die Themen Operative Umsetzung in Höhe von 3,5 lag. 2021 hat sich der Gesamtreifegrad für diesen Sektor marginal auf 3,3 erhöht. Diese Entwicklung ist auf die Steigerung des Reifegrades für die Aggregation Governance & Steuerung auf einen Durchschnittswert von 3,3 zurückzuführen.
- Auch im PK-Sektor wurde bereits 2020 ein Cloud Maturity Assessment ausgerollt. Im Vergleich mit den diesjährigen Ergebnissen konnten die durchschnittlichen Reifegrade sowohl für die Themenbereiche Governance & Steuerung (+0,2 auf 3,3) als auch für jene, die der Aggregationsgröße Operative Umsetzung (+0,5 auf 3,3) zugeordnet sind, im Durchschnitt gesteigert werden. Insgesamt hat sich die Cloudreife der PK von 2020 auf 2021 von 2,9 auf 3,3 erhöht.

Übersicht	*VU*	*KI*	*PK*	*BVK*	*VWG*	*WPF*	*ZI*
Reifegrad gesamt	**3,3**	**3,2**	**3,3**	**4,0**	**3,1**	**2,5**	**2,7**
Reifegrad Governance & Steuerung	3,3	3,4	3,3	3,8	3,2	2,6	2,9
Reifegrad Operative Umsetzung	3,4	3,1	3,3	4,2	3,1	2,5	2,6

Durchschnittliche Reifegrade pro Unternehmen

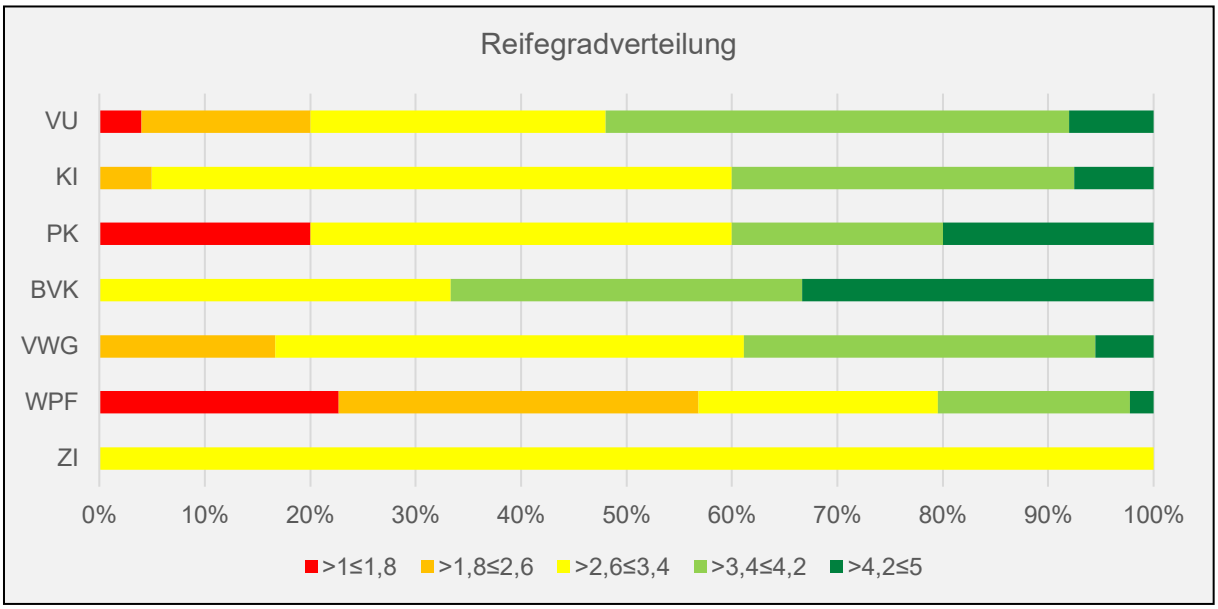


Durchschnittliche Reifegrade pro Sektor



Die Maßnahmen im Bereich Governance & Steuerung sowie Operative Umsetzung erzielen insgesamt jeweils einen gleich hohen Reifegrad in Höhe von 3,1.

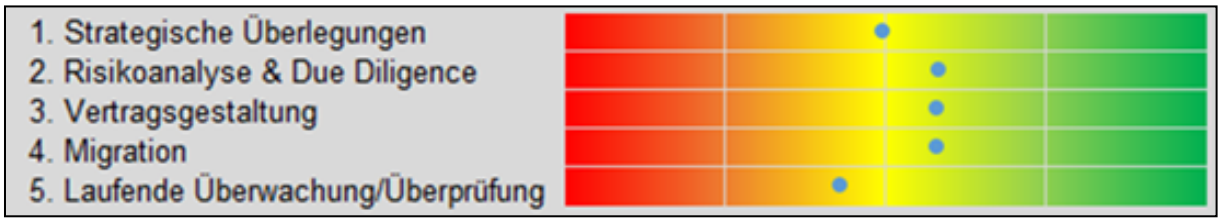
In allen Sektoren – außer bei VU und BVK – liegen die Reifegrade für Governance & Steuerung über jenen zur operativen Umsetzung. Dies liegt insbesondere am unterdurchschnittlichen Cloudrisikoreifegrad der laufenden Überwachung/Überprüfung, welche der operativen Umsetzung zugeordnet wird.



Die Graphik zu den Reifegradverteilungen veranschaulicht nach dem Ampelsystem, welcher Unternehmensanteil des spezifischen Sektors welchen Reifegrad erlangt: Dunkelgrün zeigt zB den Anteil der Unternehmen des jeweiligen Sektors, die einen hohen Reifegrad – von größer 4,2 und kleiner gleich 5 – erreicht. Die Farbskala reicht dabei, absteigend geordnet nach der erreichten Cloudmaturität, von dunkelgrün über hellgrün, gelb, orange und rot.

ZB befinden sich vor allem BVK, VU, KI, PK und VWG in den dunkel- und hellgrünen Bereichen. Rote Bandbreiten werden von WPF, PK, aber auch von VU belegt.

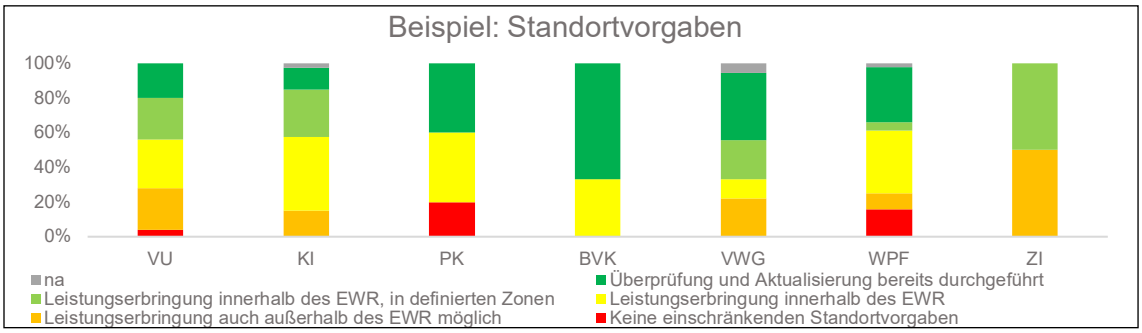
Die Gesamtdurchschnittsreifegrade pro Themenbereich:



Themenbereiche, deren Cyberreifegrad jeweils über dem Gesamtreifegraddurchschnitt liegt:

- **Migration** belegt im Durchschnitt den ersten Platz im Ranking der Themenbereiche. Dabei bezeichnet Migration den Umstieg auf die Nutzung von Cloud-Diensten bzw. den Wechsel auf einen anderen Cloud-Dienstleister. In dieser Phase können leicht Fehler entstehen, weshalb begleitende organisatorische und technische Maßnahmen von Bedeutung sind. Deren konkrete Ausgestaltung ergibt sich dabei in Abhängigkeit von den in Anspruch genommenen Cloud-Diensten bzw. von der Art der geplanten Datenmigration. Die Festlegung von Rollen und Verantwortlichkeiten für die Migration, die Planung von Test- und Übergabeverfahren und auch eine Migrationsabnahme bzw. die Beendigung der Migrationsphase sind grundsätzlich vorgesehen.

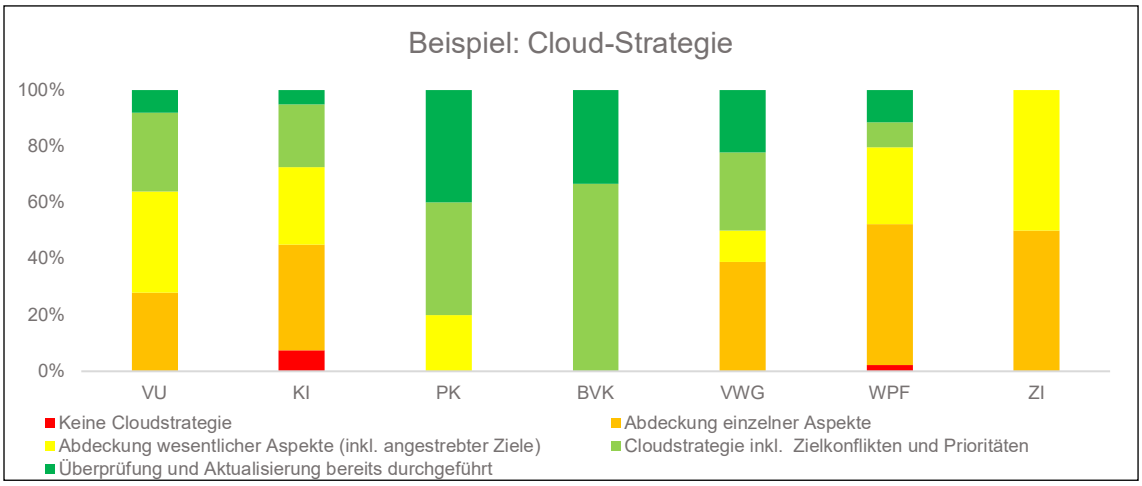
- Bei **Vertragsgestaltungen** mit Cloud-Dienstleistern kann auf vorformulierte Vertragsmuster zurückgegriffen werden. Insbesondere technische Verfügbarkeitsvorgaben sowie Berichts- und Informationspflichten sind in den Verträgen prinzipiell vorgegeben. Der Standort der Leistungserbringung ist meist auf den EWR-Raum eingeschränkt.



- Im Rahmen von **Risikoanalyse & Due Diligence** erfolgen beispielsweise Bewertungen, ob durch eine Cloud-Nutzung kritische oder wichtige operative Funktionen oder Tätigkeiten ausgelagert werden. Auch spezifische Maßnahmen zum Schutz der Vertraulichkeit der Daten sind evaluiert. Exitstrategien sind teils nicht nur pauschal, sondern auch auf Serviceebene evaluiert.

Ausbaufähige Bereiche:

- Bezüglich der Kategorie **Strategische Überlegungen** liegt meist eine Strategie zur Cloud-Nutzung, in der auch die angestrebten Ziele dokumentiert sind, vor.



- Die **laufende Überwachung/Überprüfung** der Cloud-Dienste weist insgesamt das höchste Potential zur Ergreifung von Stärkungsmaßnahmen auf. Derzeit werden insbesondere Abweichungen vom vereinbarten Service-Level untersucht und darauf basierend Folgemaßnahmen vereinbart. Die Unternehmen setzen teilweise auch Kennzahlenanalysen ein. Umfassende Prüfungen der Cloud-Dienstleister wurden bislang nur vereinzelt durchgeführt.

11.1 FAZIT UND HANDLUNGSFELDER DER FMA

Mit der zunehmenden Digitalisierung entstehen neue IT-Sicherheits- und Cyber-Risiken. Cyberattacken sind in den letzten Jahren sowohl hinsichtlich deren Häufigkeit als auch deren Komplexität kontinuierlich gestiegen. Alleine von 2019 auf 2020 hat sich die Anzahl der Cybervorfälle in den beaufsichtigten Unternehmen beinahe verdoppelt. Die Cyber-Resilienz des österreichischen Finanzmarkts wird somit zu einem fixen Parameter der risikobasierten Aufsicht der FMA:

- Die Entwicklung eines gemeinsamen Verständnisses zu IKT-Themen wurde durch die Veröffentlichung themenbezogener FMA-Leitfäden gefördert.
- Die Vorbereitung auf diesbezügliche EU-Vorgaben, wie zB auf die EIOPA-Leitlinien zu Sicherheit und Governance im Bereich der Informations- und Kommunikationstechnologie, die aktiv mitgestaltet worden sind, ist erfolgt.
- Die FMA wirkt außerdem auf sektorspezifische, proportionale Anforderungen im Zuge der Verhandlungen zum Vorschlag der Europäischen Kommission für eine Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors (DORA) hin.
- Die FMA unterstützt die beaufsichtigten Unternehmen bei deren Stärkung der Cyber- und Cloudmaturität, beispielsweise durch die Durchführung von FMA-Maturity Level Assessments.
- Diese Assessments fließen im Versicherungssektor in das Risikoscoring der Unternehmen ein und dienen auch als Basis zur Auswahl von Vor-Ort-Prüfungsaktivitäten.
- Die Weiterentwicklung der aufsichtlichen Instrumente findet laufend statt. Aktuell ist etwa für ausgewählte Versicherungsunternehmen eine Pilotübung zur Überprüfung der operationalen Cyber-Resilienz in Planung.

Insbesondere die anderen schwerwiegenden Betriebs- oder Sicherheitsvorfälle zeigen, dass beaufsichtigte Unternehmen meist indirekt durch einen Dienstleister betroffen sind:

- Die FMA aktualisiert die Verflechtungen am österreichischen Finanzmarkt. 2019 wurde dazu ein Projekt zur Darstellung dieser Vernetzungen gestartet.
- Eine Erweiterung und Aktualisierung dieser Analysen ist erfolgt und bezieht auch Sub-Auslagerungen in die Betrachtungen ein.

IKT-Sicherheit erfordert aufgrund laufender technologischer Weiterentwicklungen bzw. durch Umfeldveränderungen die Umsetzung kontinuierlicher Verbesserungsprozesse:

- Die FMA kommt dieser Anforderung unter anderem durch eine jährliche Weiterentwicklung des FMA-Cyber Maturity Level Assessments nach.
- Auch Risiken im Zusammenhang mit der Rückkehr an den Arbeitsplatz im Zuge der COVID-19-Pandemie werden evaluiert.

11.2 KONSULTATION ZU DEN CYBER-RISIKEN

- Mit welchen weiteren Maßnahmen bzw. Initiativen könnte die FMA zur Erhöhung der Cybersicherheit am Finanzmarkt konkret beitragen?
- Welche konkreten regulatorischen Vorgaben sind iZm der IT-Sicherheit am Finanzmarkt noch notwendig?
- Welche Cyber-Bedrohungsszenarien könnten in Zukunft besonders relevant für den österreichischen Finanzmarkt sein?
- Welche Kernbereiche der IT-Sicherheit sollten von Unternehmen des österreichischen Finanzmarktes prioritär verstärkt werden?
- Sollten von den Unternehmen weitere Maßnahmen zur künftigen Abwehr von Cyber-Attacken eingesetzt werden?
- Ist die Bedrohungslage zwischen den Branchen des Finanzmarktes aus Ihrer Sicht einheitlich zu sehen, oder sind bestimmte Sparten besonders exponiert?
- Welche konkreten Entwicklungen hinsichtlich der Cyber-Angriffe sind zu beobachten?
- Welche Rechtsunsicherheiten, Chancen und Risiken sehen Sie iZm den Cyberversicherungen?

12 ABKÜRZUNGSVERZEICHNIS

AI	Artificial Intelligence
AIFM	Alternative Investmentfonds Manager
API	Application Programming Interface
BVK	Betriebliche Vorsorgekassen
BWG	Bankwesengesetz
dh	das heißt
DLT	Distributed Ledger Technology
DOS	Denial of Service
DSGVO	Datenschutzgrundverordnung
EBA	European Banking Authority
EIOPA	European Insurance and Occupational Pensions Authority
ENISA	European Union Agency for Network and Information Security
ESMA	European Security Markets Authority
ETF	Exchange-Traded Fund
EK	Europäische Kommission
EU	Europäische Union
FSB	Financial Stability Board
FMABG	Finanzmarktbehördenaufsichtsgesetz
IAIS	International Association of Insurance Supervisors
IaaS	Infrastructure as a Service
IDD	Versicherungsvertriebsrichtlinie (EU) 2016/97
idZ	in diesem Zusammenhang
IoT	Internet of Things
iZm	in Zusammenhang mit
KfZ	Kraftfahrzeug
KI	Kreditinstitute / künstliche Intelligenz
KMU	kleine und mittelgroße Unternehmen
KYC	Know your Customer
MI	Marktinfrastrukturen
o.Ä.	oder Ähnliches
PaaS	Platform as a Service
PK	Pensionskassen

PKV	Private Krankenversicherung
P2P	Peer-to-Peer
PSD	Payment Service Directive
RPA	Robotic Process Automation
VU	Versicherungsunternehmen
SaaS	Software as a Service
SCR	Solvenkapitalforderung
SI	signifikante Institute
UK	Vereinigtes Königreich
uU	unter Umständen
VAG	Versicherungsaufsichtsgesetz 2016
VU	Versicherungsunternehmen
VWG	Verwaltungsgesellschaften (KAG, ImmoKAG, AIFM)
WPF	Wertpapierdienstleister und Wertpapierfirmen
ZaDiG	Zahlungsdienstegesetz
zB	zum Beispiel