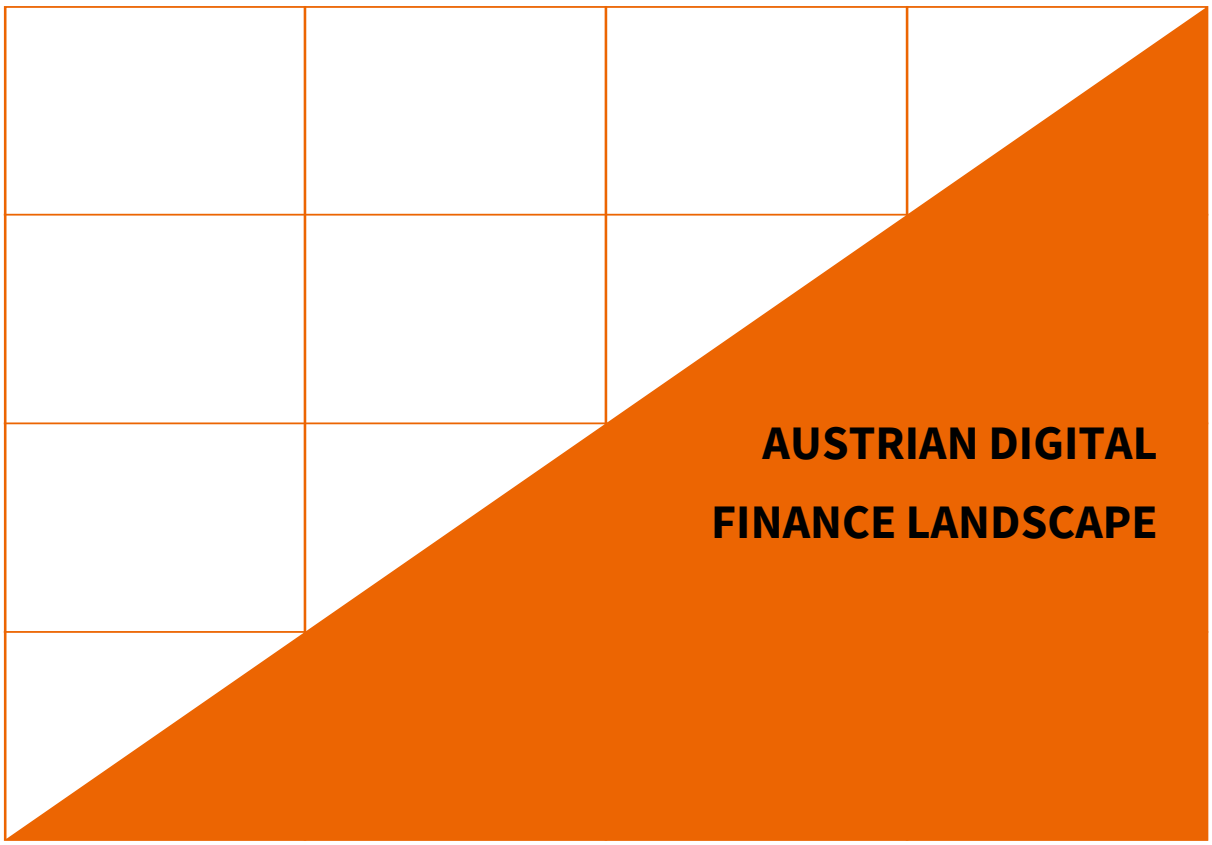
ÖSTERREICHISCHE
FMA · FINANZMARKTAUFSICHT



Jänner 2025

INHALTSVERZEICHNIS

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 2024 ihre Analyse zur Digitalisierung am österreichischen Finanzmarkt fortgeführt. Wir haben uns dabei das Ziel gesetzt, das digitale Risikoprofil der Unternehmen am österreichischen Finanzmarkt sowie die IKT-Vernetzungen zu ermitteln. Dieser Aufsichtsschwerpunkt folgte den bereits 2018 und 2021 durchgeführten Studien zur Digitalisierung am österreichischen Finanzmarkt und diente dazu, entlang der Geschäftsprozesskette zu erheben,

- welche digitalen Technologien in den einzelnen Prozessen und bei der Produktgestaltung eingesetzt werden,
- welche Rolle die digitalen Vertriebsplattformen und die Vergleichsportale auch vor dem Hintergrund der Entwicklungen im Bereich Open Finance einnehmen,
- welche Ökosysteme und IKT-Verflechtungen am österreichischen Finanzmarkt bestehen,
- ob die bestehende IT-Infrastruktur mit der zunehmenden Digitalisierung Schritt hält und
- inwieweit die Maßnahmen zur Prävention und Detektion von Cybervorfällen und Betriebsstörungen die DORA-Anforderungen an die digitale operationale Resilienz reflektieren.

Wir haben dazu im Sommer 2024 von den beaufsichtigten Unternehmen aus allen Sektoren des Marktes Rückmeldungen erhalten. Dabei konnten wir in fast allen Sektoren des Finanzmarkts eine beinahe vollständige Marktabdeckung erreichen:

Sektroteilnehmer	*Anzahl*	*Marktabdeckung*
Kreditinstitute (KI)	51 (explizit) / 384 (implizit)	92,4%
Zahlungsinstitute (ZI)	6	100%
E-Geld-Institut	1	100%
Versicherungsunternehmen (VU)	32	100%
Pensionskassen (PK)	8	100%
Betriebliche Vorsorgekassen (BVK)	8	100%
Wertpapierfirmen und Crowdfunding-Dienstleister (WPF)	63	98%
Verwaltungsgesellschaften (KAG, ImmoKAG, AIFM [KAG])	24	100%
Marktinfrastrukturen (MI)	3	100%
virtuelle Asset Provider (VASP)	1	Marktanteil nicht abschließend darstellbar[1]

Mit dieser enorm hohen Marktabdeckung haben wir auch 2024 die umfassendste Daten- und Informationsbasis geschaffen, die es derzeit zum Thema Digitalisierung am österreichischen Finanzmarkt gibt.

[1] Der Grund ist die unterschiedliche Gestaltung der Geschäftsmodelle und die hohe Technologisierung in diesem Sektor.

Die Ergebnisse dieses sektorübergreifenden Aufsichtsschwerpunkts haben wir im Rahmen von Querschnittsanalysen evaluiert und daraus eine **„Austrian Digital Finance Landscape“** abgeleitet. Diese Digitalisierungslandkarte soll der FMA ermöglichen, die digitalisierungsgetriebenen Entwicklungen und Abhängigkeiten am Finanzmarkt zu identifizieren, um

- diese in die Risikobeurteilung sowie in die Priorisierung der Aufsichtsagenden einfließen zu lassen,
- die Aufsichtsintensität der einzelnen Unternehmen risikoadäquat zu bestimmen und ggf.
- zielgerichtete präventive Maßnahmen zu ergreifen.

CALL FOR INPUT

Die Ergebnisse unserer Analyse sollen auch dafür genutzt werden, eine breitere Diskussion zu den vielschichtigen Aspekten der Digitalisierung anzustoßen und den Dialog zum digitalen Wandel am österreichischen Finanzmarkt zu intensivieren.

Wir laden Sie – beaufsichtigte Unternehmen, Investor:innen, Sparer:innen, Versicherungsnehmer:innen, öffentliche Institutionen und die interessierte Öffentlichkeit – deshalb ein, die in diesem Bericht skizzierten Erkenntnisse und Schlussfolgerungen kritisch zu hinterfragen und um Ihre Sichtweisen, Erfahrungen und Lösungsansätze anzureichern. Um die Diskussion möglichst effizient zu strukturieren, haben wir dazu am Ende dieses Berichtes als Orientierungshilfe einige Fragen an Sie formuliert.

Bis **31. März 2025** können Sie formlos Ihren Input zum Bericht an digitalisierung@fma.gv.at übermitteln. Ihre Feedbacks können von der FMA publiziert werden. Falls eine Veröffentlichung (in der Originalfassung oder anonymisiert in einem aggregierten Bericht zum Call for Input) nicht gewünscht ist, bitte dies ausdrücklich anzugeben. Wir werden Ihren Input gerne aufnehmen und bei der strategischen Planung der FMA bzw. bei der Festlegung der Aufsichtsschwerpunkte berücksichtigen.

Hinweise:

Die rechtlichen Grundlagen bleiben durch diesen Bericht unberührt. Über die gesetzlichen Bestimmungen hinausgehende Rechte und Pflichten können aus diesem Dokument nicht abgeleitet werden.

Im vorliegenden Bericht wird aufgrund der leichteren Lesbarkeit überwiegend die männliche Form verwendet. Diese Bezeichnungen sind als geschlechtsneutral zu betrachten.

Trotz sorgfältiger Aufbereitung und Recherche übernimmt die FMA keine Haftung für die Richtigkeit und Vollständigkeit der Daten und Inhalte in diesem Bericht.

EXECUTIVE SUMMARY

Folgende wesentliche Trends und Entwicklungen am österreichischen Finanzmarkt konnte die FMA im Rahmen ihrer Analyse zur Austrian Digital Finance Landscape identifizieren:

Strategien / Governance 	▪ **Geschäftsoptimierung und Effizienzgewinne** durch Automatisierung bestehender Prozesse und Verbesserung der Kundenbindung sind Haupttreiber der Digitalisierung am österreichischen Finanzmarkt. ▪ Die **Bedeutung innovativer Technologien** steigt rasant. Dennoch wird selbst der zunehmende Einsatz von künstlicher Intelligenz bloß als Innovationstreiber, **nicht** aber als Grund für eine **Disruption am Finanzmarkt** betrachtet. ▪ Um die Vorteile der digitalen Innovation schneller nutzen zu können, gehen die beaufsichtigten Unternehmen weiterhin **Kooperationen mit FinTech-Startups** ein, die nicht mehr als Konkurrenz wahrgenommen werden. So steigt nicht nur die Anzahl der Kooperationen mit FinTech/InsurTechs; auch der Anteil der beaufsichtigten Unternehmen, die mit derartigen Start-ups kooperieren, ist – trotz der Konsolidierung und Marktbereinigung am FinTech-Markt in den letzten 3 Jahren – erneut gestiegen. ▪ Der **Bedarf nach qualifiziertem Personal mit IT-Skills** bleibt nach wie vor sehr hoch. Dass die beaufsichtigten Unternehmen weiterhin ihre **IKT-Sicherheit**-Skills ausbauen wollen, ist teils auf den neuen regulatorischen Rahmen (DORA) zurückzuführen. Es zeigt aber auch die Awareness für die zunehmende Bedrohung durch Cyberattacken auf. In fast allen Sektoren wird überdies ein erhöhter Bedarf an Fachkräften im Bereich **Data Science** gesehen, was auf die intensivere Nutzung von Systemen künstlicher Intelligenz (KI-Systemen) hindeutet. ▪ Trotz der andauernden Dynamik im **Krypto-Bereich**, des steigenden Kostendrucks und der Suche nach renditebringenden Investments bleiben die beaufsichtigten Unternehmen bei Veranlagungen in Krypto-Assets sehr zurückhaltend.
Technologien 	▪ **Cloudservices** haben seit 2018 stark an Bedeutung gewonnen und werden nun praktisch universell von den Unternehmen aller Finanzmarktsektoren eingesetzt. Das Servicemodell „Software as a Service“ (84%) und das Nutzungsmodell Public-Cloud (80% aller genutzten Cloud-Services) werden hier in der Regel in Anspruch genommen. ▪ **Robotic Process Automation** wird primär für die Abarbeitung repetitiver Formulare, zB bei der Anlage und Übertragung von Datensätzen in den eigentlichen Analysesystemen, eingesetzt. ▪ **Blockchain-Technologie** wird immer noch kaum genutzt. Entgegen manchen Ausbauplänen im Jahr 2021 ist die Nutzung mangels konkreter Anwendungsfälle sogar noch zurückgegangen. ▪ **Edge Computing & Internet of Things** bleiben eine Nische, die aktuell lediglich von drei KI, drei VU und einer PK genutzt wird; bis 2027 möchten zusätzlich lediglich ein ZI, ein weiteres KI und ein weiteres VU Edge Computing & IoT nutzen. ▪ **Big Data Analytics** werden am häufigsten im Risikomanagement sowie in den Bereichen Produktentwicklung, Reporting und Fraudanalytics eingesetzt.

- **Automatisierte Datenschnittstellen** sind ein sehr vielseitiges Werkzeug und werden in der Zwischenzeit praktisch von allen KI, ZI und VU genutzt. Von vielen Unternehmen werden sie gleichzeitig in mehreren Bereichen eingesetzt. Die starke Nutzung verdeutlicht den steigenden Wert von Daten durch die zunehmende Digitalisierung.
- **AI-basierte Systeme** stellen starke Wachstumsgebiete dar. Die 2021 kommunizierten Ausbaupläne wurden über alle Sektoren hinweg erfüllt. Mehr als ein Viertel der beaufsichtigten Unternehmen setzt in ihrem operativen Geschäftsbetrieb bereits **Machine Learning** ein. Die Haupteinsatzbereiche sind Rating-Systeme, Fraudanalytics, Unterstützung in den Bereichen IT, Verwaltung und Marketing. Auffallend hoch sind die Ausbaupläne in allen Sektoren: Bis 2027 wollen etwa ¾ der KI, ZI, VU aber auch KAG Machine Learning-Techniken einsetzen. **Natural Language Processing** hat im Vergleich zu 2021 bereits eine deutliche Verbreitung im österreichischen Finanzsektor gefunden. Bei den KI, ZI, VU und BVK beträgt der Nutzungsgrad über 20%. Hierbei werden vor allem Chatbots genutzt und als Instrument für die Kommunikation mit Kund:innen eingesetzt. In den kommenden drei Jahren streben KI, ZI und VU gar einen Nutzungsgrad von weit über 50% an.
- Je mehr digitale Technologien ein Unternehmen insgesamt einsetzt, desto häufiger macht es sich auch die künstliche Intelligenz zu Nutze.

Vertrieb

- Die digitale Kundenbetreuung macht personalisierte Interaktionen, schnellere Reaktionszeiten und proaktive Problemlösung möglich. Im Wettbewerb um Vertragsabschlüsse ist es überdies ein Vorteil, Kund:innen über möglichst viele Kanäle ansprechen zu können. Den Einsatz von **Kundenportalen** (personalisierten Websites) sowie **mobilen Apps**, die in der Zwischenzeit zum Standardrepertoire der meisten Unternehmen gehören, werden in den nächsten drei Jahren insb. WPF noch stärker ausbauen, die im Hinblick auf die Besonderheiten ihres Geschäftsmodells Online-Portale und mobile Applikationen bisher weniger oft nutzen.
- **Marketing-Automatisierung**, bei der Nutzerprofile mit verhaltensbasierten Daten angereichert werden, um automatisierte Kampagnen für individuelle Kommunikation einzurichten (zB personalisierte Angebote im Kundenportal, personalisierte Landingpages basierend auf Kundenverhalten, gezielte Werbung basierend auf Kundendaten in den sozialen Medien, Retargeting, Kampagnen in Suchmaschinen), setzen bereits ⅔ der KI und ⅓ der VU ein. Die Nutzung von Marketing-Automation-Software wird bis 2027 insb. im KI-Sektor noch weiter steigen.
- In einigen Sektoren, insb. bei KI und VU, wird stark auf **automatisierte Beratung** gesetzt, wobei insgesamt ein steigender Trend zu beobachten ist.
- Konventionelle Wege des Vertriebs verlieren durch den Einsatz von Robo-Advice, Vergleichsportalen und digitalen Vertriebsplattformen zunehmend an Bedeutung.
- **Vergleichsportale** haben stark an Bedeutung gewonnen und setzten sich seit 2018 praktisch in allen Sektoren als Pre-Sales-Instrument durch. Der prozentuelle Anteil des Absatzes über Vergleichsportale und Vertriebsplattformen liegt zwar bei den meisten Unternehmen nach wie vor im einstelligen Prozentbereich oder darunter. In den nächsten Jahren ist hier allerdings mit einem weiteren Wachstum zu rechnen. Mit steigender Nutzung von Vergleichsportalen steigt implizit auch der Bedarf an Fairness und Transparenz dieser Anbieter.

Cyber-Resilienz

- Der österreichische Finanzmarkt hat im Aggregat die wesentlichsten Vorkehrungen zur **Sicherstellung der DORA-Compliance** getroffen, wenngleich es im Sommer 2024 bei der Erfüllung der organisatorischen und technischen Vorgaben individuell noch deutliche Unterschiede gab.
- Bei der **Umsetzung technischer Sicherheitsmaßnahmen** sind, auch auf Basis von in der Vergangenheit bereits getätigter Investitionen, bei den meisten österreichischen Finanzunternehmen die wichtigsten Schritte schon erfolgt oder in der Finalisierung.
- Das Ranking der Themenbereiche zeigt, dass der größte Handlungsbedarf beim IKT-Drittpartei-Risikomanagement und beim IKT-Vorfallsmanagement besteht.
- Insb. die Operationalisierung der Vorgaben zum IKT-Drittparteienrisiko und das Aufsetzen des **Informationsregisters der IKT-Dienstleister**, das alle vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen umfasst, ist praktisch in allen Sektoren noch im Gange und stellt eine der größten Herausforderungen von DORA dar. Insofern konnten die österreichischen Finanzunternehmen durch ihre Teilnahme an der **Generalprobe der Meldung des Informationsregisters** (Dry Run) die Implementierung forcieren und die Datenqualität steigern. Oft wird risikobasiert vorgegangen, um zuerst kritische Dienstleistungen in vollem Umfang abbilden zu können. Viele Unternehmen planen, das Informationsregister aus dem bestehenden Vertragsmanagement-System zu generieren.
- Bei der Umsetzung der Vorgaben betreffend Governance & Organisation ist teils noch eine **Funktion zur Überwachung der Verträge mit IKT-Drittdienstleister** einzurichten oder ein Mitglied der Geschäftsleitung ist mit dieser Funktion noch zu betrauen. Unternehmen evaluieren beispielsweise, ob das Konzept des Outsourcing-Managements und die zugehörige Definition der Risikoverantwortlichen für alle IKT-Verträge umgesetzt werden kann.
- Die **Inventarisierung von IKT-Assets** ist eine notwendige Basis für die meisten IKT-Sicherheitsmaßnahmen. Die meisten beaufsichtigten Unternehmen verfügen bereits über umfassende Hardware- und Softwareinventare. Unter DORA sind allerdings nicht nur diese grundlegenden Inventare zu führen. Als zusätzliche Informationen zu den Assets sind hier auch Konfigurationen, Abhängigkeiten, Kritikalitäten und Zertifikate zu erfassen. Diese zusätzlich zu erfassenden Informationen sind oft noch nicht oder in unterschiedlichsten Systemen (zB Lizenzmanagement) vorhanden und teilweise noch zu ergänzen. Nicht alle Unternehmen verfügen dabei über ein Inventarisierungstool, in welchem all diese Informationen abbildbar und über automatisierte Schnittstellen aktualisierbar sind.
- KI und VU weisen die vielfältigsten **Testprogramme** auf, die neben Penetrationstests etwa Lückenanalysen, Schwachstellen- und Netzwerksicherheitsbewertungen sowie Überprüfungen der physischen Sicherheit umfassen und nun in allen Sektoren risikobasiert zu konzipieren sind.
- IZm der **Behandlung von IKT-bezogenen Vorfällen** und Cyberbedrohungen verfügen die beaufsichtigten Unternehmen bereits über ausgeprägte Erfahrungen hinsichtlich der Erkennung anomaler Aktivitäten, zB aus Logs oder aus potentiellen internen und externen Cyberbedrohungen. Demgegenüber sind die Vorgaben zu verpflichtenden Meldungen schwerwiegender IKT-bezogener Vorfälle für viele Finanzunternehmen vollkommen neu und erfordern eine Vorbereitung auf die Klassifizierung und ggf. Übermittlung der Meldung an die FMA. Teilweise ist auch die Verfügbarkeit der Meldeinhalte noch sicherzustellen.

Cyber-Bedrohungen

- Wie auch in den Vorjahren entfallen rund **¾ der IKT-bezogenen Vorfälle** am österreichischen Finanzmarkt, die gemäß DORA als schwerwiegend einzustufen sind und in diesem Rahmen der FMA gemeldet wurden, auf den **KI-Sektor**. Dies ergibt sich u.a. dadurch, dass für KI bereits vor DORA entsprechende Meldeverpflichtungen galten. Danach folgen VU, auf die etwa ein Fünftel der Meldungen entfällt. Aus den restlichen Sektoren liegen nur vereinzelte Meldungen vor.
- Beinahe **⅔ der schwerwiegenden IKT-Vorfälle** gehen **von Drittdienstleistern** aus. Das veranschaulicht die Sinnhaftigkeit der neuen DORA-Vorgaben zum IKT-Drittparteien-Risikomanagement und zum europäischen Überwachungsrahmen für kritische IKT-Drittdienstleister.
- Mehr als ¾ der schwerwiegenden IKT-Vorfälle sind auf **Systemfehler** (d.h. nicht aus Angriffen resultierende Probleme wie zB Softwarefehler oder ausgefallene Netzwerkinfrastruktur) zurückzuführen. Cybersicherheitsbezogene Meldungen beliefen sich nur auf einen niedrigen einstelligen Prozentbereich. Hier kommen vor allem Denial-of-Service-Angriffe sowie Datenexfiltration und Manipulation durch externe Angreifer vor. Die restlichen IKT-Vorfälle sind auf Prozessfehler oder externe Ereignisse zurückzuführen.

IKT-Vernetzungen

- Der Grad der Vernetzung des Finanzsektors mit Dienstleistern steigt durch die Digitalisierung. Das **IKT-Risiko beaufsichtigter Unternehmen verlagert sich** somit zunehmend an die **Schnittstelle zu Dritten** (Kooperationspartner, IKT-Dienstleister).
- Die **Generalprobe der Meldung des Informationsregisters** (Dry Run) zeigte trotz der noch unvollständigen Daten bereits wichtige Trends und Strukturen der Vernetzung österreichischer Finanzunternehmen mit dem IKT-Dienstleistungssektor auf:
- Die FMA konnte 7952 Dienstleistungsverträge von Finanzunternehmen mit 1626 unterschiedlichen Dienstleistern aus 1312 individuellen Konzernen identifizieren. Diesen liegen 4390 Subdienstleisterbeziehungen bis hin zur 5. Stufe zugrunde.
- Die **Zahl kritischer IKT-Dienstleister** pro Unternehmen liegt in der Regel in einem zweistelligen Bereich (so sind es zB bei KI im Durchschnitt 17, bei VU 12 und bei KAG 10 kritische IKT-Dienstleister). Bei der **Ersetzbarkeit kritischer IKT-Dienstleistungen** werden sektorale Unterschiede sichtbar: Insb. bei KI, ZI und VU wäre ein Großteil der IKT-Dienstleistungen nur schwer zu ersetzen.
- Inhaltlich fällt in den Daten die **steigende Bedeutung von Clouddiensten** sowie die hohe Anzahl von Dienstleistern auf, welche sowohl kritisch als auch schwer ersetzbar sind. Dies stimmt mit den Ergebnissen der FMA-Studie kritischer IKT-Dienstleister im Jahr 2021 überein und zeigt, dass die Inklusion des Drittdienstleisterrisikos in DORA tatsächlich ein wichtiger und nötiger Schritt ist.
- Gleichzeitig steigt aber auch die Qualität der eigenen IKT-Sicherheitsmaßnahmen der beaufsichtigten Unternehmen. Dies zeigt zuletzt auch die DORA-Gap-Analyse, die im Anschluss an die von der FMA entwickelten Cyber und Cloud Maturity Level Assessments erstmalig einen Einblick in die Cyber-Resilienz des österreichischen Finanzmarktes erlaubt. Im Hinblick auf die sich laufend weiterentwickelnden Cyberbedrohungen und die steigenden digitalen Kundenansprüche erfordert die IKT-Sicherheit laufende Anpassungen der Sicherheitsmaßnahmen.

Die Analyse der FMA zur Austrian Digital Finance Landscape und der Vergleich mit den Ergebnissen der Digitalisierungsstudien 2021 und 2018 bestätigen eine technologiegetriebene Transformation des österreichischen Finanzmarktes. Die FMA hat bereits verschiedene Schritte gesetzt, um diese Entwicklungen zu begleiten und in ihren Aufsichtsansatz zu integrieren. Die identifizierten Trends lassen erkennen, dass künftig insb. folgende strategische Bereiche von der FMA zu adressieren sind:

- **Digitale Transformation am Finanzmarkt aktiv begleiten; die Spielregeln klar kommunizieren:** Die Struktur der Wertschöpfungskette wandelt sich, (Teil-)Leistungen werden zunehmend von Dienstleister bzw. Kooperationspartner erbracht. Durch diese vernetzten Abhängigkeiten können für Unternehmen diverse Risiken, wie etwa Konzentrationsrisiken und Unterbrechungen der digitalen Wertschöpfungskette, entstehen. Die Einbindung von Start-Ups sowie neue Geschäftsmodelle und Plattformen können außerdem Implikationen für Vertriebspraktiken und den gesamten konzessionierten Geschäftsbetrieb mit sich bringen.
- **Neue Verflechtungen, Ansteckungskanäle und Konzentrationsrisiken in die laufende Aufsicht sowie die Risikoklassifizierung einfließen lassen:** Die Geschäftsmodelle beaufsichtigter Unternehmen ändern sich. 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 Dienstleister sowie die zuliefernden Strukturen und die Konzentrationsrisiken sind dementsprechend auch in Zukunft in zunehmendem Maße von der Aufsicht zu berücksichtigen.
- **Auf adäquate Transparenz und Klarheit bei Produktinnovationen hinwirken:** Die Digitalisierung bringt nicht nur innovative, sondern teilweise auch komplexere Produkte mit sich. Um dem gesteigerten Informationsbedürfnis von Kund:innen zu begegnen und sie auf Informationspflichten für sensible Themenbereiche aufmerksam zu machen, ist es für die FMA wichtig, ihre Verbraucherinformationen weiter zu forcieren und die Kundeninteressen unabhängig davon zu sichern, ob die Kommunikation im Vertrieb traditionell oder digital aufgesetzt ist.
- **Die Kontaktstelle FinTech und die Sandbox laufend den Marktentwicklungen und der Regulierung anpassen:** Mit FinTechs drängen weiterhin neue innovative Anbieter auf den österreichischen Finanzmarkt; FinTech-Geschäftsmodelle können freilich auch etablierte, beaufsichtigte Unternehmen betreiben. Die genaue Abgrenzung des Umfangs konzessionspflichtiger Geschäfte ist häufig nicht leicht zu treffen, daher hat die FMA für aufsichtsrechtlich relevante Fragen die Kontaktstelle FinTech sowie eine Sandbox etabliert, die laufend den Anforderungen des Marktes und der Regulierung anzupassen sind.
- **Rechtspolitischen 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 schlechte Risiken nicht mehr versichert werden können – und damit ein partielles Marktversagen droht (Auswirkungen auf die finanzielle Inklusion und Exklusion).
- **Aufsichtsrechtliche Implikationen von bislang wenig verwendeten digitalen Technologien (Robo Advice, Vergleichsportale, soziale Medien, Chatbot, sonstige KI-Ansätze etc.) beurteilen:** Zu adressieren sind etwa Rechtsunsicherheiten hinsichtlich der möglichen Einflussnahme auf die Reihung in einem Vergleichsportal (zB im Hinblick auf potentielle Interessenkonflikte), der Beurteilung, welche Technologien die Anforderungen an einen dauerhaften Datenträger erfüllen, sowie hinsichtlich der Beurteilung, welche Anforderungen an die Beratungsalgorithmen und die menschliche Aufsicht bei der Nutzung von KI-Systemen zu beachten sind.
- **Das Monitoring der Veranlagung in Krypto-Assets durch institutionelle Investoren und Asset Manager fortsetzen:** Trotz der bisherigen Zurückhaltung der beaufsichtigten Unternehmen bei Veranlagungen im Krypto-Bereich müssen in das Monitoring weiterhin auch die indirekt gehalten Positionen einbezogen werden.

Bei einer etwaigen indirekten Veranlagung in neue Anlageformen über Investmentfonds ist zu hinterfragen, welche Investment-Prozesse und Risikomanagementanforderungen hierfür angewendet werden. Da in den Bewertungen von Wachstumsunternehmen oft die hohen Wachstumsraten eingepreist werden, sind bei Investments in FinTech-Start-Ups wiederum die gewählten Bewertungsansätze vor dem Hintergrund des Prudent Person Prinzips zu evaluieren. IZm der Veranlagung in Blockchain-Emissionen sollte Klarheit darüber herbeigeführt werden, inwiefern diese die Belegenheitsanforderungen erfüllen.

- **Die Informationen zu Verflechtungen mit IKT-Dienstleistern und Subdienstleitern am österreichischen Finanzmarkt in der Aufsichtstätigkeit gezielt berücksichtigen:** Kommt es etwa zu schwerwiegenden Vorfällen bei IKT-Unternehmen, die kritische Geschäftsprozesse der beaufsichtigten Unternehmen unterstützen, kann die FMA künftig auf Basis der Daten zu Informationsregistern noch präziser die potentiell betroffenen Unternehmen und Dienstleistungskategorien ermitteln. Aufgrund der exponentiell mit jedem Schritt der Delegationskette 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 Cyber-Resilienz des österreichischen Finanzmarkts als fixen Parameter der risikobasierten Aufsicht der FMA forcieren:** Mit der zunehmenden Digitalisierung entstehen neue und verstärken sich bestehende IT-Sicherheits- und Cyber-Risiken. Cyberattacken sind in den letzten Jahren sowohl hinsichtlich deren Häufigkeit als auch deren Komplexität kontinuierlich gestiegen. Mit den Instrumenten aus ihrem Cyber-Toolkit unterstützt die FMA die beaufsichtigten Unternehmen seit 2019 bei der Stärkung von deren Cyber- und Cloudmaturität. Die EU-Verordnung über die Betriebsstabilität digitaler Systeme des Finanzsektors (DORA) bringt nun einen umfassenden regulatorischen Rahmen, der noch für mehr Standardisierung und Sicherheit sorgt. Die Widerstandsfähigkeit der beaufsichtigten Unternehmen muss entsprechend strukturiert in deren Risikoscoring einfließen.
- **Mit technologischen Entwicklungen und Umfeldveränderungen bei der Entwicklung moderner Aufsichtsinstrumente Schritt halten**: 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 2018 noch 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.

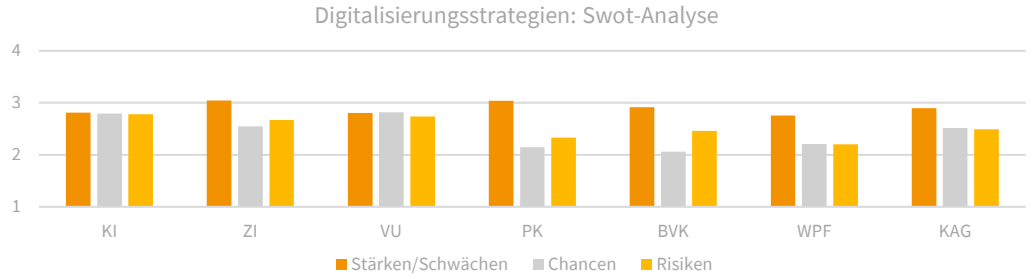
Die Ergebnisse der vorliegenden Analyse zur Austrian Digital Finance Landscape verdeutlichen die Sinnhaftigkeit der bisher von der FMA gesetzten Maßnahmen. Konkrete weitere strategische und operative Schritte werden unter Berücksichtigung des Feedbacks der teilnehmenden Unternehmen sowie anderer Stakeholder im Rahmen des Call for Input gesetzt.

1 STRATEGIEN

Die Unternehmen am österreichischen Finanzmarkt stufen die Digitalisierung als sehr relevantes Thema ein und sind bereit, Maßnahmen zu setzen, um diese Entwicklung für sich zu nutzen.

Die Möglichkeit, dass es infolge der zunehmenden Digitalisierung zu disruptiven Veränderungen kommt, wird nach wie vor als kaum denkbar eingestuft. Auch der zunehmende Einsatz von künstlicher Intelligenz wird als Innovationstreiber, nicht jedoch als Grund für eine Disruption am Finanzmarkt betrachtet. Dementsprechend richten sich beaufsichtigte Unternehmen derzeit in erster Linie auf eine Geschäftsoptimierung und weniger auf eine diesbezügliche Transformation ein.

- Die Erzielung von **Effizienzgewinnen und Synergieeffekten** steht im Vordergrund, während Überlegungen zu neuen Ideen, die auch zu einer Disruption von Geschäftsmodellen führen könnten, in den Hintergrund treten.

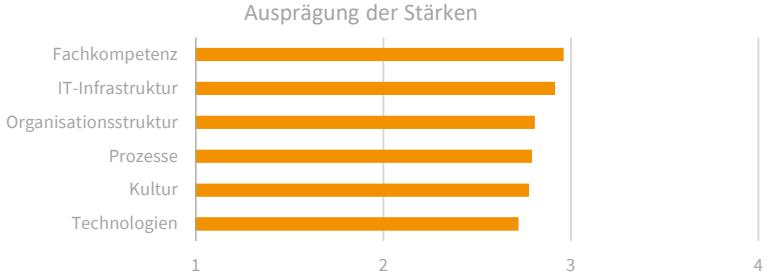


Notiz: Durchschnittswerte pro Sektor mit 1 für die geringste und 4 für die größte Ausprägung von Stärken / Chancen / Risiken

- Die beaufsichtigten Unternehmen betonen in allen Sektoren primär deren **Stärken** (in den Bereichen Kultur [zB stark ausgeprägte Innovationskultur und deren laufende Förderung], Technologien [zB umfassender Einsatz neuer Technologien], Organisationsstruktur [bereits an die digitalen Prozesse angepasste Aufbauorganisation], IT-Infrastruktur [zB kein Handlungsbedarf in Bezug auf Legacy-Systeme], Prozesse, Fachkompetenz im Bereich Digitalisierung & Cybersicherheit) und geben keine spezifischen Schwächen preis.
- Insgesamt halten auch **Chancen und Risken** die Waage, wobei die Einschätzungen zwischen den Sektoren unterschiedlich ausgeprägt sind: Die größten Chancen der Digitalisierung (dazu unter Pkt. 1.2) sehen KI und VU; sie bewerten aber auch die Risiken (dazu unter Pkt. 1.3) am höchsten.

1.1 STÄRKEN UND SCHWÄCHEN

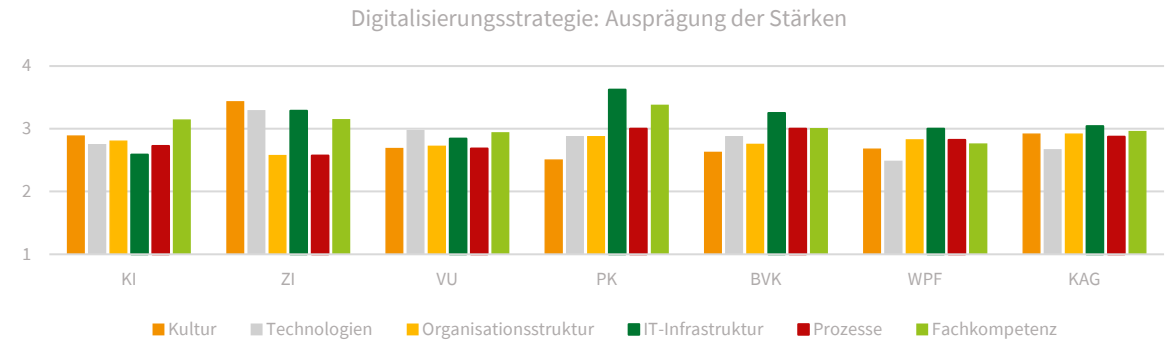
Bei der Analyse ihrer Digitalisierungsstrategie identifizieren die beaufsichtigten Unternehmen deren Stärken vor allem in der Fachkompetenz und der IT-Infrastruktur.



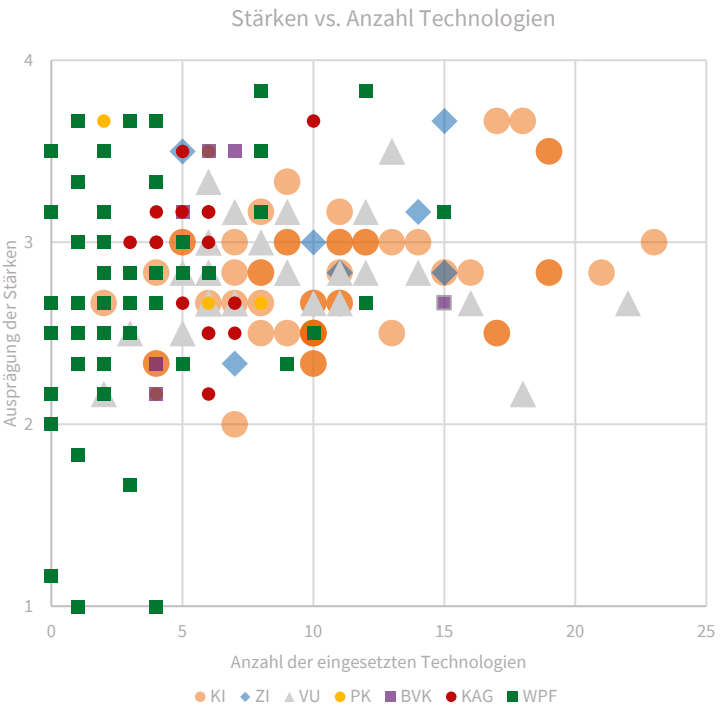
Notiz: Durchschnittswerte pro Sektor mit 1 für die geringste und 4 für die größte Ausprägung von Stärken

Die Ergebnisse divergieren allerdings nach Sektor:

- Die **eigene Innovationskultur** stufen fast alle Sektoren als ihre Stärke ein. Besonders stark ausgeprägt ist dies bei ZI. PK schwanken dagegen bei der Frage, ob sie ihre Innovationskultur als Stärke oder als Schwäche einschätzen sollen. Dieses ambivalente Bild ist wohl den Besonderheiten ihres Geschäftsmodells geschuldet.
- Bis auf die WPF wird der umfassende **Einsatz neuer Technologien** von allen Sektoren eher als Stärke eingestuft. Erneut stufen sich ZI an dieser Stelle besonders stark ein.
- Die **eigene Organisationsstruktur** wird in allen Sektoren tendenziell als Stärke gesehen; ein Ausreißer sind hier lediglich die ZI, die hier den durchschnittlich geringsten Score erreichen.
- Als größte Stärke wird in den meisten Sektoren die eigene **IT-Infrastruktur** wahrgenommen. Lediglich KI und VU schwanken, ob ihre IT-Infrastruktur ihre Stärke oder eher ihre Schwäche darstellt.
- **Optimierte Prozesse** sind bei ZI nicht als eindeutige Stärke ausgeprägt, während der Rest des Marktes diesen Aspekt als seine Stärke einstuft.
- Die **eigene Fachkompetenz** im Bereich Digitalisierung & Cybersicherheit sehen alle Sektoren als Stärke.
- Eindeutige Schwächen sehen die Unternehmen bei keiner der möglichen Kategorien.

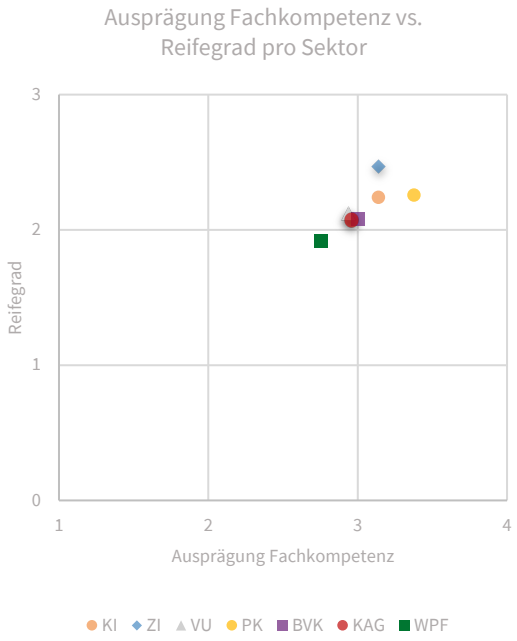


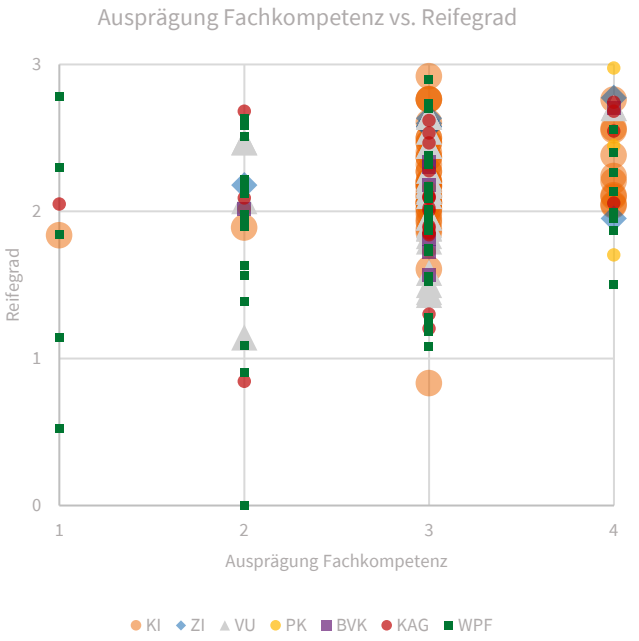
Notiz: Durchschnittswerte pro Sektor mit 1: schwach, 2: eher schwach, 3: stark, 4: besonders stark



Ein Blick auf die Stärken / Schwächen in Kombination mit der Anzahl der verwendeten Technologien zeigt, dass die Ausprägung der Stärken im Bereich der Digitalisierung nicht mit der Anzahl der eingesetzten digitalen Technologien korreliert.

Zu erkennen ist allerdings, dass WPF und KAG, die keine ausgeprägten Stärken im Bereich Technologien und Fachkompetenz aufweisen, im Vergleich zu den anderen Sektoren auch nur wenige Technologien einsetzen.





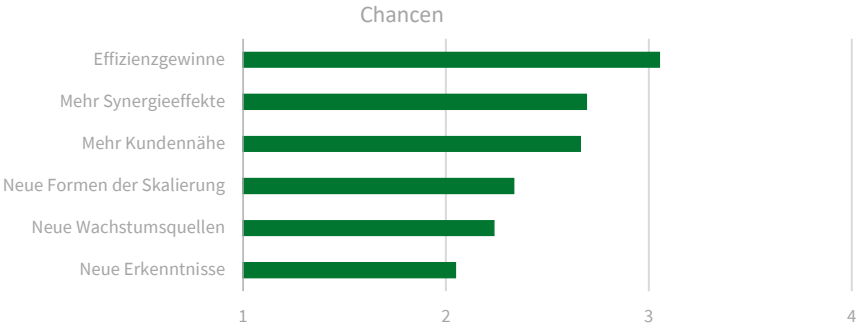
Ein Blick auf die Ausprägung der Fachkompetenz in Kombination mit dem Reifegrad im Rahmen der DORA-Gap-Analyse zeigt, dass

- je höher die eigene Fachkompetenz im Bereich der Digitalisierung ist,
- desto professioneller ist das Unternehmen auch im Bereich der IKT-Sicherheit aufgestellt.

Somit ist ein positiver Zusammenhang zwischen dem Reifegrad und der unternehmensindividuellen Stärke im Bereich Fachkompetenz gegeben.

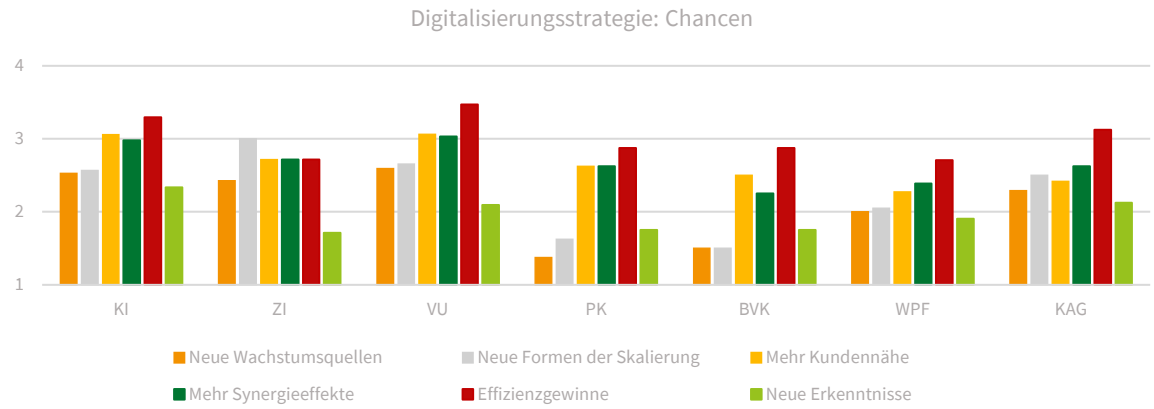
1.2 CHANCEN DER DIGITALISIERUNG

Die beaufsichtigten Unternehmen sehen bei der Digitalisierung primär die Chance, Synergieeffekte zu generieren und Effizienzgewinne zu erzielen. Neue Erkenntnisse (zB infolge der Nutzung von Daten aus Sensoren, sozialen Medien) stellen demgegenüber insgesamt einen schwachen Anreiz dar. Somit kann davon ausgegangen werden, dass Unternehmen derzeit in erster Linie auf eine Geschäftsoptimierung und weniger auf eine diesbezügliche Transformation abzielen.

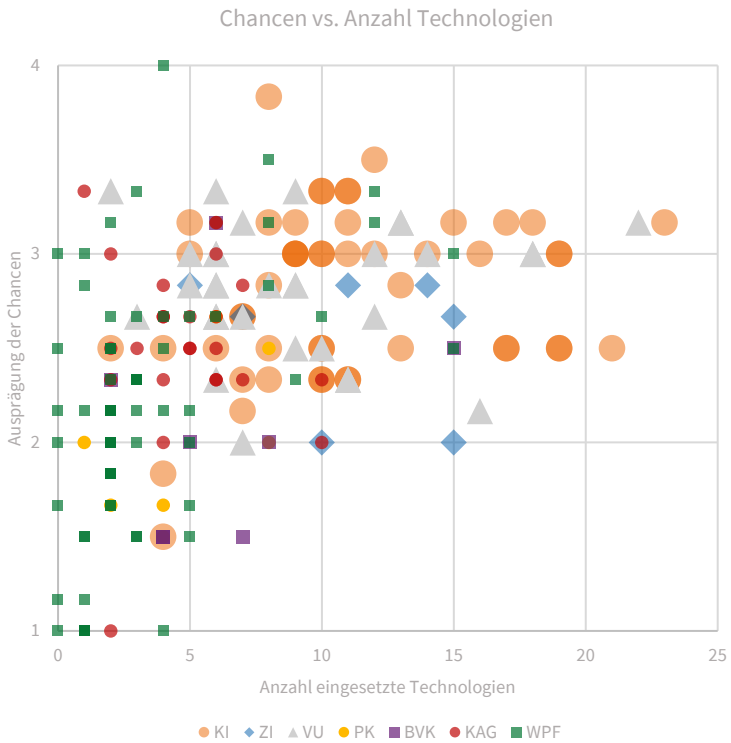


Notiz: Durchschnittswerte pro Sektor mit 1 für die geringste und 4 für die größte Ausprägung von Chancen

- **Effizienzgewinne** und größere **Nähe zur Kundschaft** werden von KI, VU, PK, BVK und VASP als größte Chancen der Digitalisierung eingestuft.
- **Neue Erkenntnisse** und **neue Wachstumsquellen** (zB neue Geschäftsfelder) werden im Durchschnitt eher eingeschränkt als Chancen wahrgenommen. Bei letzterem Aspekt zeigen sich zwischen den Sektoren jedoch unterschiedliche Wahrnehmungen: Insb. VU und KI sehen bei neuen Wachstumsquellen eher Chancen.
- Lediglich ZI sehen **neue Formen der Skalierung** wie einen schnelleren Go-to-Market als die größte Chance.



Notiz: Durchschnittswerte pro Sektor mit 1 für die geringste und 4 für die größte Chance

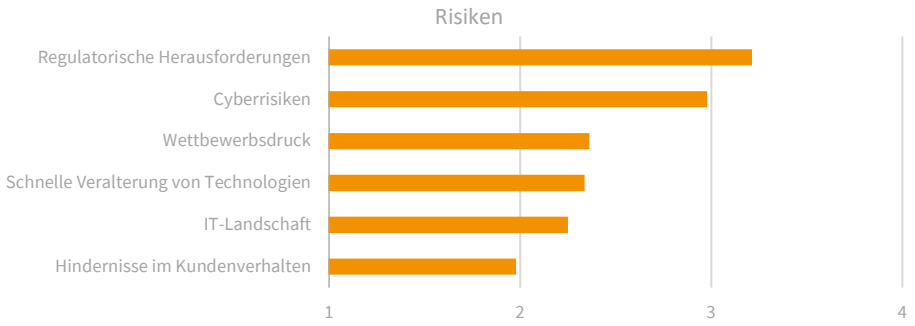


Stellt man die Wahrnehmung der Chancen der Digitalisierung der Anzahl verwendeter Technologien gegenüber, ist bei KI und ZI ein leichter Zusammenhang zwischen der Ausprägung der Chancen und der Anzahl der Technologien zu erkennen: Je mehr Chancen die Unternehmen im Einsatz der Digitalisierung sehen, desto mehr digitale Technologien setzen sie ein.

Auffällig ist erneut bei WPF, dass sie tendentiell weniger Chancen in der Digitalisierung erblicken und gleichzeitig auch eine kleinere Anzahl digitaler Technologien einsetzen. Auf Basis dieser Daten sehen WPF tendenziell geringere Chancen in der Digitalisierung.

1.3 RISIKEN DER DIGITALISIERUNG

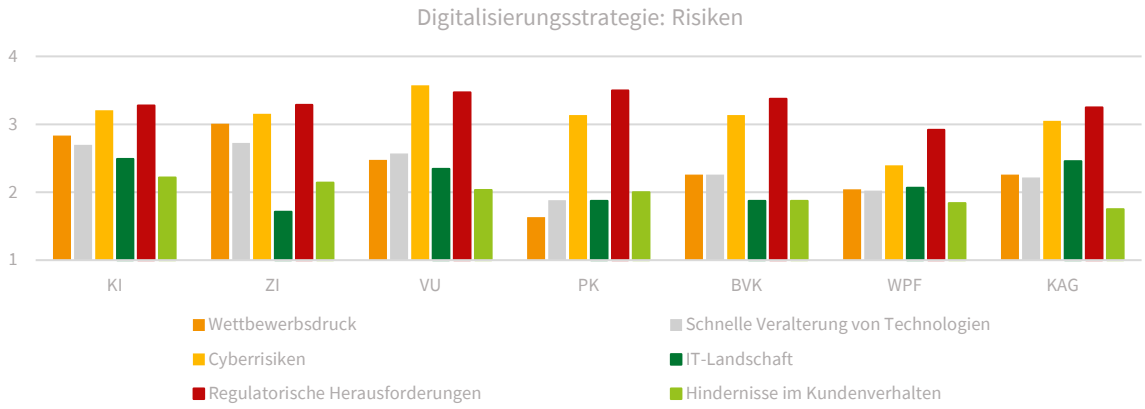
Die Unternehmen am österreichischen Finanzmarkt sehen im Rahmen der Digitalisierung große Herausforderungen auf ihre Organisationen zukommen. Diese werden allgemein am stärksten in den Bereichen Regulatorik und Cyberrisiken gesehen.



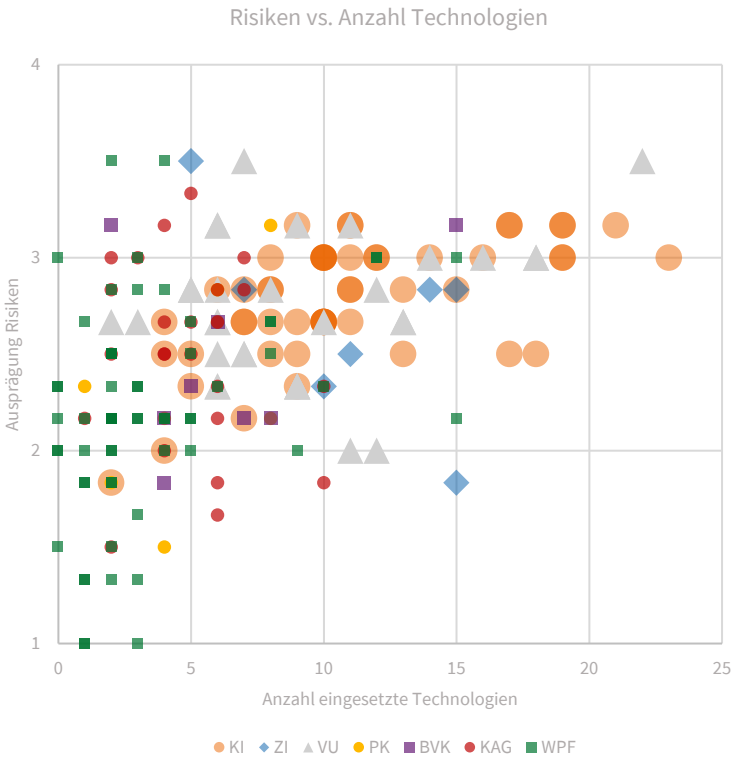
Notiz: Durchschnittswerte pro Sektor mit 1 für die geringste und 4 für die größte Ausprägung von Risiken

- **Größte Risiken:** Cyberrisiken und regulatorische Herausforderungen werden in allen Sektoren als die größten Risiken eingestuft.
- **Geringste Risiken:** Bei den geringsten Risiken ist das Bild heterogener:
    - KI, ZI, VU und BVK stufen die eigene IT-Landschaft und Hindernisse im Kundenverhalten als die geringsten Risiken ein, während bei den PK Wettbewerbsdruck, IT-Landschaft und Veralterung der Technologien die kleinsten Risiken darstellen.
    - WPF und KAG betrachten Hindernisse im Kundenverhalten und Veralterung der Technologien als geringste Risiken.

Insgesamt bewerten **KI**, aber auch **ZI** und **VU** Risiken (Wettbewerbsdruck [zB neue und schnellere Marktteilnehmer], schnelle Veralterung von Technologien, Cyberrisiken, IT-Landschaft [zB fragmentierte und veraltete IT-Landschaft], regulatorische Herausforderungen, Hindernisse im Kundenverhalten) durchschnittlich am stärksten, während VASP und WPF Risken meist eher schwach einschätzen.



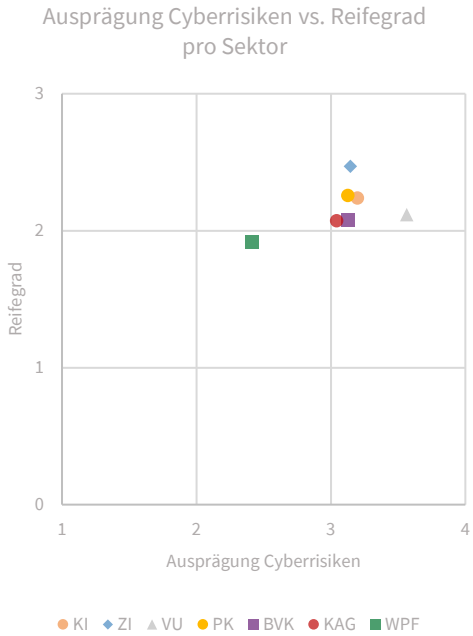
Notiz: Durchschnittswerte pro Sektor mit 1 für das geringste und 4 für das größte Risiko

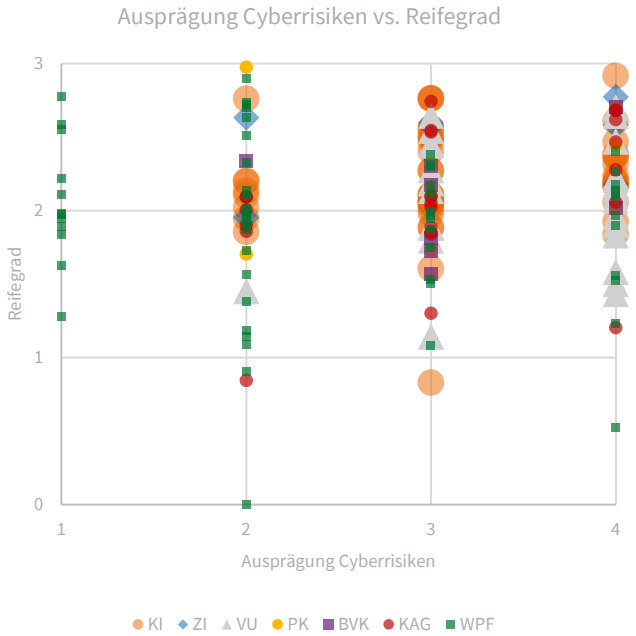


Ein Blick auf die Wahrnehmung der Risiken verglichen mit der Anzahl der eingesetzten Technologien legt nahe, dass Unternehmen umso risikobewusster sind, je mehr digitale Technologien sie in ihrem Geschäftsbetrieb nutzen.

Dieser Zusammenhang ist insb. bei den KI ersichtlich.

Auch in dieser Darstellung sind bei den WPF die geringsten Risikowahrnehmungen bei einer eher geringen Anzahl verwendeter Technologien festzustellen.





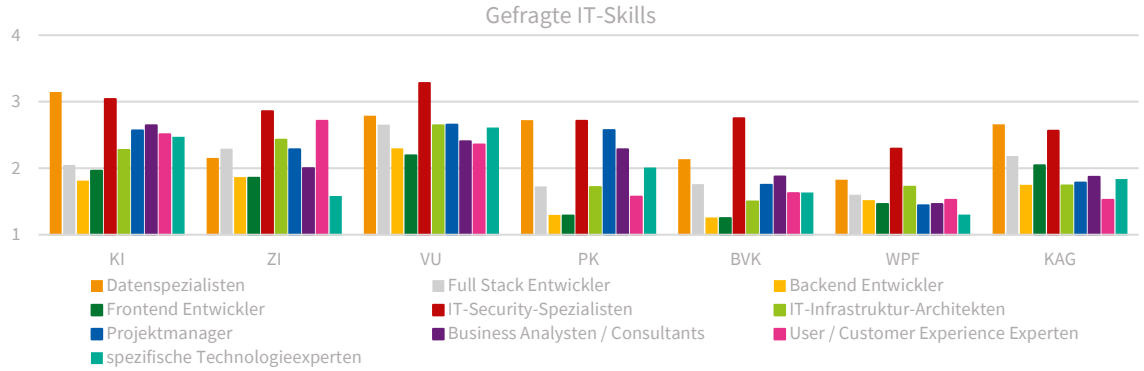
Je risikobewusster die Einschätzung der Unternehmen bei den Cyberrisiken ist, desto professioneller ist man im Bereich der IKT-Sicherheit aufgestellt. Es ist also ein positiver Zusammenhang zwischen dem Reifegrad und dem unternehmensindividuellen Risikobewusstsein im Bereich Cyberrisiken gegeben.

1.4 GEFRAGTES KNOW-HOW

Durch die voranschreitende Digitalisierung können neue Chancen und Möglichkeiten entstehen, welche gerade vor dem Hintergrund des steigenden Konkurrenzdrucks spezialisierte IT-Kompetenzen erfordern. Während 2021 neben IT-Security- Spezialist:innen (welche 2018 nur begrenzt im Fokus standen) Projektmanager:innen und Analyst:innen gesucht wurden, welche ein entsprechendes technisches Verständnis haben, um digitale Unterfangen zu leiten und zu unterstützen, herrscht nun Bedarf an Fachkräften verschiedener Disziplinen.

Mit gewissen sektorspezifischen Unterschieden lassen sich folgende Trends erkennen:

- In fast allen Sektoren wird ein erhöhter Bedarf an Fachkräften für **IT-Sicherheit und Datenmanagement** gesehen. Dass die beaufsichtigten Unternehmen ihre IT-Security Skills weiter ausbauen wollen, zeigt eine stark gestiegene Awareness für die zunehmende Bedrohung durch Cyberattacken auf. Die Kehrseite dürfte jedoch auch ein gewisser Mangel an ausreichend qualifizierten Kräften am Arbeitsmarkt sein, der 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. Bei ZI sind zudem insb. Fachkräfte im **Bereich User / Customer Experience** gefragt.
- Tendenziell wird **Management- bzw. Analystenstellen mit Technikaffinität** aktuell eine höhere Relevanz zugeschrieben als dem Tätigkeitsbereich der reinen Softwareentwicklung.
- Im Hinblick auf IT-Entwicklung geht hervor, dass einer Erweiterung von Generalist:innen (**Full-Stack-Entwickler:innen**) im Vergleich zum Ausbau von Know-How im Bereich Frontend- bzw. Backend-Entwickler:innen größere Bedeutung beigemessen wird, in dem die Unternehmen im Moment den geringsten Ausbaubedarf sehen.



Notiz: Durchschnittswerte pro Sektor mit 1 für den geringsten und 4 für den größten Bedarf

Im Vergleich zu 2021 zeigt sich, dass die beaufsichtigten Unternehmen bzgl. ihrer IT-Kompetenzen einen weniger starken Ausbaubedarf sehen. Lediglich bzgl. einzelner IT-Skills ist der Ausbaubedarf im Vergleich zu 2021 gestiegen. Hier lässt sich jedoch kein klarer Trend bzgl. der gefragten IT-Kompetenzen ableiten. Folgende Know-How-Kategorien weisen im Vergleich mit 2021 erhöhten Ausbaubedarf auf:

- Datenspezialist:innen werden seitens der BVK mit einem höheren Bedarf eingestuft.
- Entwickler:innen werden von ZI, PK und KAG stärker nachgefragt.
- User Experience Expert:innen werden von ZI verstärkt benötigt.
- Bei Fachkräften mit spezialisierten Technologie Know-How ist der Bedarf bei ZI, VU, PK und BVK größer geworden.

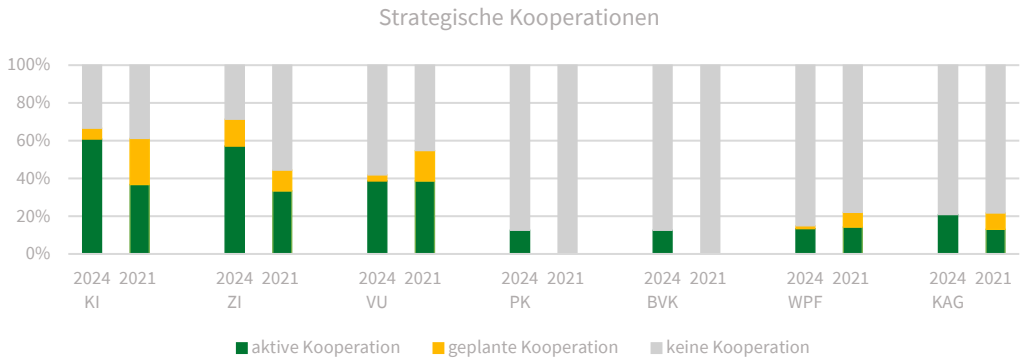
2 STRATEGISCHE KOOPERATIONEN

Trotz der Marktbereinigung und Konsolidierung am FinTech-Markt in den letzten drei Jahren setzt sich der Trend, mit FinTech-StartUps Kooperationen einzugehen, weiter fort. Es steigt nicht nur die Anzahl der Kooperationen mit FinTechs/InsurTechs. Auch der Anteil der beaufsichtigten Unternehmen, die mit FinTechs / InsurTechs kooperieren, ist seit 2021 von 22,9% auf 32,3% gestiegen. Vor allem KI, ZI (jeweils ca. 60%) und VU (40%) gehen Partnerschaften mit FinTechs/InsurTechs ein.

2.1 KOOPERATIONEN MIT FINTECHS / INSURTECHS

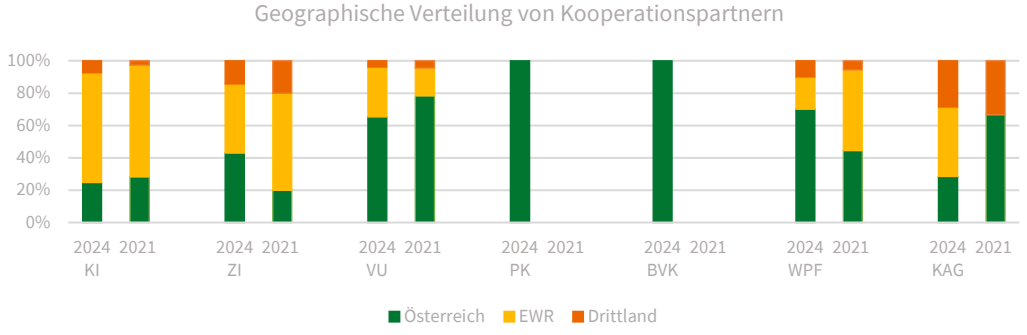
Ungeachtet der Sorge einiger beaufsichtigter Unternehmen, dass FinTechs/InsurTechs künftig zur Konkurrenz werden könnten, geht der österreichische Finanzmarkt davon aus, dass die Zahl der Kooperationen voraussichtlich **auch in den nächsten drei Jahren steigen** wird. Bis 2027 wollen jeweils etwa 2/3 der KI und ZI zumindest mit einem FinTech/InsurTech kooperieren.

- Ein Vergleich zu 2021 zeigt, dass KI, ZI und KAG ihren Ausbauplänen ganz oder teilweise nachgekommen sind,
- während VU und WPF entgegen ihren Ausbauplänen die Kooperation reduziert haben.
- Jeweils eine PK und eine BVK sind erstmalig strategischen Kooperationen mit FinTechs eingegangen, obwohl dies aus ihren Ausbauplänen 2021 nicht hervorging.



Hinsichtlich der geographischen Verteilung kooperieren die beaufsichtigten Unternehmen zum größten Teil mit Partnern aus **Österreich** oder dem **EWR**. Es bestehen dabei allerdings folgende sektorspezifische Unterschiede:

- Während VU, PK, BVK und WPF in erster Linie mit österreichischen Unternehmen kooperieren,
- arbeiten KI nach wie vor überwiegend mit ausländischen StartUps, zumeist aus anderen EWR-Ländern, zusammen.

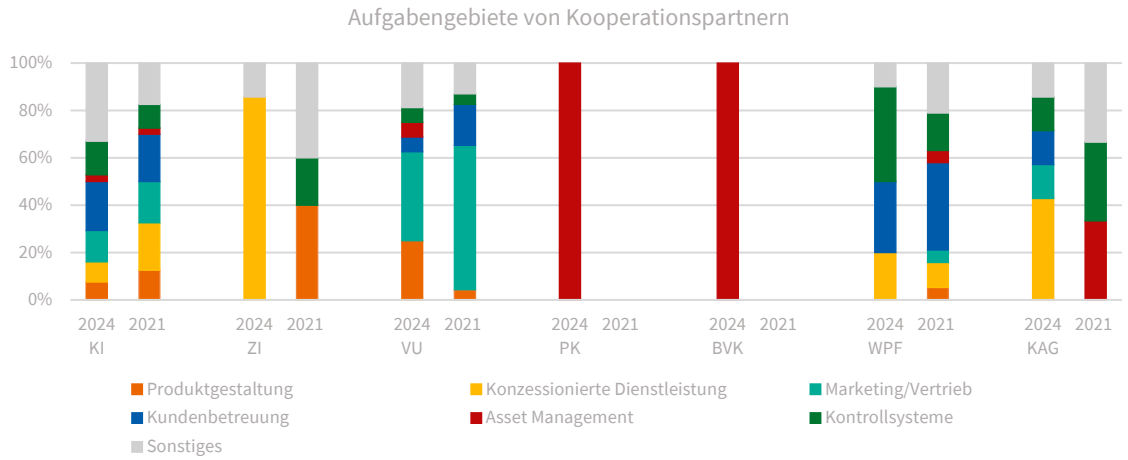


Ein Vergleich zu 2021 zeigt, dass

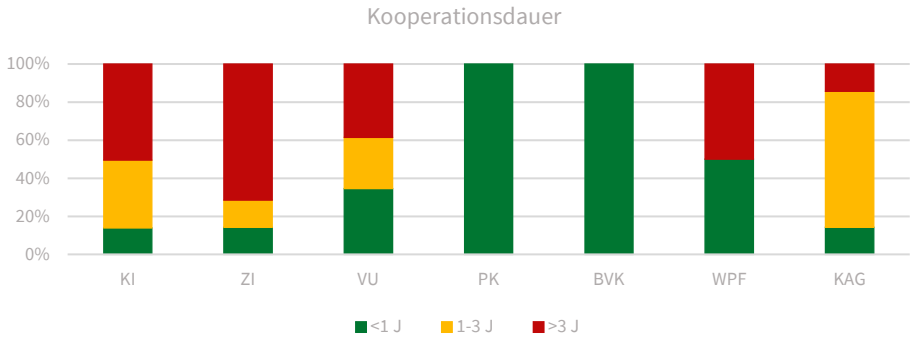
- ZI und WPF den Anteil der Kooperation mit österreichischen Unternehmen erhöht haben.
- die erstmalige Kooperation bei PK und BVK gänzlich mit österreichischen Unternehmen erfolgte.
- bei KI, VU und KAG der Anteil österreichischer Unternehmen leicht zurück ging.

Hinsichtlich der **Aufgabengebiete** der Kooperationen mit StartUps zeigt sich, dass während bei ZI konzessionierte Dienstleistungen und bei PK sowie BVK das Asset Management im Fokus stehen, ist in anderen Sektoren eine größere Vielfalt an Kooperationsfeldern zu beobachten. Dabei kristallisieren sich

- bei VU ein Überhang zu Marketing/Vertrieb,
- bei WPF zu Kontrollsystemen und
- bei KAG zu konzessionierten Dienstleistungen.



Hinsichtlich der **Kooperationsdauer** weisen bis auf PK und BVK alle Sektoren eine Kooperationsdauer von **in der Regel mehr als einem Jahr** auf, wobei die Hälfte der mit einem FinTech kooperierenden WPF erst seit weniger als einem Jahr mit einem StartUp zusammenarbeiten.



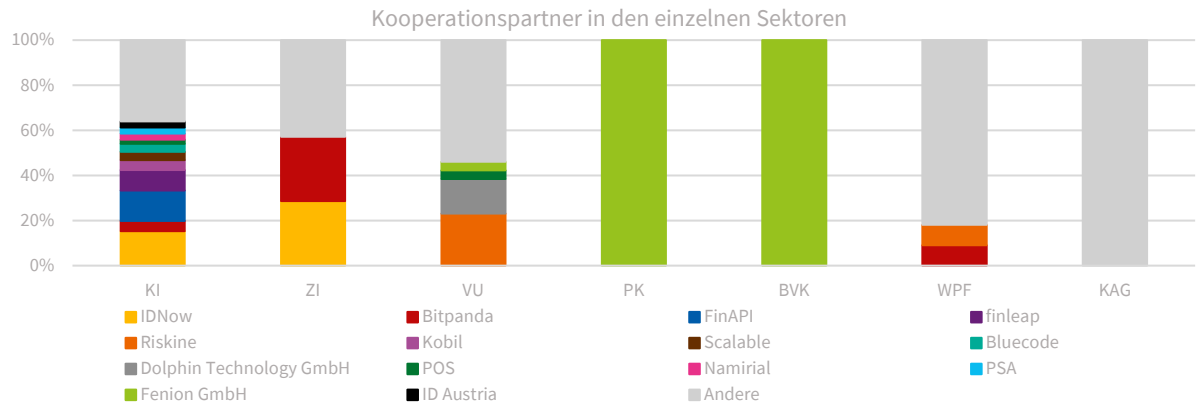
Somit stellt die Szene der FinTechs/InsurTechs ein weiteres aufsichtsrelevantes Feld für die FMA dar, die für gewisse Kooperationsmodelle bereits eine entsprechende Sandbox betreibt (§ 23a FMABG).

2.2 FINTECHS / INSURTECHS AM ÖSTERREICHISCHEN FINANZMARKT

Insgesamt etablieren sich StartUps als Teil des österreichischen Finanzmarktes. Durch Kooperationen mit konzessionierten Unternehmen bringen diese neuen Akteure Technologien und kreative, digitale Herangehensweisen in den Markt ein. Außerdem können derartige Kooperationen mit konzessionierten Unternehmen regulatorische Know-How-basierte bzw. finanzielle Einstiegshürden überwinden. Einige Unternehmen, die ursprünglich als „StartUp" charakterisiert wurden, haben Konzessionen für Finanzdienstleistungen erhalten und am Markt reüssiert.

FinTechs/InsurTechs-Landkarte

Die 14 über alle Sektoren hinweg überwiegend genannten FinTechs/InsurTechs, welche zugleich mindestens drei Mal erwähnt wurden, sind in der folgenden Darstellung visualisiert. Bei KAG gab es keine Mehrfachnennungen, sodass die genannten FinTechs/InsurTechs in dieser Darstellung nicht vorkommen. Die relativen Anteile beziehen sich nicht auf den gesamten Sektor, sondern lediglich auf jene Unternehmen innerhalb der einzelnen Sektoren, die eine Kooperation angegeben haben.



3 NEUE ANLAGEFORMEN

Trotz der andauernden Dynamik im Krypto-Bereich, des steigenden Kostendrucks und der Suche nach renditebringenden Investments sind die beaufsichtigten Unternehmen bei den Beteiligungen an FinTechs/InsurTechs sowie bei den Investitionen in Krypto-Assets und bei Beteiligungen am Crowdfunding nach wie vor sehr zurückhaltend.

Anzahl der Unternehmen mit Investitionsanteil größer 0		*KI*	*ZI*	*VU*	*PK*	*BVK*	*WPF*	*KAG*
Beteiligung an FinTech / InsurTech	Eigen aktuell	3	0	1	1	2	2	1
	Geplant	1	0	2	1	2	0	1
	Fremd aktuell	0	0	2	2	2	1	3
	Geplant	0	0	2	1	2	1	2
Crowdfunding	Eigen aktuell	0	0	0	1	2	1	0
	Geplant	0	0	0	1	2	0	0
	Fremd aktuell	0	0	2	1	2	1	1
	Geplant	0	0	2	1	2	0	1
Krypto-Assets	Eigen aktuell	0	0	0	1	2	1	0
	Geplant	0	0	0	1	2	0	0
	Fremd aktuell	2	0	2	2	2	2	1
	Geplant	0	0	2	2	2	1	1

Die Anzahl der Unternehmen mit Investitionen in FinTechs/InsurTechs, Crowdfunding oder Krypto-Assets ist weiterhin vernachlässigbar. Liegen derartige Veranlagungen vor, bewegt sich der Anteil am Gesamtportfolio in einem niederschwelligen Bereich bzw. ist nur marginal.

- **Beteiligung an FinTechs/InsurTech:** Nur ein KI, ein VU, eine PK und eine KAG sind mit mehr als 10 Mio. Euro in FinTechs/InsurTechs investiert, wobei nur ein VU und eine KAG vergleichbar hohe Veranlagungen auch in den nächsten drei Jahren planen.
- **Krypto-Assets:** Bis auf eine PK plant kein beaufsichtigtes Unternehmen direkte / indirekte Investitionen in Kryptowerte im Ausmaß von mehr als 10 Mio. Euro zu tätigen.

4 HINDERNISSE DER DIGITALISIERUNG

Digitalisierungshindernisse werden seit 2018 konstant primär in der Regulierung, teilweise aber auch in der eigenen IT-Landschaft und im Kundenverhalten gesehen.

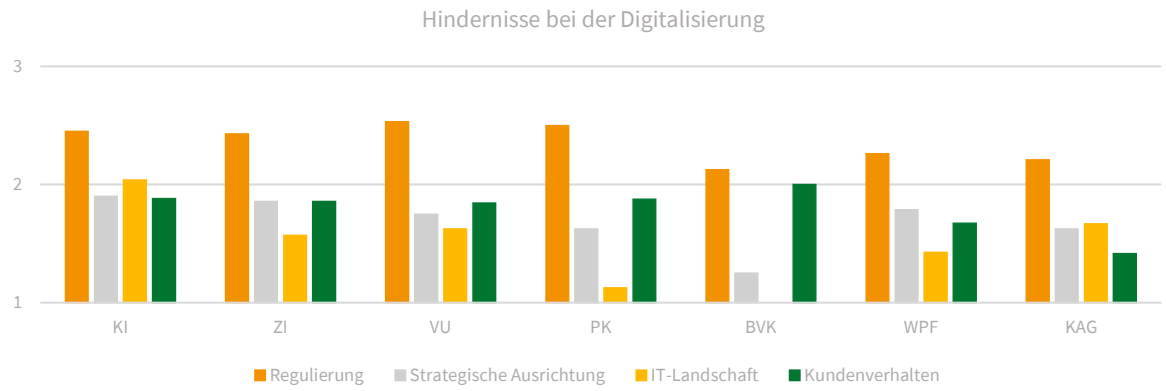
- Als größtes Hindernis der Digitalisierung wird nach wie vor die **Regulierung** gesehen. Im Vergleich zu 2021 ist die Einschätzung dieses Aspekts als Hindernis insb. bei PK, KI, VU, WPF und KAG gestiegen. Als Hauptfaktoren der Hindernisse in der Regulierung werden Vorgaben zum **Datenschutz** und zur **IKT-Sicherheit** genannt.

  Dass IKT-Sicherheitsvorgaben als „Hindernis" der Digitalisierung angegeben werden, ist wohl vor allem auf den relativ großen Aufwand iZm der Implementierung von DORA zurückzuführen.

- Hinsichtlich der Hindernisse in der **strategischen Ausrichtung** spielen hauptsächlich das generelle Mindset der eigenen Unternehmenskultur und die niedrige Priorisierung aufgrund der Besonderheiten des Geschäftsmodells und/oder der Marktgröße eine Rolle.

- Bzgl. der **IT-Landschaft** werden eine stark fragmentierte und eine veraltete IT-Landschaft im weitgehend gleichen Ausmaß genannt, was allerdings lediglich bei KI eine größere Rolle spielt. Ein starker Rückgang der Wahrnehmung dieser Kategorie als Hindernis ist im Vergleich zu 2021 insb. bei PK und BVK auffällig.

- Relevant sind auch Hindernisse, welche ihren Ursprung im **Kundenverhalten** haben. Hierbei berichten die Unternehmen vor allem über die inadäquate digitale Kompetenz von Kund:innen, welche ein Hemmnis für digitale Lösungen darstellt, sowie eine eher abwartende Haltung von Kund:innen digitalisierten Prozessen gegenüber.

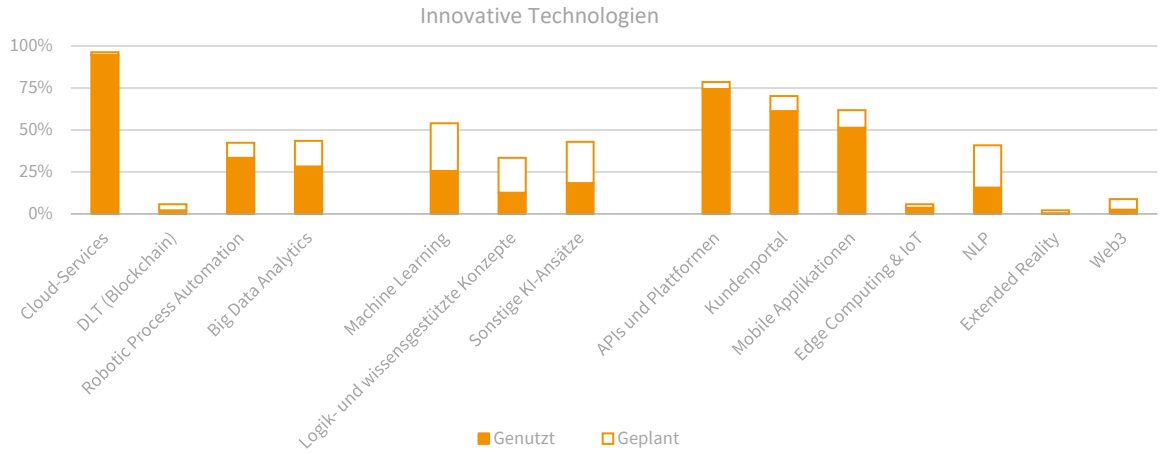


Notiz: Durchschnittswerte pro Sektor mit 1: nicht relevant, 2: teilweise relevant, 3: sehr relevant

5 DIGITALE TECHNOLOGIEN

5.1 VERBREITUNG DIGITALER TECHNOLOGIEN

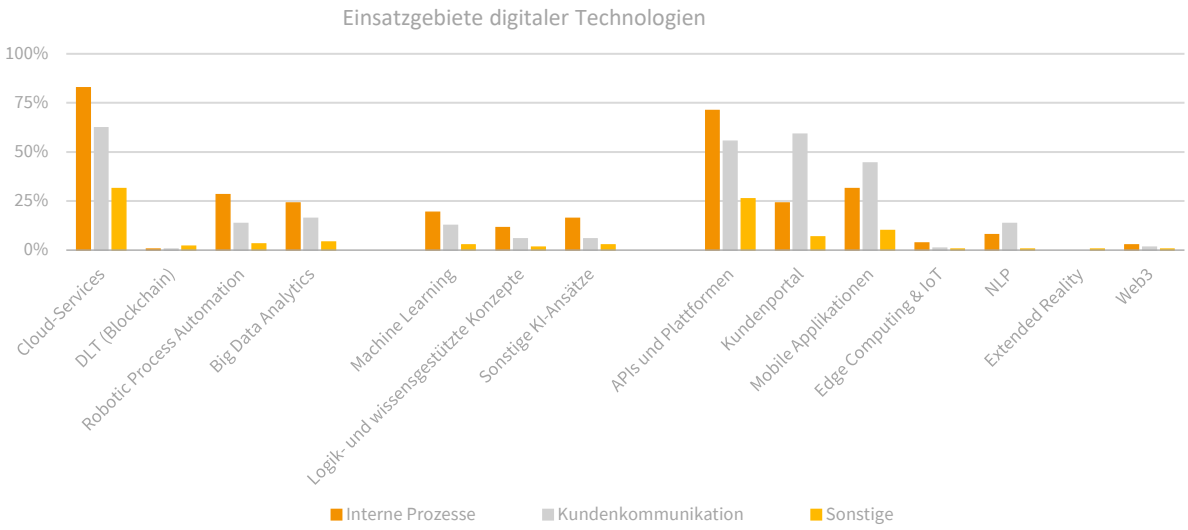
Beim Einsatz digitaler Technologien im operativen Geschäftsbetrieb dominieren am österreichischen Finanzmarkt über alle Sektoren hinweg Cloud-Services (95%) gefolgt von APIs und Plattformen (74%).



Aktuelle Trends und Entwicklungen:

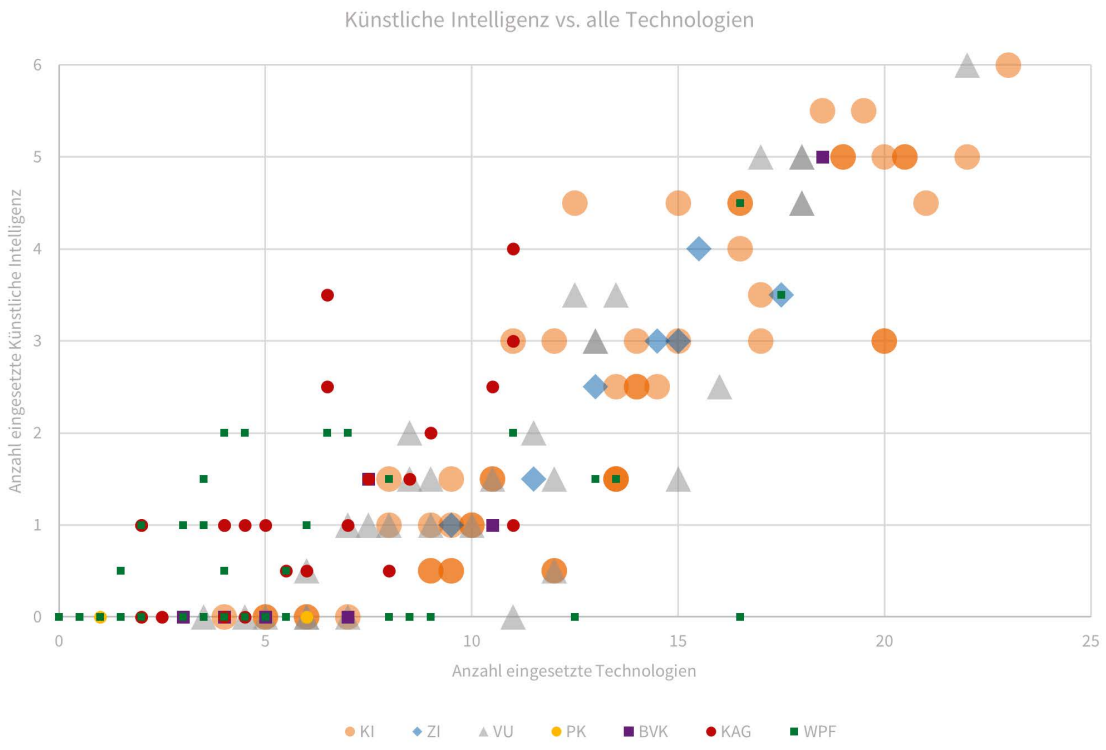
Die **Haupteinsatzgebiete** digitaler Technologien (zum einen interne Prozesse wie Risikomanagement, Compliance, Bestandsverwaltung, Veranlagung, zum anderen Marketing und Vertrieb inkl. Kundenbetreuung) bestätigen die bisherigen Wahrnehmungen der Aufsicht, wonach

- Effizienzsteigerungen, regulatorische Anforderungen an unternehmensinterne Abläufe sowie die Möglichkeit, etwa durch Fraud-Detection-Systeme eigene Kosten zu senken, den Einsatz neuer digitaler Technologien treiben;
- die Kundenschnittstelle ebenfalls jener Ort ist, an welchem sich innovative digitale Technologien besonders schnell etablieren.



Aus den Einsatzgebieten der einzelnen Technologien selbst ergeben sich folgende **Trends**:

- **Cloud-Services** werden in der Zwischenzeit praktisch universell in allen Finanzmarktsektoren eingesetzt. In der Regel wird dabei das Servicemodell „Software as a Service“ (84%) und das Nutzungsmodell Public-Cloud (80%) in Anspruch genommen.
- **Robotic Process Automation** wird primär für die Abarbeitung repetitiver Formulare, zB bei der Anlage und Übertragung von Datensätzen in den eigentlichen Analysesystemen, eingesetzt.
- Die Haupteinsatzbereiche von **Machine Learning** sind Rating-Systeme, Fraudanalytics, Unterstützung in Bereichen IT, Verwaltung und Marketing.
- **Big Data Analytics** werden am häufigsten im Risikomanagement eingesetzt. Des Weiteren kommen sie noch vermehrt in den Bereichen Produktentwicklung, Reporting und Fraudanalytics zum Einsatz.
- **Blockchain-Technologie** wird immer noch kaum genutzt. Entgegen manchen Ausbauplänen im Jahr 2021 ist die Nutzung mangels konkreter Anwendungsfälle sogar noch zurückgegangen.
- **Natural Language Processing** wird vermehrt vor allem für Chatbots und Kundenbetreuung genutzt.
- **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 durch die zunehmende Digitalisierung.
- Je mehr digitale Technologien ein Unternehmen insgesamt einsetzt, desto häufiger macht es sich auch die **künstliche Intelligenz** zu Nutze: Stellt man die Anzahl der eingesetzten digitalen Technologien der Anzahl der Technologien im Bereich Künstliche Intelligenz gegenüber, zeigt sich, dass KI, ZI und VU insgesamt die meisten Technologien einsetzen und bei der Nutzung der künstlichen Intelligenz zusätzlich noch die KAG vorne dabei sind.



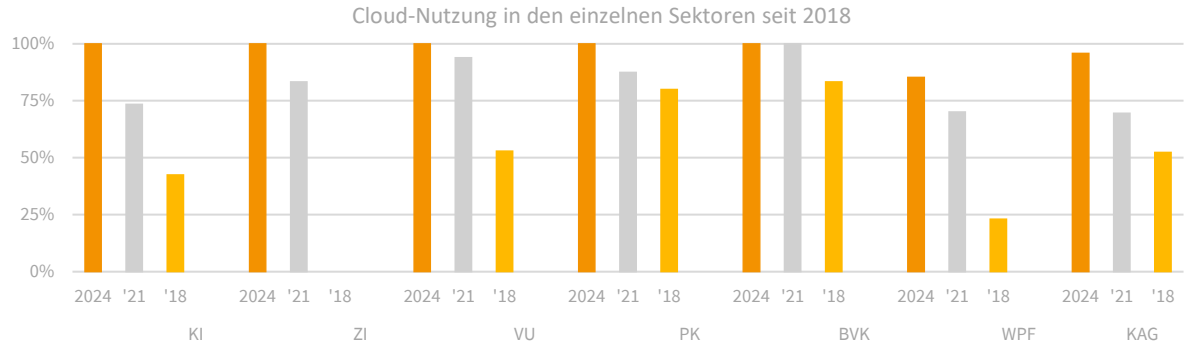
Notiz: Bei künstlicher Intelligenz war eine maximale Anzahl von 9 erreichbar, während bei allen Technologien das Maximum bei 42 liegt. Die Graphik umfasst nicht nur die bereits eingesetzten Technologien; auch der in den nächsten drei Jahren geplante Einsatz digitaler Technologien ist hier bereits zu 50% berücksichtigt.

5.2 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 Bereitstellung der Dienstleistungen erfolgt nicht von einem konkreten Rechner aus. Vielmehr besteht die virtuelle Rechenwolke aus vielen verschiedenen, miteinander vernetzten Rechnern. Die Nutzung der Cloud-Services erfolgt über ein Netzwerk durch Zugriff auf den Ressourcenpool der Cloud, wobei dynamisch die benötigten Kapazitäten zugeteilt werden.

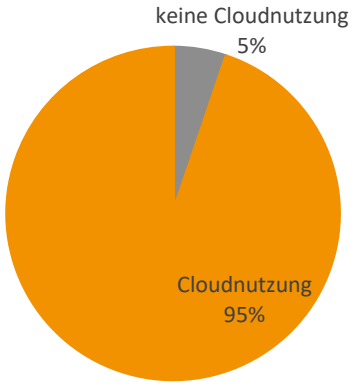
Aktuelle Trends und Entwicklungen:

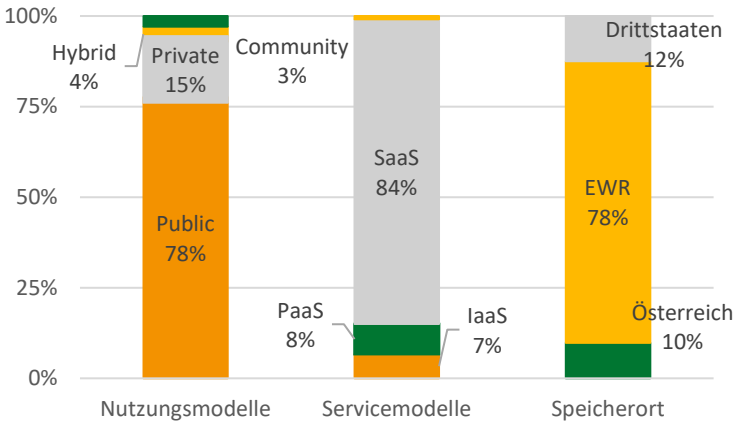
Cloud-Services haben seit 2018 stark an Bedeutung gewonnen und werden nun **praktisch universell** von den Unternehmen aller Finanzmarktsektoren eingesetzt. Seit 2021 haben alle Sektoren den Cloud-Anteil gesteigert.



Cloud Services werden **von 95% der beaufsichtigten Unternehmen genutzt**, wobei etwa 80% der Cloud-nutzenden Unternehmen in ihrem Geschäftsbetrieb mehr als eine Cloud-Lösung einsetzen. Diese Cloudlösungen fallen praktisch ausnahmslos unter die Definition einer ‚IKT-Dienstleistung' nach DORA (Art 3 VO 2022/2554 iVm Anhang III der DVO 2024/2956), sodass für ihre Nutzung die einschlägigen Regeln in Bezug auf das Risikomanagement, die Vertragsgestaltung und das Führen des Informationsregisters gelten.

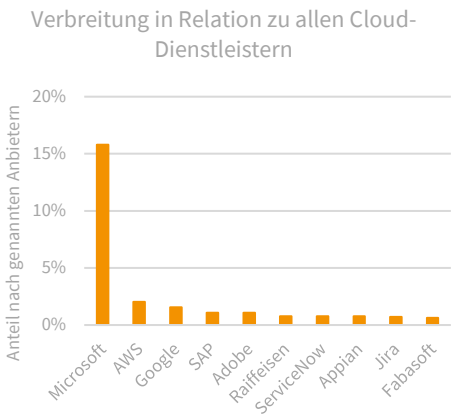
- Am weitesten verbreitet sind Cloud-Services bei den KI, ZI, VU, PK und BVK.
- Geringer aber dennoch verstärkt ist die Cloud-Nutzung bei WPF; hier liegt der Anteil bei 85% des WPF-Sektors.

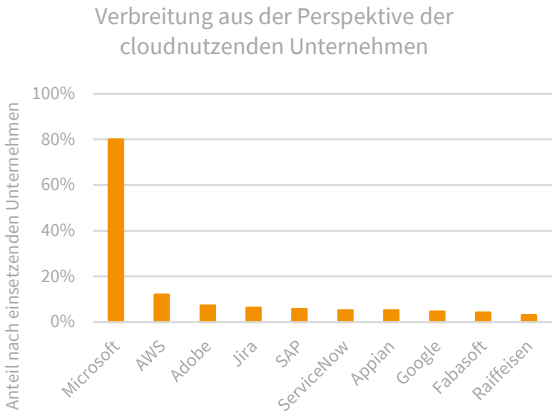




Die bei den österreichischen Finanzunternehmen am weitesten verbreiteten **Anbieter** im Verhältnis zur Gesamtmenge der Cloudnutzungen sind Microsoft, AWS, Google, SAP und Adobe, welche in Summe einen Anteil von 22% einnehmen. Von den österreichischen Anbietern ist insb. Fabasoft vertreten.

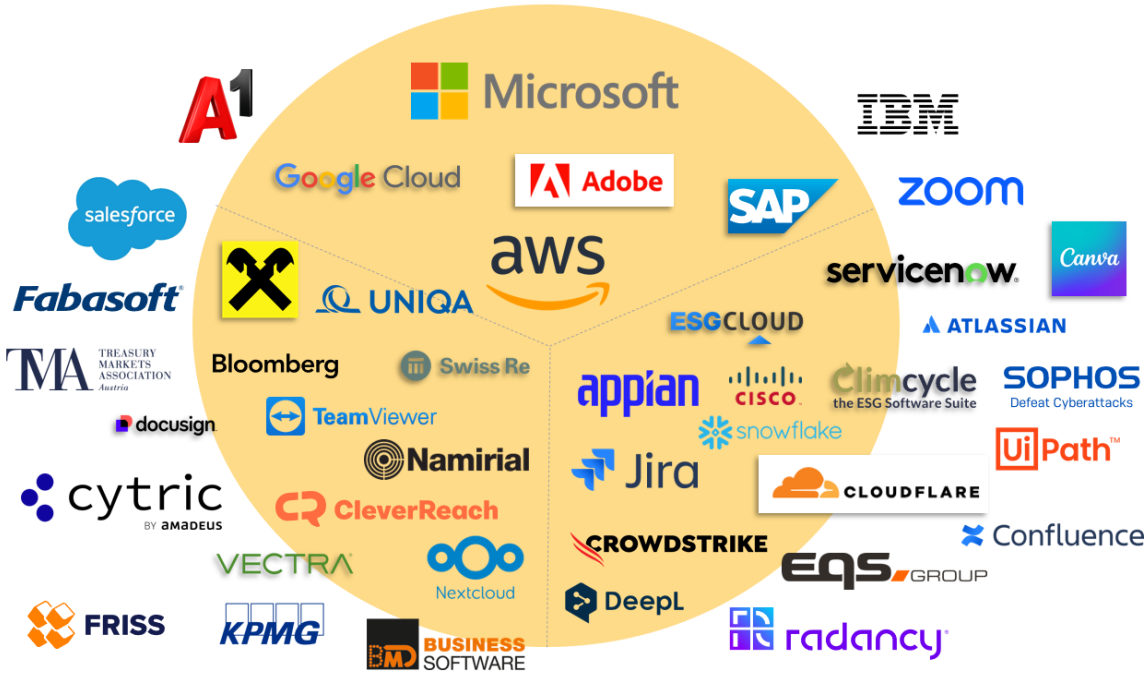
Microsoft wird nach wie vor weit verbreitet als Cloud Dienstleister in Anspruch genommen. Neben MS Office 365 wird auch die Cloudplattform Azure genutzt. Durch den verstärkten Einsatz von Cloud Services ist der Anteil von Microsoft an allen Cloud-Services seit 2021 von 21% auf 16% im Jahr 2024 zurückgegangen.



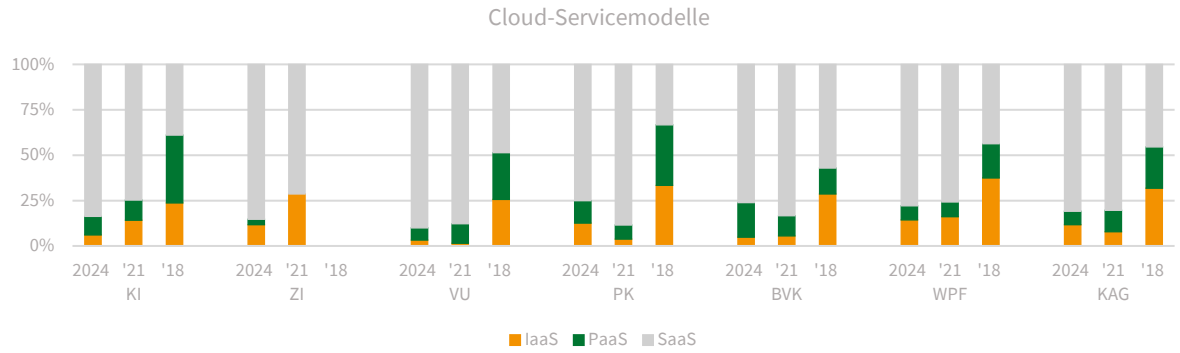


Wird die Verbreitung aus der Perspektive der cloudnutzenden Unternehmen betrachtet, so zeigt sich, dass 80% der beaufsichtigten Unternehmen am österreichischen Finanzmarkt mindestens ein Microsoft-Produkt verwenden, während AWS nur von 12% der Unternehmen verwendet wird. Alle weiteren Anbieter haben nur einen einstelligen prozentualen Anteil. Der österreichische Cloud-Anbieter Fabasoft kommt auf 4%.

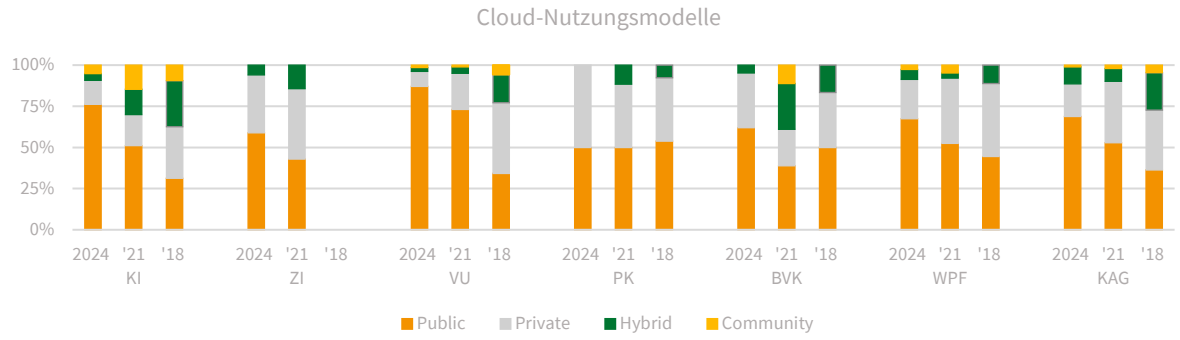
Landscape der Cloud-Dienstleister am österreichischen Finanzmarkt



Im Durchschnitt sind **84%** aller von den beaufsichtigten Unternehmen genutzten Cloud-Dienste dem **Servicemodell „Software as a Service“ (SaaS)** zuzurechnen. 2021 belief sich der auf SaaS-Modelle entfallende Anteil auf 80%. Im gleichen Betrachtungszeitraum hat sich bei den IaaS-Servicemodellen der Anteil von 14% auf 7% vermindert. Beim PaaS hat sich der Anteil von 7% auf 8% erhöht.

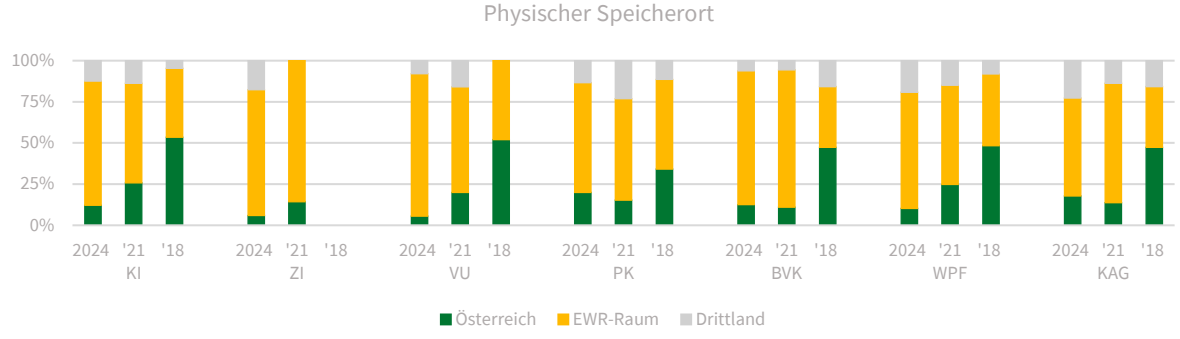


Die Inanspruchnahme von **Public Clouds** hat sich im Vergleich zu 2021 erhöht. Damals waren etwa die Hälfte aller genutzten Cloud Services solche Public Clouds. Nunmehr entfällt **rund 80%** der Cloud-Services auf dieses Nutzungsmodell.



Währenddessen ist der Anteil von Private Clouds von 34% auf 15% zurückgegangen. Der gleiche Trend ist bezüglich der Hybriden Clouds, deren Anteil sich von einem Zehntel im Jahr 2021 auf 4% reduziert hat, wodurch diese, ähnlich wie Community Clouds mit weitgehend unveränderten 3% Nutzungsanteil, eine stark untergeordnete Bedeutung einnehmen.

88% aller **physischen Speicherorte** der Cloud-Daten liegen **im EWR**, wobei der Löwenanteil mit etwa vier Fünftel nicht in Österreich, sondern in anderen EWR-Staaten liegt. Im Vergleich zu 2021 hat sich der Anteil Österreichs von damals 15% auf 10% vermindert.



5.3 DISTRIBUTED-LEDGER-TECHNOLOGIE (DLT)

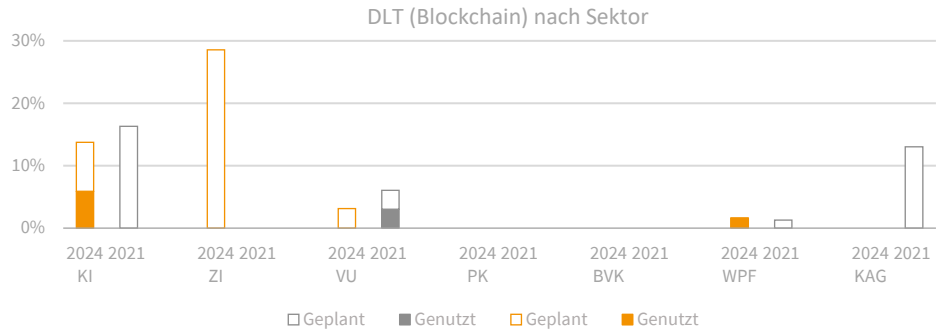
Eine „Distributed-Ledger-Technologie“ (DLT) ist eine Technologie, die den Betrieb und die Nutzung von Distributed Ledger ermöglicht. Als „Distributed Ledger“ wird ein Informationsspeicher bezeichnet, der Aufzeichnungen über Transaktionen enthält und der unter Verwendung eines Konsensmechanismus auf eine Reihe von DLT-Netzwerkknoten verteilt und zwischen diesen synchronisiert wird. DLT-Netzwerkknoten sind Geräte oder Prozesse, die als Teile eines Netzwerks eine Kopie von Aufzeichnungen aller Transaktionen in einem Distributed-Ledger enthalten. Konsensmechanismus sind Regeln und Verfahren, durch die eine Übereinstimmung unter DLT-Netzwerkknoten dahin gehend erzielt wird, dass eine Transaktion validiert ist (siehe Art 3 Z 1, 2, 3 und 4 Verordnung [EU] 2023/1114).

Chancen	■ vielseitige Anwendbarkeit; vor allem in verteilten, nicht-hierarchischen Systemen nutzbar ■ Manipulationsresistenz durch konsensuale Verifikation ■ Vereinfachung von Geschäftsfällen: automatisierte Vertragsabwicklung durch smart contracts ■ potentiell hohe Transparenz: Möglichkeit, in die gesamte Datenhistorie Einsicht zu nehmen ■ Kostenersparnis bei der Kundenidentifikation durch effizientere Authentifizierungsvorgänge ■ Reduktion von Transaktionskosten, sofern keine/weniger Intermediäre notwendig ■ kein „Single Point of Failure“: Auf Grund des dezentralen Charakters führt ein Ausfall eines Teils nicht zum Komplettausfalls des DLT-Systems
Risiken	■ Rechtsrisiken: Relativ neue und teilweise schlecht verstandene Technologie ■ dezentrale Struktur verhindert inhärent Anwendungen mit zentraler Kontrolle ■ Datenschutz: Alle in der Blockchain gespeicherten Daten zwischen den Teilnehmern öffentlich ■ Cyberrisiken: Angriffe auf Validierungsknoten oder den eingesetzten nativen Token; Ausfälle aufgrund von Protokoll- und Software-Schwachstellen

Aktuelle Trends und Entwicklungen:

Über den gesamten österreichischen Markt hinweg nutzen **nur vier Unternehmen** (3 KI und 1 WPF) DLT.

- Während eine Nutzung bei den VU nicht mehr stattfindet, ist die Nutzung bei WPF neu hinzugekommen. Die größten Ausbaupläne haben ZI (29%) und KI (8%), während KAG ihre Ausbaupläne aus 2021 zurückgefahren haben und nun mehr keine Einführung von DLT geplant haben.
- DLT kommt dabei meist bei der Reconciliation, der Prozess-Dokumentation und im Security Token Marktplatz zum Einsatz.



5.4 ROBOTIC PROCESS AUTOMATION (RPA)

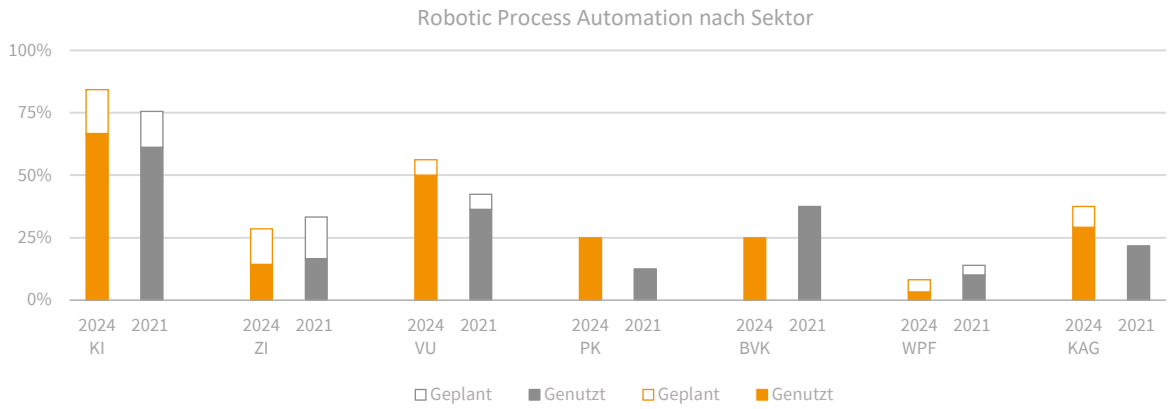
Robotic Process Automation (RPA) ist ein Sammelbegriff für Software-Roboter, die durch die vordefinierte Ausführung von Tastatureingaben und Mausbewegungen, repetitive oder fehleranfällige Tätigkeiten in Softwareanwendungen automatisiert durchführen kann. Dabei ist im Regelfall nur eine relativ einfache Entscheidungslogik hinterlegt. Durch den Einsatz derartiger intelligenter Technologien soll die Softwareanwendung bei sich wiederholenden Betriebsaufgaben, wie etwa das Extrahieren von Daten, das Ausfüllen von Formularen, das Verschieben von Dateien, auf dieselbe Weise wie eine menschliche Fachkraft arbeiten.

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

Aktuelle Trends und Entwicklungen:

RPA wird von **mehr als einem Drittel (34%)** der beaufsichtigten Unternehmen genutzt.

- Mit einem Anteil von zwei Drittel (67%) ragen hier insb. KI klar heraus, gefolgt von den VU mit 50%. Im Versicherungssektor ist auch die größte Dynamik zu verzeichnen: während 2021 nur etwa mehr als ein Drittel (36%) der VU RPA genutzt hat, ist das nun die Hälfte der Unternehmen dieses Sektors.
- Bei den KI, VU, PK und KAG ist der Anteil der Unternehmen, die RPA einsetzen, seit 2021 gestiegen, während er in den Sektoren ZI, BVK und WPF etwas zurückgegangen ist.



5.5 BIG DATA ANALYTICS

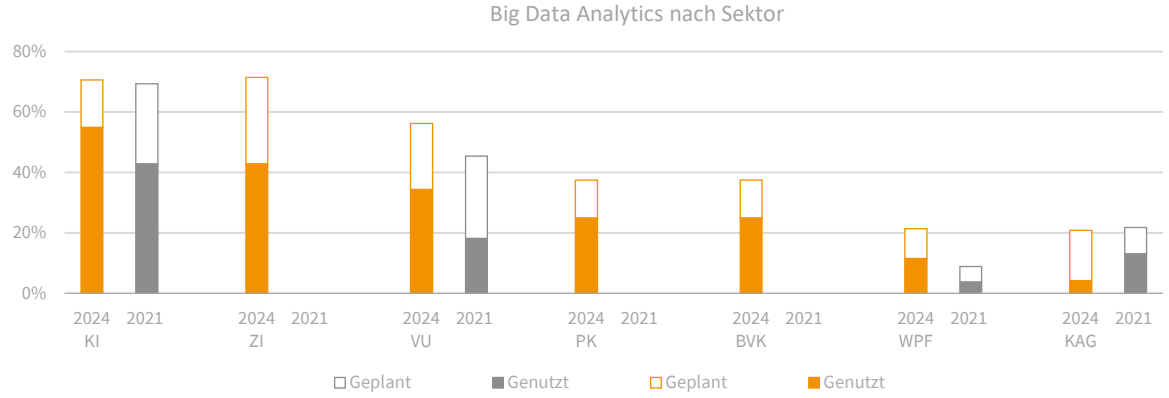
Big Data bezeichnet meist die automatisierte Verarbeitung großer Datenmengen (Volume) in engem Zeitrahmen (Velocity) aus unterschiedlichen Quellen (Variety). Im Finanzbereich gibt es zahlreiche mögliche Anwendungsfälle für diese Technologie (zB im Marketing, bei der Fraud Detection, bei der Erstellung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

Chancen	■ genauere Modelle können durch die Analyse großer Datenmengen konstruiert werden ■ individuelle Absicherungsbedarfe und Kaufwahrscheinlichkeiten lassen sich durch neue Methoden für Data Analytics genauer vorhersagen ■ Angebote können damit besser individualisiert werden ■ Analyseprozesse in der Prävention und Bekämpfung von Betrug, Geldwäsche und Terrorismusfinanzierung können durch Big Data Anwendungen verbessert werden ■ 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 Investitionen in Infrastruktur und Rechenleistung ■ im Echtbetrieb lassen sich Analysen großer Datenmengen aufgrund des Ressourcenaufwandes oft bei Bedarf nicht wiederholen

Aktuelle Trends und Entwicklungen:

Die Analyse großer Datenmengen wird von **weniger als einem Drittel (28%)** der beaufsichtigten Unternehmen genutzt, wobei seit 2021 weitere Sektoren neu hinzugekommen sind.

- Am häufigsten wird diese Technologie von KI (55%), ZI (43%) und VU (34%) eingesetzt. Bis 2027 wollen überdies beinahe ¾ der Unternehmen in diesen Sektoren Big Data Analytics nutzen.
- Big Data Analytics werden am häufigsten im Risikomanagement eingesetzt. Des Weiteren kommen sie noch vermehrt in den Bereichen Produktentwicklung, Reporting und Fraudanalytics zum Einsatz.



5.6 KÜNSTLICHE INTELLIGENZ (KI)

Ein KI-System ist „ein maschinengestütztes System, das für einen in unterschiedlichem Grade autonomen Betrieb ausgelegt ist und das nach seiner Betriebsaufnahme anpassungsfähig sein kann und das aus den erhaltenen Eingaben für explizite oder implizite Ziele ableitet, wie Ausgaben wie etwa Vorhersagen, Inhalte, Empfehlungen oder Entscheidungen erstellt werden, die psychische oder virtuelle Umgebungen beeinflussen können“ (Art 3 Z 1 der Verordnung [EU] 2024/1689).

Mit der Verordnung (EU) 2024/1689 zur Festlegung harmonisierter Vorschriften für künstliche Intelligenz (Artificial Intelligence Act, AI-Act) wird erstmalig ein einheitlicher Rechtsrahmen für die Entwicklung, das Inverkehrbringen, die Inbetriebnahme und die Verwendung von Systemen künstlicher Intelligenz innerhalb der EU geschaffen.[2] Der AI-Act, der phasenweise ab 2. Februar 2025 Anwendung findet, soll einen Ausgleich zwischen dem Schutz vor möglichen Gefahren und der Förderung von Innovation finden.

Chancen	■ Sehr komplexe Tätigkeiten, die ansonsten besondere Expertise benötigen, können unterstützt oder übernommen werden. Ein adäquat kalibriertes und angelerntes System kann sehr genau arbeiten und sich selbst laufend anhand neuer Daten verbessern. ■ Es können potenziell neue, unbekannte Zusammenhänge erkannt werden. ■ bessere Vorhersehbarkeit von Krisen und Möglichkeit frühzeitig zu reagieren ■ präzisere Vorhersage von zukünftigen Schadenssummen ■ effiziente Ressourcennutzung, Kosten- und Zeitersparnis durch automatisierte Ausführung von repetitiven Aufgaben und Verarbeitung von großen Datenmengen ■ Analyse von Kundenverhalten: Mustererkennung bei Stornoverhalten und Verbesserung des Services, dadurch erhöhte Kunden-Bindung. ■ Informative Daten, wie Forschungs- und Marktdaten, können besser genutzt werden.
Risiken	■ Komplexität und „Black Box“-Effekt können Transparenz schaden, da Entscheidungsprozesse nicht mehr nachvollziehbar sind. ■ Biases und Diskriminierung: mindere Qualität der Daten kann zu biased datasets führen. ■ Modellrisiken: Qualität der Daten kann in der „modelling stage“ deformiert werden. ■ Datenschutz: Rechtswidrige Nutzung von Daten ■ Cybersicherheit: Schwächen im KI-System ermöglichen Cyberangriffe ■ Haftungsfragen vor allem bei hoch-autonomen KI-Systemen nicht abschließend geklärt. ■ Neue operative Risiken: Zuverlässigkeit, technische Ausfälle, Systemfehler, Modellabweichungen ■ Abhängigkeit von Dritten bei der Erbringung von KI-Dienstleistungen, daraus können sich neue Möglichkeiten des Betrugs ergeben und weitere Risiken entstehen. ■ Zunehmende Abhängigkeit von KI-Systemen kann zu Verlust von Fähigkeiten führen. ■ Reputationsschäden

Der Verzicht auf eine demonstrative Aufzählung der verwendeten Techniken und Konzepte, die in den Anwendungsbereich des AI-Acts fallen, und die bloß allgemeine Definition in Art 3 iVm ErwGr 12 AI-Act, wonach sich ein KI-System durch seine Ableitungsfähigkeit von der normalen Datenverarbeitung abhebt,

[2] *ErwG 1 Verordnung (EU) 2024/1689.*

bringt einige Unsicherheiten, für welche KI-Systeme in den einzelnen Sektoren der Anwendungsbereich des AI-Acts eröffnet ist. So bleibt beispielsweise unklar, ob im Versicherungssektor verwendete mathematische und statistische Modelle wie verallgemeinerte lineare Modelle (Generalised Linear Models, GLM) unter den Begriff des KI-Systems fallen und damit einhergehend, ob den Betreiber und Anbieter die Pflichten des AI-Acts treffen. Um eine einheitliche Rechtsanwendung zu gewährleisten, sollte die EK eigene Leitlinien zur Präzisierung des KI-Begriffs ausarbeiten (Art 96 AI-Act).

Anstelle einer abschließenden Liste von KI-Ansätzen wird im ErwGr 12 AI-Act ausgeführt, dass zu den Techniken, die während der Gestaltung eines KI-Systems das Ableiten ermöglichen, Ansätze wie „maschinelles Lernen“ und „logik- und wissensgestützte Konzepte“ gehören. Entlang dieser Nomenklatur wurden auch die verschiedenen Einsatzbereiche von KI am österreichischen Finanzmarkt ermittelt.

5.6.1 MACHINE LEARNING

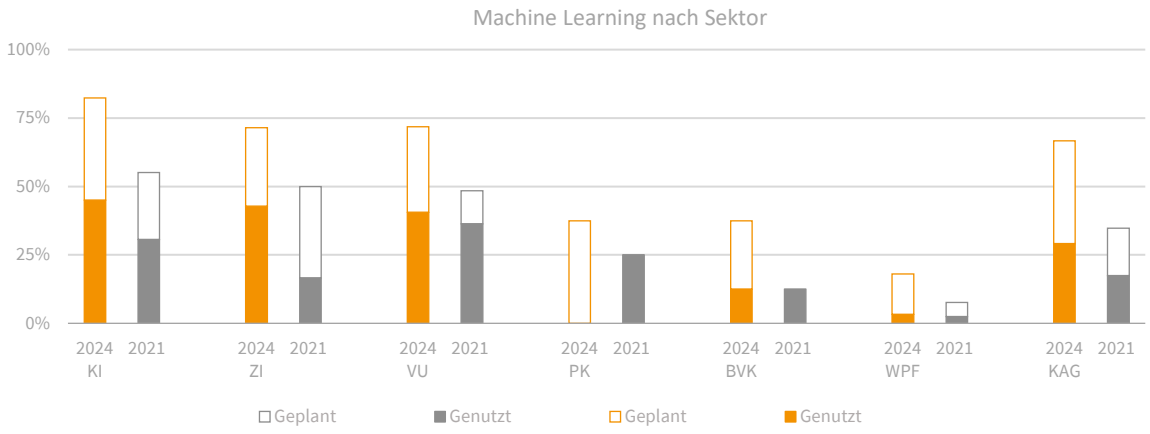
Machine Learning ist ein Teilbereich der künstlichen Intelligenz, bei dem Algorithmen genutzt werden, um Muster in einer großen Menge von Daten zu erkennen und daraus zu lernen. Diese Algorithmen verbessern ihre Leistung, indem sie aus den bereitgestellten Daten lernen, ohne dass sie explizit für bestimmte Aufgaben programmiert werden müssen. Besonders geeignet ist dieses Verfahren zur Interpretation und Mustererkennung in großen Mengen spezifischer Daten. Weiters kann Machine Learning beispielsweise zur Erkennung von Kreditkarten- oder Versicherungsbetrug genutzt werden.

Aktuelle Trends und Entwicklungen:

Mehr als ein Viertel der beaufsichtigten Unternehmen (26%) setzt in ihrem operativen Geschäftsbetrieb bereits Machine Learning ein. Die 2021 kommunizierten Ausbaupläne wurden über alle Sektoren hinweg erfüllt.

- Die Vorreiter bei der Nutzung von Machine Learning sind KI (45%), ZI (43%) und VU (41%).
- Die Haupteinsatzbereiche sind Rating-Systeme, Fraudanalytics, Unterstützung in Bereichen IT, Verwaltung und Marketing.

Auffallend hoch sind die Ausbaupläne in allen Sektoren. Bis 2027 wollen etwa drei Viertel der KI, ZI, VU aber auch KAG Machine Learning-Techniken einsetzen.



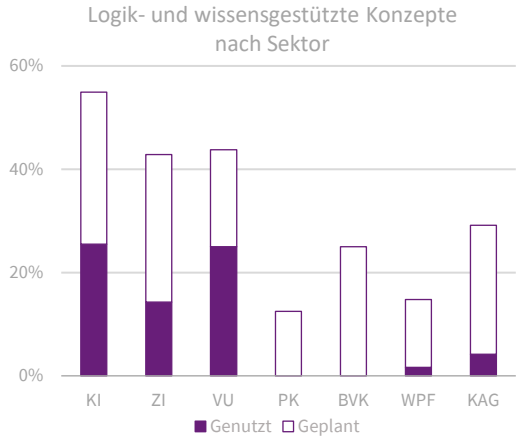
5.6.2 LOGIK- UND WISSENSGESTÜTZTE KONZEPTE

Bei logik- und wissensgestützten Konzepten erfolgt die „Ableitung“ aus kodierten Informationen oder symbolischen Darstellungen der zu lösenden Aufgabe. Wissensgestützte Konzepte sind intelligente Informationssysteme, um Wissen mit Methoden der Wissensrepräsentation und Wissensmodellierung abzubilden und nutzbar zu machen. Dabei wird auf explizites bzw. kodiertes und deshalb mittels Zeichen wie Sprache und Schrift kommunizierbares Wissen zurückgegriffen, um Entscheidungsprozesse wie durch menschliche Fachkräfte zu simulieren. Die Wissensrepräsentation mit Logik hilft dabei, Objekte der realen Welt in eine Sprache zu übersetzten, die ein Computer versteht, damit dieser mit dem Wissen umgehen kann.

Aktuelle Trends und Entwicklungen:

Logik und wissensgestützte Konzepte werden von 13% der beaufsichtigten Unternehmen, allen voran KI und VU (jeweils 25%), eingesetzt. In allen Sektoren weisen die Unternehmen jedoch hohe Ausbaupläne auf. Bis 2027 wollen demnach etwa die Hälfte der KI und VU Logik- und wissensgestützte Konzepte nutzen.

Die Haupteinsatzbereiche derzeit sind Ratingmodelle und Chatbots.



5.6.3 SONSTIGE KI-ANSÄTZE

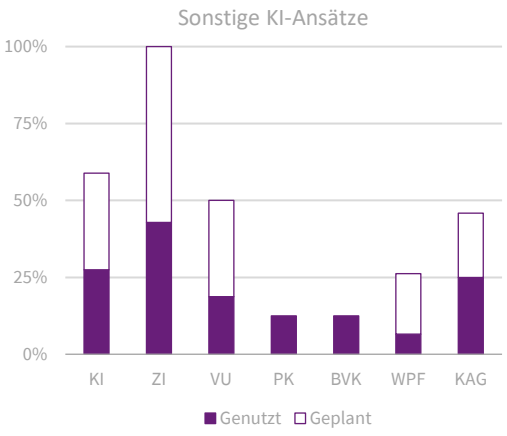
Sonstige KI-Ansätze beinhalten statistische Methoden und heuristische Verfahren, die approximative Lösungen für komplexe Probleme liefern. Dazu zählen bspw. genetische Algorithmen oder Fuzzy-Logik-Systeme, welche dabei helfen, Entscheidungsprozesse zu optimieren und anpassungsfähiger zu machen.

Aktuelle Trends und Entwicklungen:

Sonstige KI-Ansätze werden von 18% der Unternehmen genutzt, wobei überwiegend ZI (43%) herausstechen.

Allerdings planen ZI ihren Anteil in den nächsten Jahren auf 100% zu steigern.

Die häufigste Anwendung finden sonstige KI-Ansätze am österreichischen Finanzmarkt im Bereich Risikomanagement.



5.7 SCHNITTSTELLEN

Die zunehmende Komplexität und Vernetzung der globalen IT-Landschaft erfordern vermehrt, dass die beaufsichtigten Unternehmen auf die Daten und Funktionen eines externen Betriebssystems, einer Anwendung oder eines anderen Dienstes zugreifen. Digitale Schnittstellen, die Integration verschiedener IT-Systeme, den Aufbau von kollaborativen IT-Umgebungen und Application Programming Interfaces (APIs) werden insofern immer mehr zum Schlüssel für die digitale Transformation.

5.7.1 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.

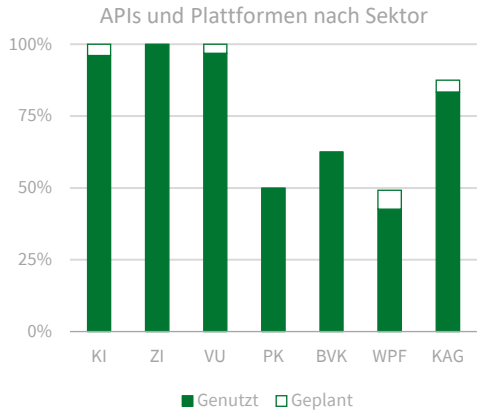
Chancen	■ APIs können die Reibungsverluste minimieren, die häufig durch die Implementierung einer „bimodalen“ IT-Strategie verursacht werden, bei der Legacy-Anwendungen neben innovativeren digitalen Lösungen laufen. APIs sind die Schicht, über die „Modus 1“ und „Modus 2“ miteinander verbunden werden können, und schließen die Lücke zwischen Kerndaten und -funktionen sowie einer experimentelleren, innovativeren Anwendung.[3] ■ APIs können die Interaktion mit Kunden vereinfachen. ■ Externe Datenprovider können Umsetzungen von Big Data Analytics und Machine Learning unterstützen; Echtzeit-Konnektivität durch schnelle und kontinuierliche Datenübertragung
Risiken	■ Jede Datenschnittstelle ist eine potenzielle 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 ■ Aufwändige Integration kann kostenintensiv sein.

Aktuelle Trends und Entwicklungen:

Automatisierte Datenschnittstellen werden im Aggregat durchschnittlich zu über 75% genutzt.

KI (96%), ZI (100%) und VU (97%) ragen dabei vor allem heraus. Am geringsten ist der Nutzungsanteil bei WPF mit 43%.

APIs werden vor allem im Kernbankensystem genutzt, finden aber unter anderem auch vermehrt in der Schadensabwicklung statt.



[3] *Gartner, APIs Are At The Heart Of Digital Business.*

5.7.2 ONLINE-PORTALE

Ein Online-Portal ist eine digitale Plattform, die es den beaufsichtigten Unternehmen erlaubt, ihrer Kund:innen einen geschützten und individuellen Zugang zu verschiedenen Services und Informationen zu bieten. Kund:innen können darüber beispielsweise ihre Daten einsehen, Transaktionen abwickeln oder Unterstützung anfordern, je nach den Funktionen, die das Unternehmen zur Verfügung stellt.

Bei der Ausgestaltung der Online-Portale sind mitunter besondere aufsichtsrechtliche Anforderungen zu berücksichtigen:

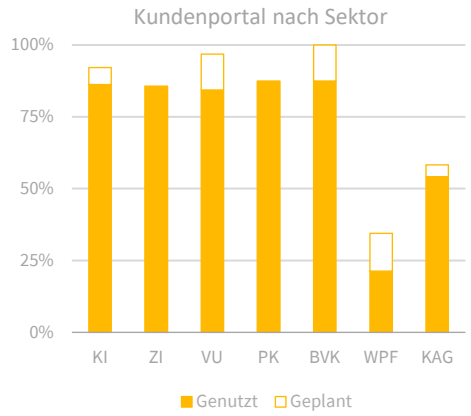
- VU können etwa die Auskünfte an ihre Kund:innen über ein Kundenportal in Form einer personalisierten Website erstellen, wenn diese den Vorgaben des § 128a Abs 2 Z 2 VAG entspricht und der Versicherungsnehmer der Erteilung der Auskünfte auf einem solchen anderen dauerhaften Datenträger zugestimmt hat.

Chancen	■ Erhöhte Zufriedenheit der Kund:innen im Hinblick auf die jederzeitige Zugriffsmöglichkeit ■ Effizienzsteigerung durch Entlastung der Kunden-Service-Stelle ■ Online-Portale können zu einer erhöhten Interaktion der Kund:innen mit dem Unternehmen führen. Die Möglichkeit, jederzeit in ihren Vertrag und dessen Wertentwicklung einzusehen oder Änderungen unmittelbar durchzuführen, kann die Attraktivität für Kund:innen erhöhen. ■ Feedback der Kund:innen kann besser gesammelt werden und darauf reagiert werden, woraus ein Unternehmen auch Wettbewerbsvorteile generieren kann
Risiken	■ Die Einrichtung ist relativ aufwändig; eines solche Kommunikationsmöglichkeit muss von Softwareentwickler:innen implementiert werden, an die IT-Infrastruktur des Unternehmens angepasst werden sowie gut abgesichert sein, da sie eine potentielle Angriffsfläche darstellt. ■ Rechtsrisiken inkl. Risiken im Bereich Datenschutz ■ Operationale Risiken inkl. Cyberrisiken

Aktuelle Trends und Entwicklungen:

Kundenportale (zB Personalisierte Websites) sind bereits über alle Sektoren hinweg stark verbreitet. Lediglich die WPF (21%) setzen Online-Portale weniger oft ein, was auf die Besonderheiten ihres Geschäftsmodells zurückzuführen ist.

In den nächsten drei Jahren planen insb. WPF, BVK und VU den Einsatz von Online-Portalen noch stärker auszubauen.



Da ein Online-Portal nicht bei jedem Geschäftsmodell gut einsetzbar ist, kann davon ausgegangen werden, dass sich dieses Werkzeug nicht bei allen Unternehmen durchsetzen wird bzw. in Einzelfällen dahingehende Prototypen auch wieder eingestellt werden.

5.7.3 MOBILE APPLIKATIONEN

Mobile Applikationen sind Softwareprogramme, die speziell für die Nutzung auf mobilen Geräten, wie Smartphones, entwickelt wurden. Diese können direkt auf dem Gerät installiert und ausgeführt werden und müssen nicht über den Browser aufgerufen werden.

Chancen	■ Erhöhte Kundenbindung und -Zufriedenheit ■ Effizienzsteigerung durch Automatisierung von Routineaufgaben
Risiken	■ Rechtsrisiken inkl. Risiken im Bereich Datenschutz ■ Operationale Risiken inkl. Cyberrisiken ■ Hohe Entwicklungskosten bzw. Abhängigkeit von Drittanbietern

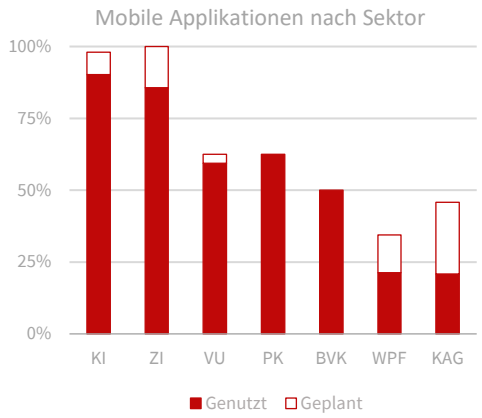
Aktuelle Trends und Entwicklungen

Beinahe alle KI (90%) und ZI (85%) verwenden bereits mobile Applikationen in ihrem Geschäftsbetrieb.

In den VU-, PK- und BVK-Sektor sind das etwa die Hälfte der Unternehmen, die mobile Applikationen nutzen. Bei den WPF und den KAG liegt der Anteil dagegen knapp bei 20%.

Praktisch in allen Sektoren planen noch weitere Unternehmen, mobile Applikationen in den kommenden drei Jahren einzusetzen. Bei den KAG ist sogar mit einer Verdoppelung der Anzahl der Nutzer zu rechnen.

Mobile Applikationen werden meist in Form von Microsoft 365 oder Onlinebanking Apps genutzt.



5.7.4 NATURAL LANGUAGE PROCESSING

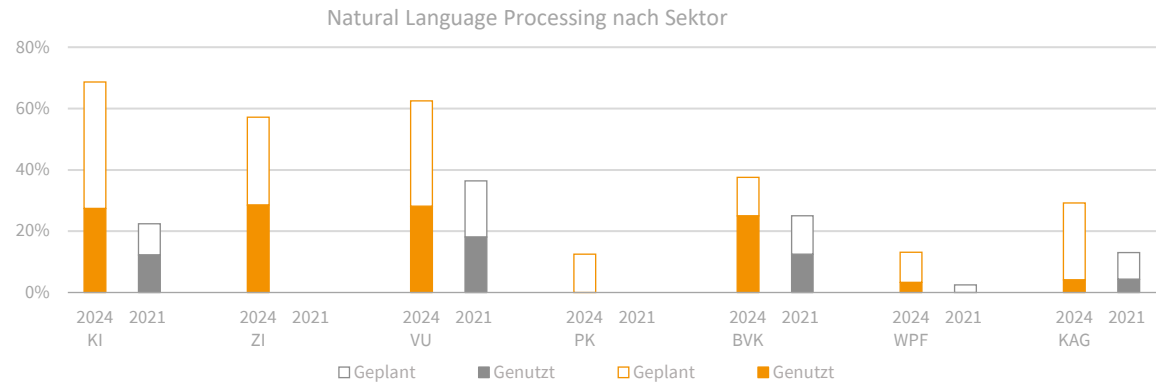
Natural Language Processing beschreibt Techniken und Methoden zur maschinellen Verarbeitung natürlicher Sprache. Ziel ist eine direkte Kommunikation zwischen Mensch und Computer auf Basis der natürlichen Sprache (beispielsweise durch Chatbots). NLP greift dabei auf Disziplinen wie die Informatik und die Computerlinguistik zurück, wodurch sie die Lücke zwischen menschlicher Kommunikation und den Sprachverarbeitungsfähigkeiten von Computern schließen will.

Natural Language Processing (NLP) ist ein Teilbereich der künstlichen Intelligenz und kann, sofern die Voraussetzungen des AI-Acts zur Klassifizierung eines KI-Systems erfüllt sind, in den Anwendungsbereich des AI-Acts fallen, was zu Pflichten für den Betreiber oder Anbieter führen kann. Voraussetzungen für die Einstufung als KI-System sind das Vorliegen eines maschinengestützten Systems, das autonom betrieben wird, Anpassungs- und Ableitungsfähigkeit besitzt, Ausgaben erstellt und damit physische oder virtuelle Umgebungen beeinflusst. Hinsichtlich der Autonomie, Anpassungs- und Ableitungsfähigkeit können Einordnungsschwierigkeiten auftreten, da NLP-Systeme unterschiedlich ausgestaltet sein können und die einzelnen Merkmale nicht immer vollumfänglich aufweisen.

Chancen	■ Effizienzgewinne etwa durch Einsatz im Kundenservice ■ Schnittstellen zu den übrigen IT-Systemen des Unternehmens durch Umsetzung von Sprache in maschinelle Daten ermöglicht ■ größere Mengen an Daten können analysiert werden, welche Menschen ohne Ermüdung und Verzerrung niemals stemmen könnten
Risiken	■ Technisch noch eher komplex; mitunter Herausforderungen bei Datenschutz und Gefahr von Fehlinterpretationen beim Einsatz im Kundenverkehr ■ Mangels technologischer Möglichkeiten/Fertigkeiten nicht für alle Kund:innen frei zugänglich

Aktuelle Trends und Entwicklungen:

Natural Language Processing hat im Vergleich zu 2021 bereits eine deutliche Verbreitung im österreichischen Finanzsektor gefunden. In den Sektoren KI, ZI, VU und BVK beträgt der Nutzungsgrad bereits über 20%. Hierbei werden vor allem Chatbots genutzt und als Instrument für die Kommunikation mit Kund:innen eingesetzt. In den kommenden drei Jahren streben KI, ZI und VU gar die Nutzung von weit über 50% an. Die weiteren Sektoren rechnen ebenfalls mit einem deutlichen Anstieg.



5.7.5 EDGE COMPUTING & INTERNET OF THINGS

Edge Computing bezeichnet die dezentrale Datenverarbeitung am Rand des Netzwerks. Die Daten werden in verbundenen Objekten in Benutzernähe verarbeitet. Durch geringe Latenzzeiten und reduziertem Bandbreitenbedarf wird den Unternehmen der Zugriff auf die Daten in nahezu Echtzeit gewährt.

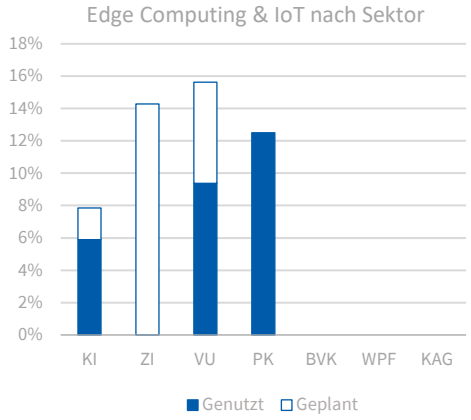
Das Internet of Things (IoT) ermöglich mittels Vernetzung von physischen und virtuellen Objekten eine reibungslose Zusammenarbeit und Kommunikation zwischen diversen Geräten, wodurch ein intelligentes und effizientes Netzwerk entsteht. Unternehmen können auf präzise Echtzeitdaten zugreifen und diese zur Automatisierung und Optimierung von Prozessen nutzen.

Chancen	■ verringerte Latenzzeiten durch die Verarbeitung von Daten näher an der Quelle ■ reduzierte Betriebskosten, da die Daten nicht mehr über das Netzwerk in die Cloud übertragen werden muss ■ höhere Sicherheit durch lokale Verarbeitung und Speicherung der Daten ■ energieeffizienter, da Edge Computing eine ortsgebundene Datenverarbeitung ermöglicht, wodurch Datenübertragung über große Entfernungen wegfallen
Risiken	■ Modelle und Algorithmen müssen rund um die Uhr aktualisiert werden. Geschieht das nicht, kann es zu inaktuellen Ergebnissen kommen. ■ Der Speicher auf Edge Devices ist oft begrenzt. Dies kann zu Datenverlusten und in weiterer Folge Wartungskosten führen. ■ Operationale Risiken inkl. Cyberrisiken

Aktuelle Trends und Entwicklungen:

Edge Computing & IoT wird aktuell von drei KI (6%), drei VU (9%) und einer PK (12,5%) genutzt.

In Zukunft plant im Sektor ZI erstmals ein Unternehmen (14%) die Nutzung von Edge Computing & IoT. Hinzu kommt noch je ein Unternehmen in den Sektoren KI und VU, während BVK, WPF und KAG weiterhin von der Implementierung absehen.



5.7.6 EXTENDED REALITY

Extended Reality (kurz XR) bezieht sich auf Technologien, die fortgeschrittene Computersysteme (Hardware und Software) kombinieren, wodurch sich Änderungen in der Art, wie Menschen miteinander und mit ihrer Umgebung in Kontakt treten, ergeben können. Primär definieren sich diese Technologien durch das Verhältnis von realer und virtueller Welt. Auch menschliche Handlungen können durch Interaktionen mit virtuellen Umgebungen beeinflusst oder manipuliert werden. Bei Extended Reality handelt es sich dabei bei allen Formen um eine immersive Technologie. Während Nutzer von Virtual Reality direkt in eine virtuelle Welt eintreten, wird der Einsatz von Augmented Reality als Erweiterung der realen Welt mithilfe virtueller Objekte wahrgenommen.

Als Beispiel bezieht sich Metaverse auf eine 3D Welt, in der Menschen miteinander durch einen Avatar in Beziehung treten, um etwa Einkäufe zu tätigen, Transaktionen auszuführen oder miteinander zu arbeiten, ohne ihren Platz zu verlassen.

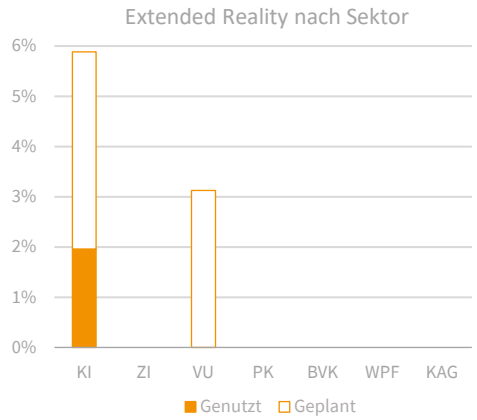
Chancen	■ Innovation in der Produktgestaltung und bei Dienstleistungen, da Kund:innen und Mitarbeitende jederzeit und von überall darauf zugreifen können ■ Bessere Zusammenarbeit durch Fernzugriff ■ Verbesserung der Anpassbarkeit und Flexibilität
Risiken	■ Cyber-Attacken in die eigene Privatsphäre sowie auf vertraute Daten ■ Negative gesundheitliche Auswirkungen bei längerer Nutzung von Virtual Reality Brillen ■ Verlust von direkten menschlichen Beziehungen

Aktuelle Trends und Entwicklungen:

Extended Reality ist im sehr geringen Ausmaß bei den KI mit nur einem Unternehmen (2%) vertreten.

In den nächsten drei Jahren planen neben zwei weiteren KI noch ein VU Extended Reality zu nutzen.

Alle anderen Sektoren planen derzeit keinen Einsatz dieser Technologie.



5.7.7 WEB3

Web3 bezeichnet ein Konzept für ein dezentrales Internet, das auf Blockchain-Technologie basiert. Es zielt darauf ab, Nutzer:innen mehr Kontrolle über ihre Daten und digitale Identitäten zu geben und ermöglicht Peer-to-Peer-Interaktionen ohne zentrale Vermittler.

Wichtige Technologien in Web3 sind Kryptowährungen, Smart Contracts und dezentralisierte Apps. Ziel ist es, ein transparenteres, sicheres und benutzerfreundlicheres Internet zu schaffen.

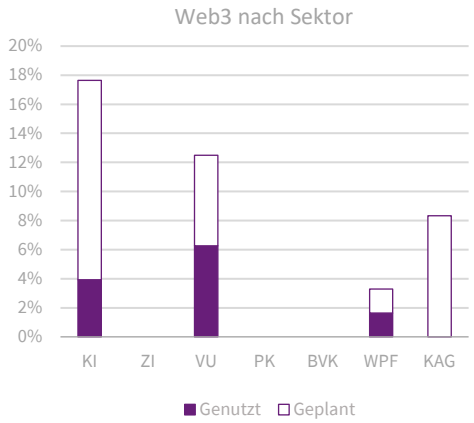
Chancen	■ Durch die Dezentralisierung kann das Vertrauen der Nutzer:innen gestärkt werden, da die Daten transparent verwaltet werden. ■ Veränderung des elektronischen Handels, elektronischer Behördenwege und elektronischer Gesundheitsdienste. ■ Kosteneinsparungen durch die Abschaffung der Mittelsperson bei Transaktionen
Risiken	■ Risiko von vermehrten Cyber-Attacken, beispielsweise auf Schwachstellen in Smart Contracts ■ Web3 ist technisch sehr komplex und kann für weniger technisch affine Nutzer:innen eine erhebliche Hürde darstellen.

Aktuelle Trends und Entwicklungen:

Jeweils nur zwei KI (4%) und zwei VU (6%) nutzen derzeit Web3.

In den nächsten drei Jahren planen weitere sieben KI und zwei VU Web3 zu nutzen, wodurch die Nutzung von KI in Summe auf rund 17% und von VU auf 13% ansteigen wird.

Im Sektor KAG planen zwei (8%) Unternehmen zukünftig die Implementierung von Web3, während PK und BVK weiterhin von der Nutzung dieser Technologie absehen.



6 DIGITALE KOMMUNIKATIONSKANÄLE

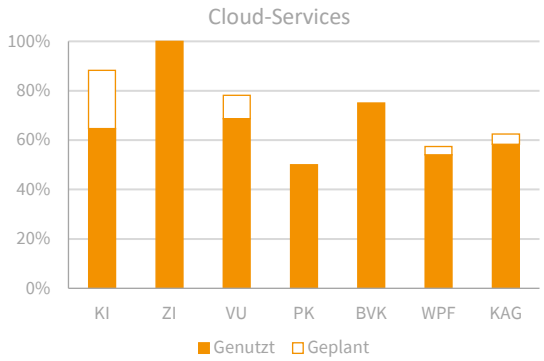
Innovationen im Kundenservice sind einer der Haupttreiber der Digitalisierung am Finanzmarkt. Im Wettbewerb um Vertragsabschlüsse ist es ein Vorteil, Kund:innen über möglichst viele Kanäle ansprechen zu können. Die digitale Kundenbetreuung macht personalisierte Interaktionen, schnellere Reaktionszeiten und proaktive Problemlösung möglich.

- Ein guter Kundenservice wirkt sich positiv auf die Zufriedenheit der Kunden aus, stärkt die **Kundenbindung** und macht die Kund:innen empfänglicher für Cross- und Up-Selling. Zufriedene Kund:innen sind eher bereit, weitere Produkte bzw. Dienstleistungen des Unternehmens in Anspruch zu nehmen.
- Innovationen wie Automatisierung, Selbstbedienungsoptionen und vorausschauende Analysen tragen außerdem zur **betrieblichen Effizienz** bei. Die beaufsichtigten Unternehmen haben dementsprechend in den letzten Jahren ihre digitalen Kommunikationskanäle weiter ausgebaut.
- Auf der Grundlage des Kundenfeedbacks können Unternehmen Trends und Leistungsmetriken ableiten. Der kundenorientierte Ansatz dient somit nicht nur der Verbesserung bestehender Dienste, sondern auch der Entwicklung neuer Produkte und Funktionen, die auf die Bedürfnisse der Kund:innen abgestimmt sind.

Die Trends beim Einsatz digitaler Technologien an der Schnittstelle zu den Kund:innen lassen sich wie folgt zusammenfassen:

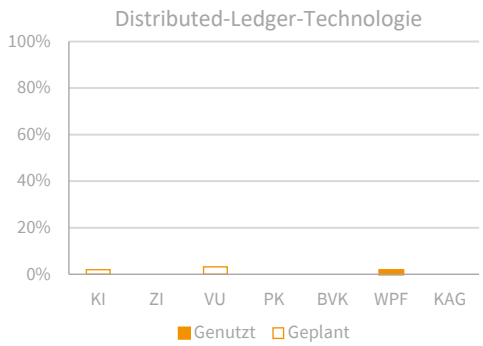
Cloud-Services: Der digitale Wandel hat auch im Vertrieb Veränderungen bewirkt. Die Mehrheit der beaufsichtigten Unternehmen setzt auch an der Kundenschnittstelle auf Cloud-basierte Vertriebslösungen.

Nur jedes zehnte KI plant keinen Einsatz von Cloud-Services an der Schnittstelle zu seinen Kund:innen.



Die **Distributed Ledger Technologie** spielt an der Kundenschnittstelle nach wie vor keine Rolle. Lediglich eine WPF setzt im Bereich Tokenization[4] diese Technologie ein.

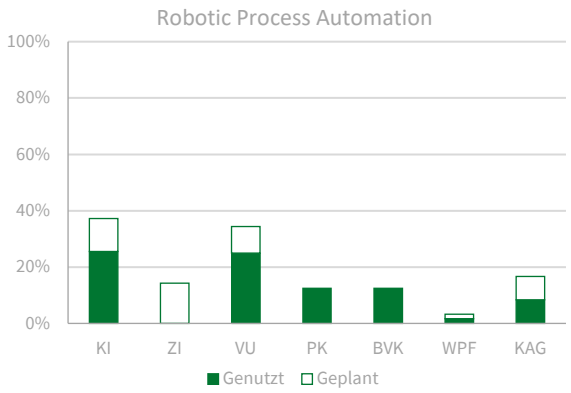
Ein KI und ein VU sind noch dabei zu evaluieren, ob sie diese Technologie in den nächsten drei Jahren einsetzen werden.



[4] *Bei der Tokenisierung wird eine digitale Information durch einen für Dritte wertlosen Ersatz, den Token, ersetzt. Dies erhöht die Sicherheit bei Transaktionen und der Speicherung von sensiblen Informationen.*

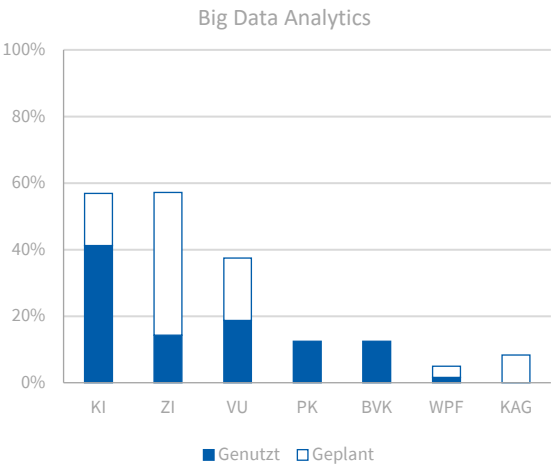
Robotic Process Automation (RPA), mit der Softwareprogramme oder Bots erstellt werden, die sich bei Anwendungen anmelden, Daten eingeben, Aufgaben erledigen und Daten zwischen Anwendungen bzw. Arbeitsabläufen kopieren, wird im Vertrieb aktuell jeweils von 25% der KI und VU genutzt.

Zukünftig planen jeweils nur etwa 1/3 der KI und VU, Robotics im Vertrieb zu nutzen.



Big-Data-Analysen, welche Methoden, Tools und Anwendungen umfassen, die zum Erfassen, Verarbeiten und Ableiten von Erkenntnissen aus großen Hochgeschwindigkeits-Datasets aus verschiedenen Quellen (zB Web, Mobilgeräten, E-Mails, sozialen Medien, vernetzten Geräten) verwendet werden, werden im Vertrieb vor allem von KI (41%) und VU (19%) genutzt.

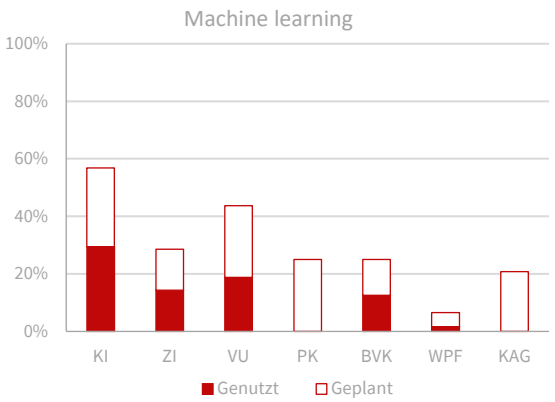
Bis 2027 planen jeweils 60% der KI und ZI und 40% der VU Big-Data-Analytics einzusetzen.



Machine Learning umfasst unterschiedliche Formen des Selbstlernens bei Systemen der Künstlichen Intelligenz und der Robotik, die Regel- und Gesetzmäßigkeiten in den Daten erkennen und Aktionen daraus ableiten.

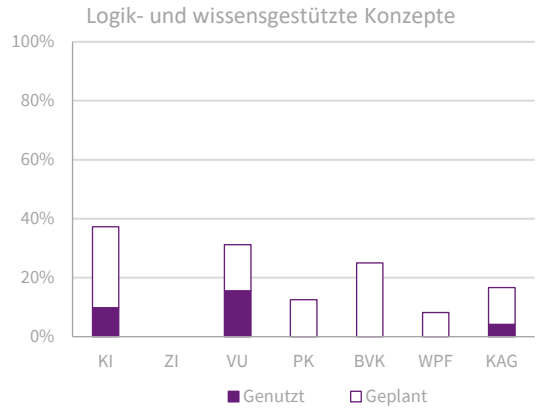
Bei **Deep Learning** werden hierfür große Datenmengen verwendet.

Nur 11% aller beaufsichtigten Unternehmen verwenden aktuell diese Technologie. In den nächsten drei Jahren planen zusätzlich weitere 19% der Unternehmen Machine bzw. Deep Learning im Vertrieb einzusetzen.



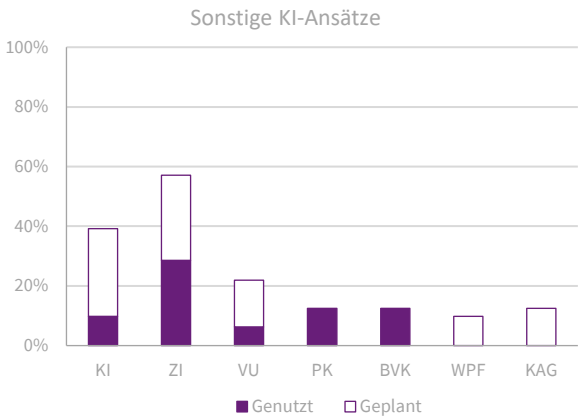
Logik- und wissensgestützte Konzepte (Künstliche Intelligenz), die als Systeme mit einem intelligenten (selbstlernenden) Verhalten ihre Umgebung analysieren und mit einem gewissen Grad an Autonomie handeln, werden aktuell primär von VU (16%) und KI (10%) genutzt.

In den nächsten drei Jahren planen insgesamt etwa ein Drittel der KI und VU, KI-Systeme im Vertrieb einzusetzen. Bei einigen PK, BVK und WPF wird ein zukünftiger Einsatz evaluiert.



Sonstige KI-Ansätze, die zB statistische Ansätze, Bayessche Schätz-, Such- oder Optimierungsmethoden verwenden, werden aktuell vor allem von ZI (29%) genutzt.

Bis 2027 planen etwa 60% der ZI, 40% der KI und 20% der VU sonstige KI-Ansätze an der Schnittstelle zu ihren Kund:innen einzusetzen.



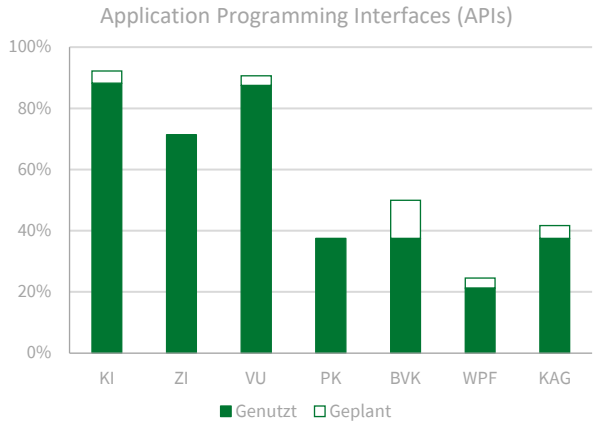
Obwohl in KI-Systemen in vielen Bereichen enormes Potential gesehen wird, sehen die beaufsichtigten Unternehmen in der Kommunikation mit ihren Kund:innen dieses Potential (noch) nicht.

7 DIGITALE SCHNITTSTELLEN

Die Bedeutung von digitalen Schnittstellen wird in Zukunft noch weiter zunehmen. Nach dem Vorschlag der Europäischen Kommission für eine Verordnung über einen Rahmen für den Zugang zu Finanzdaten („Financial Data Access“; FIDA)[5] sollen in Zukunft Inhaber von Kundendaten inkl. Finanzinstitute verpflichtet werden, ihre Kundendaten anderen Finanzinstituten oder Finanzinformationsdienstleistern zur Verfügung zu stellen und die dafür erforderlichen Schnittstellen einzurichten. Die Bereitstellung von Daten im Wege hochwertiger Anwendungsprogrammierschnittstellen (APIs) wird eine wesentliche Voraussetzung für einen nahtlosen Datenzugang in Echtzeit sein. Nach den Vorstellungen der EK wird dieser neue regulatorische Rahmen zu innovativeren Finanzprodukten und -dienstleistungen führen. Damit sollen bisher aufwendige Prozesse, wie Vergleichsdienste oder der Wechsel zu einem neuen Produkt einfacher werden.

Programmierschnittstellen (APIs), dh Programmteile, die von einem Softwaresystem anderen Programmen zur Anbindung an das System zur Verfügung gestellt werden, werden derzeit vor allem von KI, ZI und VU eingesetzt.

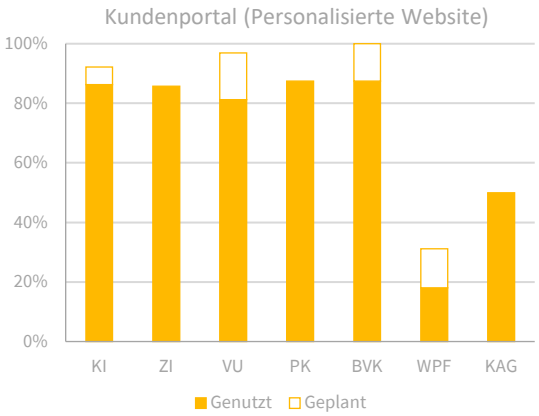
Beaufsichtigte Unternehmen, die APIs aktuell nicht einsetzten, sehen auch in den nächsten drei Jahren keinen Anwendungsbereich.



Online-Portale werden von fast allen Finanzdienstleistern eingesetzt.

Der geringe Anteil der WPF (18%) und KAG (50%), die Kundenportale verwenden, lässt sich unter anderem auf die Besonderheiten ihres Geschäftsmodells zurückzuführen.

Lediglich vier KI, ein ZI, ein VU und eine PK sehen auch zukünftig keinen Anwendungsbereich von Kundenportalen in ihrem Geschäftsmodell.

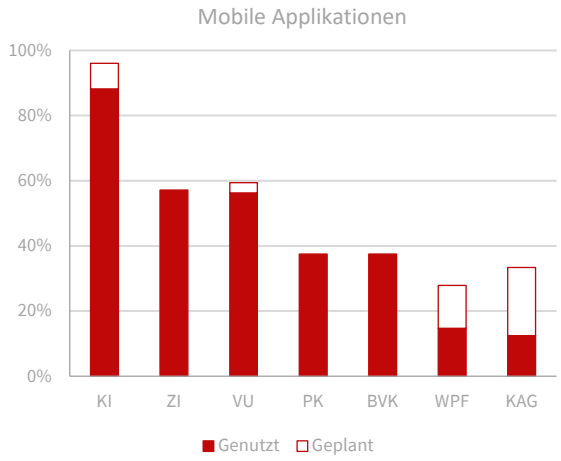


[5] *EK-Vorschlag vom 28.6.2023, COM(2023) 360 final.*

Mobile Applikationen

Vor allem KI bieten ihren Kund:innen mobile Applikationen an, die auf unterschiedlichen Plattformen, u.a. auf Handys, verwendet werden können.

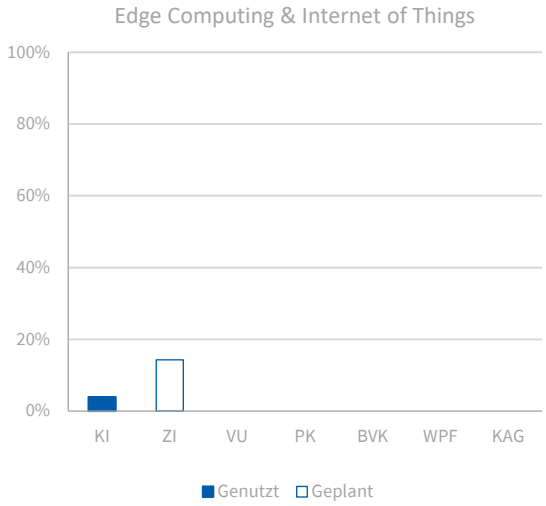
Ein weiterer Ausbau von mobilen Applikationen ist bis 2027 grds. nur von WPF und KAG geplant. Dies entspricht den bisherigen Wahrnehmungen: Auch in Zeiten der Pandemie hat die Nutzung von Apps für mobile Geräte nicht merklich zugenommen, zumal bereits die meisten Unternehmen, die einen Mehrwert in diesen Kommunikationskanälen sehen, sie bereits einsetzten.



Edge Computing bezeichnet im Gegensatz zum Cloud Computing die dezentrale Datenverarbeitung am Rand des Netzwerks, der sog. Edge (auch Local Cloud bzw. Cloudlet genannt).

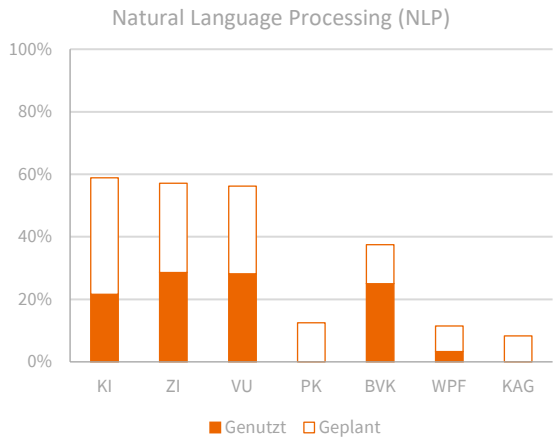
Das **Internet der Dinge (IoT)** ist ein Sammelbegriff für Technologien einer globalen Infrastruktur, die es ermöglicht, physische und virtuelle Objekte miteinander zu vernetzen und sie durch Informations- und Kommunikationstechniken zusammenarbeiten zu lassen.

Edge Computing & Internet of Things im Vertrieb werden nur von 2 KIs genutzt. Darüber hinaus plant 1 ZI, diese Technologien in der Zukunft einzusetzen.



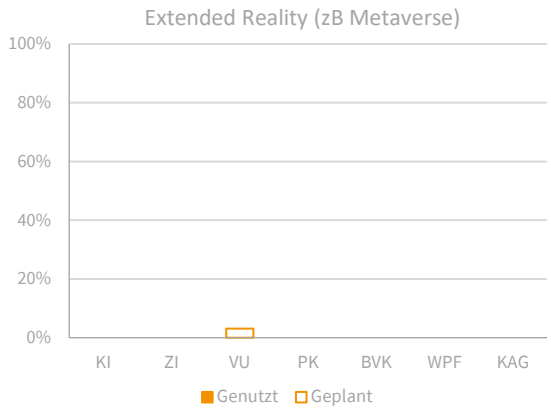
Natural Language Processing (NLP) soll Computer in die Lage versetzen, menschliche Sprache zu „verstehen", zu interpretieren und zu manipulieren. Diese Technologie zur Verarbeitung natürlicher Sprache wird an der Kundenschnittstelle insb. von ZI (29%), VU (28%), BVK (25%) und KI (22%) genutzt.

Bis 2027 wollen beinahe ⅔ der KI, ZI und VU diese Technologie im Vertrieb einsetzen.



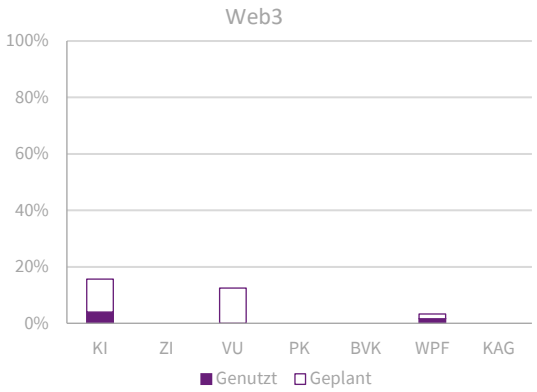
Extended Reality umfasst Technologien, die computergenerierte Umgebungen bzw. Objekte erstellen. Es können sowohl bereits entwickelte als auch in Zukunft etablierte Formen von XR sein. Während Nutzer bei Augmented Reality virtuelle Objekte als Erweiterung der realen Welt wahrnehmen, tauchen User durch den Einsatz von Virtual Reality in eine rein virtuelle Welt ein.

Lediglich ein VU plant, Extended Reality in den nächsten drei Jahren im Rahmen der Kundenkommunikation anzuwenden.



Web 3.0 beschreibt eine von Gavin Wood, einem Mitbegründer von Ethereum, geprägte Idee für eine neue Generation des World Wide Web, das auf der Blockchain-Technologie basiert und damit auf Konzepten wie Dezentralisierung und „tokenbasierter Wirtschaft“ aufbaut.

Lediglich zwei KIs und eine WPF nutzen derzeit Web 3.0; bis 2027 planen weitere 6 KI, 4 VU und eine WPF, Web 3.0 an der Kundenschnittstelle einzusetzen.



8 DIGITALES MARKETING

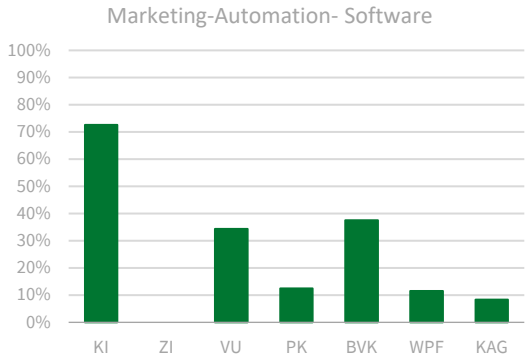
Softwaregestützte Methoden zur Automatisierung von Marketing- und Vertriebsprozessen werden unter den beaufsichtigten Unternehmen immer häufiger eingesetzt. Angefangen bei E-Mail-Newslettern bis hin zu Anzeigekampagnen in Suchmaschinen und sozialen Medien existieren bereits zahlreiche Möglichkeiten, um die Reichweite des eigenen Marketings und somit die Zahl potenzieller Neukund:innen zu vergrößern und den Werbeprozess effizienter zu gestalten.

Konkret befragt wurden die Unternehmen nach automatisiertem Marketing in folgenden Kategorien:

- Personalisierte Website (personalisierte Angebote im Kundenportal)
- Personalisierte Landingpages basierend auf Kundenverhalten
- Social Media (gezielte Werbung basierend auf Kundendaten)
- Online-Werbung (zB Retargeting, Kampagnen in Suchmaschinen etc.)
- E-Mail-Kampagnen (zB automatisierte Newsletter); automatisierte Einladungen zu Veranstaltungen

Marketing-Automation-Software wird vor allem durch KI (73%) und VU (34%) eingesetzt. Aber auch 38% der BVK nutzen bereits automatisiertes Marketing.

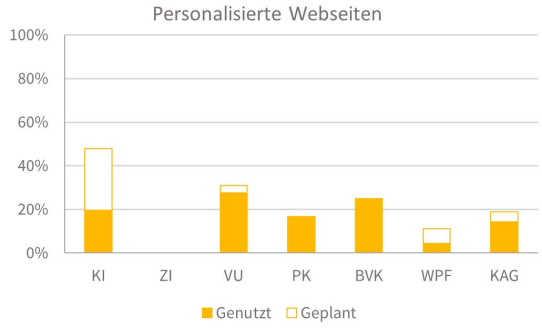
Bei der Marketing-Automatisierung werden Nutzerprofile mit verhaltensbasierten Daten angereichert, um automatisierte Kampagnen für individuelle Kommunikation einzurichten.



Ähnlich wie bei Pre-Sales Kommunikationskanälen 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** (gezielte Werbung auf den von Kund:innen genutzten Kanälen) 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 Kunden-Events) abgestellt.

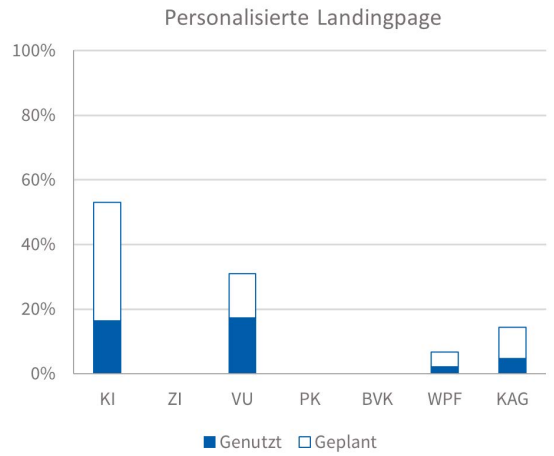
Personalisierte Webseiten (Kundenportale) sind bereits über alle Sektoren hinweg stark verbreitet (siehe dazu Kapitel „Technologien“). Für Zwecke der Marketing-Automatisierung werden personalisierte Webseiten allerdings primär von VU (28%), BVK (25%) und KI (20%) genutzt.

Bis 2027 planen weitere 13 KI, personalisierte Webseiten (zB Kundenportale) für Zwecke der Marketing-Automatisierung neu einzusetzen.



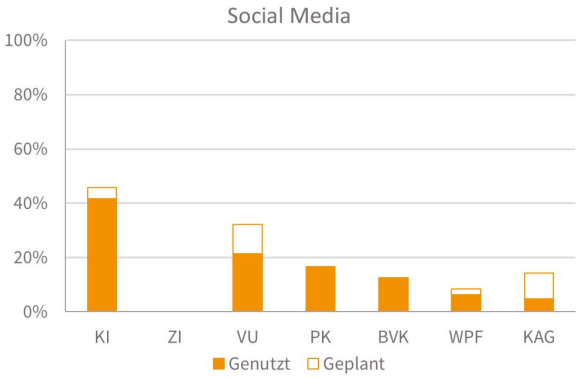
Eine **Landingpage** ist eine speziell eingerichtete Webseite, die nach einem Mausklick auf ein Werbemittel oder nach einem Klick auf einen Eintrag in einer Suchmaschine erscheint. Diese Landingpage ist oftmals auf den Werbeträger und dessen Zielgruppe optimiert.

Vor allem KI und VU planen Landingpage (dh Anzeige angepasster Landingpage-Mutationen in Abhängigkeit davon, auf welches Werbemittel reagiert wurde) zukünftig vermehrt einzusetzen. Bei PK und BVK haben Landingpage aktuell keine Bedeutung, was sich bereits daraus ergibt, dass ihre Kund:innen Unternehmen sind.



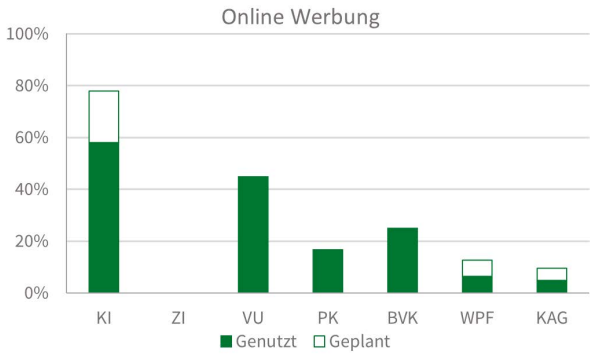
Von den Kund:innen genutzte **Social Media** werden im Rahmen der Vertriebsaktivitäten für Zwecke der Marketing-Automatisierung insb. von KI (42%) und VU (21%) eingesetzt.

Gezielte Werbung wird dabei in Abhängigkeit vom Fortschritt des Nutzers im Marketing-Funnel (ein Marketing-Trichter visualisiert schematisch die Customer Journey aus der Sicht des Unternehmens vom Erstkontakt bis hin zur Bindung des Kunden) eingesetzt.



Mit der **Online-Werbung** (zB Google-Ads im Rahmen von Werbekampagnen) können die passenden Informationen gegeben werden, um so eine Steigerung der Anfragen sowie der Vertragsabschlüsse zu erreichen.

Online-Werbung wird für Zwecke der Marketing-Automatisierung (zB Retargeting, Kampagnen in Suchmaschinen) insb. von KI (58%), VU (45%) und BVK (25%) genutzt.

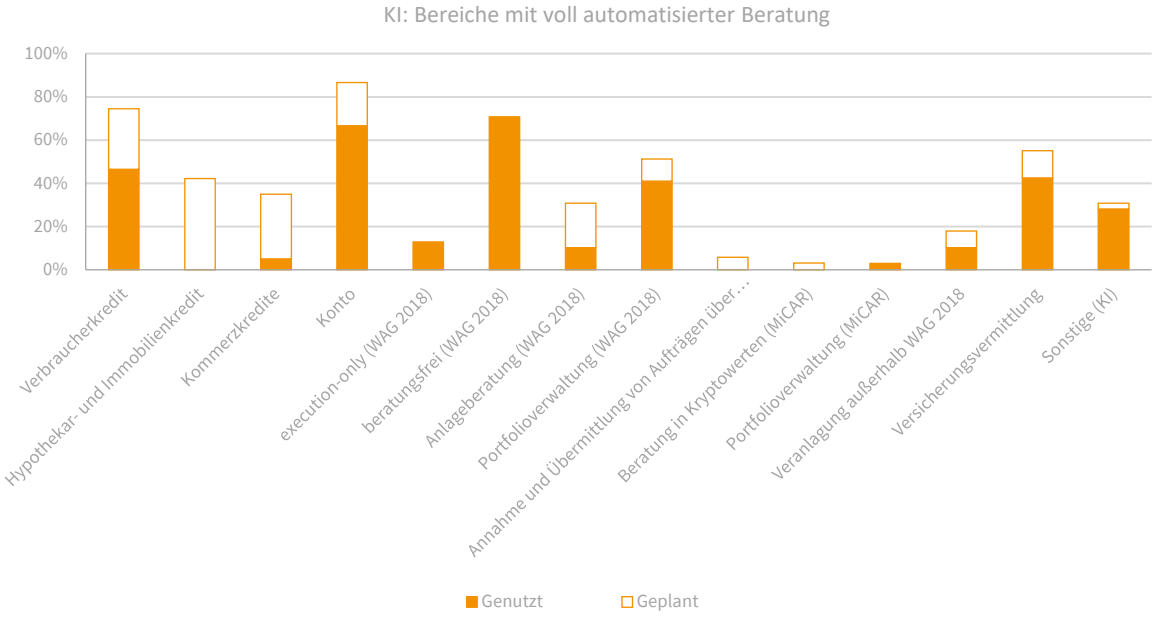


Unter „Andere“ Methoden der Marketing-Automatisierung wurden etwa **Newsletter, E-Mail-Kampagnen** In-Game-Ads, Geburtstags- bzw. Terminerinnerungs-SMS genannt.

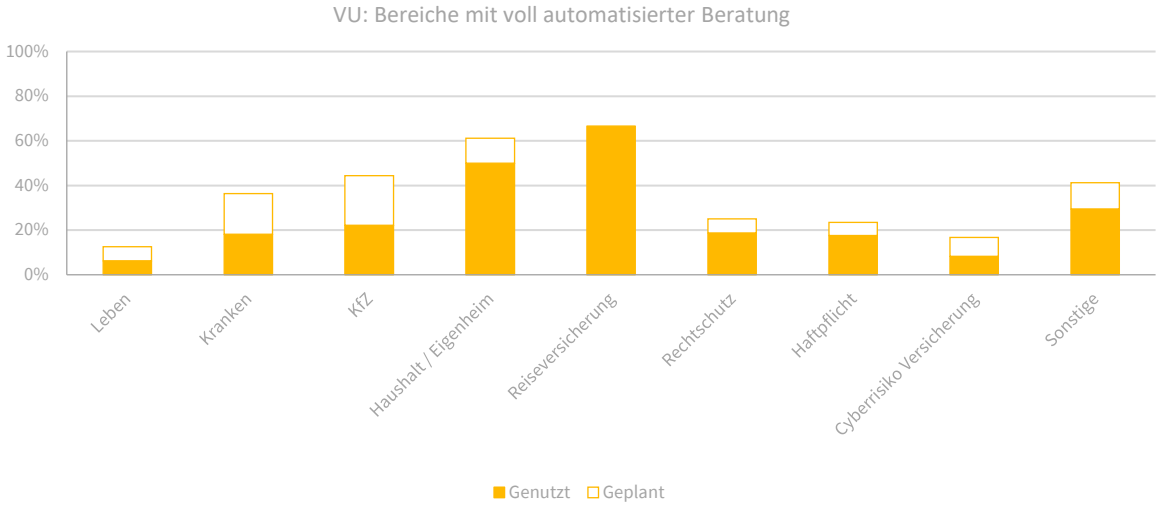
9 DIGITALE BERATUNG

Automatisierte Beratung ist eine Form der Beratung, bei der die Beratung vollständig von einem automatisierten System erstellt wird. Die persönlichen Anforderungen und Informationen des Kunden werden digital analysiert, wonach das automatisierte System die Beratung erstellt und sie dem Verbraucher oder Kunden übermittelt.

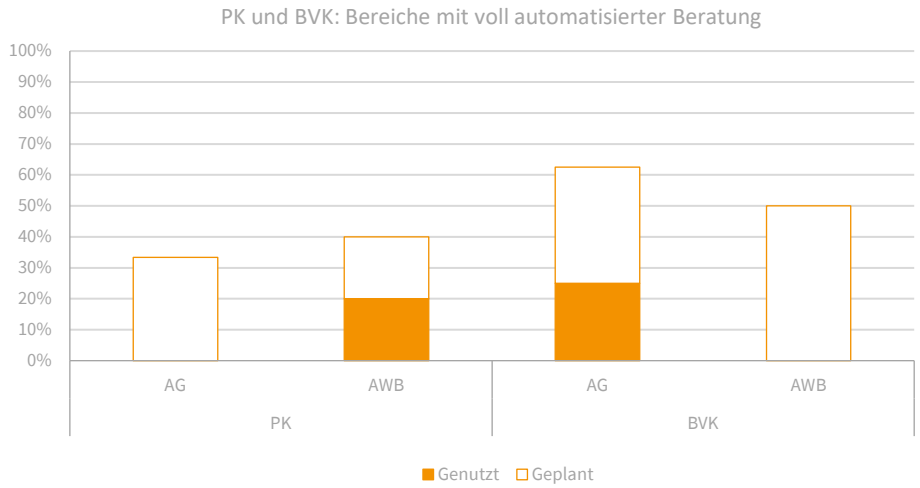
KI bieten eine automatisierte Beratung vor allem in den Bereichen Konto und Verbrauchkrediten an. In den nächsten drei Jahren werden insb. im Bereich Hypothekar-, Immobilien- und Kommerzkredite Erweiterungspotentiale gesehen.



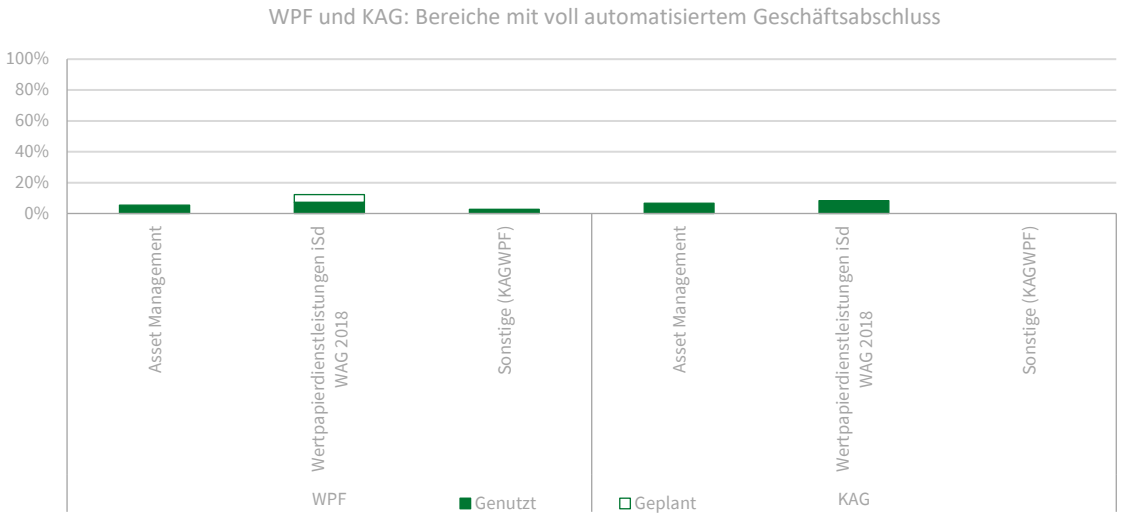
Im Bereich der Reiseversicherung bieten bereits 2/3 der VU, die dieses Produkt vertreiben, Abschlüsse mit einer voll automatisierten Beratung an. Diese erfolgen oftmals online mit einer Reisebuchung. In der Kranken- und KFZ-Versicherung wird bis 2027 mit einem weiteren signifikanten Anstieg der automatisierten Beratung gerechnet.



Bei PK planen ca. 30% der PK zukünftig dem Arbeitgeber eine automatisierte Beratung anzubieten. Eine Arbeitnehmerberatung wird aktuell von 20% aller PK zur Verfügung gestellt und soll zukünftig ausgebaut werden. Die BVK planen ebenfalls einen Ausbau der automatisierten Beratung.



Bei den WPF und KAG wird eine eine automatisierte Beratung aktuell nur von sehr wenigen Unternehmen angeboten. Lediglich bei Wertpapierdienstleistungen gemäß WAG 2018 wird in den nächsten drei Jahren mit einem Anstieg beim automatisierten Geschäftsabschluss, wenngleich nur im geringen Ausmaß, gerechnet.

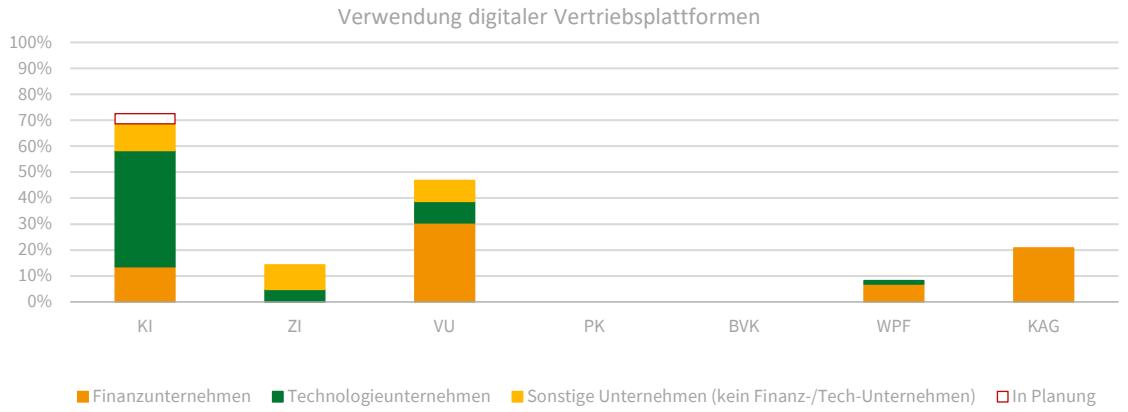


10 DIGITALE VERTRIEBSPLATTFORMEN

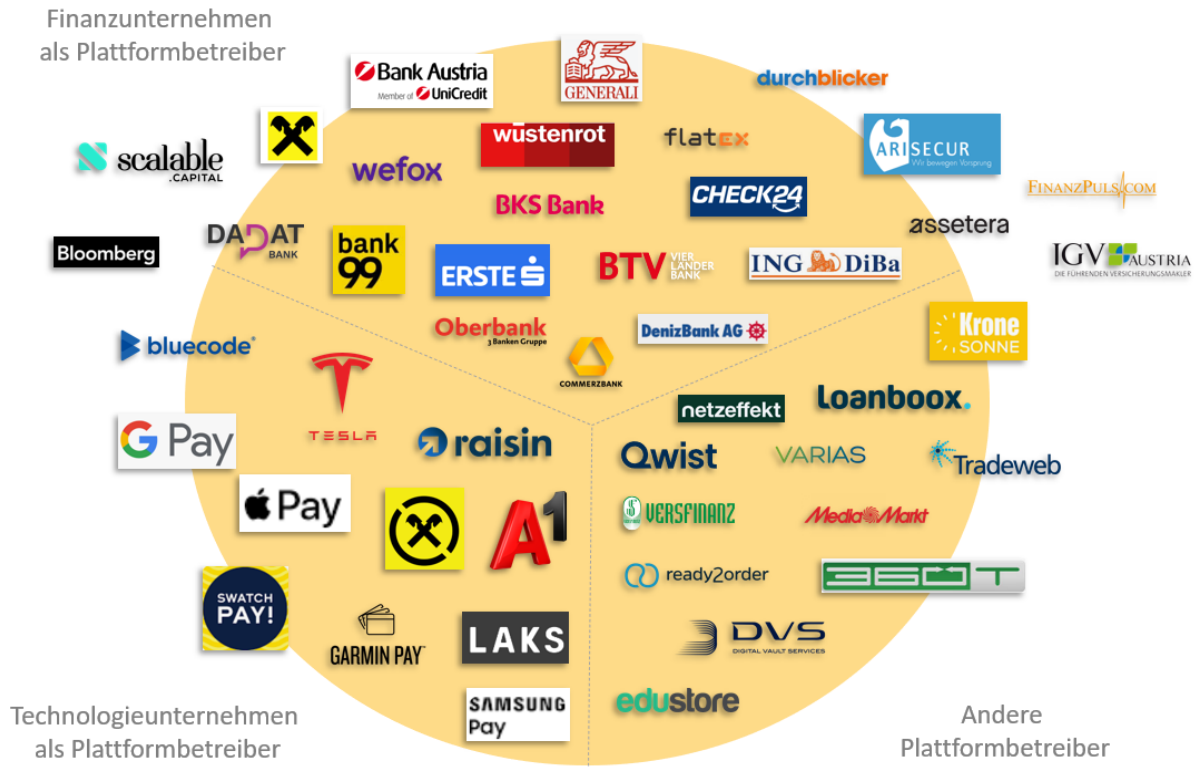
Eine digitale Vertriebsplattform bündelt verschiedene Informationen und Services für (potentielle) Kund:innen. Die traditionellen Vertriebswege allein reichen nicht mehr aus, um den sich verändernden Kundenbedürfnissen gerecht zu werden. Der digitale Vertrieb bietet eine Vielzahl von Möglichkeiten, um die eigene Kosteneffizienz und gleichzeitig die Kundenzufriedenheit zu steigern.

Die zunehmende Digitalisierung erleichtert und fördert die Nutzung von digitalen Vertriebsplattformen. Datenschutz und Sicherheitsbedenken gehen aber einher, ebenso wie die steigende Komplexität der Vertriebsabläufe. Zudem erfordert die Umstellung auf einen digitalen Vertrieb eine Anpassung der Unternehmenskultur und der Arbeitsweisen.

Am häufigsten werden folgende Vertriebsplattformen genutzt:

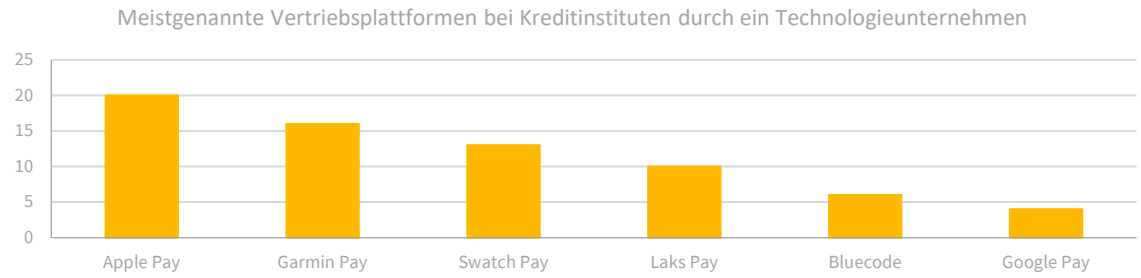


Landkarte der digitalen Vergleichsplattformen in Österreich

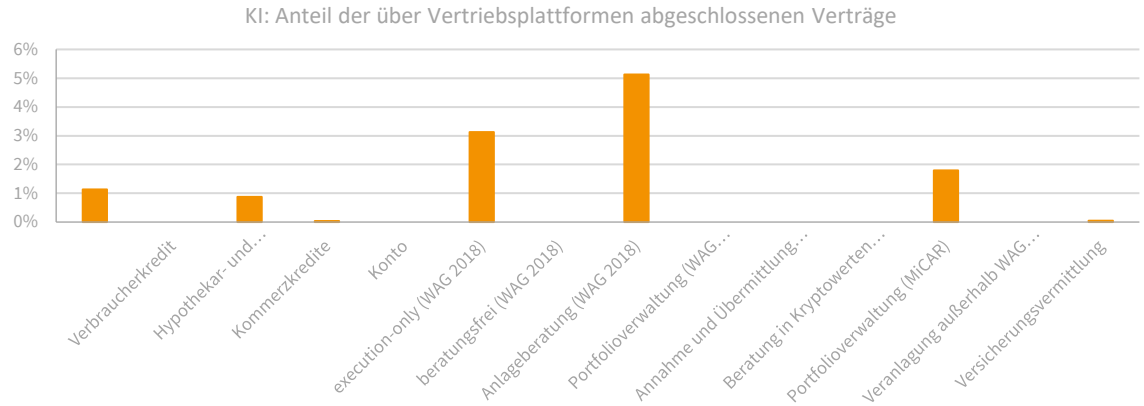


Das Etablieren von digitalen Vertriebsplattformen verdeutlicht das Voranschreiten der Digitalisierung im Vertriebsprozess, andererseits unterstreicht diese Entwicklung auch die wachsende Bedeutung von Kooperationen zwischen beaufsichtigten Unternehmen und digitalen Dienstleistern.

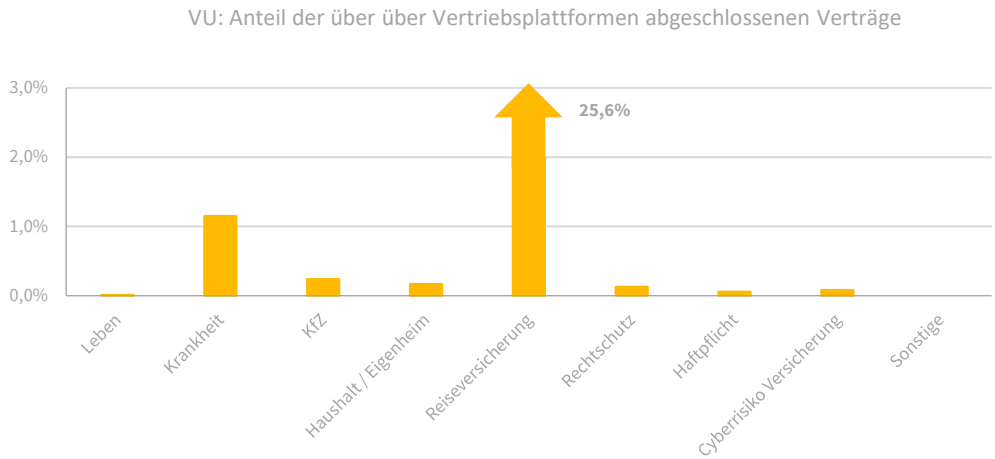
Lediglich bei den KI zeigt sich eine **Konzentration** bei den digitalen Zahlungssystemen.



Obwohl fast 70% aller KI Vertriebsplattformen in irgendeiner Form verwenden, erfolgt nur eine geringe **Anzahl an Vertragsabschlüssen** über diese, wie die nachfolgende Statistik für das Jahr 2023 zeigt.



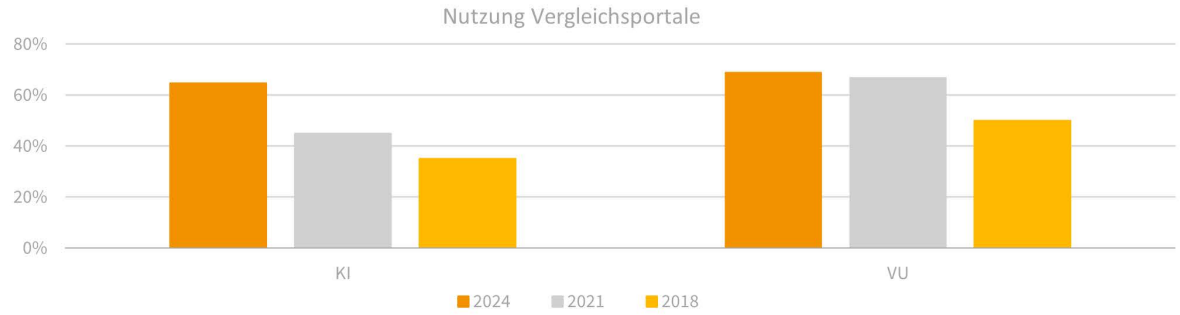
Bei VU ist der Anteil der Vertragsabschlüsse über Vertriebsplattformen nur bei der Reiseversicherung markant. 2023 wurden über diese Vertriebsschiene ca. 26% der Verträge abgeschlossen. Alle anderen Geschäftszweige in der Versicherungsbranche, wie im folgenden Diagramm ersichtlich, weisen eine Abschlussrate über Vertriebsplattformen von ca 1% bzw. wesentlich weniger auf.



11 VERGLEICHSPORTALE

Ein Vergleichsportal ist eine Online-Plattform, die es den Verbrauchern ermöglicht, Produkte oder Dienstleistungen verschiedener Anbieter miteinander zu vergleichen und ggf. ein Produkt bzw. Dienstleistung online zu erwerben. Diese Plattformen dienen als zentraler Ort, an dem Kunden verschiedene Optionen auf einen Blick sehen können.

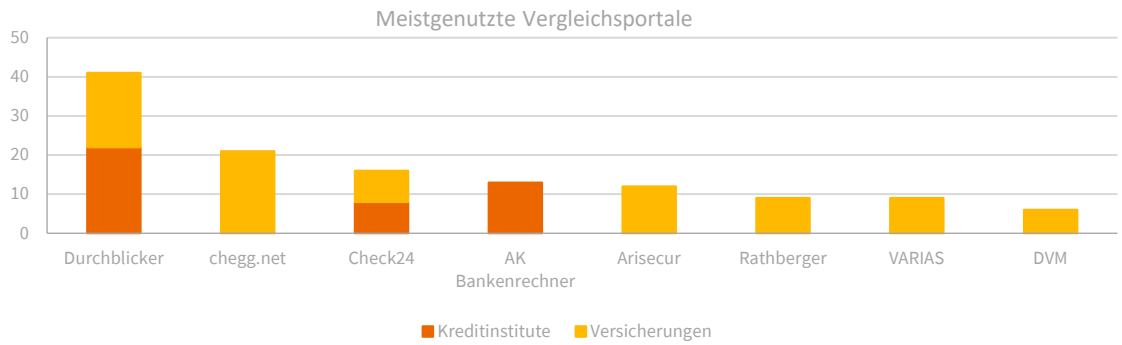
Vergleichsportale haben stark an Bedeutung gewonnen: während 2018 im Grunde nur VU und KI ihre Produkte listen ließen, setzten sich Vergleichsportale über die letzten Jahre praktisch in allen Sektoren als Pre-Sales-Instrument durch. Die starke Konkurrenz im Bereich Pre-Sales ist hier möglicherweise ein wichtiger Faktor. Potentielle Kund:innen und Dienstleister können sich über Vergleichsportale einfach über Dienstleistungen und Produkte informieren und stehen im Zuge dessen oftmals bereits nahe an einem Geschäftsabschluss. Wenn konkurrierende Unternehmen mit Vergleichsportalen kooperieren, steigt auch der Druck, die eigenen Produkte in Vergleichsportalen zu listen.



Die beaufsichtigten Unternehmen nutzen zahlreiche unterschiedliche Vergleichsportale. Insgesamt wurden 60 unterschiedliche Vergleichsportale angegeben. Über alle Sektoren hinweg entfällt jedoch der mit Abstand größte Nutzeranteil auf „Durchblicker.at“.

- VU setzen insb. auf „chegg.net“, „Durchblicker.at“, „Arisecur“ und „Rathberger“.
- KI sind ebenfalls vorwiegend über „Durchblicker.at“ und den Bankenrechner der Arbeitskammer Österreich in Vergleichsportale eingebunden.
- PK und BVK werden auf Vergleichsportalen des VKI, der GPA sowie „Mercer“ und „Greco“ gelistet.
- In den Sektoren der KAG und WPF spielen Finanzinformationsunternehmen wie Morningstar und Bloomberg im Rahmen von Vergleichsmöglichkeiten die größte Rolle.
- Aktuell plant kein Unternehmen, welches aktuell noch keine Vergleichsportale verwenden, zukünftig welche zu nutzen.

Die 8 meistgenannten Vergleichsportale werden von KI und VU genannt.

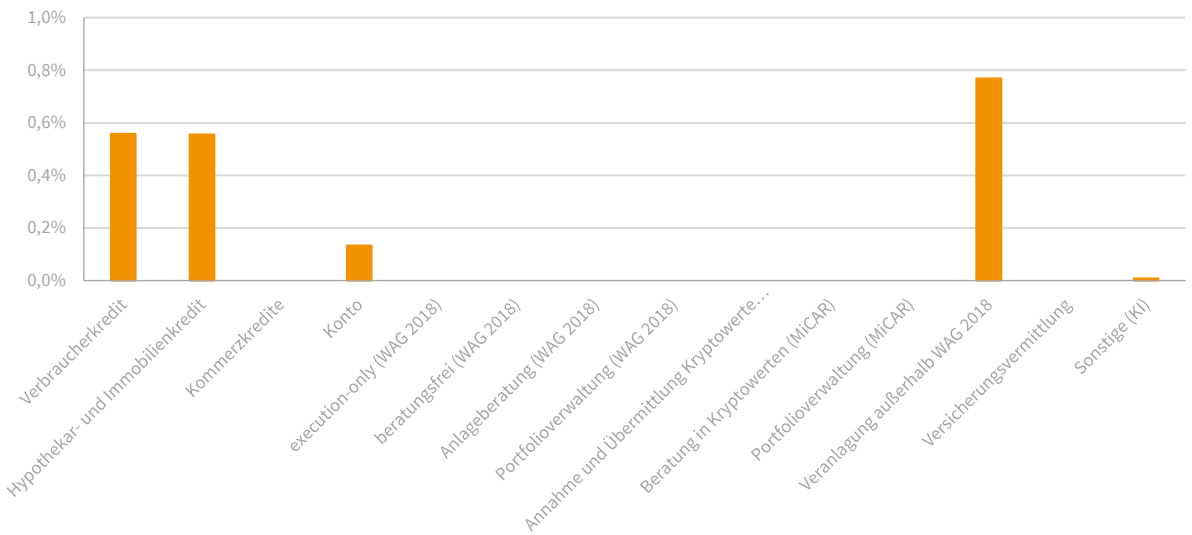


Landkarte der Vergleichsportale in Österreich

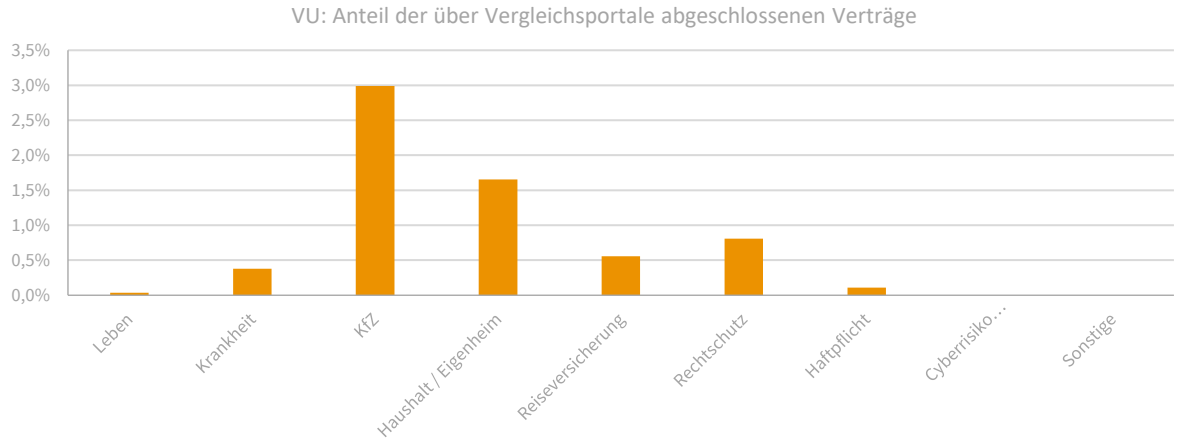
Der prozentuelle **Anteil des Absatzes über Vergleichsportale** und Vertriebsplattformen liegt bei den meisten Unternehmen nach wie vor im einstelligen Prozentbereich oder darunter. Hier kann jedoch in den nächsten Jahren ein weiteres Wachstum erwartet werden. Mit steigender Nutzung von Vergleichsportalen steigt implizit auch der Bedarf an Fairness und Transparenz dieser Anbieter.

Wie aus dem folgenden Diagramm ersichtlich, ist der Anteil der im Jahr 2023 über Vergleichsportale abgeschlossenen Verträge bei KI weiterhin sehr niedrig, und dies obwohl über 60% der KI Vergleichsportale verwenden.

KI: Anteil der über Vergleichsportale abgeschlossenen Verträge



Auch im Versicherungssektor werden zwar Vergleichsportale von fast 70% der VU verwendet, der Anteil der im Jahr 2023 über Vergleichsportale abgeschlossenen Verträge bei Versicherungen bleibt aber auch hier sehr niedrig.



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.[6]

[6] *FMA, Informationsbroschüre Vergleichsportale im Versicherungssektor - FMA Österreich*

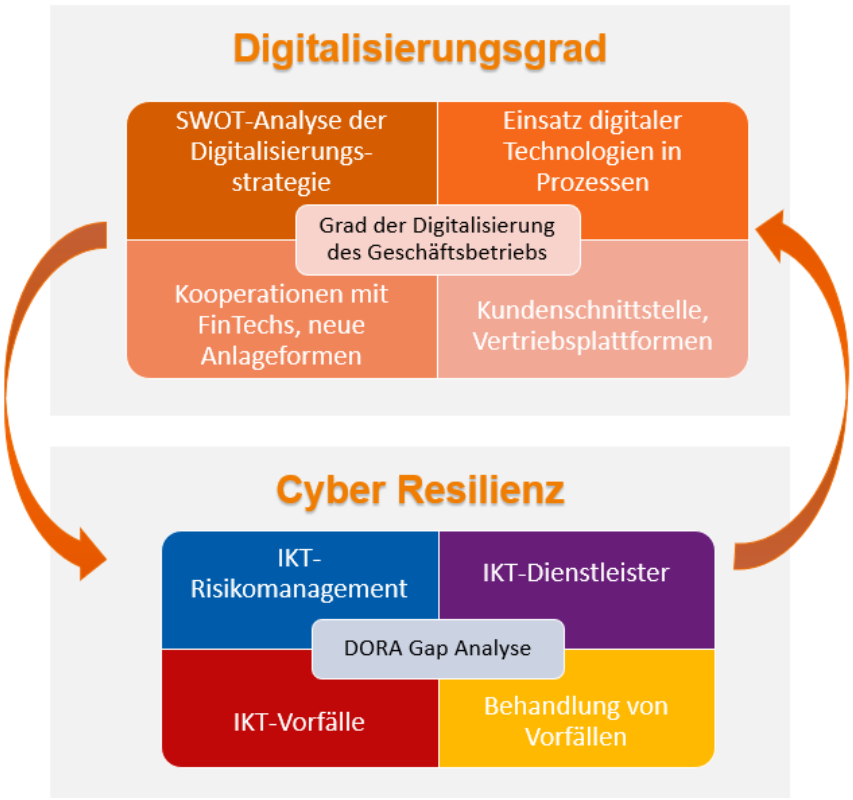
12 CYBER RESILIENZ / DORA-GAP-ANALYSE

Zur Stärkung der digitalen operationalen Resilienz am österreichischen Finanzmarkt setzt die FMA seit 2019 innovative Aufsichtsinstrumente ein, mit denen sie die Widerstandsfähigkeit der beaufsichtigten Unternehmen gegenüber Cyberbedrohungen und Betriebsstörungen überprüft. Ein Instrument der „FMA Cyber Security Toolbox“ ist auch das von der FMA entwickelte **Cyber Maturity Level Assessment**.

Im Zuge der Ermittlung der Austrian Digital Finance Landscape hat die FMA anhand der DORA-Vorgaben evaluiert, inwieweit die Maßnahmen der Unternehmen zur Prävention und Detektion von Cybervorfällen und Betriebsstörungen die **DORA-Anforderungen an die digitale operationale Resilienz** reflektieren.

Dieser Aufsichtsschwerpunkt hat den beaufsichtigten Unternehmen die Möglichkeit gegeben, die unternehmensinterne Implementierung der neuen regulatorischen Vorgaben kritisch zu hinterfragen und bei Bedarf gezielt weitere Verbesserungen vorzunehmen. Der FMA hat die Durchführung dieser DORA-Gap-Analyse wiederum ermöglicht,

- die digitalisierungsgetriebenen Entwicklungen und Abhängigkeiten am Finanzmarkt in die (individuelle) Risikobeurteilung und die Priorisierung der Aufsichtsagenden einfließen zu lassen,
- die Aufsichtsintensität der einzelnen beaufsichtigten Unternehmen risikoadäquat zu bestimmen und ggf. zielgerichtete präventive Maßnahmen zu ergreifen und
- die für den ö Finanzmarkt relevanten IKT-Dienstleister zu identifizieren.

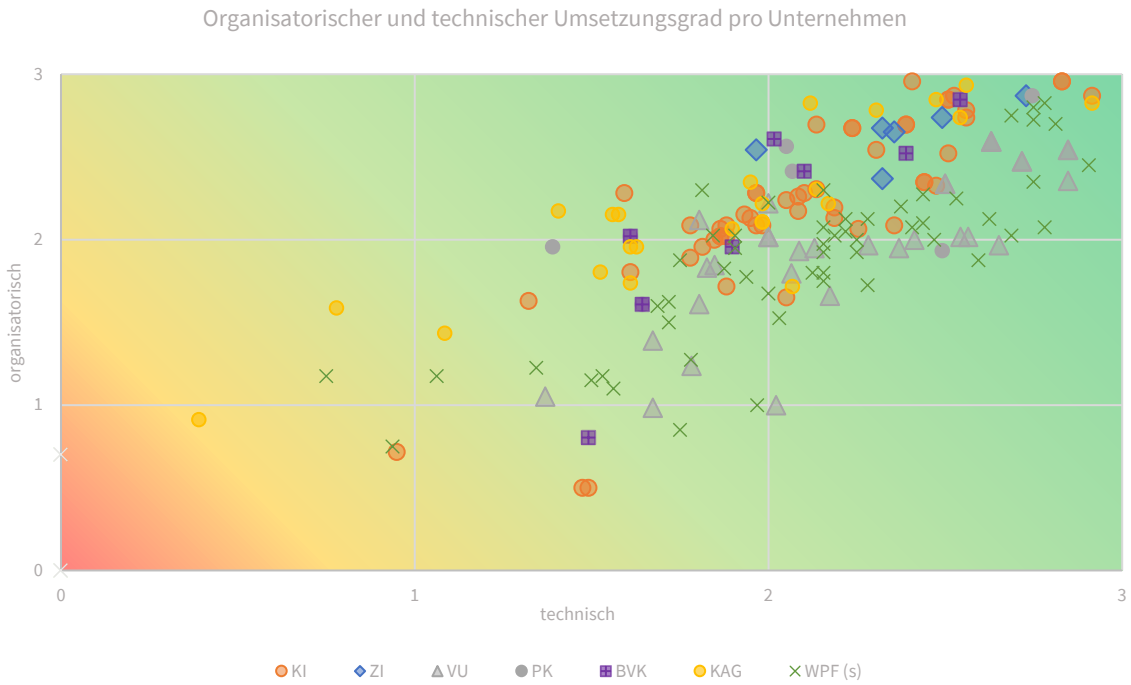


Zahlreiche Vorgaben von DORA sind grundsätzlich proportional anzuwenden. Um beurteilen zu können, in welcher Ausprägung die einzelnen Anforderungen zu erfüllen sind, ist jedoch zunächst das eigene digitale Risikoprofil bzw. der **Grad der Digitalisierung des Geschäftsbetriebs** zu ermitteln.

DORA legt umfassende Vorgaben zum Umgang mit IKT-Risiko fest. Die vorgeschriebenen Maßnahmen sind teilweise aus vorhandenen sektoralen Vorgaben oder internationalen Standards bekannt, gehen teilweise aber auch über diese hinaus. Sowohl organisatorische als auch technische Maßnahmen sind enthalten, wobei es zwei Varianten des DORA-IKT-Risikomanagementrahmens gibt:

- den vollen IKT-Risikomanagementrahmen, welcher alle Vorgaben enthält und in Österreich von den meisten beaufsichtigten Unternehmen anwendbar ist;
- den vereinfachten IKT-Risikomanagementrahmen, in welchem einige besonders aufwändige Maßnahmen gestrichen oder abgewandelt wurden. Diese Variante ist in Österreich vor allem von den meisten kleineren Wertpapierfirmen anwendbar.

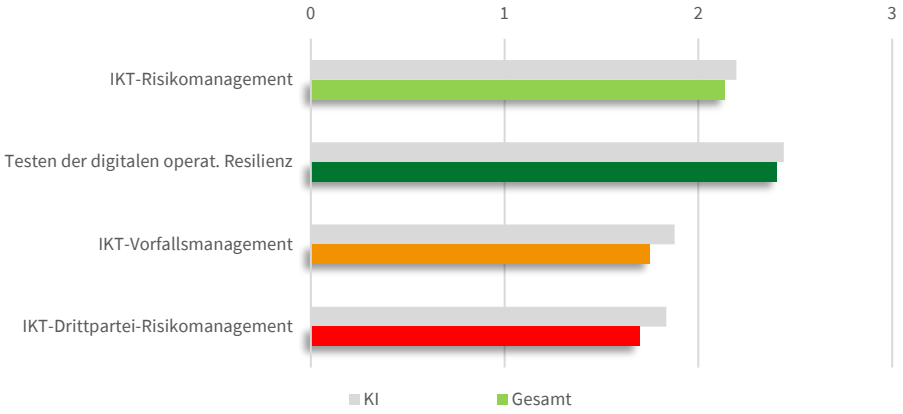
Auf der vierteiligen Reifegradskala (Anforderungen voll erfüllt [3], geringfügiger Anpassungsbedarf [2], starker Anpassungsbedarf [1], Umsetzung erforderlich [0]), hat die DORA-Gap-Analyse bei betroffenen Unternehmen beider Versionen des DORA-IKT-Risikomanagementrahmens ergeben, dass der österreichische Finanzmarkt **im Aggregat die wesentlichsten Vorkehrungen zur Sicherstellung der DORA-Compliance getroffen** hat, wenngleich es im Sommer 2024 bei der Erfüllung der organisatorischen und technischen Vorgaben („Umsetzungsgrad“) individuell noch deutliche Unterschiede gab.



Wesentliche Erkenntnisse:

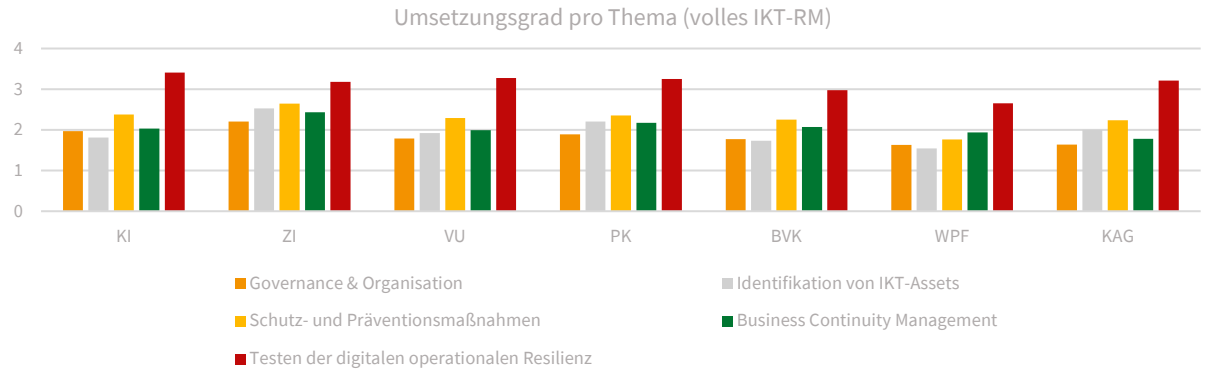
- Allgemein befinden sich die Durchschnittswerte der meisten Unternehmen im oberen Segment der Grafik und sind in ihren DORA-Vorbereitungen schon relativ weit fortgeschritten.
- Es sind, bis auf einen recht hohen Umsetzungsgrad bei ZI, keine besonderen Trends in Bezug auf die einzelnen Finanzmarktsektoren erkennbar.
- Die Spannweite der Ergebnisse ist relativ groß, einige Unternehmen haben ihre DORA-Vorbereitungen schon beinahe abgeschlossen, andere haben noch vergleichsweise viele offene Punkte zu adressieren.

Das **Ranking der Themenbereiche** zeigt, dass der größte Handlungsbedarf beim IKT-Drittpartei-Risikomanagement und IKT-Vorfallsmanagement besteht:



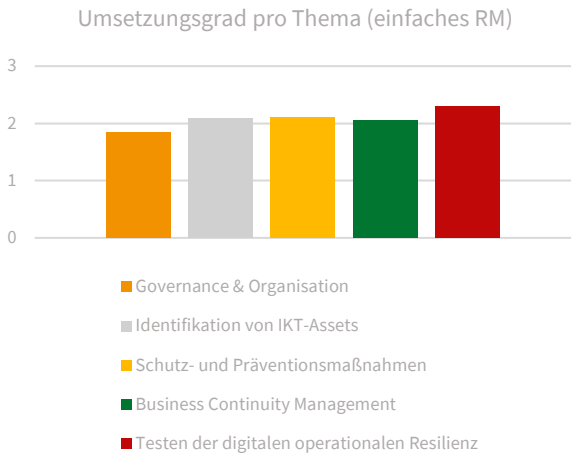
12.1 IKT-RISIKOMANAGEMENT

Die wichtigsten Maßnahmen im Bereich IKT-Risikomanagement wurden von den meisten Unternehmen bereits getroffen, sodass hier im Aggregat nur ein relativ geringfügiger Anpassungsbedarf besteht. Der größte Handlungsbedarf besteht noch bei der Umsetzung der Vorgaben betreffend Governance & Organisation sowie die Inventarisierung von IKT-Assets.



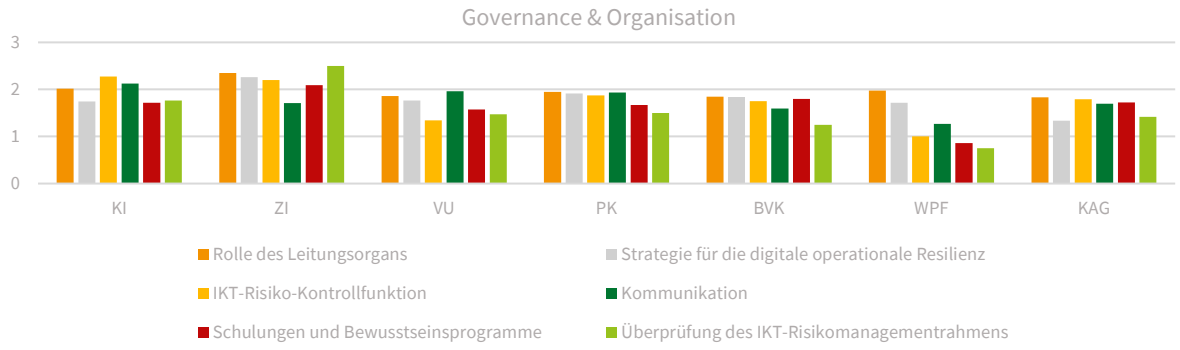
In Puncto Governance sind teilweise noch dokumentarische Aufgaben und Freigaben der Geschäftsleitung offen; bei der Inventarisierung der IKT-Assets teilweise auch noch umfangreichere technische Umsetzungen.

Die Aufstellung der Unternehmen, die einem vereinfachten Risikomanagementrahmen unterliegen, hat zu ähnlichen Gesamtergebnissen geführt. Dies legt nahe, dass die betroffenen Unternehmen trotz der Vereinfachungen noch einige Aufgaben zu bewältigen haben.

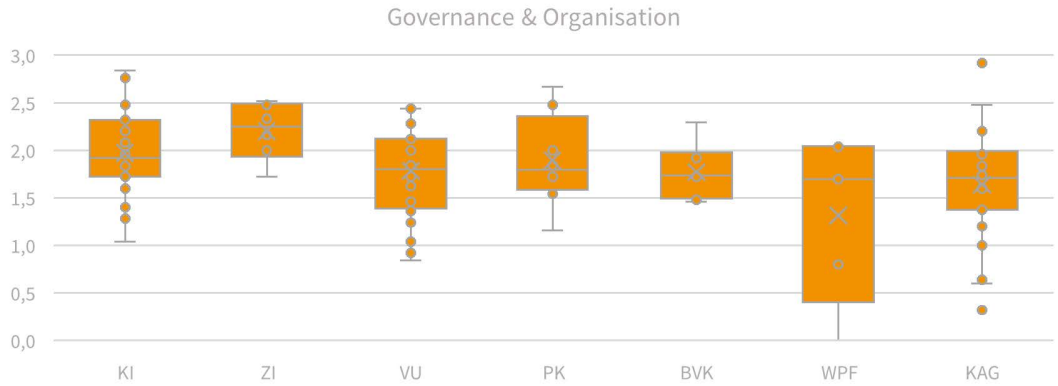


12.1.1 GOVERNANCE & ORGANISATION

Innerhalb des Themenbereichs Governance & Organisation haben Finanzunternehmen insgesamt einen Schwerpunkt auf Anforderungen betreffend die **Rolle des Leitungsorgans** und **Kommunikation** gelegt und erreichen bei diesen Subthemen vergleichsweise hohe durchschnittliche Scores.

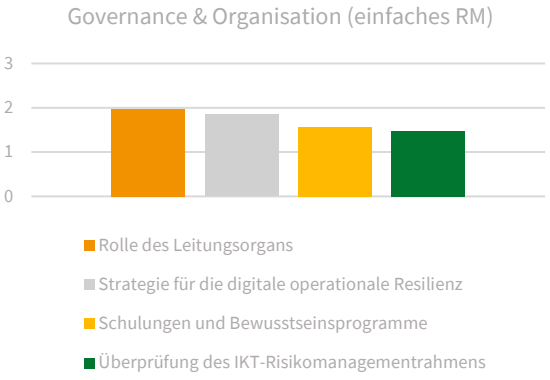


Demgegenüber wird insb. noch an der **Überprüfung des Risikomanagementrahmens** gearbeitet. Insb. WPF und KAG weisen in Teilbereichen Aufholbedarf auf.



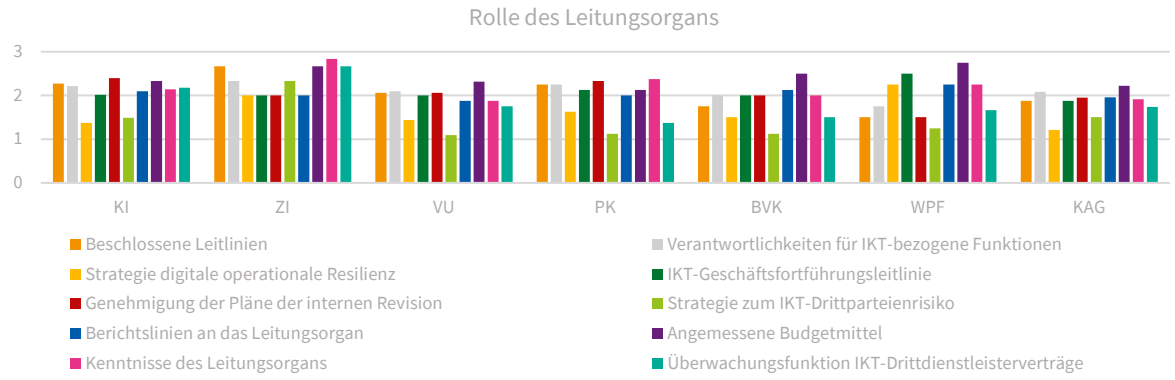
Vergleichbare, wenngleich reduzierte Vorgaben, sind im „vereinfachten“ IKT-Risikomanagementrahmen enthalten, welcher in Österreich insb. auf kleinere WPF anwendbar ist.

Wie die Graphik rechts zeigt, sind die Ergebnisse grob vergleichbar mit jenen der anderen Finanzsektoren, die dem „vollen“ IKT-Risikomanagementrahmen unter DORA unterliegen. Die betroffenen Unternehmen haben mitunter jedoch deutlich weniger Ressourcen als andere Finanzmarktteilnehmer zur Verfügung, sodass die detaillierte Umsetzung eine nicht zu unterschätzende Herausforderung darstellt, auch wenn erste Schritte bereits erfolgt sind.



12.1.1.1 Rolle des Leitungsorgans

Anforderungen bezüglich der Rolle des Leitungsorgans zeigen insgesamt geringfügigen Anpassungsbedarf, wobei insb. die Strategien für die digital operationale Resilienz und jene zum IKT-Drittparteienrisiko noch auszuarbeiten bzw. zu beschließen sind.



Themenbereiche mit einem bloß geringfügigen Anpassungsbedarf:

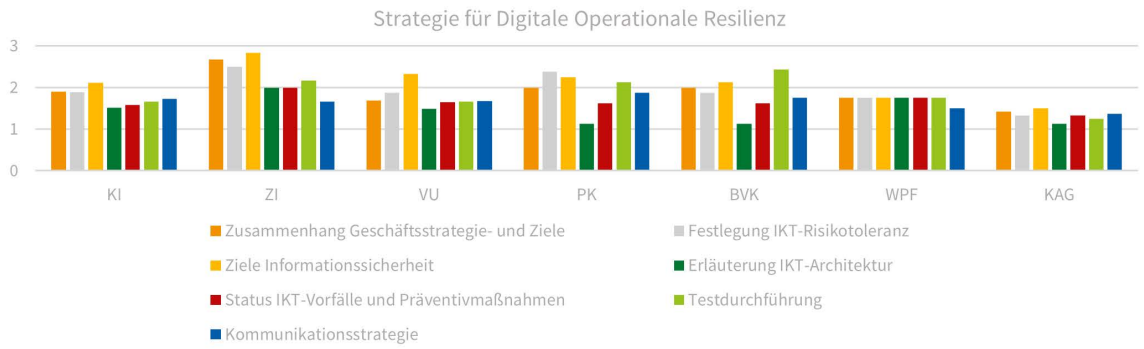
- **Leitlinien**, die auf die Aufrechterhaltung hoher Standards bzgl. Verfügbarkeit, Authentizität, Integrität und Vertraulichkeit von Daten abzielen, wurden bereits verbreitet beschlossen. In diesen wird zB nunmehr auch Authentizität, welche auf die Vertrauenswürdigkeit der Datenquelle abstellt, explizit thematisiert.
- Bei der **IKT-Geschäftsfortführungsleitlinie** besteht meist nur noch geringfügiger Anpassungsbedarf. WPF weisen hierzu den höchsten Score von durchschnittlich 2,5 aus.
- Ein ähnliches Bild zeigt sich hinsichtlich der Genehmigung der **Pläne der internen Revision** in Bezug auf die Prüfungen im IKT-Bereich für 2025 bzw. die darauffolgenden Jahre (bei mittelfristigen Prüfplänen). Vor allem KI, PK und VU haben diese Erfordernisse schon größtenteils umgesetzt.
- IZm der Sicherstellung, dass Kenntnisse und Fähigkeiten des Leitungsorgans aktiv auf aktuellem Stand gehalten werden, sollen beispielsweise **Schulungsprogramme** bezüglich DORA teils noch erweitert werden.
- Auch Aufgaben und Verantwortlichkeiten für alle **IKT-bezogenen Funktionen** sowie angemessene Governance-Regeln wurden schon verbreitet festgelegt.
- Geringfügiger Anpassungsbedarf besteht meist bezüglich eingerichteter **Berichtslinien**, die es dem Leitungsorgan ermöglichen, ordnungsgemäß über IKT-Drittdienstleister, Erkenntnisse zu Tests der digitalen operationalen Resilienz, IKT-bezogene Vorfälle und Herausforderungen bei der Aktivierung von IKT-Geschäftsfortführungsplänen und IKT-Reaktions- und Wiederherstellungsplänen informiert zu werden. Beispielsweise werden diese Anforderungen im Rahmen des Security Committees umgesetzt.
- Eine **Funktion zur Überwachung der Verträge mit IKT-Drittdienstleistern** ist teils noch einzurichten oder ein Mitglied der Geschäftsleitung ist mit dieser Funktion noch zu betrauen. Unternehmen evaluieren beispielsweise, ob das Konzept des Outsourcing-Managements und die zugehörige Definition des Risikoverantwortlichen für alle IKT-Verträge umgesetzt werden kann. Am intensivsten haben sich schon ZI mit diesen Fragestellungen beschäftigt; sie erreichen bezüglich dieser Anforderungen im Vergleich mit den anderen Sektoren den höchsten durchschnittlichen Score.
- **Angemessene Budgetmittel** zur Erfüllung der Anforderungen an die digitale operationale Resilienz gemäß DORA sind grundsätzlich zugewiesen. Anforderungen wurden zum Beispiel über die jährlichen Budgetierungen erfüllt. WPF und ZI weisen für diese Frage die höchsten durchschnittlichen Scores aus.

Themenbereiche mit dem größten Ausbaubedarf:

Verbesserungsbedarf zeigt sich insb. bei den folgenden Strategien für die digitale operationale Resilienz und der Strategie zum IKT-Drittparteienrisiko.

- Bei der **Strategie für die digitale operationale Resilienz** (einschließlich IKT-Risiko-Toleranzschwellen) weisen WPF und ZI bei einem Ranking der Sektoren die höchsten Werte, die auf durchschnittlich geringfügigen Anpassungsbedarf hinweisen, aus. Die sonstigen Ergebnisse zeigen, dass solche Strategien, bzw. teils noch IKT-Risikotoleranzschwellen, zu entwickeln und zu beschließen sind.
- Die zu beschließende **Strategie zum IKT-Drittparteienrisiko**, welche Leitlinien zur Nutzung von IKT-Dienstleistungen zur Unterstützung kritischer oder wichtiger Funktionen, die von IKT-Drittdienstleistern bereitgestellt werden, umfasst, weist in der Kategorie „Rolle des Leitungsorgans“ den kleinsten durchschnittlichen Score auf. Beispielsweise verweisen VU, PK, BVK auf starken Anpassungsbedarf, der auch im Rahmen von DORA-Projekten adressiert wird.

12.1.1.2 Strategie für die digitale operationale Resilienz



DORA verlangt, dass die beaufsichtigten Unternehmen ein strategisches Dokument zum Thema operationale Resilienz führen, welches u.a. folgende Punkte umfasst:

- Überblick zu Strategie, Zielen und Aufbau der IT,
- Ziele, Messbarkeit und Tests der Informationssicherheit,
- Statusbild in Bezug auf IKT-Vorfälle und Präventionsmaßnahmen.

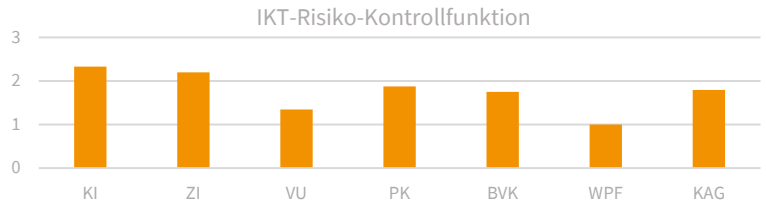
Diese Punkte sollen insb. mit der Geschäftsstrategie und dem Risikomanagement des Unternehmens abgestimmt sein.

Der Umsetzungsgrad diesbezüglich ist insgesamt mit einem durchschnittlichen Gesamtwert von 1,7 noch nicht so weit fortgeschritten wie bei anderen Themen.

- Die Kommentare legen nahe, dass hier oft schon Inhalte vorhanden sind, durch DORA aber erweitert und neu strukturiert werden müssen.
- In einigen Umsetzungsprojekten werden auch bewusst zuerst technische Themen bearbeitet, bevor die strategische Dokumentation nachgezogen wird.

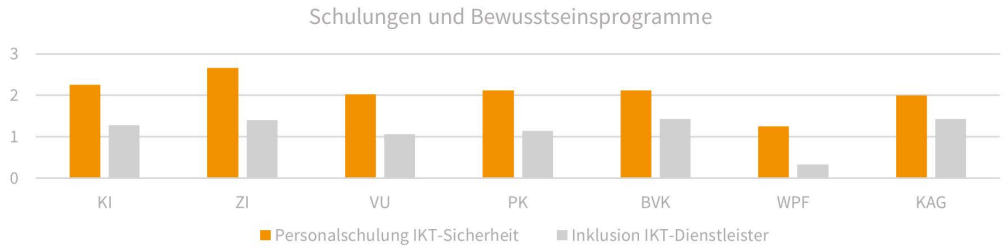
12.1.1.3 IKT-Risiko-Kontrollfunktion

DORA sieht eine eigene Kontrollfunktion für IKT-Risiko vor, welche spezifisch für das Management des IKT-Risiko zuständig ist. Sie existiert konzeptuell getrennt von Enterprise Risk Management und der internen Revision, auch wenn personelle Überschneidungen mit ersterem nicht ausgeschlossen werden.



Der aktuelle durchschnittliche Umsetzungsgrad von 1,9 reflektiert, dass einerseits viele Unternehmen eine Chief Information Security Officer (CISO) Position eingerichtet hatten, welche diese Aufgaben wahrnehmen wird, andererseits aber insb. kleinere Unternehmen Schwierigkeiten haben, eine solche Stelle zu schaffen, zu besetzen und ihre operationale Unabhängigkeit zu gewährleisten.

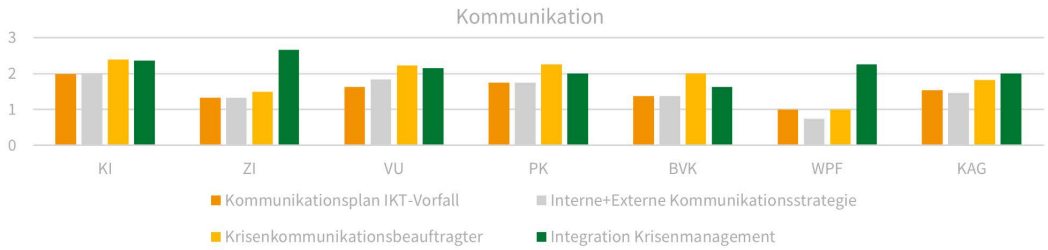
12.1.1.4 Schulungen und Bewusstseinsprogramme



Ähnlich wie die internationalen Standards verlangt auch DORA **Programme für Personalschulungen**, die a) Programme zur Sensibilisierung für IKT-Sicherheit und b) Schulungen zur digitalen operationalen Resilienz umfassen. Diese Programme und Schulungen gelten für alle Beschäftigten und die Geschäftsleitung und sind so komplex, dass sie deren jeweiligem Aufgabenbereich angemessen sind (Art. 13 Abs 6 DORA-VO). Mit einem Durchschnittswert von über 2 in beinahe allen Sektoren sind interne Schulungsprogramme zumeist schon etabliert und müssen allenfalls noch an DORA angepasst werden. Die beaufsichtigten Unternehmen führen hierfür Schulungsmaßnahmen u.a. in Form von e-Learnings, Informationsveranstaltungen, TownHall (Informationsveranstaltungen des Top Management an die Mitarbeitenden) durch. Schulungsmaßnahmen werden zielgruppenspezifisch adressiert.

DORA verlangt aber auch, dass gegebenenfalls auch **Mitarbeitende von IKT-Drittdienstleistern** auf Basis einer vertraglichen Vereinbarung über die Nutzung von IKT-Dienstleistungen in solche Schulungsprogramme eingebunden werden. Es zeigte sich, dass zahlreiche beaufsichtigte Unternehmen hier vor allem mit dieser zweiten Anforderung auf Schwierigkeiten und Unklarheiten stoßen. Schulungen für Dienstleister gibt es im Regelfall bislang nicht, sodass bezüglich der praktischen Implementierung dieser Maßnahme oft Unsicherheiten herrschen. Angesichts der DORA-Vorgabe, IKT-Drittdienstleister eventuell in die eigenen Schulungsprogramme aufzunehmen, müssen künftig vertragliche Vereinbarungen über die Nutzung von IKT-Dienstleistungen ggf. Bedingungen für die Teilnahme dieser Dienstleister an den von den Finanzunternehmen angebotenen Programmen zur Sensibilisierung für IKT-Sicherheit und Schulungen zur digitalen Resilienz umfassen.

12.1.1.5 Kommunikation

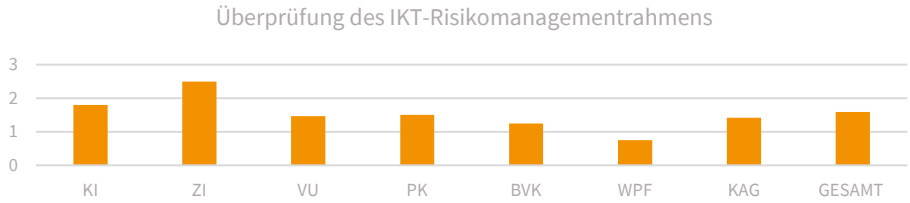


In DORA wird der aktiven Kommunikation bei IKT-Vorfällen und Krisen ein hoher Stellenwert eingeräumt. Insb. müssen

- **Kommunikationsstrategien** gegenüber eigenem Personal sowie externen Stakeholdern und
- **Pläne für den Ernstfall** vorliegen, die (je nach Sachlage) die Offenlegung zumindest schwerwiegender IKT-bezogener Vorfälle oder Schwachstellen gegenüber den folgenden Adressaten vorsieht: a) den Kund:innen, b) den anderen Finanzunternehmen, c) der Öffentlichkeit, und
- Verantwortlichkeiten (ein **Krisenkommunikationsbeauftragter** ist zu benennen, der in Umsetzung der Kommunikationsstrategie die Aufgabe gegenüber der Öffentlichkeit und den Medien wahrnimmt) sowie
- organisatorische Schnittstellen mit dem Krisenmanagement (die **Krisenmanagementfunktion** legt bei Aktivierung von a) IKT-Geschäftsfortführungsplänen und b) IKT-Reaktions- und Wiederherstellungsplänen Verfahren für die Abwicklung der internen und externen Krisenkommunikation fest) definiert sein.

Der durchschnittliche Umsetzungsgrad von 2,0 reflektiert, dass Kommunikationsstrategien in einigen Unternehmen enthalten, oft aber nicht so umfassend wie unter DORA vorgesehen sind, oder noch rein im Krisenplan integriert vorliegen. Einige kleinere Unternehmen haben darauf hingewiesen, dass die Anforderungen iZm den vorgesehenen Rollen und Verantwortlichkeiten sinngemäß umgesetzt werden können, sich aber aufgrund der Unternehmensgröße teilweise Überschneidungen ergeben.

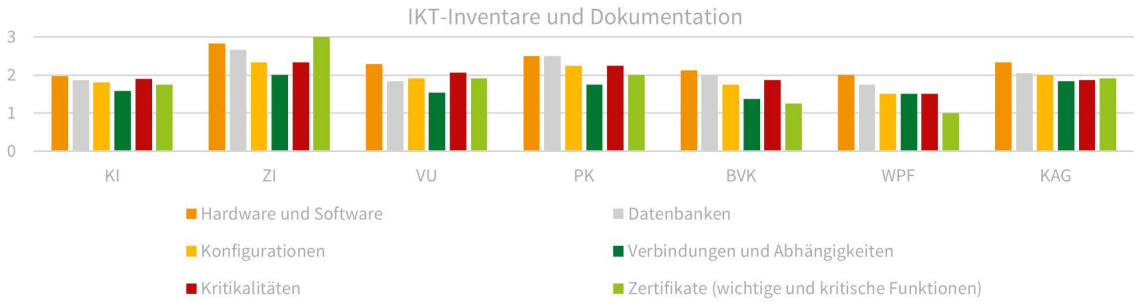
12.1.1.6 Überprüfung des IKT-Risikomanagementrahmens



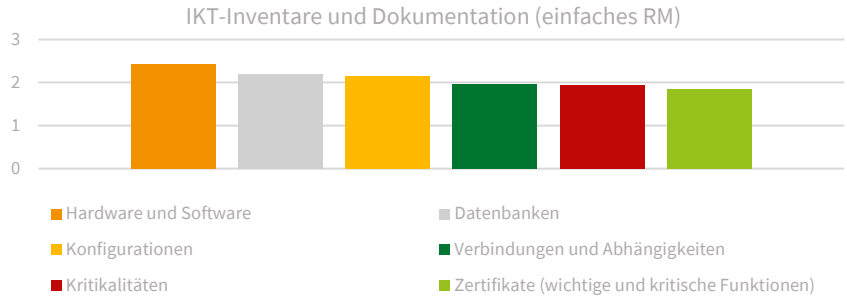
DORA sieht die regelmäßige Erstellung eines **Berichtes zum IKT-Risikomanagementrahmen** des Unternehmens vor. Um diesen Bericht erstellen zu können, ist ein **tourlicher Reviewprozess** zu Risikomanagement inklusive Sicherheitsmaßnahmen und Bedrohungslage nötig.

Dieser ist bei vielen Unternehmen noch nicht gänzlich etabliert bzw. auf die DORA-Vorgaben angepasst, wie der durchschnittliche Umsetzungsgrad zeigt. Bei einigen Unternehmen scheint dieser und andere organisatorische Aspekte der DORA-Umsetzung hinter den technischen Arbeiten eingereiht zu sein.

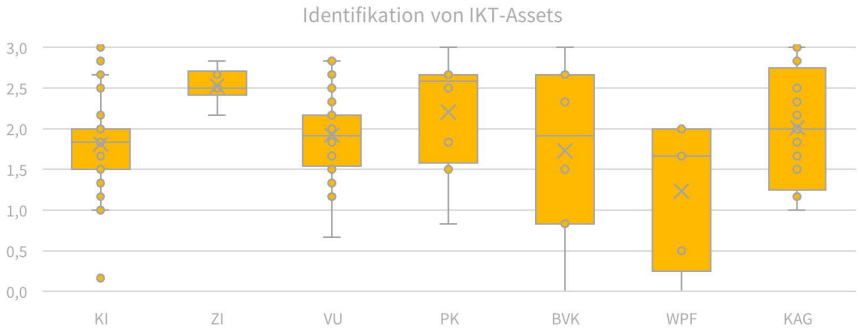
12.1.2 IDENTIFIKATION VON IKT-ASSETS



Aktuelle Inventare der genutzten **Daten, Hardware und Software** sind eine notwendige Basis für die meisten IKT-Sicherheitsmaßnahmen. Die meisten beaufsichtigten Unternehmen verfügen bereits über umfassende Hardware- und Softwareinventare. Unter DORA sind allerdings nicht nur diese grundlegenden Inventare zu führen. Als zusätzliche Informationen zu den Assets sind hier auch **Konfigurationen, Abhängigkeiten, Kritikalitäten** und **Zertifikate** zu erfassen. Die zusätzlich zu erfassenden Informationen sind oft noch nicht oder in unterschiedlichsten Systemen (zB Lizenzmanagement) vorhanden und noch zu ergänzen oder zu zentralisieren. Die Erfahrung aus der Aufsichtspraxis legt überdies nahe, dass nicht alle Unternehmen über ein Inventarisierungstool verfügen, in welchem all diese Informationen abbildbar und über automatisierte Schnittstellen aktualisierbar sind. Teilweise lässt sich dies möglicherweise auf die umfangreiche Nutzung von IKT-Dienstleistern zurückführen.



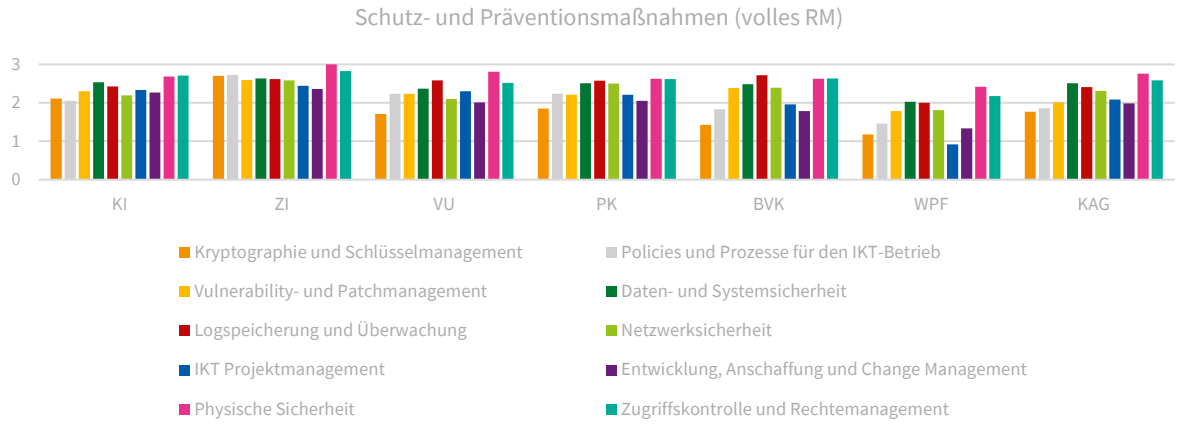
Die Verteilung der Umsetzungsgrade weisen auf eine große Spannweite des DORA-Umsetzung hin, insb. in jenen Finanzsektoren, welche in höherem Maße kleinere Unternehmen umfassen:



Die Vorgaben für die Inventarisierung der IKT-Assets gelten auch für den vereinfachten IKT-Risikomanagementrahmen. Die Unternehmen, die diesem Regime unterliegen, weisen einen ähnlichen Vorbereitungsstand auf diese neuen DORA-Anforderungen auf.

12.1.3 SCHUTZ- UND PRÄVENTIONSMAßNAHMEN

Zu Schutz- und Präventionsmaßnahmen zählen unterschiedlichste technische Sicherheitsmaßnahmen sowie bestimmte organisatorische Aspekte der IKT-Sicherheit. Mit wenigen Ausnahmen und gewissen Unterschieden zwischen den Sektoren ist hier bereits ein relativ hohes Umsetzungsniveau gegeben:

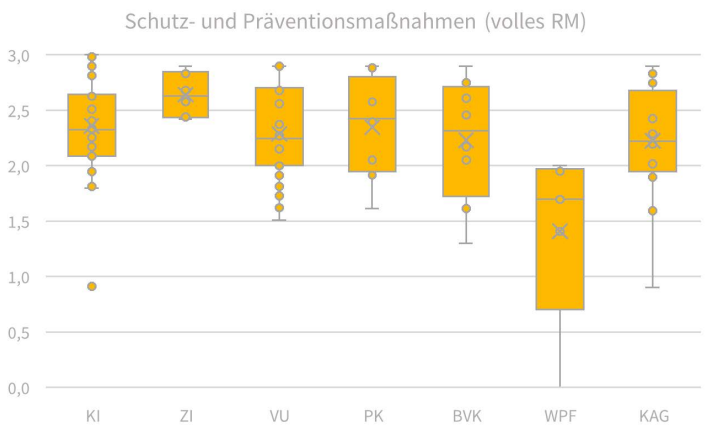


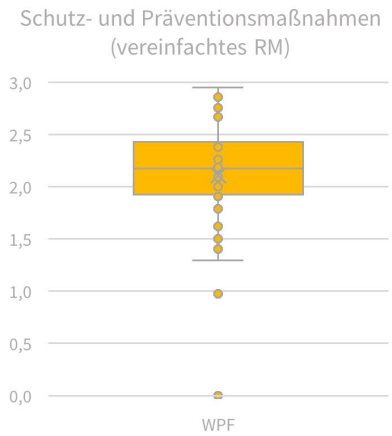
Anforderungen, die auch in etablierten IKT-Sicherheitsframeworks und/oder sektoralen Vorgaben gestellt werden, sind hier regelmäßig bereits weitgehend umgesetzt.

- **Kryptographie, Projektmanagement** und **Changemanagement** gehören dagegen im von DORA vorgeschriebenen Maße nicht zu den gängigen Leitlinien.
- Einige Vorgaben sind überdies sehr umfangreich (zB **Einsatz eines effektiven Systems zur aktiven Überwachung von Logs**), sodass auch Unternehmen mit hohem Durchschnittsscore hier möglicherweise noch große Herausforderungen zu bewältigen haben.

Sektoral fallen, wie auch in anderen Bereichen von DORA, die Zahlungsdienstleister positiv auf (durchschnittlicher Umsetzungsgrad 2,6), während die zur Umsetzung des vollen Risikomanagementrahmens verpflichteten Wertpapierfirmen noch einen gewissen Aufholbedarf haben.

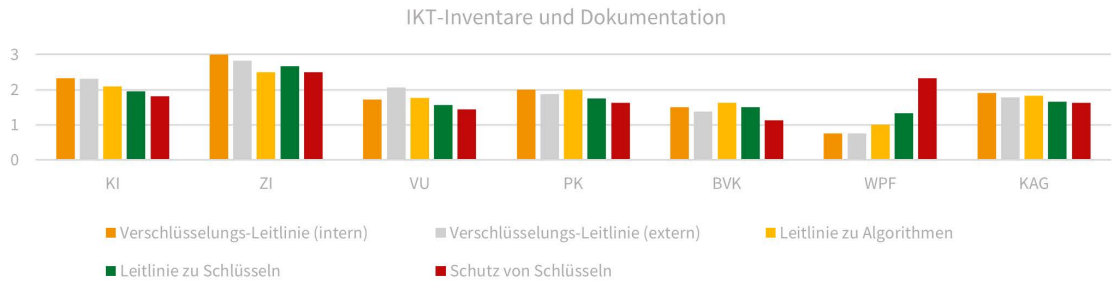
Abseits von den Durchschnittswerten ist hier auch die große Spanne an Ergebnissen festzuhalten:





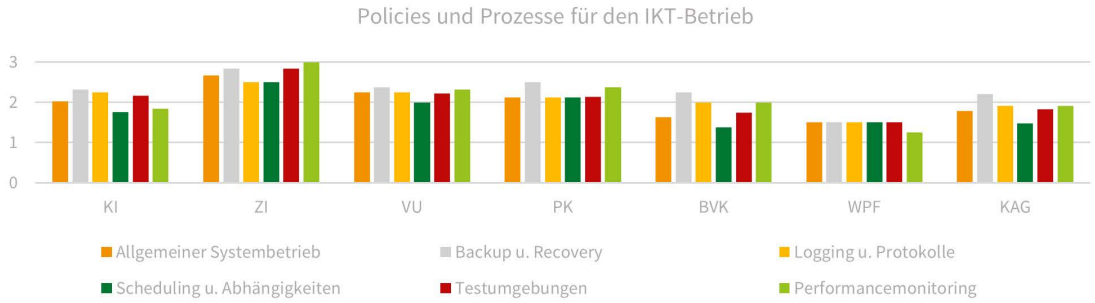
Bei einigen Unternehmen sind die Vorbereitungen auf DORA schon weitgehend abgeschlossen, während sich bei anderen noch deutlich mehr Maßnahmen erst in Umsetzung befinden. Hiervon scheinen Institute in allen Finanzmarktsektoren in ähnlichem Ausmaß betroffen zu sein.

12.1.3.1 Kryptographie und Schlüsselmanagement



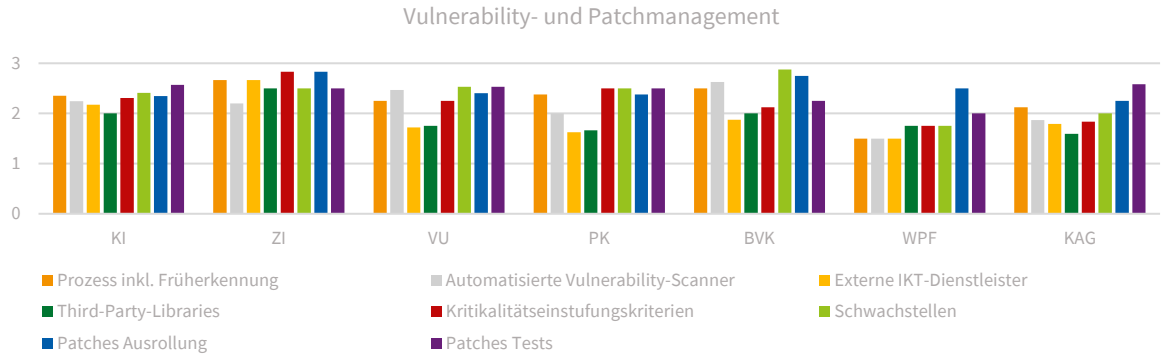
Im Bereich Kryptographie sieht DORA **umfassende Dokumentationen** vor, die Vorgaben zur Verschlüsselung, dem Schutz von Schlüsseln und den genutzten Algorithmen enthalten. Diese Anforderungen gehen über die Empfehlungen der gängigen Standards hinaus. Wohl deshalb sind die durchschnittlichen Umsetzungsgrade nicht so hoch wie bei den anderen „Schutz- und Präventionsmaßnahmen". Allerdings legen die Spezifika der Vorgaben als auch die Kommentare der Finanzinstitute nahe, dass hier großteils prozedurale Vorgaben und Dokumentation und eher wenige technische Maßnahmen zu setzen sind, da Kryptographie weitgehend im Rahmen vorgefertigter Systeme und Services eingesetzt wird.

12.1.3.2 Policies und Prozesse für den IKT-Betrieb



Der insgesamt noch etwas niedrige Umsetzungsgrad von 2,1 der Prozesse für den IKT-Betrieb ist teilweise darauf zurückzuführen, dass diese (zB die Einrichtung einer Logging-Infrastruktur) umfangreiche **technische Maßnahmen** erfordern. Teilweise kann dies laut den beaufsichtigten Unternehmen auch daher erklärt werden, dass Maßnahmen bereits etabliert sind, jedoch noch nicht den DORA-Standards entsprechend dokumentiert wurden. Der IKT-Betrieb wird überdies von einigen Unternehmen an Drittdienstleister übertragen, sodass die Einhaltung der relevanten Vorgaben bei diesen zu prüfen ist.

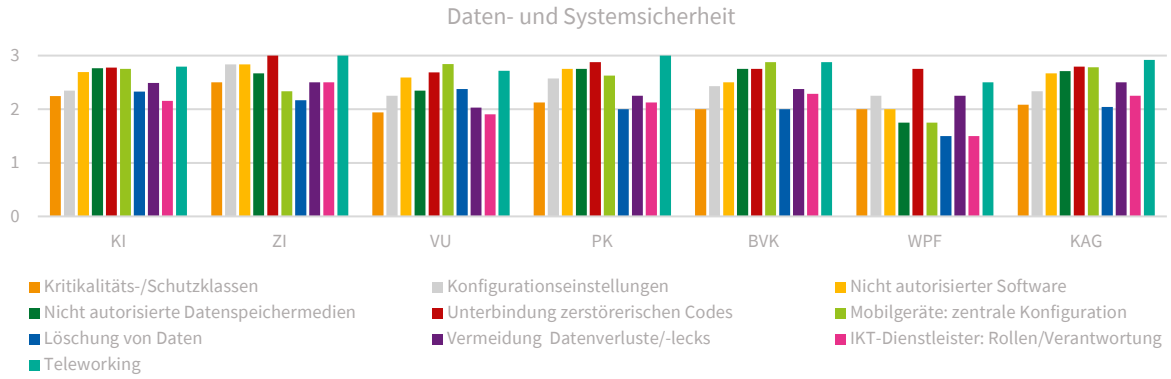
12.1.3.3 Vulnerability- und Patchmanagement



Beim Vulnerability- und Patchmanagement sind insb. Maßnahmen zur Erhebung und Dokumentation der verwendeten **Third-Party-Libraries** und zur **Verifikation der schwachstellenbezogenen Maßnahmen** von externen IKT-Dienstleistern noch auszubauen.

- Teils wurden **Verträge** bzw. Service Level Agreements mit Dienstleistern im Hinblick auf deren Erfordernisse zur Ergreifung geeigneter Maßnahmen, um Schwachstellen in den für das Unternehmen erbrachten Services zu schließen, bereits angepasst. Es wird auch evaluiert, solche Informationen in Cyberrisikoratings von Drittanbietern hinzuzufügen. Auch auf ISO/IEC 2000-Zertifizierungen wird verwiesen. Diese Zertifizierung wird auch bzgl. der Erhebung und Dokumentation zur Verwendung von Third-Party-Libraries, insb. bei eigenentwickelter Software oder Software die kritische oder wichtige Geschäftsprozesse unterstützt, genannt.
- **Prozesse** zum Vulnerability-Management, welche das Monitoring geeigneter Informationsquellen zur frühzeitigen Erkennung relevanter Schwachstellen umfassen, scheinen im Aggregat ausreichend dokumentiert.
- Automatisierte **Vulnerability-Scanner** werden nach Maßgabe der Kritikalität von IKT-Systemen eingesetzt, wobei es keine spezifischen Hinweise zum Erfordernis der mindestens wöchentlichen Prüfung kritischer und wichtiger Systeme gab. Einige Unternehmen weisen darauf hin, dass eine solche Prüfung unabhängig von der Kritikalität erfolgt.
- **Kriterien für die Einstufung der Kritikalität** von erkannten Schwachstellen und zugehörigen Patches sind grundsätzlich definiert und mit Zeitvorgaben und Eskalationen für die Installation der Patches hinterlegt.
- **Identifizierte Schwachstellen** und deren Korrektur werden grundsätzlich durchgängig dokumentiert.
- **Patches** werden identifiziert und nach Tests im Release-Prozess ausgerollt. Manche Unternehmen haben bei relevanten Betriebssystemupdates eine **Warteperiode** mit externen Dienstleistern vereinbart, um sicherzustellen, dass Fehler in neuen Patches vor breiter Ausrollung identifiziert werden.

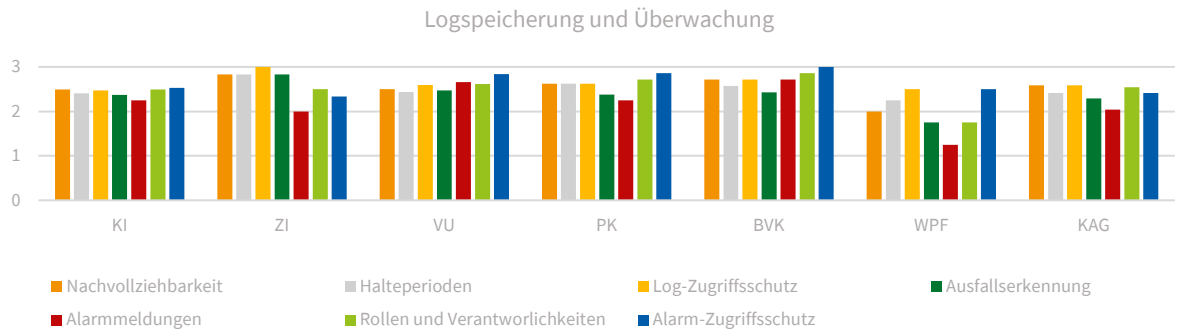
12.1.3.4 Daten- und Systemsicherheit



Im Bereich „Daten- und Systemsicherheit“ besteht insgesamt nur ein geringfügiger Anpassungsbedarf.

- Auch in diesem Fall ist besonderes Augenmerk auf die **Schnittstellen zu IKT-Drittdienstleistern** zu legen. Die Aufteilung von Rollen und Verantwortlichkeiten im Bereich IKT-Sicherheit soll mit diesen klar geregelt und dokumentiert sein. Vor allem an Dokumentationen wird derzeit gearbeitet.
- Ebenfalls die **Zuordnung von Daten und IKT-Systemen zu Kritikalitäts-/Schutzklassen** ist teils noch vorzunehmen. Dazu werden Governance-, Risk- und Compliance-Tools eingesetzt oder Zuordnungen zu Klassen in der Configuration Management Database umgesetzt.
- **Fernzugriffe auf das Netzwerk** im Rahmen von Teleworking sowie gegebenenfalls die Nutzung von privaten Geräten (BYOD) scheinen demgegenüber durch VPN, Multi-Faktor-Authentifizierung, Citrix oder BYOD-Verbote so abgesichert, dass die IT-Sicherheit des Unternehmens dadurch nicht gefährdet ist. Bei Mobilgeräten wird unter anderem Mobile-Device-Management eingesetzt.
- Technische Maßnahmen (zB Anti-Malware, Software-Whitelisting) zur **Unterbindung der Ausführung von zerstörerischen Codes** werden verbreitet (zB über Endpoint Discovery and Response-Lösungen) eingesetzt.
- Zur **Unterbindung der Installation nicht autorisierter Software** sind Nutzerrechte eigeschränkt, entsprechende Vorgaben definiert oder Softwareinstallationen sind nur auf Basis einer Whitelist möglich.
- In Dienstanweisungen ist die **Verwendung nicht autorisierter Datenspeichermedien** ausgeschlossen. Auch diesbezügliche technische Maßnahmen sind umgesetzt. Teils ist die Verwendung verschlüsselter USB-Sticks zulässig. In Ausnahmefällen dürfen in manchen Unternehmen bestimmte Nutzer:innen für Geschäftszwecke nicht autorisierte Datenspeichermedien verwenden, wobei solche Aktivitäten durch Data Loss Prevention- und Endpoint Detection and Response-Systeme überwacht werden.
- Zur **Vermeidung von Datenverlusten bzw. Datenlecks** ist zB Data Loss Prevention implementiert bzw. in Planung.
- Vorgaben zu **Konfigurationseinstellungen für IKT-Systeme** sind beispielsweise in entsprechenden Hardening-Vorgaben definiert.
- An der Granularität von Prozessen zur **Löschung von Daten**, welche insb. eine sichere Vernichtung nicht mehr benötigter sensibler Daten sicherstellen, wird teilweise noch gearbeitet.

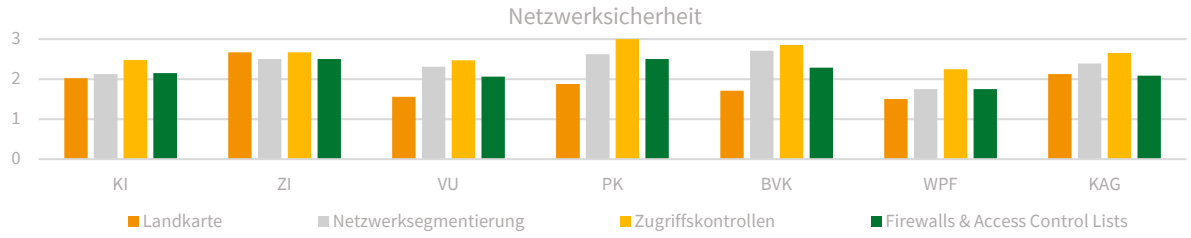
12.1.3.5 Logspeicherung und Überwachung



Die abgefragten Prozeduren und Werkzeuge zur Logspeicherung und Überwachung werden zu einem großen Teil durch die Finanzunternehmen erfüllt. Den größten Nachschärfungsbedarf haben auch in diesem Bereich jene WPF, welche unter den vollen Risikomanagementrahmen fallen.

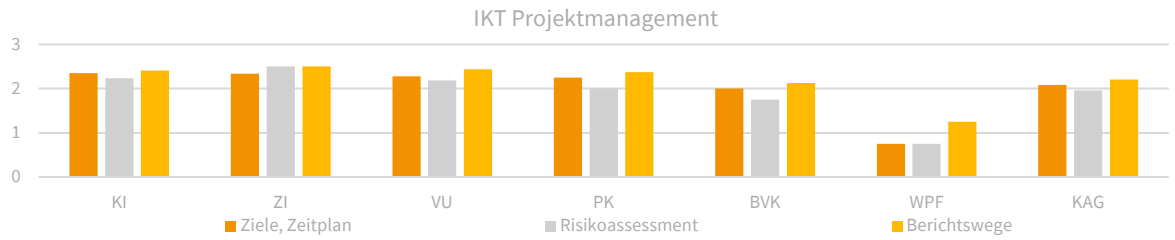
- Logs werden durch Sicherheitsmaßnahmen **vor unautorisiertem Zugriff geschützt**. Zugriffe auf Logdateien, die teilweise an zentrale Log-Management-Lösungen und an SIEM weitergeleitet werden, sind beispielsweise nur Administratoren möglich. **Log-Halteperioden** sind teilweise noch zu definieren.
- Zur **Nachvollziehbarkeit von Zugriffen** und der Performance von Daten, IKT-Systemen und Netzwerkverbindungen werden beispielsweise Log-Anbindungen an das SIEM erweitert.
- Bei der Frage zum **Ausfall von Logging-Systemen** wurde beispielsweise angeführt, dass gelöschte Logs teils erkannt werden können oder ungewöhnliche Mengen an Logüberleitungen an SIEM auffällig wären.
- Die Anforderung, wonach ein automatisiertes System **bei identifizierten Anomalien Alarmmeldungen** erzeugen soll, welche mit einer Prioritätsklassifizierung versehen sind, wird zB über Managed SOC-Services erfüllt. SIEM-Lösungen sind teils noch auszubauen. Auch Security Orchestration, Automation and Response (SOAR)-Technologien, durch welche Bedrohungen erkannt und automatisierte Gegenleistungen eingeleitet werden, werden hier erwähnt.
- Definierte und dokumentierte **Rollen und Verantwortlichkeiten**, welche sicherstellen, dass von den Überwachungssystemen generierte Alarmmeldungen gesichtet und bearbeitet werden, sind teilweise ausgelagert.

12.1.3.6 Netzwerksicherheit



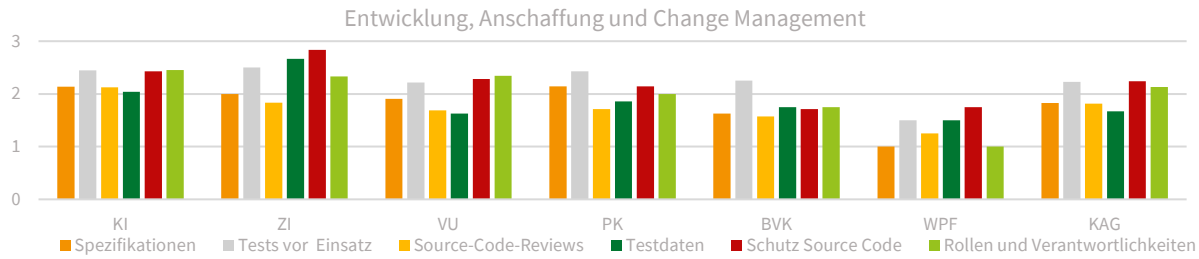
Vor allem die Dokumentation und Aktualisierung der **Landkarte aller Netzwerkverbindungen und Datenflüsse** befindet sich noch in Umsetzung. So sind insb. Datenströme noch zu analysieren und zu dokumentieren sowie Netzwerksegmentierungen nach Maßgabe der Kritikalität der dort betriebenen Systeme sind teils noch weiter auszubauen. Ein regelmäßiger Review zu Vorgaben, Rollen und Verantwortlichkeiten für die Konfiguration von Firewalls und Zugriffskontrolllisten (Access Control Lists – ACLs) findet grundsätzlich statt.

12.1.3.7 IKT Projektmanagement



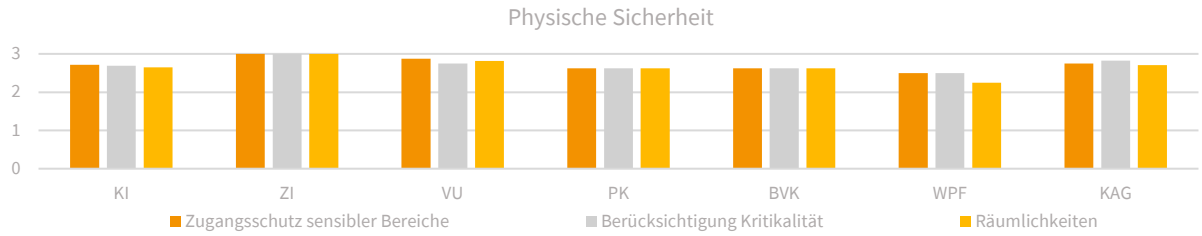
Bis auf die WPF besteht bei den Leitlinien für das IKT-Änderungsmanagement iZm Änderungen an Software, Hardware, Firmware-Komponenten, den Systemen oder von Sicherheitsparametern meist lediglich geringfügiger Anpassungsbedarf. Ziele, Zeitpläne und relevante Milestones werden in der Regel durch bestehende Projektmanagement-Richtlinien abgedeckt. Beim Assessment zu Projektrisiken sind teilweise Verbesserungen möglich. An die Geschäftsleitung sind häufig monatliche Updates vorgesehen, wobei die Ausgestaltungen konkret von der Größe und der Kritikalität der Projekte abhängig sind.

12.1.3.8 Entwicklung, Anschaffung und Change Management



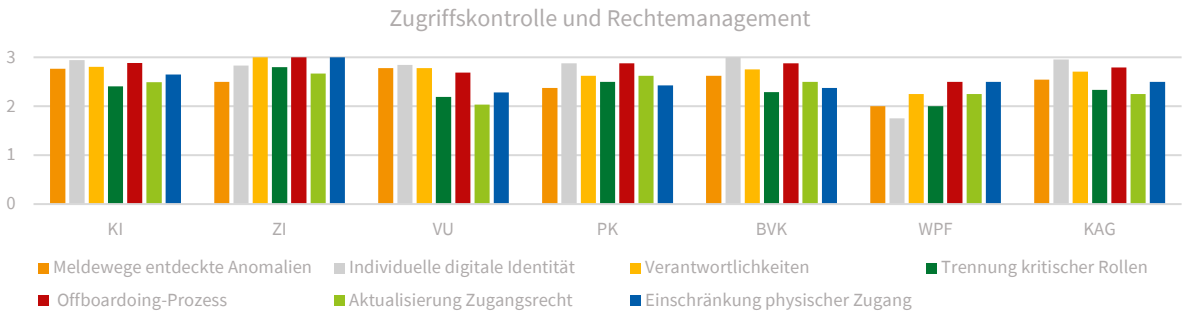
Besonders umsichtig agieren Unternehmen **vor dem Einsatz von IKT-Systemen** und sehen hier grundsätzlich verpflichtende Tests vor. Verschiedene **Tests**, wie zB Entwicklertests, Integrationstest, Systemintegrationstest oder Kundenabnahmetests, und Teststufen sind definiert. Programmcode wird beispielsweise im Zuge der Abnahme signiert und im Rahmen einer Kontrolle vor Produktivsetzung wird verifiziert, dass der Code unverändert übernommen wird. Statische oder dynamische Tests werden durchgeführt, wobei letztere während aktiv laufender Anwendungen eingesetzt werden. In Testumgebungen werden meist ausschließlich anonymisierte Daten eingesetzt. Ausnahmen würden durch den Datenschutzbeauftragten genehmigt und dokumentiert. Rollen und Verantwortlichkeiten im Change-Management sind in der Regel definiert und dokumentiert, wobei auch eine Rollentrennung zwischen anfordernden, ausführenden und genehmigenden Stellen grundsätzlich eingehalten wird.

12.1.3.9 Physische Sicherheit



Zur physischen Sicherheit ergeben sich kaum feststellbare Gaps bzw. lediglich solche im Hinblick auf die Dokumentation. Räumlichkeiten werden durch technische Absicherungsmaßnahmen kombiniert mit regelmäßigen Berechtigungsreviews geschützt.

12.1.3.10 Zugriffskontrolle und Rechtemanagement



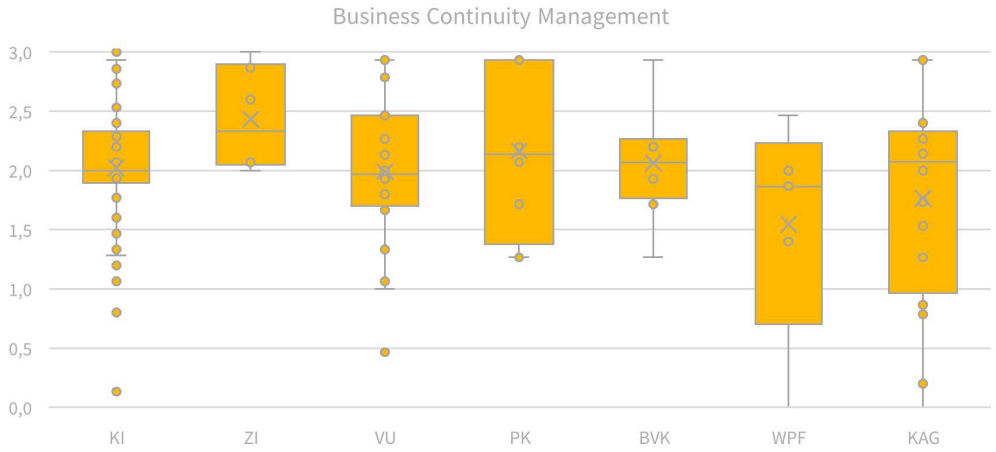
Bezüglich Zugriffskontrolle und Rechtemanagement errechnen sich insgesamt Durchschnittsscores über alle Sektoren von 2,3 bis 2,9.

- Der höchste Durchschnittswert wird dabei für **individuelle digitale Identitäten** der Mitarbeitenden erreicht.
- **Verantwortlichkeiten und Prozesse** bei Zuteilung, Veränderung und Entzug von Rechten sind zB in Workflows definiert.
- Erteilte **Zugangsrechte** in IKT-Systemen werden regelmäßig kontrolliert und ggf. aktualisiert. Die vorgesehenen Frequenzen unterscheiden sich teils voneinander, zB sehen manche Unternehmen jährliche Überprüfungen vor, während teils auch vierteljährliche Kontrollen implementiert sind.
- Mitarbeitende werden über die IKT-Sicherheitsrichtlinien des Unternehmens und die Meldewege für die Entdeckung von Anomalien in IKT-Systemen zB **im Rahmen von Bewusstseinsschulungen informiert** bzw. sind diese Informationen intern geordnet auffindbar.
- Auch **Offboarding-Prozesse**, welche bei Kündigungen den möglichst unmittelbaren Entzug aller Rechte in IKT-Systemen vorsehen, sind grundsätzlich implementiert.
- **Physische Zugänge** sind eingeschränkt und werden überwacht.
- Der niedrigste Durchschnittsscore von 2,3 ergibt sich hinsichtlich der **Trennung kritischer Rollen**. Dadurch soll verhindert werden, dass sich Einzelpersonen durch Kombination mehrerer Zugriffsrechte unautorisierten Zugang zu kritischen IKT-Systemen oder Daten verschaffen können. Teils sind hier noch zu viele Domain Admins eingesetzt bzw. wird auf kleine Unternehmensgröße verwiesen.

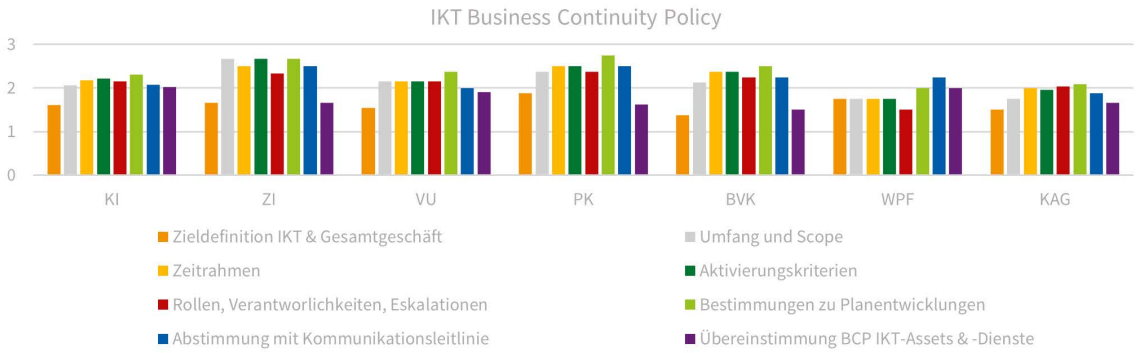
12.1.4 BUSINESS CONTINUITY MANAGEMENT

Die Maßnahmen im Bereich Business Continuity Management zeigen insgesamt geringfügigen Anpassungsbedarf. Der errechnete Durchschnittsscore über alle Sektoren beläuft sich auf 2,0. Lediglich Tests von IKT-Geschäftsfortführungsplänen liegen unter diesem Wert.

Der Boxplot zeigt, dass insb. bei WPF noch Handlungsbedarf besteht.



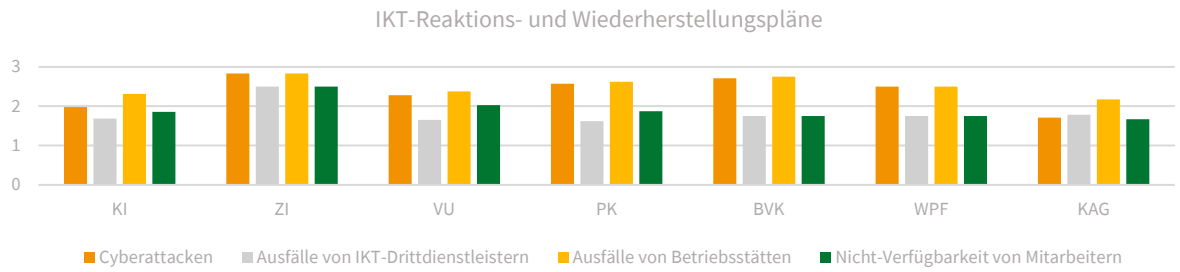
12.1.4.1 IKT-Geschäftsfortführungsleitlinie



Die Mindestinhalte der IKT-Geschäftsfortführungsleitlinie sind in Art. 24 der Delegierten Verordnung zum IKT-Risikomanagement (EU) 2024/1774 präzisiert. So sind in diesen Leitlinien etwa Ziele der IKT-Geschäftsfortführungsleitlinie, darunter auch die Wechselwirkungen zwischen der IKT- und der allgemeinen Geschäftsfortführung, zu beschreiben.

- Der größte Anpassungsbedarf quer durch alle Sektoren besteht hinsichtlich der **Definition der Ziele** der IKT-Geschäftsfortführungsleitlinie und deren **Wechselwirkungen**. Auch sind Recovery Time Objectives und Recovery Point Objectives noch nicht vollständig auf Ebene der IKT-Geschäftsfortführungsleitlinie integriert.
- Als Teil der allgemeinen Geschäftsfortführungsleitlinie führen Finanzunternehmen eine **Business-Impact-Analyse (BIA) der bestehenden Risiken** für schwerwiegende Betriebsstörungen durch. IKT-Assets und -Dienste sind in Folge in Übereinstimmung mit der BIA zu konzipieren und zu nutzen, wobei insb. die Redundanz kritischer Komponenten angemessen zu gewährleisten ist. Diese Anforderung ist in vielen Unternehmen noch zu adressieren.
- Vorgaben zu **IKT-Geschäftsfortführungsplänen** und **IKT-Reaktions- und Wiederherstellungsplänen** sind dagegen am weitesten umgesetzt.

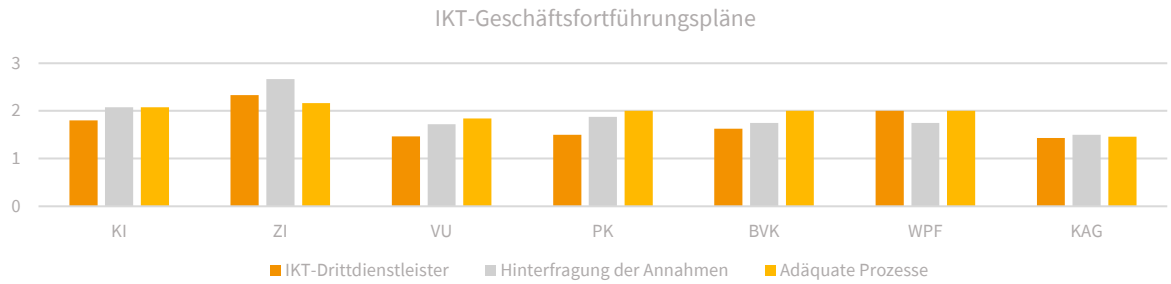
12.1.4.2 IKT-Reaktions- und Wiederherstellungspläne



Finanzunternehmen implementieren als Teil IKT-Risikomanagementrahmens damit verbundene IKT-Reaktions- und Wiederherstellungspläne. In diesen Plänen sind auch vorgegebene Szenarien, wie zB Cyberattacken oder die Nichtverfügbarkeit einer kritischen Anzahl von Mitarbeitenden, zu berücksichtigen. Dabei zeigt sich, dass insb. Auswirkungen von Insolvenzen oder sonstigen **Ausfällen eines relevanten IKT-Drittdienstleisters** noch in diese Pläne einzubeziehen bzw. hier adäquat zu adressieren sind.

Lediglich ZI erreichen diesbezüglich einen Durchschnittsscore von 2,5, während in allen anderen Sektoren die erreichten Durchschnittswerte bei 1,8 oder darunter liegen.

12.1.4.3 IKT-Geschäftsfortführungspläne

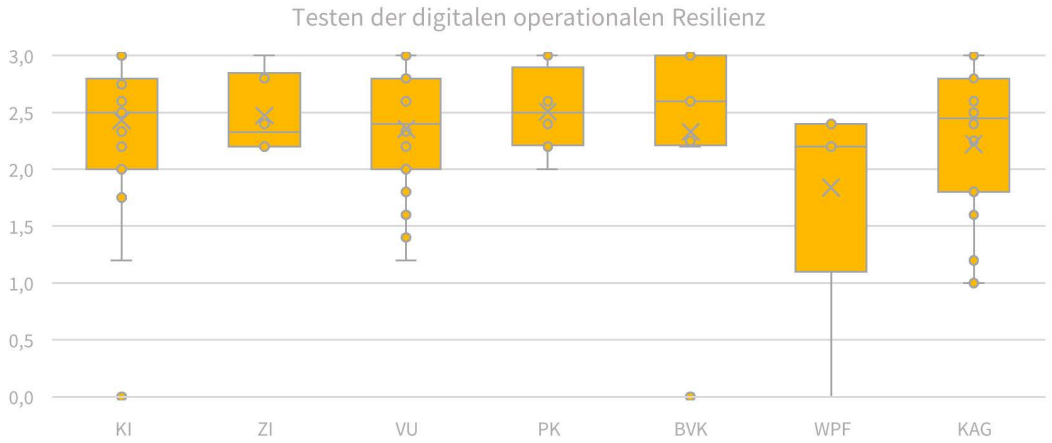


Gemäß Art. 11 (4) DORA-VO erstellen, pflegen und testen Finanzunternehmen regelmäßig angemessene IKT-Geschäftsfortführungspläne, insb. in Bezug auf kritische oder wichtige Funktionen, die ausgelagert oder durch vertragliche Vereinbarungen an IKT-Drittdienstleister vergeben werden.

Der größte Anpassungsbedarf im Themenbereich Business Continuity Management zeigt sich hinsichtlich **Tests von IKT-Geschäftsfortführungsplänen**. Diese haben unter anderem Tests der durch IKT-Drittdienstleister erbrachten IKT-Dienstleistungen zu umfassen, zielen auf die Hinterfragung der Annahmen, auf welchen die Geschäftsfortführungspläne beruhen, ab und umfassen Prozesse, um die Fähigkeit auf Szenarien adäquat reagieren zu können zu verifizieren.

12.2 TESTEN DER DIGITALEN OPERATIONALEN RESILIENZ

Unternehmen haben gemäß DORA ein Programm zu Tests der digitalen operationalen Resilienz vorzusehen und umzusetzen. Schon vor Anwendbarkeit der DORA-Vorgaben führten Finanzunternehmen laufend Schwachstellenbewertungen und -scans sowie Penetrationstests durch. Für die Durchführung der Tests wurden verbreitet externe Tester eingesetzt. Insgesamt geringfügiger Anpassungsbedarf ergibt sich für die Priorisierung, Klassifizierung und Behebung der im Rahmen von Tests identifizierten Probleme. Die folgende Grafik zeigt, dass Unternehmen in einzelnen Sektoren durchgängig hohe durchschnittliche Scores erzielen.

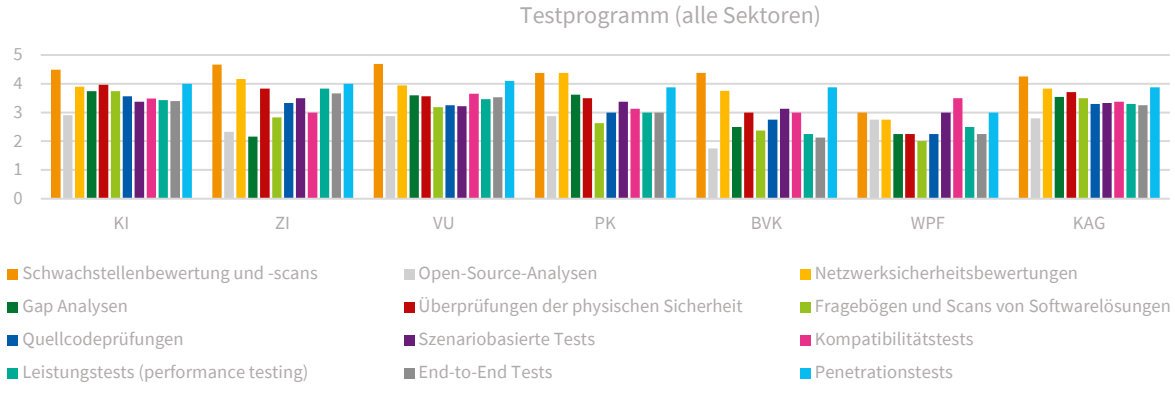


12.2.1.1 Testprogramm

Um die Vorbereitung auf die Handhabung IKT-bezogener Vorfälle zu bewerten sowie um Schwächen, Mängel und Lücken in Bezug auf die digitale operationale Resilienz zu erkennen und Korrekturmaßnahmen umgehend umzusetzen, haben Finanzunternehmen ein umfassendes Programm für das Testen der digitalen operationalen Resilienz zu erstellen. Das Programm ist risikobasiert zu konzipieren und hat etwa Schwachstellenbewertungen und -scans, Netzwerksicherheitsbewertungen, Lückenanalysen, Überprüfungen der physischen Sicherheit, Fragebögen und Scans von Softwarelösungen oder Penetrationstests zu umfassen.

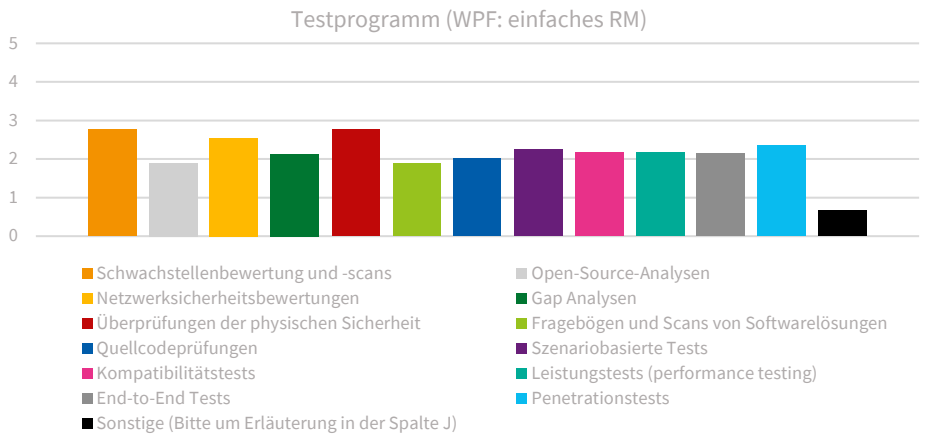
KI und VU weisen die vielfältigsten Testprogramme auf.

Insgesamt werden am österreichischen Finanzmarkt folgende Tests eingesetzt (Erläuterungen zur Skala: 1-nicht angewendet, 2-in Planung, 3-punktuell durchgeführt, 4-laufend für Teilbereiche durchgeführt, 5-laufend bzgl. eines breiten Scopes durchgeführt):



- In Unternehmen sind **Schwachstellenbewertungen und -scans**, die laufend, auch bzgl. eines breiteren Scopes, durchgeführt werden, Standard. Punktuelle Durchführungen werden durch WPF angegeben. Die DORA-Vorgaben sehen die Durchführung automatisierter Schwachstellenbewertungen und -scans für IKT-Assets, die kritische oder wichtige Funktionen unterstützen, mindestens einmal wöchentlich vor. Darauf scheinen die beaufsichtigten Unternehmen grundsätzlich vorbereitet zu sein.
- Auch **Penetrationstests** werden verbreitet auf laufender Basis für Teilbereiche eingesetzt. Bei WPF finden wiederum primär punktuelle Tests statt.
- Hinsichtlich **Quellcodeprüfungen** wird auch darauf hingewiesen, dass dieser bei Anwendungen oft nicht offengelegt wird, weshalb beispielsweise im Prozess der Einführung eine sehr genau Prüfung des spezifischen Verkäufers erfolgt.
- **Szenariobasierte Tests** sind oft in Form von Table Top Exercises, im Rahmen von Penetrationstests oder für relevante Applikationen durchgeführt.
- **Kompatibilitätstests** werden beispielsweise bei Bedarf während der Entwicklung oder bei Neuanschaffungen im Rahmen von Projekten sowie im Anlassfall bei Updates/Upgrade durchgeführt.
- **Leistungstests** werden zB in Folge von Performanceprobleme initiiert oder für relevante Applikationen durchgeführt.
- Sowohl **statische** als auch **dynamische Sicherheitstests** werden bzgl. des Scans von Softwarelösungen eingesetzt.
- Für Applikationen erfolgende **End-to-End Tests** werden meist durch IKT-Drittdienstleister vorgenommen.
- Bei **Gap Analysen** wird beispielsweise auf den Vergleich zu Vorgaben der ISO/IEC 27000-Familie oder zu Gruppenkontrollkatalogen verwiesen.
- **Überprüfungen der physischen Sicherheit** sind teilweise über Penetrationstests abgedeckt.
- Im Vergleich zu den zuvor genannten Tests ist die Durchführung von **Open-Source-Analysen** weniger verbreitet.
- Zusätzlich zu den in der Abfrage angegebenen Tests wurden unter anderem **Backup- und Recovery-Tests**, **Blackout-Tests**, **Prüfungen der Passwortqualität** und **Phishingtests, Social Engineering Tests** genannt.

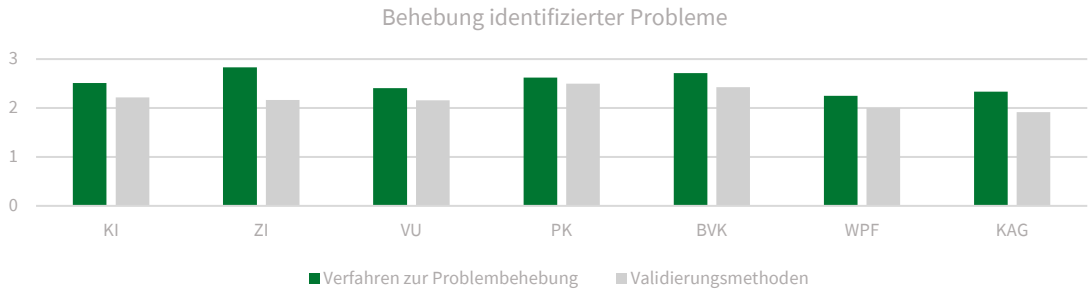
WPF, welche unter den vereinfachten RM-Rahmen von DORA fallen, setzen im Aggregat weniger umfassende Testprogramme als die Unternehmen in anderen Sektoren ein, wenngleich für sie dieselben Arten von IKT-Tests von Relevanz sind:



12.2.1.2 Testdurchführung

Bei KI und PK erfolgt die Testdurchführung überwiegend durch externe Tester, während zB ZI auf solche gelegentlich zurückgreifen. Vollständige Unabhängigkeit der **externen Tester** wird bei VU, BVK und WPF angegeben. Bei Heranziehen **interner Tester** ergibt sich in einigen Unternehmen Anpassungsbedarf hinsichtlich ausreichender Ressourcen und der Vermeidung von Interessenskonflikten während der Konzeptions- und Durchführungsphase der Prüfung.

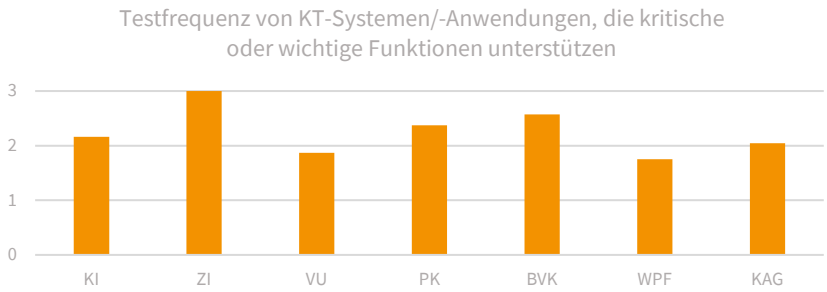
12.2.1.3 Behebung identifizierter Probleme



Einzelne Unternehmen haben **Verfahren zur Priorisierung, Klassifizierung und Behebung** von im Rahmen von Tests identifizierten Problemen anzupassen. Der größte Verbesserungsbedarf ergibt sich in WPF und KAG. Unternehmen verweisen hinsichtlich der angewendeten Verfahren zB auf Change-Management Prozesse oder auf IKT-Drittdienstleister oder allgemein auf Arbeitsanweisungen.

Infolge ergeben sich Verbesserungsmöglichkeiten hinsichtlich Validierungsmethoden zur Sicherstellung der vollständigen **Adressierung von identifizierten Schwächen, Mängeln oder Lücken**. Unter anderem wird nach fristgerechter Behebung der Findings, je nach Typ der Sicherheitslücke, eine Nachtestung durchgeführt oder die Behebung des Findings durch einen Information Security Officer validiert.

12.2.1.4 Testfrequenz



Die DORA-Vorgaben sehen mindestens jährliche Tests von IKT-Systemen und -Anwendungen, die kritische oder wichtige Funktionen unterstützen, vor.

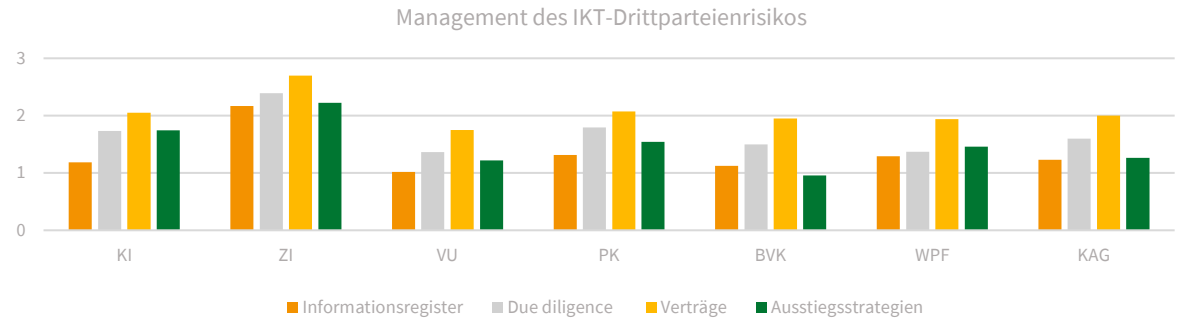
- ZI erfüllen diese Vorgabe schon zur Gänze.
- Bei WPF, VU und KAG besteht dbzgl. der größte Anpassungsbedarf.

12.3 MANAGEMENT DES IKT-DRITTPARTEIENRISIKOS

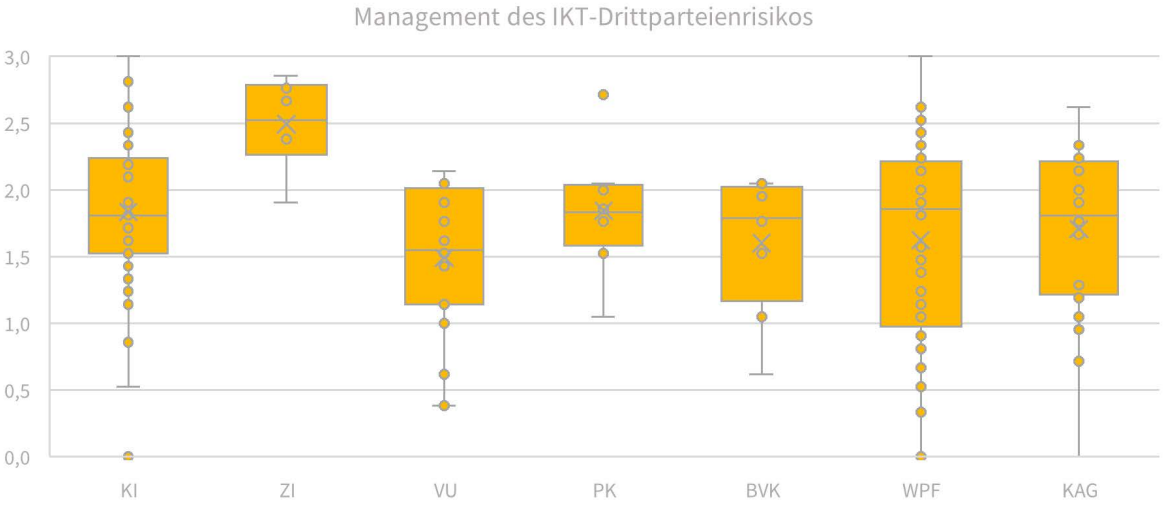
Der Umgang mit IKT-Dienstleistern stellt einen Eckpfeiler von DORA dar. In allen Phasen der Einbindung einer Drittpartei – dh vor, während und nach Bezug einer IKT-Dienstleistung – sind hier Maßnahmen zu setzen und ist die Dienstleistung im Rahmen des Risikomanagements aktiv zu erfassen. Konkret sind folgende Themenkomplexe zu behandeln:

- Vor Bezug einer IKT-Dienstleistung hat eine interne Risikoabwägung und eine **Due Diligence Prüfung** des Anbieters zu erfolgen.
- Bei IKT-Dienstleistungsverträgen sind **Mindestvertragsinhalte** zu berücksichtigen.
- Bestehende IKT-Dienstleistungen sind, mitsamt umfassender Metadaten, in einem laufend zu aktualisierenden **Register** zu erfassen.
- Für eine (vorzeitige) Beendigung des Dienstleistungsbezuges sind **Ausstiegspläne** vorzubereiten.

Als größte Herausforderung wird nach wie vor das Register der Dienstleister gesehen, während bei den Vertragswerken schon viel Vorarbeit geleistet wurde.

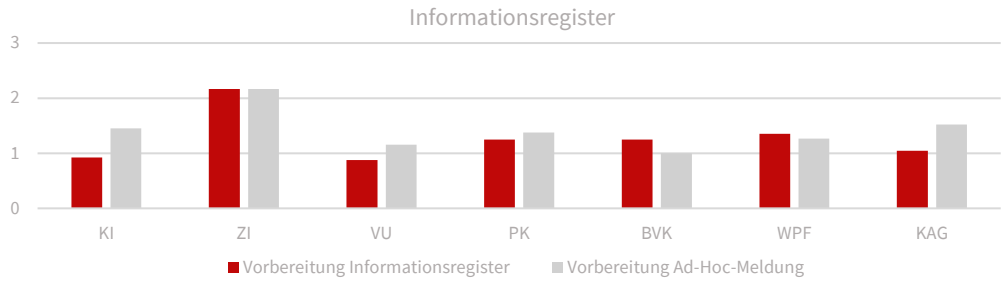


Gerade beim Management des IKT-Drittparteienrisikos ist allerdings die Spanne der Ergebnisse besonders groß, was bedeutet, dass bestimmte Unternehmen noch in allen Teilgebieten erheblichen Änderungsbedarf haben:



12.3.1.1 Informationsregister

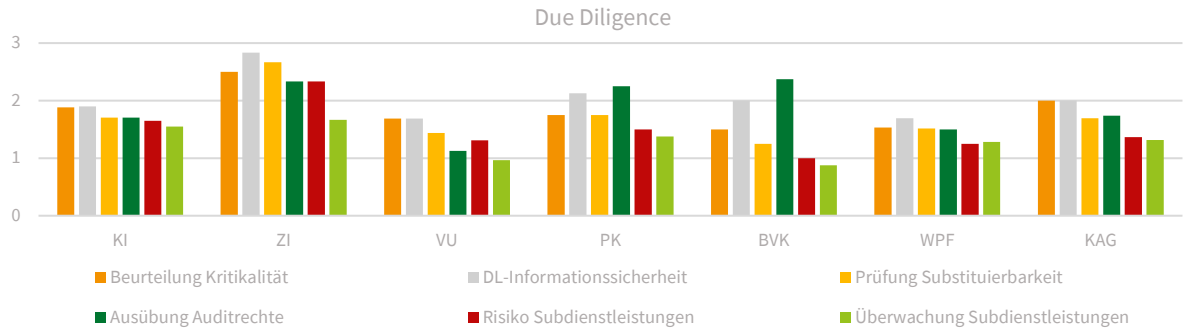
Das Aufsetzen des Informationsregisters der IKT-Dienstleister, das alle vertraglichen Vereinbarungen über die Nutzung von IKT-Dienstleistungen umfasst (Art 28 Abs 3 DORA), ist praktisch in allen Sektoren noch im Gange und stellt eine der größten Herausforderungen von DORA dar.



Insofern konnten die österreichischen Finanzunternehmen durch ihre Teilnahme an der Generalprobe der Meldung des Informationsregisters die Implementierung forcieren und die Datenqualität steigern. Oft wird risikobasiert vorgegangen, um zuerst kritische Dienstleistungen in vollem Umfang abbilden zu können. Viele Unternehmen planen, das Informationsregister aus dem bestehenden Vertragsmanagement-System zu generieren. Die Scores bei der Ad-Hoc Meldung (künftiger) IKT-Dienstleistungen, die kritische/wichtige Geschäftsfunktionen unterstützen, sind auch im Hinblick auf mehrere offene Interpretationsfragen auf EU-Ebene noch relativ niedrig.

12.3.1.2 Due Diligence

Die DORA-Vorgaben betreffend Due Diligence vor Abschluss eines Vertrags mit einem IKT-Dienstleister sowie während der Vertragsbeziehung (zB hinsichtlich der Ausübung der Auditrechte) wurden noch nicht in allen Unternehmen vollumfänglich umgesetzt:

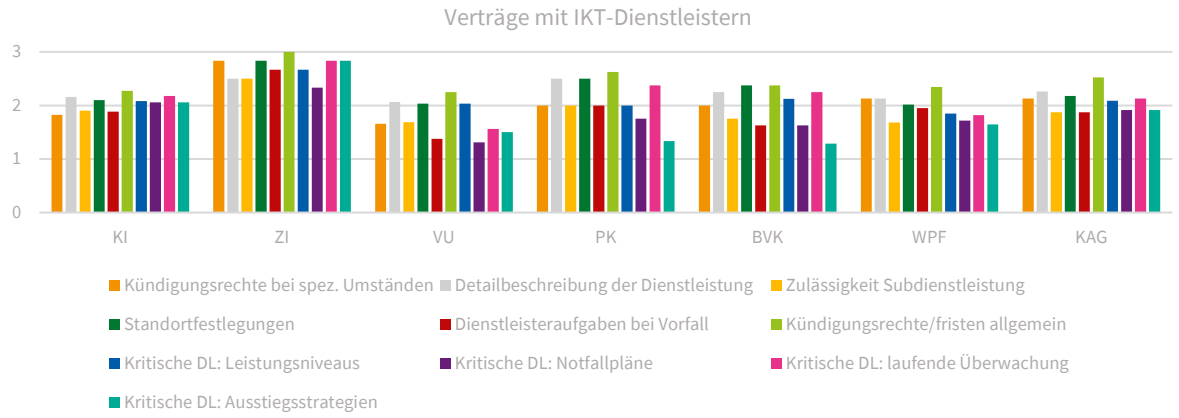


Die offenen Tasks betreffen zwar großteils Erweiterungen und Formalisierungen bereits vorhandener Due Diligence Prozesse, die bereits iZm aufsichtsrechtlich relevanten Auslagerungen etabliert wurden. Zwischen den sektoralen Anforderungen an Auslagerungen und den DORA-Vorgaben betreffend die Nutzung von IKT-Dienstleistungen können sich Überschneidungen ergeben. Eine besondere Herausforderung ist hierbei jedoch oft die **Überwachung der Subdienstleisterkette** und die Bewertung, wie sich potentiell lange oder komplexe Ketten der Unterauftragsvergabe auf die Fähigkeit auswirken können, betroffene Funktionen vollständig zu überwachen.

12.3.1.3 Verträge mit IKT-Drittdienstleistern

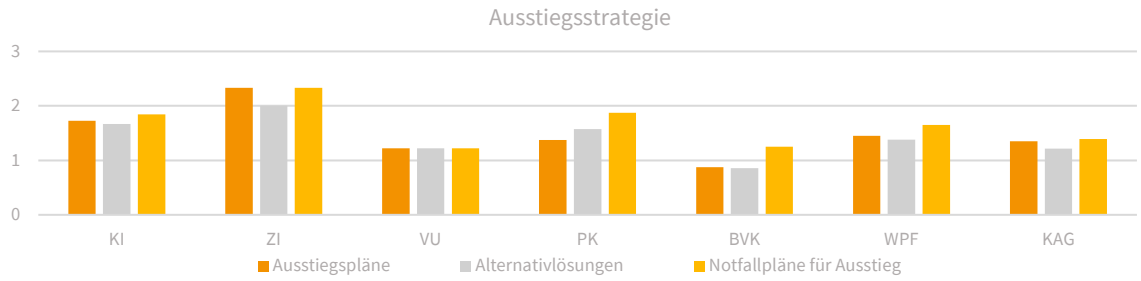
DORA sieht eine detaillierte Liste an Elementen vor, welche in IKT-Dienstleisterverträgen enthalten sein müssen. Für Dienstleistungen, welche kritische oder wichtige Funktionen unterstützen, kommt ein erweiterter Katalog zur Anwendung (zB Angabe, ob die Vergabe von Unteraufträgen für IKT-Dienstleistungen, die kritische oder wichtige Funktionen oder wesentliche Teile davon unterstützen, zulässig ist; zulässige Standorte, an denen die vertraglich vereinbarten oder an Unterauftragnehmer vergebenen Funktionen und IKT-Dienstleistungen bereitzustellen sind; Verpflichtung des IKT-Drittdienstleister, bei einem IKT-Vorfall Unterstützung zu leisten).

Trotz der umfangreichen Vorgaben haben die Unternehmen im Aggregat ihre Verträge bereits angepasst bzw. hatten die Vorgaben schon teilweise in bestehenden Vertragswerken berücksichtigt. Auch hier gibt es punktuell noch ausständige Nachverhandlungen und problematische Einzelfälle; insgesamt scheinen sich aber die meisten IKT-Dienstleister schon grundsätzlich auf die DORA-Vorgaben eingestellt zu haben.



12.3.1.4 Ausstiegsstrategien

DORA verlangt überdies die Planung eines strukturierten Ausstieges aus IKT-Dienstleistungen. Bei der Erfüllung dieser Vorgabe zeigen sich einerseits deutliche Unterschiede zwischen Unternehmen, andererseits auch noch ein relativ großer durchschnittlicher Umsetzungsbedarf:



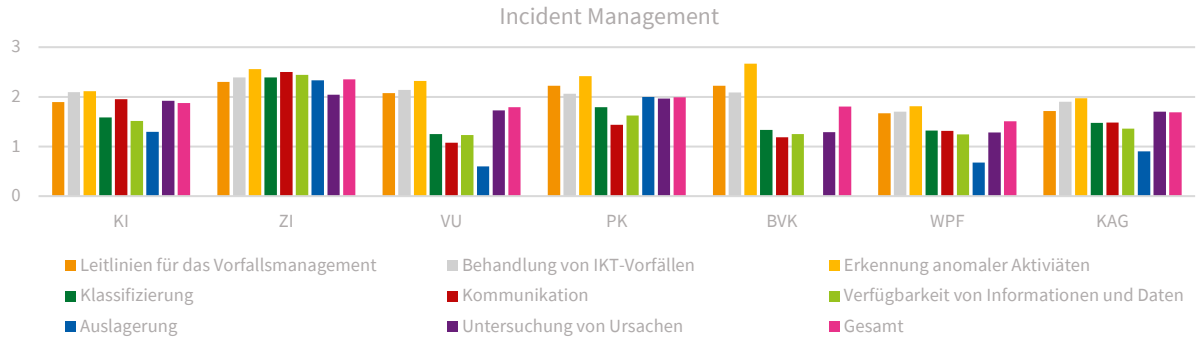
Da solche Pläne pro IKT-Dienstleistung vorzubereiten sind, ist davon auszugehen, dass diese DORA-Anforderung noch nicht in allen Fällen vollumfänglich erfüllt ist. Einige Unternehmen dürften den Vorteil haben, detaillierte Ausstiegspläne bereits vor DORA vorgesehen zu haben. Hier sind teilweise auch Tests und Übungen (zB in Form von Tabletop-Exercises) vorgesehen, was eine gute Best Practice darstellen könnte, um möglichst viel Mehrwert aus den Ausstiegsplänen zu ziehen.

12.4 IKT-BEZOGENE VORFÄLLE

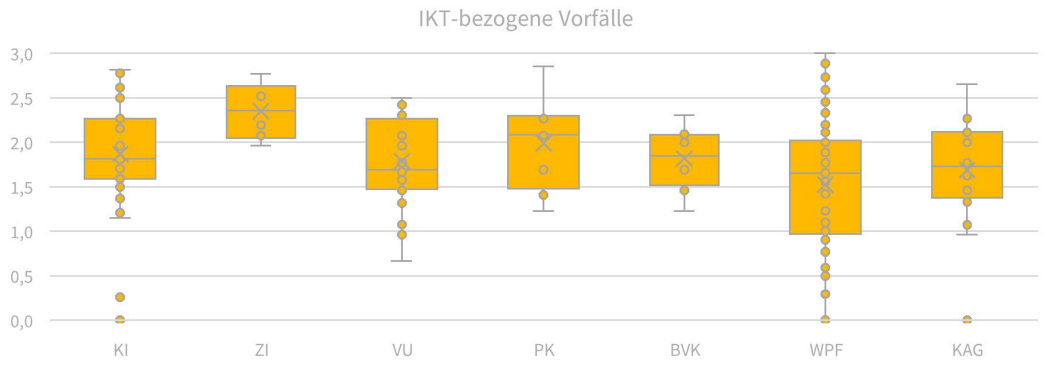
DORA sieht Vorgaben zum Management von IKT-bezogenen Vorfällen und Cyberbedrohungen und Meldeverpflichtungen zu schwerwiegenden IKT-bezogenen Vorfällen vor. Insb. Meldeverpflichtungen sind für viele Finanzunternehmen vollkommen neu und erfordern eine Vorbereitung auf die Klassifizierung und ggf. Übermittlung der Meldung an die FMA.

12.4.1 INCIDENT MANAGEMENT

Finanzunternehmen verfügen bereits über ausgeprägte Erfahrung hinsichtlich der Erkennung anomaler Aktivitäten, zB aus Logs oder aus potentiellen internen und externen Cyberbedrohungen. Demgegenüber sind die Vorgaben zu künftig verpflichtenden Meldungen schwerwiegender IKT-bezogener Vorfälle für viele Finanzunternehmen neu und die Verfügbarkeit der Meldeinhalte ist noch sicherzustellen.



ZI, die auf Erfahrungen aufgrund von ZaDiG zurückgreifen, erreichen in diesem Themenbereich insgesamt den höchsten durchschnittlichen Score. Dass ZI mit dem Thema vertrauter sind als die anderen Sektoren, wird auch im folgenden Boxplot veranschaulicht:



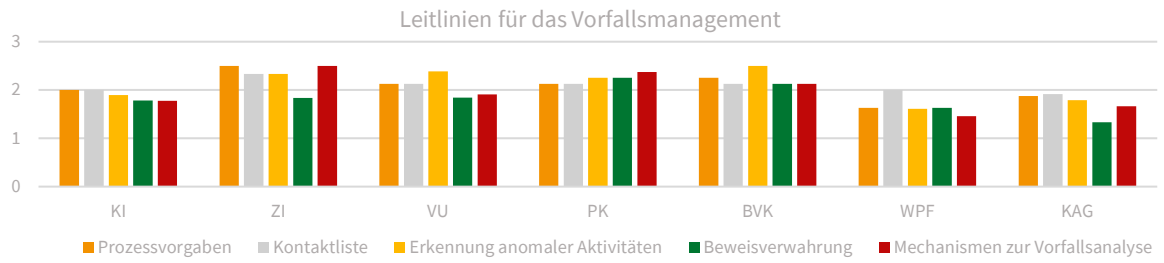
12.4.1.1 Leitlinien für das Vorfallsmanagement

Die Leitlinien für das Vorfallsmanagement umfassen jedenfalls die folgenden Elemente:

- **Prozessvorgaben:** Diese weisen meist lediglich geringfügigen Anpassungsbedarf auf. In WPF und KAG ist der Handlungsbedarf diesbezüglich höher als in den anderen Sektoren. Entsprechende Regelwerke werden aufgrund von DORA-Vorgaben überarbeitet.
- **Kontaktlisten:** Eine Auflistung von Kontakten zu internen Funktionen sowie zu externen Stakeholdern ist in Unternehmen gs vorhanden, ist aber teils noch nicht Bestandteil der genannten Policy. Alle Sektoren weisen hier im Durchschnitt einen Score von 2,0 oder höher auf. Eine Ausnahme stellen KAG dar; hier liegt der Durchschnittswert bei 1,9.

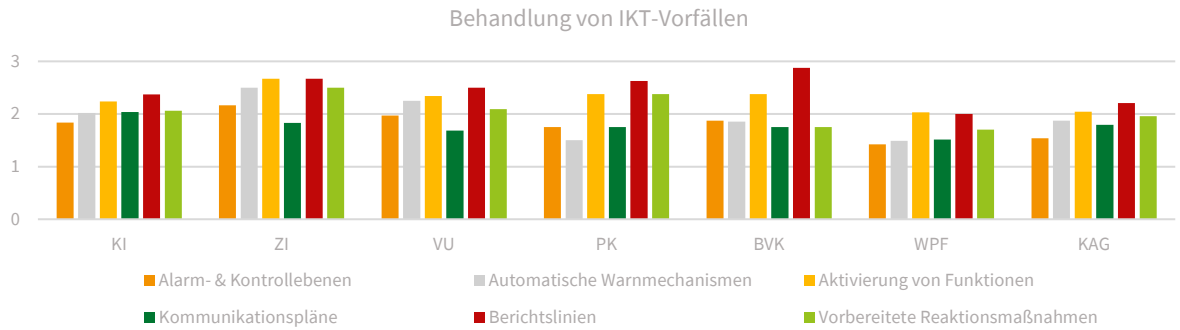
- **Mechanismen zur schnellen Erkennung anomaler Aktivitäten:** Diese weisen in den Sektoren meist geringfügigen Adaptionsbedarf auf. WPF und KAG zeigen hier das größte Verbesserungspotential. Die Aufgaben werden teils im Rahmen von SLAs mit IKT-Drittdienstleistern oder über SIEM/SOC erfüllt.
- **Beweisverwahrung:** Mit 1,7 erreicht die Umsetzung der Vorgaben zur Beweisverwahrung (dh Vorgaben für eine sichere Verwahrung von Beweisen zu IKT-Vorfällen) das niedrigste durchschnittliche Scoring.
- **Mechanismen zur Analyse signifikanter oder sich wiederholender IKT-bezogener Vorfälle:** ZI führen das Ranking der Sektoren zu diesem Thema an. Am Ende der Skala liegen hier WPF.

Die IKT-Leitlinien für das Vorfallsmanagement weisen insgesamt nur einen geringfügigen Anpassungsbedarf auf:



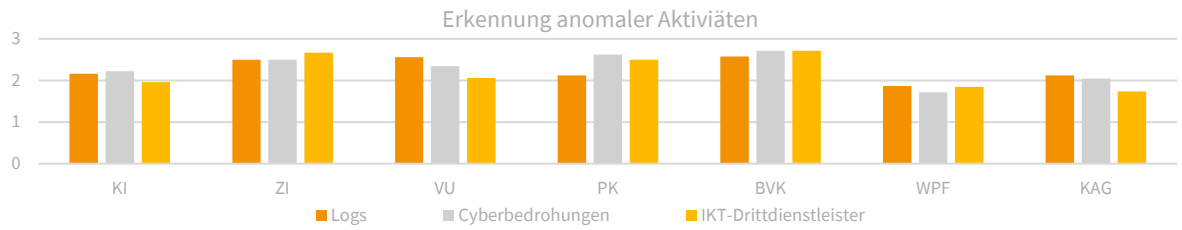
12.4.1.2 Behandlung von IKT-Vorfällen

Auch bei der Behandlung von IKT-Vorfällen zeigt sich im Durchschnitt lediglich geringer Anpassungsbedarf.



- Besonderen Wert legen die Unternehmen auf **Berichtslinien**. Die Meldung zumindest schwerwiegender IKT-bezogener Vorfälle an die zuständige höhere Führungsebene sowie die Information der Geschäftsleitung inkl. einer Erläuterung der Auswirkungen und Gegenmaßnahmen soll sichergestellt werden.
- **Kommunikationspläne**, die je nach Sachlage das Personal, externe Interessenträger, Medien, Kund:innen, interne Eskalationsverfahren sowie andere Finanzunternehmen, die als Gegenparteien fungieren, zu umfassen haben, werden noch fertiggestellt. Bislang haben einige Unternehmen Kommunikationserfordernisse bloß anlassbezogen erfüllt, indem sie auf die individuellen Anforderungen im Ereignisfall abstellen.
- Auch **Verfahren für Reaktionsmaßnahmen** bei IKT-bezogenen Vorfällen sind einzurichten, um Auswirkungen zu mindern und sicherzustellen, dass Dienste zeitnah verfügbar sind. Manche Unternehmen planen in diesem Zusammenhang, Erweiterungen der Incident Response Pläne vorzunehmen.
- Bezüglich des obligatorischen Einsatzes mehrerer Kontrollebenen und der **Festlegung von Alarmschwellen und -kriterien** inkl. Frühwarnindikatoren verweisen Finanzunternehmen beispielsweise auf die geplante Einführung von Key Risk Indicators oder auf die Anpassung von relevanten Verträgen.

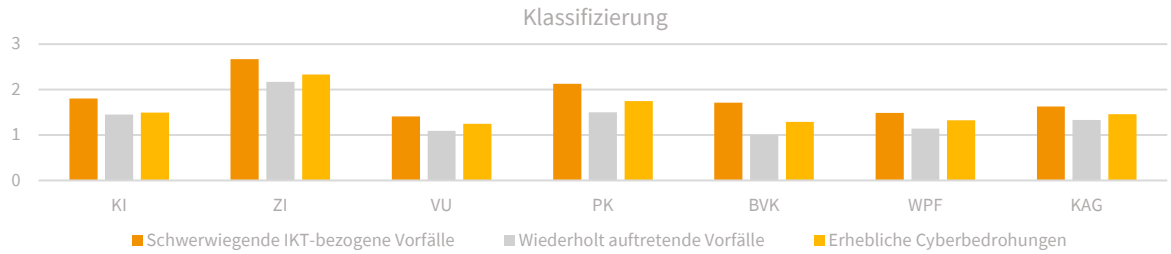
12.4.1.3 Erkennung anomaler Aktivitäten



Das Erkennen anomaler Aktivitäten schneidet innerhalb des Themenbereichs IKT-bezogene Vorfälle am besten ab. Jedenfalls folgende Informationen werden zur Erkennung bzgl. anomaler Aktivitäten genutzt:

- **Logs, interne Informationen und von Anwendern gemeldete Probleme:** Nur WPF weisen einen Durchschnittsscore von < 2 aus. VU und BVK erreichen die höchsten Werte.
- **Potentielle interne und externe Cyberbedrohungen:** Zur Erkennung anomaler Aktivitäten werden von Unternehmen auch Informationen zu internen und externen Cyberbedrohungen verbreitet genutzt. Beispielsweise werden mögliche Angriffe bei der Ergreifung erforderlicher Maßnahmen berücksichtigt. Auch SOC/SIEM Projekte und Awareness-Maßnahmen werden genannt.
- **Meldungen von IKT-Drittdienstleistern:** Meldungen von IKT-Dienstleistern wurden bereits vor DORA für die Erkennung anomaler Aktivitäten herangezogen. Künftig werden IKT-Dienstleistern allerdings noch stärker in die Pflicht genommen. Hierfür sind Verträge bzw. SLAs hinsichtlich Meldepflichten und Kontaktstellen teilweise noch individuell anzupassen.

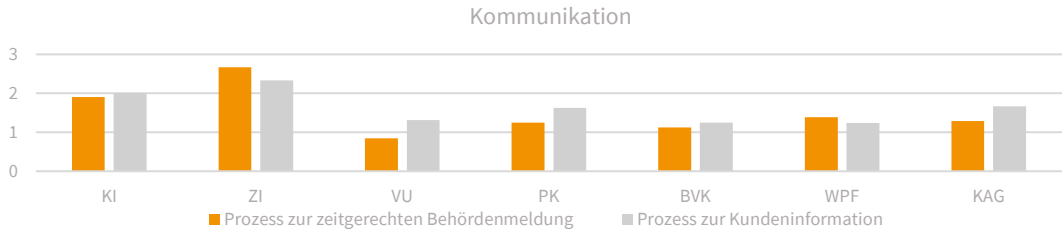
12.4.1.4 Klassifizierung IKT-bezogener Vorfälle und Cyberbedrohungen



Gemäß DORA sind schwerwiegende IKT-bezogene Vorfälle verpflichtend an die zuständige Behörde, und somit an die FMA, zu melden. Erhebliche Cyberbedrohungen können auf freiwilliger Basis an diese übermittelt werden. Um Vorfälle korrekt als schwerwiegend und Cyberbedrohungen als erheblich einstufen zu können, ist eine zeitnahe Klassifizierung von Vorfällen und Bedrohungen sicherzustellen. Dieses Themengebiet weist jedoch einen unterdurchschnittlichen Gesamtscore auf. Vor allem hinsichtlich der Analyse möglicher gemeinsamer Ursachen bezüglich wiederholt auftretender Vorfälle und der Klassifizierung von Cyberbedrohungen sind noch Maßnahmen zu treffen.

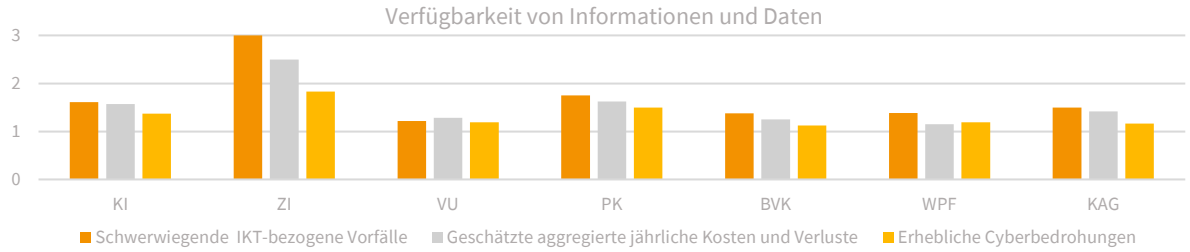
- **Wiederholt auftretende Vorfälle** sind im Hinblick auf mögliche gemeinsame Ursachen (innerhalb eines 6-Monats-Zeitraums) monatlich zu analysieren. Darauf aufbauend ist ein Prozess zur Überprüfung der kumulativen Überschreitung der Schwellenwerte eines schwerwiegenden IKT-bezogenen Vorfalls einzurichten. Nur ZI weisen hier einen Score > 2 aus.
- Bei der **Klassifizierung von Cyberbedrohungen** zeigt sich ein ähnliches Bild. Mit Abstand erreichen ZI den höchsten durchschnittlichen Score in Höhe von 2,3. Auf die künftige Erstellung einer Cyber Threat Landscape durch externe Dienstleister wird im zugehörigen Freitextfeld vereinzelt verwiesen.

12.4.1.5 Kommunikation



- Ein Prozess zur zeitgerechten **Meldung von schwerwiegenden IKT-bezogenen Vorfällen** (inkl. ggf freiwilliger erheblicher Cyberbedrohungen) an die FMA ist zu einem großen Teil noch vorzunehmen.
- Zu definieren sind auch **Prozesse zur Kundeninformation** über einen schwerwiegenden IKT-bezogenen Vorfall, der auch die finanziellen Interessen von Kund:innen betrifft, sowie die Maßnahmen, die ergriffen worden sind, um die nachteiligen Auswirkungen eines solchen Vorfalls zu mindern. ZI und KI sind diesbezüglich am besten vorbereitet.

12.4.1.6 Verfügbarkeit von Informationen und Daten zur Meldung

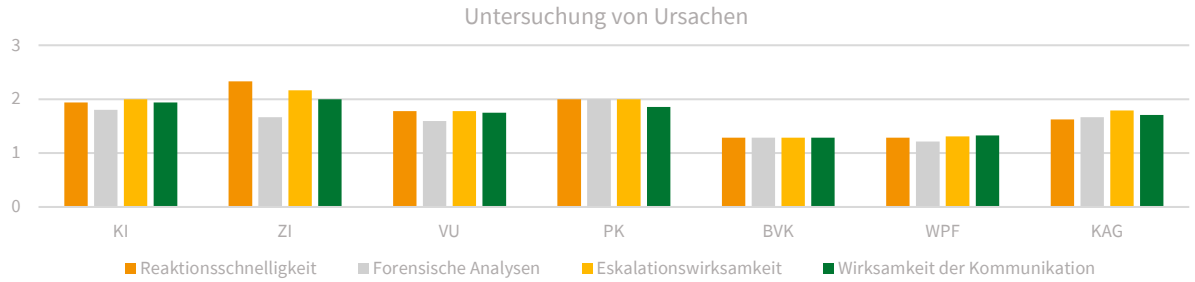


- Meldungen zu schwerwiegenden IKT-Vorfällen bzw. zu Cyberbedrohungen stellen für die meisten Unternehmen neue Vorgaben dar. Insofern überrascht es nicht, dass die **Verfügbarkeit von Meldeinhalten** bei schwerwiegenden IKT-bezogenen Vorfällen den niedrigsten durchschnittlichen Score erreicht. Beispielsweise arbeiten VU noch an der Sicherstellung der Verfügbarkeit der Meldeinhalte zu Erst-, Zwischen- und Abschlussmeldungen schwerwiegender IKT-bezogener Vorfälle (inkl. wiederholt auftretender Vorfälle). Auch alle anderen Sektoren – mit Ausnahme von ZI – haben hier noch Anpassungsbedarf.
- Auch hinsichtlich der Verfügbarkeit der Meldeinhalte zu (auf Anfrage der Aufsichtsbehörde zu übermittelnden) **geschätzten aggregierten jährlichen Kosten und Verlusten**, die durch schwerwiegende IKT-bezogene Vorfälle verursacht worden sind, sind weitgehend noch Anpassungen in unternehmensinternen Prozessen vorzunehmen. ZI führen wieder die Rankingliste mit einem Durchschnittswert von 2,5 an, während WPF und VU, mit Durchschnittsscores von 1,1 bzw. 1,3, am Ende der Liste aufscheinen. Unternehmen verweisen teils auf vorhandene Daten, die in entsprechende Prozesse einzupflegen sind.
- Die Frage zur Verfügbarkeit der **Meldeinhalte zu erheblichen Cyberbedrohungen** erreicht den geringsten durchschnittlichen Score in Höhe von 1,3. Auch ZI weisen hier einen Wert kleiner 2 auf.

12.4.1.7 Auslagerung der Meldung

Bei Auslagerung der Meldepflichten zu schwerwiegenden IKT-bezogenen Vorfällen sowie zu freiwilligen Meldungen erheblicher Cyberbedrohungen an Drittdienstleister ist eine diesbezügliche Information an die FMA zu übermitteln. Zur Vorbereitung dieser Meldung ergibt sich der niedrigste durchschnittliche Score in diesem Themenbereich zu IKT-bezogenen Vorfällen in Höhe von 1,1. Allerdings verweisen 55% der Unternehmen auf einen Ausschluss der Auslagerung der Meldeverpflichtung bzw. auf ein Nicht-Vorsehen einer solchen.

12.4.1.8 Untersuchung von Ursachen schwerwiegender IKT-bezogener Vorfälle



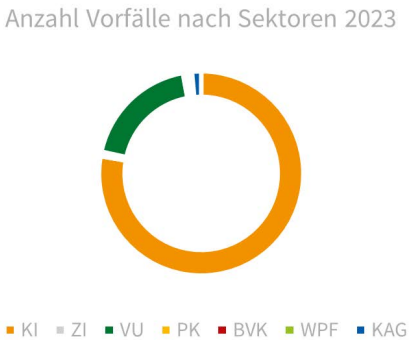
Nach schwerwiegenden IKT-bezogenen Vorfällen sehen Finanzunternehmen nachträgliche Prüfungen dieser Vorfälle vor, um die Ursachen für Störungen zu untersuchen und erforderliche Maßnahmen zu identifizieren. Auch hier ist ein Nachschärfen von Beurteilungskriterien bzw. das Einarbeiten erweiterter Anforderungen teils noch erforderlich. Insgesamt weisen ZI und PK die höchsten Durchschnittswerte in Höhe von 2,0 aus. Bzgl. forensischer Analysen wird beispielsweise auf Prozessüberarbeitungen, auf kontinuierliche Verbesserungen sowie auf Drittdienstleister hingewiesen.

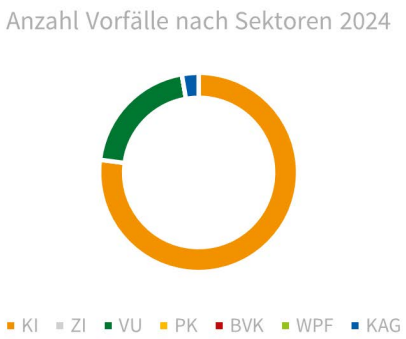
12.4.2 INCIDENTS

12.4.2.1 Anzahl der gemeldeten Vorfälle

Cybercrime-Anzeigen haben sich in Österreich von 2022 auf 2023 um 9,4% auf 65.864 Anzeigen erhöht.[7] Somit wurde ein neuer Spitzenwert erreicht. Die FMA-Analyse umfasste IKT-bezogene Vorfälle, die gemäß DORA als schwerwiegend einzustufen sind, für 2023 sowie für 2024 (bis 30.4.2024).

- Insgesamt zeigt sich, dass KI – wie auch in den Vorjahren – für beide Abfragejahre die höchste Anzahl an Vorfällen ausweisen; **rund drei Viertel der gemeldeten Vorfälle entfallen auf den KI-Sektor**. Dies ergibt sich unter anderem dadurch, dass bei Kreditinstituten bereits vor DORA entsprechende Meldeverpflichtungen vorlagen.
- Danach folgen VU. Auf sie entfällt ein Fünftel der Meldungen.
- Ansonsten liegen aus den restlichen Sektoren vereinzelte Meldungen vor.

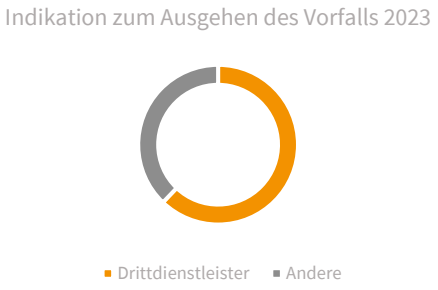


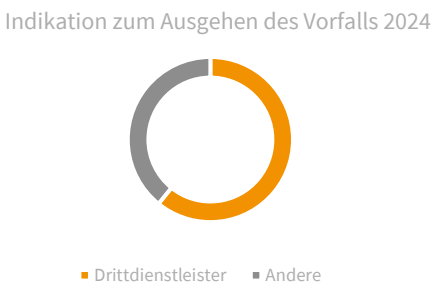


[7] *Bundesministerium für Inneres, Bundeskriminalamt, Cybercrime Report 2023, Lagebericht über die Entwicklung von Cybercrime, 2024, 23.*

12.4.2.2 Ausgehen des Vorfalls

Bei rund 60% der Vorfälle sind Indikationen zum **Ausgehen des Vorfalls von Drittdienstleistern** gegeben. Dies gilt sowohl für 2023 als auch für 2024. Das veranschaulicht die Sinnhaftigkeit der neuen DORA-Vorgaben zu IKT-Drittdienstleistern und zur Implementierung eines Überwachungsrahmens für kritische IKT-Drittdienstleister.

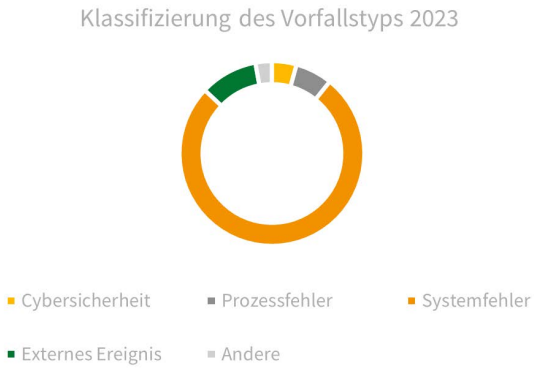


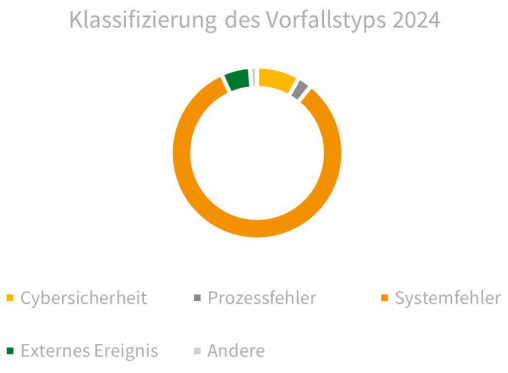


12.4.2.3 Klassifizierung des Vorfallstyps

Die meisten schwerwiegenden IKT-Vorfälle sind auf **Systemfehler** (dh nicht aus Angriffen resultierende Probleme wie zB Softwarefehler oder ausgefallene Netzwerkinfrastruktur) zurückzuführen: 2023 waren das 76% und 2024 82% der schwerwiegenden IKT-Vorfälle.

Die restlichen IKT-Vorfälle waren auf Cybersicherheit, Prozessfehler oder externe Ereignisse zurückzuführen; Auslöser waren hier etwa Datenexfiltration und Manipulation durch externe Angreifer, Denial-of-Service-Angriffe (DDoS), Absturz einer zentralen Programmbibliothek aufgrund eines Fehlers im Zuge der Einrichtung von neuen Cookies, Probleme während eines Umzugs des Rechenzentrums, Unterbrechungen während eines Disaster-Recovery-Tests, Auslastung einer zentralen Firewall aufgrund der Verdoppelung des Netzwerkverkehrs, fehlerhafte Einrichtung eines Setup-Services, Ausfalls des SMS-Services bei einem Telekom-Provider, Ausfall eines Marktinformationsdienstes, Performanceprobleme auf einer Gateway-Firewall, Leitungsfehlverbindung im Zuge eines Stromausfall-Tests in einem Rechenzentrum, Ausfall der Telefonie im Kundenservice.





12.4.2.4 Kosten und Verluste

Unternehmen haben nicht für jeden Vorfall finanzielle Auswirkungen angegeben. Teils wird beispielsweise auch darauf verwiesen, dass direkte und indirekte Kosten über Service Level Agreements abgedeckt seien. Jedenfalls zeigt sich, dass **ein einzelner Vorfall Kosten bzw. Verluste von mehr als hunderttausend Euro** verursachen kann.

12.4.3 CYBERVERSICHERUNG

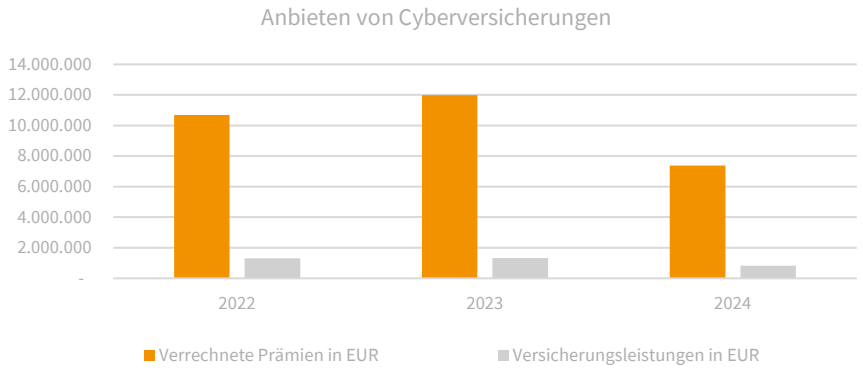
12.4.3.1 Abschluss von Cyberversicherungen

Der Deckungsumfang einer Cyberversicherungen ist vom jeweiligen Angebot abhängig. Auch Betreuungsdienste, zB zum Management von Cybervorfällen, können in diesen enthalten sein. Eine Cyberversicherung ist kein standardisiertes Produkt. Zudem können auch Haftpflicht- oder Rechtsschutzversicherungen Cyberrisiken umfassen.

- Die **Prämiensumme**, die insgesamt auf mit beaufsichtigten Unternehmen abgeschlossenen Cyberversicherungen entfällt, belief sich 2023 auf rd. 41 Mio. Euro. Sie entfällt zum Großteil auf den KI-Sektor. Unternehmen verweisen teilweise auch auf Gruppenlösungen zur Abdeckung von Cyberrisiken.
- Die von den Finanzunternehmen erhaltenen **Versicherungsleistungen** betragen 2023 rd. 71 Tsd. Euro.

12.4.3.2 Anbieten von Cyberversicherungen

11 VU bieten expliziten Cyberrisikoschutz an, wobei zwei Drittel dieser Anbieter diesbezügliche Rückversicherungen zur Risikoreduktion abgeschlossen haben.



- Die von den österreichischen VU verrechneten **Prämien** für Cyberversicherungen belaufen sich 2023 auf 12 Mio. Euro und sind gegenüber 2022 um 12% gestiegen. Zum Vergleich: Die im gesamten Versicherungsmarkt 2023 verrechneten Prämien in der Gesamtrechnung haben rd. 22 Mrd. Euro betragen.
- Die **Versicherungsleistungen** der österreichischen VU lagen 2023 bei rd. 1,3 Mio. Euro und haben sich im Vergleich zu 2022 um 3% erhöht.

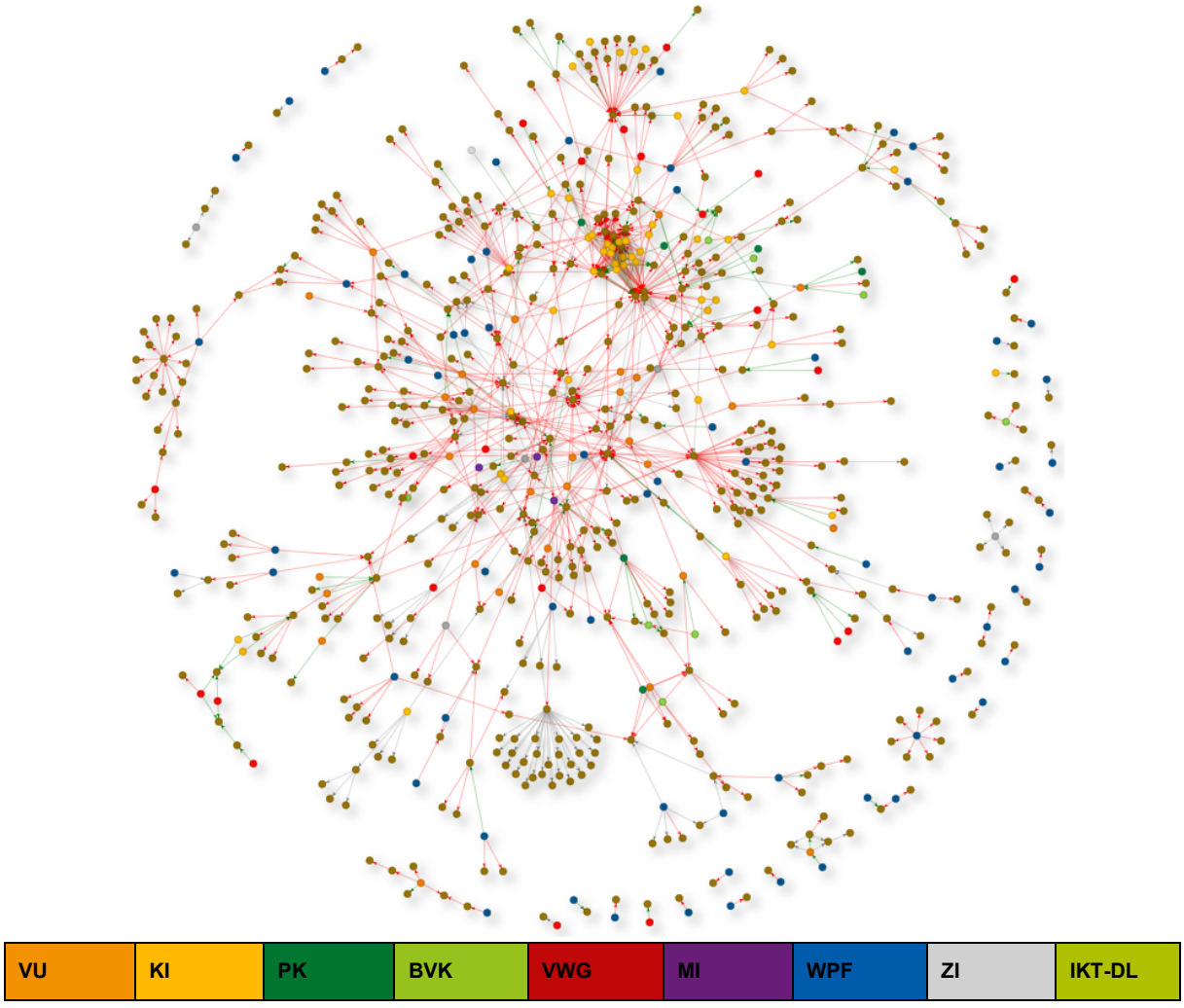
13 IKT-VERNETZUNGEN

13.1 IKT-VERFLECHTUNGEN AM ÖSTERREICHISCHEN FINANZMARKT

Die zunehmende Digitalisierung und die stetig wachsende technische Komplexität begünstigen auch die Verflechtungen zwischen den beaufsichtigten Unternehmen mit IKT-Dienstleistern sowie untereinander. Bereits die Analyse der FMA im Zuge der Digitalisierungsstudie 2021 zeigte, dass am österreichischen Finanzmarkt rund **1.000 kritische Vernetzungen mit IT-Dienstleistern und Subdienstleistern** bestehen. Diese IKT-Vernetzungen am österreichischen Finanzmarkt sind dabei durch folgende Aspekte geprägt:

- Ein überwiegender Teil der beaufsichtigten Unternehmen ist über Dienstleister und Subdienstleister, welche kritisch für die Geschäftsprozesse der Unternehmen sind, miteinander vernetzt.
- Die Zahl der durchschnittlich eingesetzten Dienstleister und Subdienstleister variiert zwar zwischen den Sektoren des Finanzmarktes relativ stark; deren Verteilung auf Einsatzgebiete ist jedoch relativ vergleichbar. Bei den am stärksten konzentrierten Sektoren, insb. den KI, ist eine große Anzahl der Marktteilnehmer direkt für die Erbringung ihrer Leistungen von einigen wenigen Dienstleistern abhängig.
- Neben wohlbekannten internationalen IKT-Anbietern haben auch lokale Unternehmen eine gewisse Relevanz.

Der hohe Grad der **Vernetzung mit IKT-Dienstleistern** wird von folgender Übersichtsgrafik illustriert:

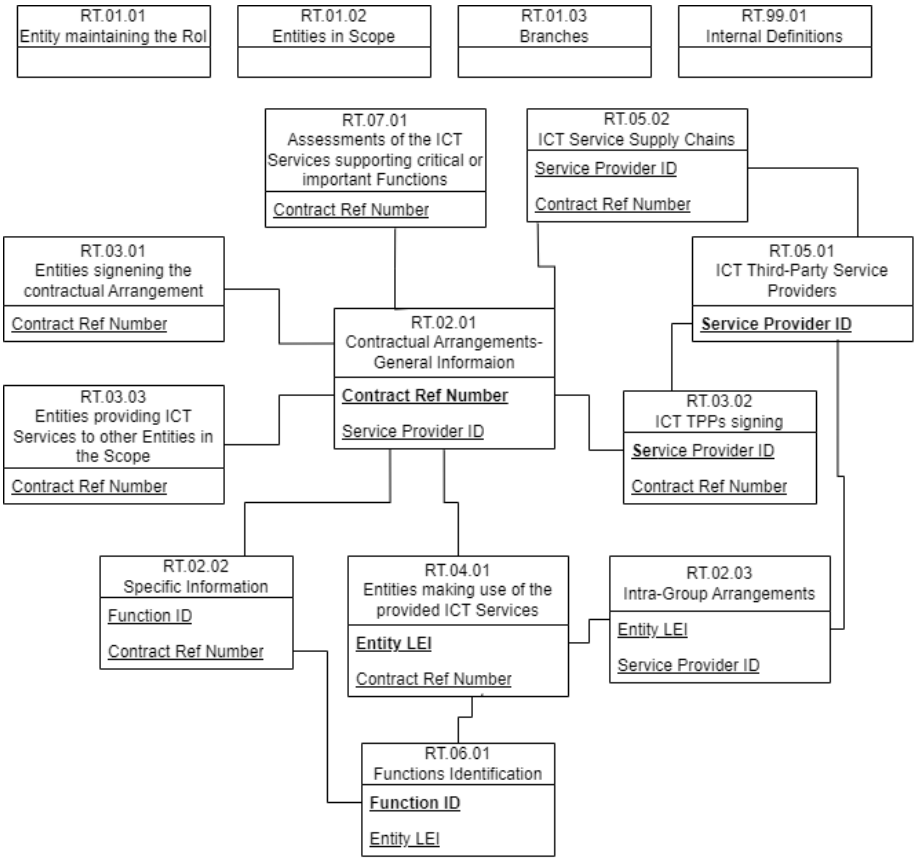


13.2 INFORMATIONSREGISTER ZU IKT-DIENSTLEISTUNGEN

Diese auch von der FMA attestierte hohe Abhängigkeit der Finanzbranche von einzelnen IKT-Dienstleistern ist einer der Gründe, warum dem **Management des Drittparteienrisikos** im DORA-Regelwerk ein prominenter Platz eingeräumt wird. Gleichzeitig sind die von den IKT-Dienstleistern erbrachten Services einer umfassenden Bedrohungslandschaft ausgesetzt. Den ersten Schritt zur Behandlung der daraus resultierenden Risiken stellt das **Führen eines umfassenden Informationsregisters über bezogene IKT-Dienstleistungen** durch die Finanzunternehmen dar. Im Informationsregister sind zahlreiche Metadaten zu den Dienstleistungen zu erfassen wie etwa:

- Detailinformationen zum IKT-Dienstleister, welcher das Service erbringt (Konzernzugehörigkeit, geographischer Sitz etc.),
- Details zum Vertrag sowie in Gruppen ggf. zur Konstellation an unterzeichnenden und nutzenden Entitäten,
- Informationen zu den Geschäftsfunktionen des Unternehmens, welche von den einzelnen Leistungen unterstützt werden,
- im Falle kritischer/wichtiger Funktionen auch Informationen über die Kette an involvierten Subdienstleistern.

Diese Informationen werden in einer Struktur aus 15 einzelnen Tabellen erfasst, welche durch Schlüsselwerte miteinander verbunden sind. Folgende Darstellung gibt einen Einblick in die Komplexität des Informationsregisters:



Die Erstellung und Übermittlung dieses Registers wurden im Zuge des vorliegenden Aufsichtsschwerpunkts einer **Generalprobe („Dry Run“)** unterzogen. Das Ziel dieser Generalprobe des Informationsregisters war, die Finanzinstitute bei ihrer Vorbereitung auf die erste Meldung 2025 zu unterstützen und der FMA einen aktuellen Einblick in die IKT-Dienstleistungslandschaft zu ermöglichen.

Zum Zeitpunkt der Durchführung dieses Dry Runs befanden sich viele der teilnehmenden Unternehmen noch mitten in der Umsetzungsphase, außerdem waren etliche Auslegungsfragen zum Begriff der „IKT-Dienstleistung“ auf EU-Ebene offen. Die FMA hat deshalb auch unvollständige oder von der Datenqualität noch nicht ausgereifte Einbringungen akzeptiert und jene Unternehmen, die noch nicht adäquate Daten liefern konnten, auf Einzelbasis aus dem Sample ausgenommen. Von den ursprünglich eingeladenen Unternehmen wurden die Einbringungen der folgenden Teilnehmer berücksichtigt:

- 47 von 51 Kreditinstituten
- 3 von 6 Zahlungsinstituten
- 32 von 32 Versicherungsunternehmen
- 4 von 8 Pensionskassen
- 5 von 8 Betrieblichen Vorsorgekassen
- 3 von 3 Marktinfrastrukturen
- 21 von 23 Kapitalanlagegesellschaften
- 48 von 64 Wertpapierfirmen

Zusätzlich zu den Daten dieser **163 Institute**, waren noch **Daten weiterer 146 Finanzunternehmen**, die nicht unmittelbar zur Teilnahme aufgefordert waren, zumindest teilweise in den Abgaben konsolidierter Meldungen enthalten. Dabei handelte es sich um österreichische sowie ausländische Institute.

Aus diesem Kontext heraus sind die Daten aus der Generalprobe mit einigen Einschränkungen behaftet, die bei der Ableitung von Schlussfolgerungen, aber auch bei der Vorbereitung auf den ersten produktiven Durchlauf der Informationsregisterabgabe zu berücksichtigen sind:

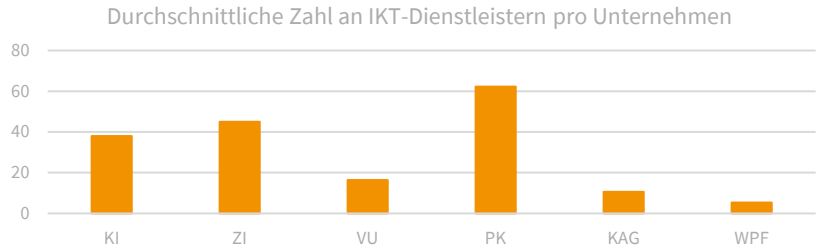
- Im Hinblick auf die eingeschränkte Datenverfügbarkeit sowie die zahlreichen offenen Auslegungsfragen zum Begriff der „IKT-Dienstleistung“ hatten sich die beaufsichtigten Unternehmen bei der Erstellung des Informationsregisters **vorerst auf die kritischeren und wichtigeren Dienstleister fokussiert**.
- Das Informationsregister basiert auf einer **komplexen Datenstruktur**; auch kleine Probleme im Datensyntax konnten somit die Verarbeitung und Interpretierbarkeit einiger Abgaben stark beeinträchtigen. Datenqualitätsprobleme, insb. nicht-zusammenpassende Schlüsselwerte, aber auch Abweichungen in den Daten selbst (zB falsch angegebener Konzessionstyp) machen die Verarbeitung der Daten herausfordernd. Die Unternehmen sollten hier vor Abgabe der Echtmeldung jedenfalls genug Zeit für interne Qualitätssicherung der Abgaben einplanen.
- Selbst bei korrekt befüllten Templates wurden bei einigen Punkten die **unterschiedlichen internen Zugänge** der teilnehmenden Unternehmen offensichtlich: zB bei der Aufspaltung einzelner Verträge in Unterverträge. Dies erschwert mitunter eine quantitative Analyse.

Diese Herausforderungen zeigen gleichzeitig die Wichtigkeit der Generalprobe. Die FMA ist davon überzeugt, dass die Erfahrungen aus dieser Übung einigen Problemen beim ersten Durchlauf des Prozesses zur Übermittlung der Informationsregister 2025 vorbeugen wird. Die Einblicke in die Dienstleisterlandschaft am österreichischen Finanzmarkt unterstreichen klar die Sinnhaftigkeit des Informationsregisters. Die wichtigsten allgemeinen quantitativen Eckpunkte zur Generalprobe sind:

- In den abgegebenen Meldungen waren Daten zu 309 Finanzunternehmen aus 23 Ländern vorhanden.
- 7952 Dienstleistungsverträge von Finanzunternehmen mit 1626 unterschiedlichen Dienstleistern aus 1312 einzelnen Konzernen konnten identifiziert werden.
- 4390 Subdienstleisterbeziehungen bis hin zur 5. Stufe waren in den Daten enthalten.

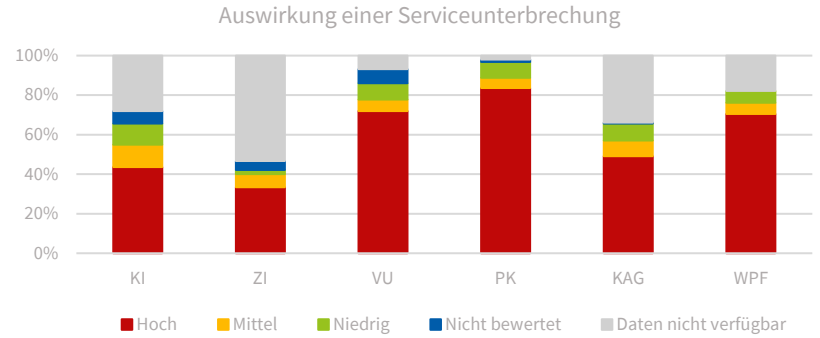
13.3 BEZUG VON IKT-DIENSTLEISTUNGEN

Alle Sektoren am österreichischen Finanzmarkt sind von IKT-Dienstleistern abhängig, wenngleich es deutliche sektorenabhängige Unterschiede gibt. Die **Anzahl an bezogenen IKT-Dienstleistungen** pro Unternehmen variiert von Organisation zu Organisation sowie von Sektor zu Sektor:



- Neben der Unternehmensgröße und der Komplexität des Geschäftsmodells müssen bei der Ableitung von Schlussfolgerungen auch die potentiell noch unvollständigen Register sowie die relativ geringe Samplegröße, die auf die Resultate durchschlagen können, bedacht werden. Allgemein entspricht aber die Beobachtung, dass **große und komplexere Unternehmen** wie zB KI **mehr Dienstleistungen als kleinere** (zB WPF) beziehen, auch den Erwartungen und den Daten von 2021.

Der **Anteil an kritischen IKT-Dienstleistungen** (gemessen an der Auswirkung eines potentiellen Ausfalls- von Hoch bis Niedrig) ist über alle Sektoren hinaus durchwegs groß:

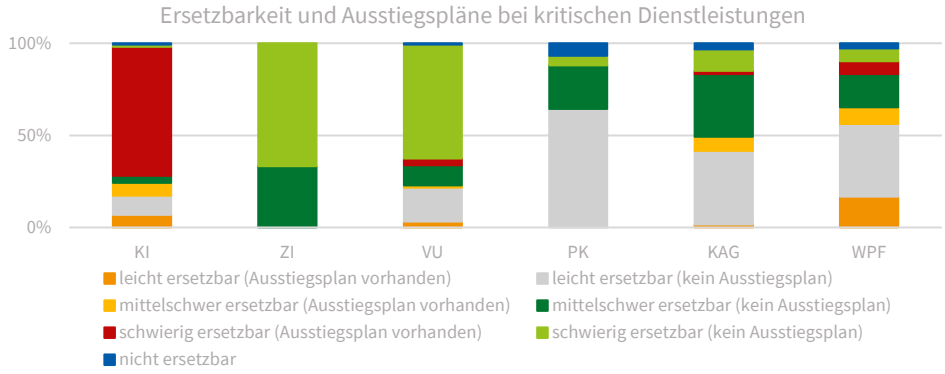


- Ein Vergleich mit der obigen Abbildung ermöglicht es, die **Zahl kritischer Dienstleister pro Unternehmen** abzuschätzen: so sind es zB bei KI im Durchschnitt 17, bei VU 12 und bei KAG 10 kritische IKT-Dienstleister.
- Der **hohe prozentuale Anteil an kritischen Dienstleistern** rührt großteils von der Datenlage der Generalprobe her: viele Unternehmen haben ihre Register erst teilweise erstellt und dabei die wichtigsten Dienstleister priorisiert, wodurch diese überrepräsentiert sind. Eine Steigerung der gemeldeten weniger kritischen IKT-Dienstleister wird für 2025 erwartet.

Die **Ersetzbarkeit** und das Vorhandensein von **Ausstiegsplänen** für jene Dienstleistungen, deren Ausfall mit ‚Hohen' Auswirkungen verbunden wäre, kann der folgenden Grafik entnommen werden:

- Bei der **Ersetzbarkeit kritischer Dienstleistungen** werden sektorale Unterschiede sichtbar: insb. bei KI, ZI und VU wäre ein Großteil dieser Services nur schwer zu ersetzen. Die unterschiedliche Einschätzung der PK, KAG, WPF ist den Einschränkungen der Datenlage geschuldet oder kann durch deren kleinere und weniger komplexe IKT-Infrastruktur erklärt werden.

- Bis auf Kreditinstitute, haben die meisten Unternehmen noch **keine oder wenige Ausstiegspläne** aus kritischen Dienstleistungen formuliert. Bei KI gibt es mit der EBA/GL/2019/02 eine sektorale Vorgabe, welche die Vorbereitung solcher Pläne fordert, was deren Vorhandensein in speziell diesem Sektor erklärt.



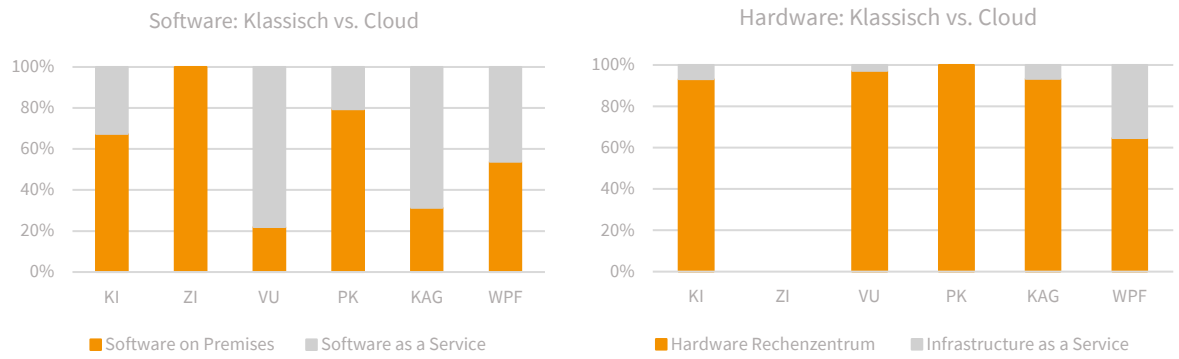
- Der blaue Teil des Balkens repräsentiert Systeme, die sowohl als kritisch, als auch als unersetzbar eingestuft werden. Dies bedeutet effektiv, dass der Verlust der Dienstleistung potentiell das Unternehmen als solches gefährden könnte, was der Organisation entsprechend bewusst sein muss.

13.4 WICHTIGSTE KATEGORIEN VON IKT-DIENSTLEISTUNGEN

Ein Trend, welcher in den Daten aus der Generalprobe zum Informationsregister klar nachvollzogen werden kann, ist die **wachsende Nutzung cloudbasierter Software-as-a-Service (SaaS)**.

Im Template zum Informationsregister werden **20 Kategorien von IKT-Dienstleistungen** unterschieden. Der sektorale Vergleich der Nutzung all dieser Kategorien gibt an diesem Punkt kein aussagekräftiges Bild. Es bleibt bis zur vollen Meldung 2025 abzuwarten, ob dies an Faktoren der Vollständigkeit oder Samplegröße liegt, oder die genutzten Services sich tatsächlich so stark unterscheiden.

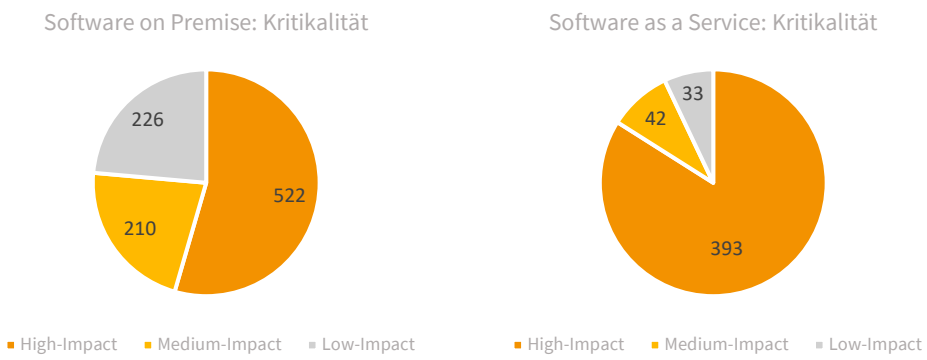
Der Vergleich von **klassischen (on-premise) Modellen** von Dienstleistungen im Bereich Hardware und Software mit der Nutzung entsprechender Cloudservices zeigt einen klaren Trend:



Die Ergebnisse legen somit eine signifikante Nutzung von SaaS-Angeboten in allen Sektoren bis auf ZI (die auch keine Angaben zur Nutzung von Rechenzentren gemacht haben) nahe.

Die **Anmietung reiner Rechenkapazität im Rahmen von IaaS** scheint, verglichen mit dem Bezug klassischer Rechenzentrumsleistungen hingegen, außer bei WPF, **eher wenig verbreitet** zu sein.

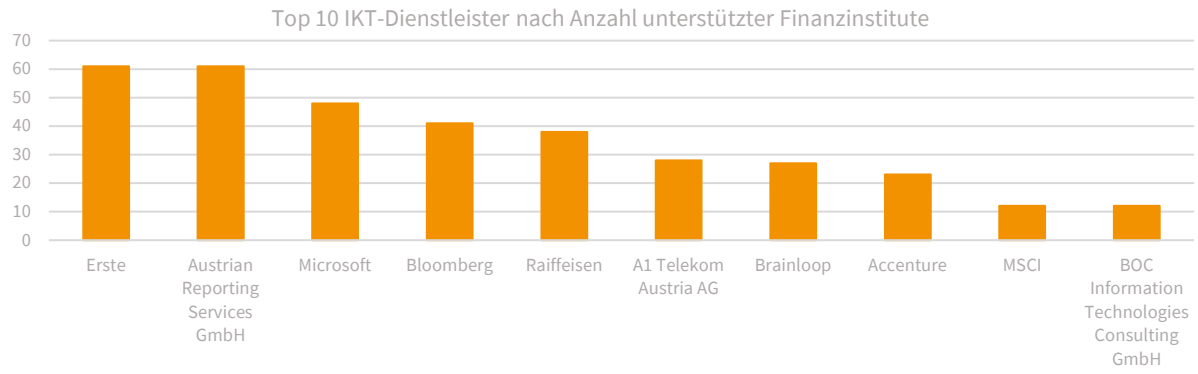
Die bezogenen SaaS-Dienstleistungen waren in den Daten der Generalprobe außerdem auffallend häufig mit kritischen Systemen verbunden, wie der Vergleich in den folgenden Grafiken zeigt:



13.5 WICHTIGSTE IKT-DIENSTLEISTER

Aufgrund der noch nicht vollständigen Informationsregisterdaten ist die Identifikation der wichtigsten Dienstleister noch nicht zuverlässig möglich. Hier geben die Daten von 2021 noch einen besseren Einblick. Es ergeben sich aber einige Indizien für die Interpretation der Informationsregister im Jahr 2025.

Die folgende Grafik zeigt die Top-10 Dienstleister, die sich nach Aggregation und Aufbereitung der Daten aus der Generalprobe ergeben haben.



Die Reihung scheint hier jedoch aufgrund folgender Faktoren die tatsächliche Relevanz der Dienstleister für den österreichischen Finanzmarkt nicht voll widerzuspiegeln:

- Aufgrund deren Konzernstruktur und Anzahl verbundener Unternehmen sind aus den Gruppen von Erster Bank und Raiffeisen viele praktisch idente Einzelabgaben zu erwarten.
- Die Verträge mit internen Gruppendienstleistern sind zumeist im Unternehmen vollständig erfasst und wurden dementsprechend berichtet.
- Die Verträge mit externen IKT-Dienstleistern scheinen hingegen noch nicht voll in die Informationsregister eingearbeitet zu sein- Unternehmen wie Microsoft und A1 wären ansonsten erwartungsgemäß von deutlich mehr Finanzinstituten als IKT-Dienstleister gemeldet worden.

14 KONSULTATION / CALL FOR INPUT

Wir laden Sie ein, die in unserer Analyse zur Austrian Digital Finance Landscape skizzierten Erkenntnisse und Schlussfolgerungen kritisch zu hinterfragen und um Ihre Sichtweisen, Erfahrungen und Lösungsansätze anzureichern. Um die Diskussion möglichst effizient zu strukturieren, haben wir dazu hier als Orientierungshilfe einige Fragen an Sie formuliert:

Strategien / Governance 	■ Wie schätzen Sie die Auswirkungen der Digitalisierung auf den Finanzmarkt ein? 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 sind disruptive Entwicklungen am Finanzmarkt (dh bis zu einer Ablösung des Grundprinzips des Kerngeschäfts) aus Ihrer Sicht mittel- bis langfristig zu erwarten? ■ 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? ■ Welche konkreten positiven, aber auch negativen Entwicklungen bezüglich „digitaler“ Finanzprodukte sind aus Ihrer Sicht zu beobachten? ■ In welchen Bereichen bestehen aus Ihrer Sicht Hindernisse für die Digitalisierung bzw. die Entwicklung von neuen digitalen Finanzprodukten? ■ Welche konkreten regulatorischen Vorgaben sind durch die Digitalisierung des Finanzsektors noch notwendig? ■ Wie soll der Aufbau von Allgemeinbildung in den Bereichen Finanzen (financial literacy) und digitale Technologien (digital literacy) gefördert und ggf. gefordert werden? ■ Was ist Ihre Erwartungshaltung hinsichtlich der Rolle der Aufsicht bei der digitalen Transformation des österreichischen Finanzmarktes? Welche Aufgaben soll aus Ihrer Sicht die FMA im Rahmen des Anleger-, Versicherten- und Gläubigerschutzes bezüglich „digitaler“ Finanzprodukte wahrnehmen?
Technologien 	■ Sollen weitere digitale Technologien bzw. Einsatzmöglichkeiten in die Betrachtung der Implikationen der Digitalisierung für den österreichischen Finanzmarkt einbezogen werden? ■ 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? ■ Welche Rechtsunsicherheiten sind aus Ihrer Sicht mit dem Einsatz neuer digitaler Technologien verbunden? ■ Was ist Ihre Erwartungshaltung hinsichtlich der Rolle der Aufsicht in den einzelnen Sektoren des Finanzmarkts in Bezug auf die einzelnen Technologien und insb. in Bezug auf den Einsatz künstlicher Intelligenz?

Vertrieb 	▪ Welche Aufgaben soll die FMA im Rahmen des Anleger-, Versicherten- und Gläubigerschutzes im Hinblick auf die Digitalisierung der Kundenschnittstellen 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 (inkl. Marketing-Automatisierung, Robo advice, Vergleichsportale und digitale Vertriebsplattformen) sind aus Ihrer Sicht zu beobachten?
Cyber-Resilienz 	▪ Mit welchen weiteren Maßnahmen bzw. Initiativen könnte die FMA zur Erhöhung der Cybersicherheit am Finanzmarkt konkret beitragen? ▪ Welche Kernbereiche der IKT-Sicherheit sollten von beaufsichtigten Unternehmen prioritär verstärkt werden? ▪ Sollten von den Unternehmen des österreichischen Finanzmarktes spezielle (im DORA nicht unmittelbar normierte) Maßnahmen zur künftigen Abwehr von Cyber-Attacken eingesetzt werden? ▪ Welche Rechtsunsicherheiten, Chancen und Risiken sehen Sie iZm Cyberversicherungen?
Cyber-Bedrohungen 	▪ Welche konkreten Entwicklungen hinsichtlich von Cyber-Angriffen sind zu beobachten? ▪ Sind aus Ihrer Sicht einige Sektoren / Finanzdienstleistungen besonders exponiert / verwundbar bzw. speziellen Cyber-Bedrohungen ausgesetzt? ▪ Welche Cyber-Bedrohungsszenarien könnten in Zukunft besonders relevant für den österreichischen Finanzmarkt sein?
IKT-Vernetzungen 	▪ 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?

ABKÜRZUNGSVERZEICHNIS

ACL	Access Control Lists
AI	Artificial Intelligence
AIFM	Alternative Investmentfonds Manager
API	Application Programming Interface
AWS	Amazon Web Services
BIA	Business-Impact-Analyse
bspw.	beispielsweise
BVK	Betriebliche Vorsorgekassen
bzgl.	Bezüglich
ca.	circa
CISO	Chief Information Security Officer
DACH	bezeichnet die drei deutschsprachigen Länder Deutschland, Österreich und Schweiz
DDoS	Denial-of-Service-Angriffe
dh	das heißt
DLT	Distributed Ledger Technology
DORA	Digital Operational Resilience Act
dzbgl.	diesbezüglich
EK	Europäische Kommission
Etc.	et cetera
ESG	Environmental, Social und Governance
ETF	Exchange-Traded Fund
EU	Europäische Union
EWR	Europäischer Wirtschaftsraum
FIDA	Financial Data Access
FMA	Finanzmarktaufsicht
FMABG	Finanzmarktbehördenaufsichtsgesetz
ggf.	gegebenenfalls
GLM	Generalized Linear Model
IaaS	Infrastructure as a Service
IDD	Versicherungsvertriebsrichtlinie (EU) 2016/97
IKT	Informations- und Kommunikationstechnik
ImmoKAG	Immobilienkapitalanlagegesellschaften
inkl.	inklusive
insb.	Insbesondere
IoT	Internet of Things
iSv	Im Sinne von
IT	Informationstechnologie
iZm	in Zusammenhang mit
KAG	Kapitalanlagegesellschaften; hier iSv Verwaltungsgesellschaften, dh KAG, ImmoKAG, AIFM
KfZ	Kraftfahrzeug
KI	Kreditinstitute / künstliche Intelligenz
KMU	kleine und mittelgroße Unternehmen
KYC	Know your Customer
MI	Marktinfrastrukturen
Mio.	Millionen
Mrd.	Milliarden
MS Office	Software-Paket von Microsoft (beinhaltet beispielsweise Word, Excel und Powerpoint)
NLP	Natural Language Processing
o.Ä.	oder Ähnliches
PaaS	Platform as a Service
PK	Pensionskassen
Pkt.	Punkt

rd.	rund
RPA	Robotic Process Automation
SaaS	Software as a Service
SAP	ein Softwarekonzern mit Sitz in Deutschland
SI	signifikante Institute
SIEM	Security Information and Event Management
SLA	Service-Level-Agreement
SOC	Security Operations Center
sog.	sogenannt
Tsd.	Tausend
u.a.	unter anderem
uU	unter Umständen
VAG	Versicherungsaufsichtsgesetz 2016
VASP	virtuelle Asset Provider
vs.	versus
VU	Versicherungsunternehmen
XR	Extended Reality
WPF	Wertpapierfirmen; hier Wertpapierfirmen und Crowdfunding-Dienstleister
ZaDiG	Zahlungsdienstegesetz
zB	zum Beispiel
ZI	Zahlungsinstitute