inventx

Die Zukunft der IT-Architektur von Banken und Versicherungen

Der Weg zur innovativen, skalierbaren & resilienten Finanz-IT

Vorwort

Die Schweizer Finanz- und Versicherungsindustrie befindet sich in einer Phase tiefgreifender technologischer und organisatorischer Transformation. Der Druck zur Digitalisierung, neue Kundenanforderungen, stetig steigende Regulierungen und der intensivere Wettbewerbsdruck stellen Banken und Versicherungen vor die Herausforderung, ihre IT-Architekturen grundlegend neu zu denken. Traditionelle, monolithisch geprägte Anwendungslandschaften stossen zunehmend an ihre Grenzen – in ihrer Innovationsfähigkeit, ihrer Skalierbarkeit und den steigenden Kosten.

In diesem Kontext gewinnen moderne Ansätze der IT-Architektur wie «Composable Architecture» an strategischer Bedeutung. Der Ansatz verspricht eine modulare, flexible und erweiterbare IT-Architektur, die es Unternehmen ermöglicht, schneller auf Marktveränderungen zu reagieren, Innovationen gezielt zu integrieren und die technologische Komplexität nachhaltig zu beherrschen. Doch der Weg dorthin ist kein rein technischer: Er erfordert ein Umdenken in Governance, Betriebskonzept, Sourcing und Kultur.

Dieses Booklet entstand im Rahmen eines Innovationsprojekts im InventxLab. Es soll Entscheidungsträgerinnen und Entscheidungsträgern im Banking und Versicherungswesen einen Orientierungsrahmen bieten, wie die Modernisierung der IT-Architektur strategisch gestaltet und umgesetzt werden kann. Das Booklet verbindet konzeptionelle Grundlagen mit praktischen Einblicken, bewertet Chancen und Risiken und zeigt auf, welche Weichenstellungen heute notwendig sind, um die Zukunft aktiv zu gestalten. Wir laden die Leserinnen und Leser ein, die folgenden Seiten als Impuls zu verstehen – als Grundlage für den Dialog über die nächste Evolution der Enterprise-IT.

Mein besonderer Dank gilt Hans Nagel, dem Co-Founder von Inventx. Nicht nur hat er das InventxLab im Jahr 2021 zum Leben erweckt, sondern unermüdlich unsere Ideen reflektiert und wertvollen Input geliefert. Ebenso danke ich all den Kolleginnen und Kollegen, die mit ihren Impulsen massgeblich zu diesem Booklet beigetragen haben. In diesem Sinne geht ein grosses Dankeschön an Fabio Cortesi, Rino Decurtins, Philippe Müller, Marco Luzi, Damian Soldera, Richard Schmid, Thomas Fröhlich, Benjamin Scheiwiler, Sven Lenz und Carla Caspar. Ebenso bedanke ich mich herzlich bei Roman Dinkel für die Realisierung dieses Booklets in unserem Marketing.

Urs Rhyner, Leiter InventxLab, Dezember 2025

Inhaltsverzeichnis

Abbildungsverzeichnis

IT-Architektur-Blueprints für Banken & Krankenkassen

Die Durchdringung von Informationstechnologien bei den Banken und Versicherungen ist im Vergleich mit anderen Branchen hoch. Insbesondere in der Schweiz, wo die Arbeitskosten im internationalen Vergleich überdurchschnittlich relevant sind. Die zunehmende (Hyper-)Digitalisierung führt dazu, dass weitere Business-Applikationen in die bestehenden Landschaften integriert werden. Manch ein Unternehmen setzt zudem in der Modernisierung der IT-Anwendungslandschaft auf spezialisierte Applikationen, die funktional zwar oft mit dem branchenspezifischen Kernsystem abgedeckt wären – aber eben nicht ganz optimal. Entsprechend nehmen die Kosten und die Komplexität laufend zu. Zeit also, einen Blick in die Zukunft der Finance-IT zu werfen und einen Orientierungsrahmen für die kontinuierliche Transformation der IT-Architektur zu schaffen.

Die Dynamik wird weiterhin zunehmen und anstehende IT-Investitionen sollen reflektiert und zielorientiert sein. Wir haben uns deshalb zuerst gefragt, welches die kritischen Trigger der Veränderung der IT-Architektur sind. Diese haben wir in «Designprinzipien» zusammengefasst und anschliessend ein standardisiertes, high-level Architektur-Modell geschaffen. Dieser modellartige IT-Architektur-Blueprint soll eine logische Grundstruktur für die Transformation schaffen und Funktionen zu logischen Clustern bzw. Domänen bündeln – bewusst noch ohne vertikale Differenzierung für Banken oder Versicherungen.

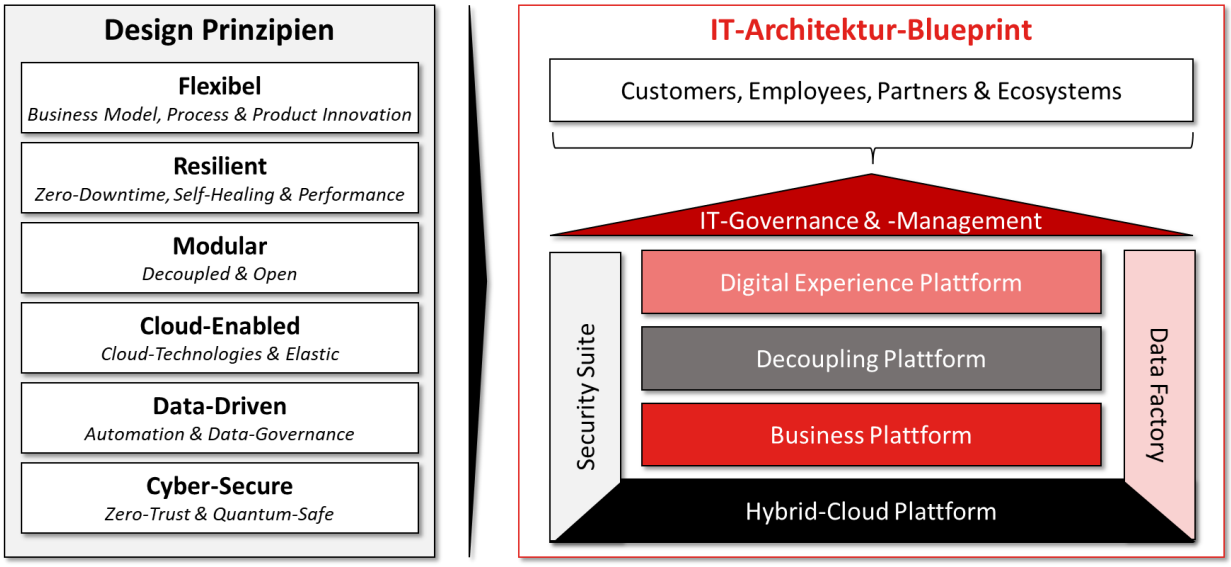


Abbildung 1: Plattform-Modell der IT-Architektur

Mit diesem plattformorientierten Basis-Modell haben wir im Anschluss die Anwendungslandschaften in den Ausprägungen «Bank» und «Krankenversicherung» definiert, wobei sich die Vertikalisierung primär in der «Business-Plattform» zeigt. Auf die branchenspezifischen Unterschiede in der «Digital-Experience-Plattform» sind wir auf dieser Abstraktionsebene bewusst nicht eingegangen. Ziel ist es, mit diesen Referenz-Architekturen eine praktische Hilfestellung und Diskussionsbasis für die Weiterentwicklung der IT-Architektur zur Verfügung zu stellen.

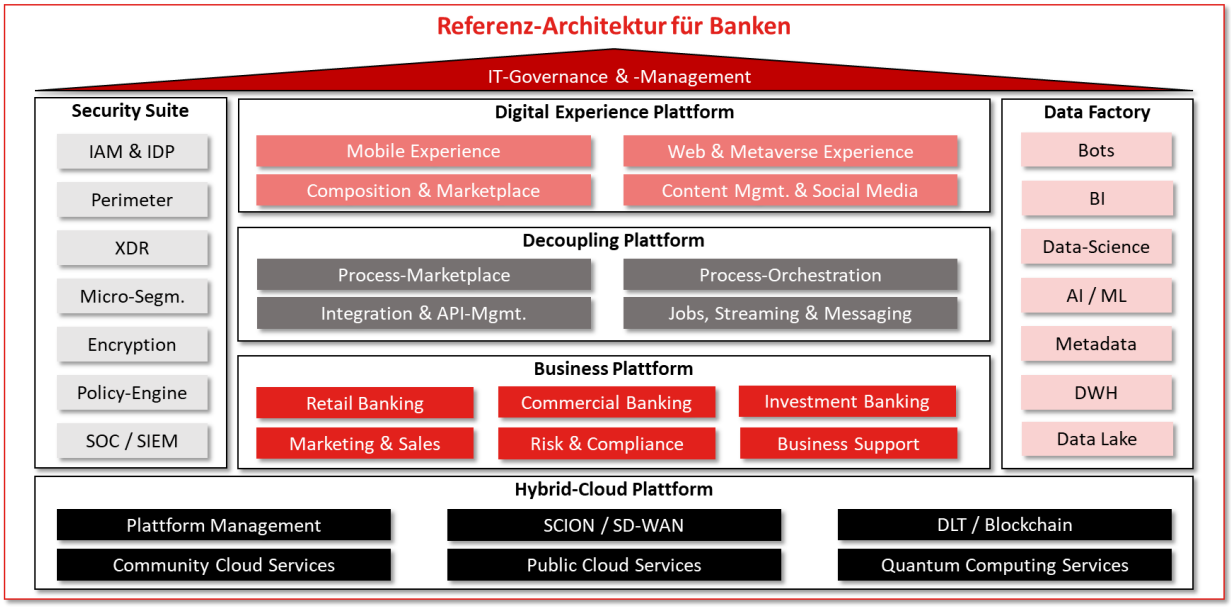


Abbildung 2: Architektur-Blueprint für Banken

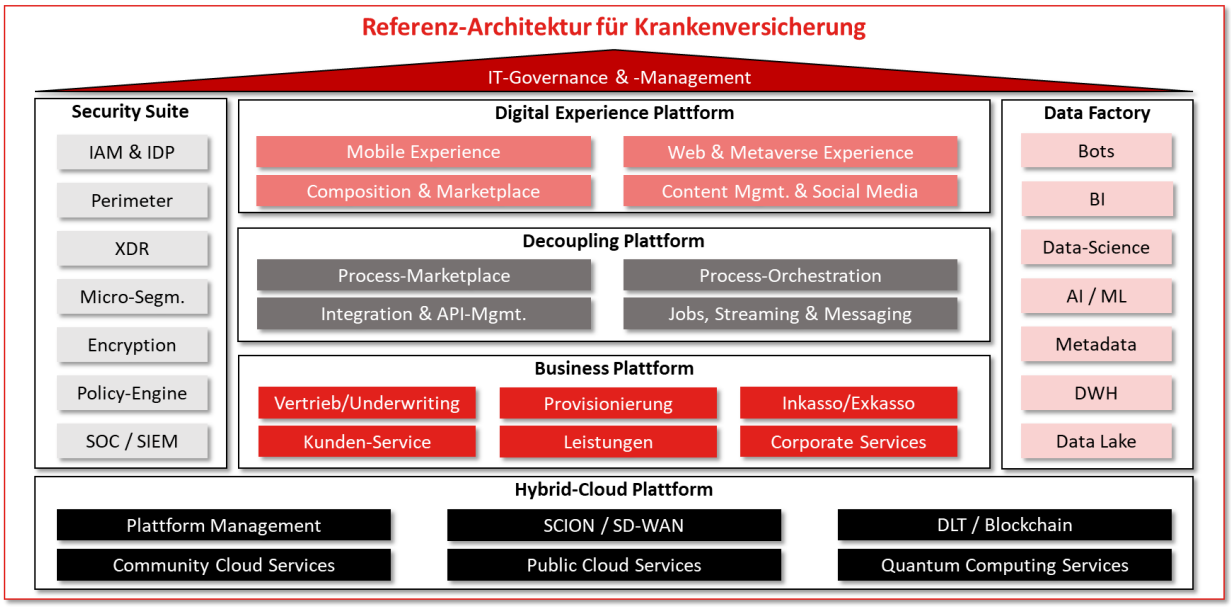


Abbildung 3: Architektur-Blueprint für Krankenversicherungen

Hybrid-Cloud-Plattform: Die künftige Infrastruktur-Plattform (IaaS/PaaS) besteht einerseits aus Community-Cloud- und Public-Cloud-Services aber auch aus den aufstrebenden Technologien Quantum Computing und Blockchain. Diese Plattformen sorgen dafür, dass alle Workloads die optimalen Betriebsbedingungen vorfinden, ganz egal ob CPU, GPU, Qbit oder DLT. Weiter gilt es die sichere und performante Inter-Konnektivität (WAN) der dezentralen Cloud-Plattformen sicherzustellen, das Schutzlevel zu erhöhen und die Plattform in die erforderlichen Desaster-Recovery-Zonen zu strukturieren. Die Microsegmentierung (Cloud-LAN) – obwohl per Definition Teil des IaaS-Stack – führen

wir im Bereich der Security Suite, da für uns nicht das Netzsegment per se, sondern die Kontrolle der Kommunikation zentral ist.

Business-Plattform: Die Business-Plattform bildet die Geschäftsmodelle sowie die Geschäftsprozesse des Unternehmens ab. Aktuelles Herzstück dieser Gruppe bildet das Kernsystem (z. B. Finnova, Avaloq oder Syrius), wobei dieses mit diversen Umsystemen ergänzt wird. Umsysteme können vertikalen Charakter aufweisen (z. B. Zahlungsverkehr, Leistungsabrechnung) oder branchenneutral/horizontal sein (z. B. Dokumentenarchiv, Output-Management). Die monolithischen Strukturen der heutigen Kernanwendung werden noch weiter aufgebrochen und die Funktionalität und die Datenhaltung dadurch zunehmend dezentralisiert.

Decoupling-Plattform: Der Decoupling-Plattform kommt eine zentrale Rolle in der Integrationsarchitektur zu. Hier werden die einzelnen (internen und externen) Services orchestriert, die zahlreichen Anwendungen auf Basis von Schnittstellen (API-first) integriert und sicher gegen aussen geöffnet (Stichwort: Open Finance). Weiter wird der Datentransfer zwischen den Anwendungen gesteuert resp. die Konsistenz der dezentralen Datenhaltung sichergestellt. Dies ist ein zentraler Paradigma-Wechsel im Vergleich zur heutigen «Golden Record»-Architektur.

Experience-Plattform: Eine moderne Experience-Plattform bildet die digitale Interaktionsschicht für Kunden, Mitarbeitende und Partner von Banken und Versicherungen. Sie integriert Frontend-Kanäle wie Web, Mobile und Self-Service-Portale mit den dahinterliegenden Systemen und Datenplattformen. Durch ihre hohe Flexibilität und die Fähigkeit, personalisierte Services schnell auszuspielen, wird die Experience-Plattform zu einem zentralen Differenzierungsfaktor im Wettbewerb und stärkt nachhaltig die digitale Positionierung am Markt.

Security Suite: In der Security Suite werden die IT-Sicherheitsfunktionen über alle Service-Modelle (IaaS/PaaS/SaaS) auf Basis des Zero-Trust-Konzepts zentral verwaltet. Dem Access Management kommt dabei eine zentrale Rolle und faktisch der gleiche Stellenwert wie dem klassischen Perimeter (Firewall, WAF etc.) zu. Die IT-Security-Konfiguration soll dabei auf Basis der definierten Policies als Code verwaltet und auf den Systemen der Hybrid-Cloud angewendet werden. Die Logs aller Endpoints (Clients, Server, Anlagen) werden in einem Data Lake gesammelt und auf Anomalien geprüft, wobei die Anwendung von künstlicher Intelligenz (KI) und die risikobasierte Ausgestaltung von Detection Use Cases besonders hervorzuheben sind.

Data Factory: Dem dezentralen Datenmanagement und der systematischen Nutzung von Geschäftsdaten in Kombination mit externen Daten kommt eine strategische Rolle zu. Um KI-Anwendungen wie Bots und Machine Learning Services wie Fraud Detection optimal zu nutzen, gilt es Daten im Data Lake zu sammeln und allenfalls anzureichern, um sie dann den Ziel-Anwendungen in der richtigen Qualität, Struktur und möglichst real-time zur Verfügung zu stellen. Die Regeln der Dateninterpretation (Metadaten) sorgen für die automatisierte und sichere Verarbeitung der Daten.

IT-Governance und -Management: Ein leistungsfähiges IT Service Management (ITSM) und eine klare Governance-Struktur bilden das Rückgrat einer stabilen und regelkonformen IT-Landschaft in Banken und Versicherungen. Standardisierte Prozesse, transparente Verantwortlichkeiten und durchgängige Automatisierung sorgen für hohe Servicequalität, schnelle Reaktionszeiten und effiziente Betriebsprozesse über verschiedene Leistungserbringer hinweg. Gleichzeitig stellen integrierte Governance-Mechanismen sicher, dass regulatorische Vorgaben jederzeit erfüllt und Risiken konsequent gesteuert werden. Durch eine robuste, automatisierte und auditfeste ITSM- und Governance-

Architektur schaffen Banken und Versicherungen eine nachhaltige Differenzierung im Wettbewerb, da sie Innovation schneller, sicherer und mit höherer Verlässlichkeit in den Markt bringen können.

In den folgenden Kapiteln tauchen wir nun vertieft in die einzelnen Plattformen der Referenz-Architektur ein und beleuchten aktuelle Herausforderungen, Trends und Lösungsansätze für die Zukunft.

Business-Plattform: Zentrales Organ der Anwendungs-landschaft

Als erstes Element unserer Referenz-Architektur beleuchten wir in den Motor des Geschäftsmodells: die Business-Plattform. Sie bildet die Funktionen der wichtigsten Geschäftsprozesse ab – gewissermassen den «Blutkreislauf» des Geschäftsmodells und ist absolut zentral für die Erfüllung des Zwecks einer jeden Unternehmung. Je komplexer das Geschäftsmodell, desto umfassender muss die Anwendungslandschaft in der Business-Plattform ausgestaltet werden.

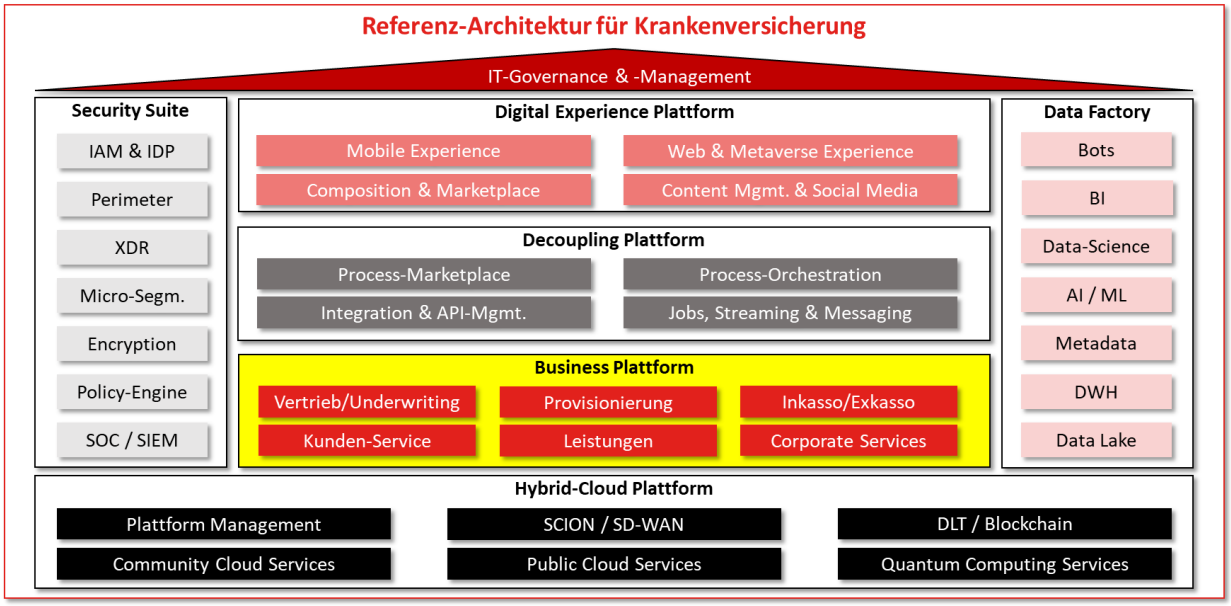


Abbildung 4: Business-Plattform

Die Business-Plattform von Banken und Krankenversicherungen ist mittlerweile in die Jahre gekommen und wird von monolithischen Kernsystemen geprägt. Die etablierten Kernsystem-Hersteller arbeiten derzeit an der Modernisierung ihrer Software. Der Umbau muss von Kunden in den kommenden Jahren vollzogen werden. Dieser Schritt wird bei allen involvierten Parteien signifikante Ressourcen binden und beträchtliche Investitionen erfordern. Ob die aktuellen Systeme mit diesem Umbau die Anforderungen der Zukunft erfüllen, ist allerdings noch ungewiss. Dies hängt primär von der Wettbewerbsdynamik ab – also dem Kosten- und Innovationsdruck der Branche.

Das Gebot der Stunde muss also sein, die IT-Architektur auf unterschiedliche Szenarien der Zukunft auszurichten. Am Anfang steht deshalb die Frage, welche Treiber die Modernisierung anstossen. Als wichtigste Kriterien können wir die steigenden Kosten, die mangelnde Flexibilität und den stetig sinkenden Beitrag für die Geschäftsentwicklung festmachen, wie nachfolgende Abbildung zeigt.

Abbildung 5: Treiber der Modernisierung

Im nächsten Schritt müssen die Anforderungen an die moderne Business-Plattform betrachtet werden. Die wichtigste Anforderung ist aus unserer Sicht die Flexibilität. Es geht darum, dass das bestehende und neue Geschäftsmodelle abgebildet und die dazugehörenden Geschäftsprozesse organisations-übergreifend und effizient abgewickelt werden können. Die Halbwertszeit von Geschäftsmodellen und insbesondere Prozessen sinkt jedoch weiter und es ist darauf zu achten, dass neue Produkte und Business-Prozesse einfach implementiert werden können. Die wichtigsten Anforderungen haben wir wie folgt zusammengefasst:

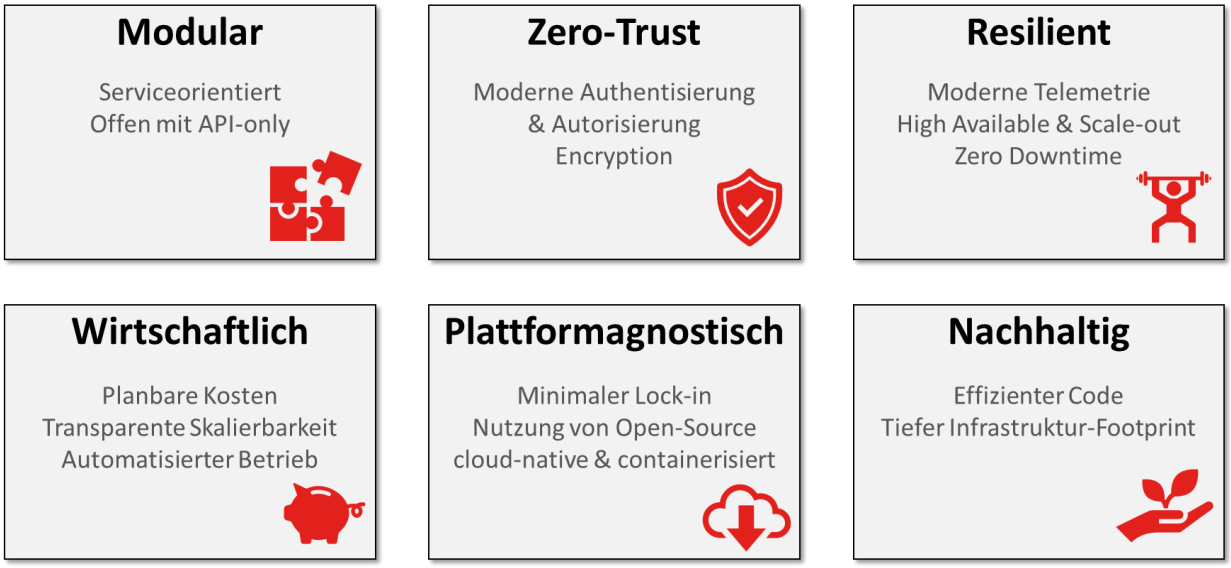
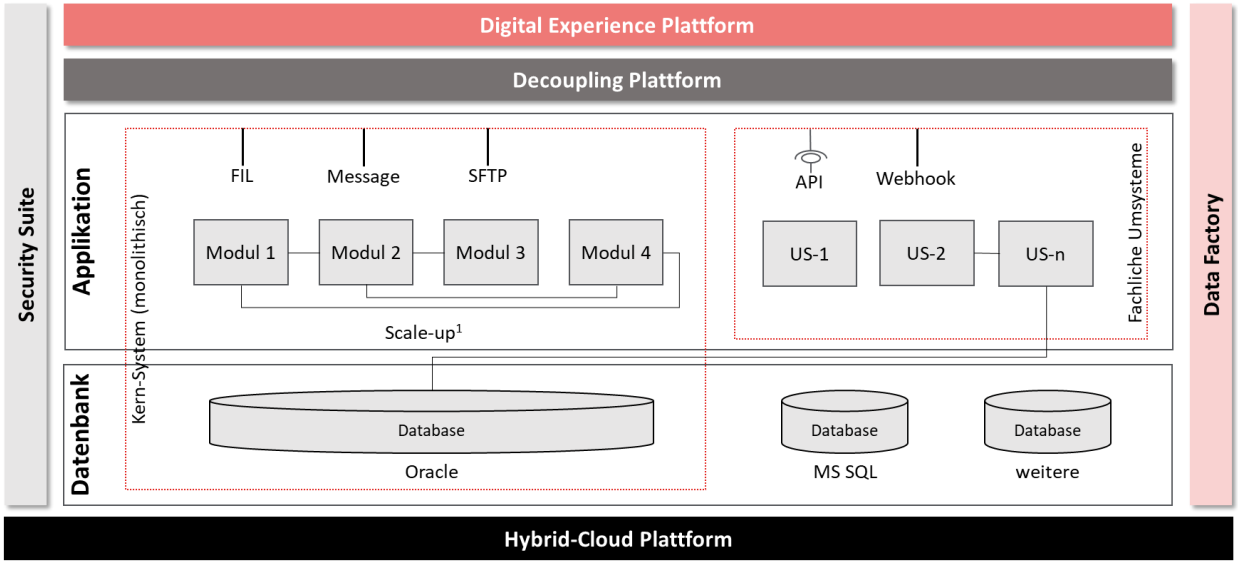


Abbildung 6: Anforderungen an die Business-Plattform

Stärken und Schwächen

Die aktuelle Anwendungslandschaft der Business-Plattform ist über die vergangenen Jahre organisch gewachsen. Neben funktionalen Erweiterungen müssen regelmässig neue regulatorische Vorgaben integriert werden. Die Heterogenität und Komplexität, die Gesamtkosten und der «technische Schuldenberg» nehmen laufend zu. In den letzten Jahren führte diese Entwicklung (vgl. itopia, 2024) bei Banken zu einem Kostenanstieg von rund 14 Prozent pro Jahr. Für die Versicherungsindustrie liegen uns keine Daten vor, jedoch gehen wir von ähnlichen Werten aus, da der Regulationsdruck vergleichbar ist. Neue Vorhaben sind zusehend schwierig in der Umsetzung und erfordern eine aufwändige Koordination – typischerweise über mehrere Parteien hinweg. Die laufenden Kosten des IT-Betriebs sowie der unausweichliche Technologie-Refresh verdrängen zunehmend die Budgets für Digitalisierungsprojekte, die im Business oder bei Kunden spürbaren Mehrwert erzeugen.

Auch im Betrieb stellt die derzeitige Business-Plattform eine grosse Herausforderung dar. Die Orchestrierung von Wartungsvorhaben und die Steuerung der Abhängigkeiten innerhalb der Applikationslandschaft ist eine Herkulesaufgabe. Im Störungsfall gestaltet sich die Fehlersuche als zunehmend schwierig. Folglich ist die Einhaltung der Service Levels für Verfügbarkeit oder Wiederherstellung sehr anspruchsvoll, auch weil verschiedene Single Points of Failure existieren. Und eben: Nur weil Applikationen aktuell gewartet und fast ausnahmslos verfügbar sind, applaudieren weder Kunden noch die internen Fachbereiche!



[1] Der Applikationsserver-Syrius ist Scale-out

Abbildung 7: Typische Kernsystem-Architektur

Die heute betriebene Anwendungslandschaft der Business-Plattform hat jedoch auch Vorteile: Beim Grossteil der Applikationen können wir auf profundes Wissen von erfahrenen Mitarbeitenden zurückgreifen. Diese Anwendungen basieren auf etablierten Technologien, die von zahlreichen Unternehmen seit Jahren genutzt werden. Kommt hinzu, dass die Stabilität der Anwendungen (Solidität) nach all den Jahren grundsätzlich gegeben ist. Wären da nur nicht Wartung und Weiterentwicklung sowie die dynamischen Kundenbedürfnisse!

Transformation der Kernsysteme

Die technologische Transformation der Business-Plattform muss einerseits das Szenario abdecken, dass das monolithische Kernsystem durch den SW-Hersteller erfolgreich umgebaut wird. Andererseits aber auch die Flexibilität bieten, damit andere Lösungsansätze umsetzbar sind. Der Entkopplung und Modularisierung kommt dabei eine absolut strategische Rolle zu (die Vertiefung der Decoupling-Plattform folgt).

Unsere Analyse der laufenden Vorhaben der Kernsystem-Hersteller zeigt folgende Trends:

- Der Monolith wird aufgebrochen und in eine (micro-)serviceorientierte Struktur überführt.
- Die einzelnen Module werden unabhängig und können daher individuell entwickelt, betrieben und gewartet werden.
- Die einzelnen Module werden geöffnet und entsprechende Standard-Schnittstellen (API) zur Verfügung gestellt.
- Module werden containerisiert und können auf PaaS-Services betrieben werden.
- Syrius von Adcubum kann mit Oracle oder PostgreSQL betrieben werden – ein gewichtiger Lock-in würde aufgelöst.

Es bewegt sich etwas bei den Kernsystemen und es geht in eine positive Richtung. Die effektive Maturität (Stichwort: 12-Factors) der neuen Software kann aber erst mit der Veröffentlichung beurteilt werden. Wir stellen jedoch auch fest, dass die Infrastruktur-Plattform und damit die Wahl des Kunden hinsichtlich Betriebsplattform eingeschränkt wird. Dies führt zu neuen resp. zusätzlichen Lock-ins (z. B. OpenShift statt open-source Kubernetes). Diese Vorgabe ist aus Sicht Support & Wartung des Software-Hersteller zwar nachvollziehbar, aber bzgl. Skalierung und Betrieb der gesamten IT-Anwendungslandschaft nachteilig. Ferner stellen wir fest, dass die Kernsystem-Hersteller durch funktionale Erweiterungen wachsen und einen proprietären Integration Layer zur Verfügung stellen. Damit wird den Kunden die Integrationstechnologie der Kernapplikation vorgegeben, eine weitere, indirekte Abhängigkeit zum Kernsystem geschaffen und der Lock-in potenziell verstärkt.

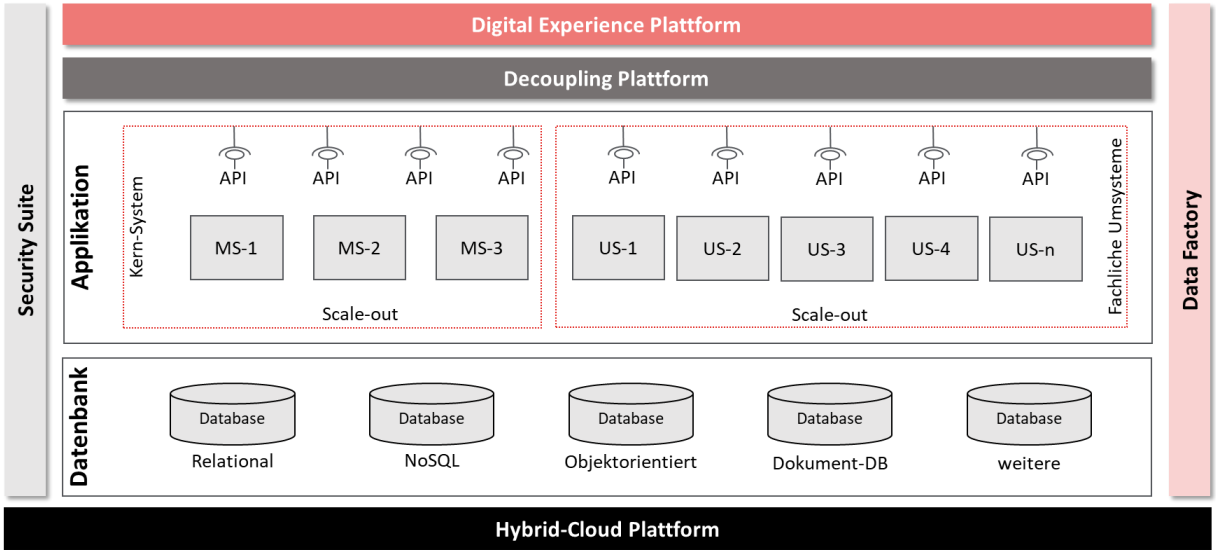


Abbildung 8: Modernisierung des Kernsystems

Auch bei den Umsystemen bewegt sich etwas. Bei den Herstellern von Standard-Produkten sehen wir nur zögerliche Efforts, die Applikationen zu modernisieren. Dies erklären wir uns primär mit knappen Entwicklungsressourcen für die Modernisierung im Vergleich zur Software-Wartung oder neuen Funktionalitäten (insb. bei KMU). Eine ähnliche Maturität beobachten wir auch bei Neueinführungen von Standard-Software-Produkten. Bei Individualentwicklungen ist die Maturität grundsätzlich höher. All das bedeutet, dass die Umsystem-Landschaft in absehbarer Zeit keine drastische Vereinfachung und technische Harmonisierung erlaubt und folglich in vier Pattern strukturiert werden kann:

1. Pattern – Legacy: Monolithische Applikationen (Scale-up, Legacy-Technologien, keine API, Fat Client)
2. Pattern – Cloud enabled: Klassische 3-Tier-Anwendung (Scale-up, Intranet-zentriert, Fat Client)
3. Pattern – Cloud ready: Moderne 3-Tier-Anwendung (Scale-out, public adressiert, API, WebGUI)
4. Pattern – Cloud native: 12-Factor-App (Container, public adressiert, API, Composable Experience)

Neben den technischen Umbauarbeiten gilt es das Augenmerk auch auf das IT-Betriebskonzept zu richten. Klar ist, dass die Modernisierungen der Anwendungen in der Business-Plattform das IT-Betriebskonzept nur marginal vereinfachen wird. Aus unserer Sicht ist deshalb zentral, dass eine gesamtheitliche Perspektive eingenommen wird. Der Anteil an SaaS wird bei den Umsystemen zunehmen. Ebenso arbeiten die Kernsystem-Hersteller an SaaS-Angeboten. Je mehr Parteien und Plattformen in der Integration, Wartung und dem Support der Applikationslandschaft beteiligt sind, desto aufwändiger wird die Koordination unter den Parteien. Es stellt sich die Schlüsselfrage, ob die Bank oder Versicherung diese Orchestrierung übernehmen will. Kommt hinzu, dass Applikationen ohne Möglichkeiten des asynchronen Datenaustauschs die technische und örtliche Nähe zu anderen Anwendungen benötigen. Es ist folglich ratsam, eine Multi-Cloud-Strategie hinsichtlich der gesamten Anwendungslandschaft zu konzeptionieren und diese finanziell, technisch und organisatorisch eingehend zu beleuchten. Neben den klassischen Kernprozessen wie Incident, Change und Release rücken IT Service Continuity Management und Cyber Defence zunehmend in den Fokus – nicht zuletzt durch die Regulation (Resilienz).

Moderne Neo-Core-Systeme

Parallel zur Modernisierung der traditionellen Kernsysteme werden derzeit Core-Applikationen der neusten Generation entwickelt. Am Beispiel Vault von Thought Machine, einem führenden Hersteller eines solchen Kernsystems für Banken, stellen wir signifikante Unterschiede im Konzept der Software und der IT-Architektur fest:

A) Scope: Vault Core ist ein reines Kernsystem mit sehr fokussiertem Funktionsumfang.
B) Offenheit: Datenströme und Konfigurationen werden über API orchestriert (API-only).
C) Modern: Die Anwendung ist cloud-nativ, scale-out und plattform-agnostisch.
D) Resilient: Moderne Technologien sorgen für hohe Verfügbarkeit und Resilienz.

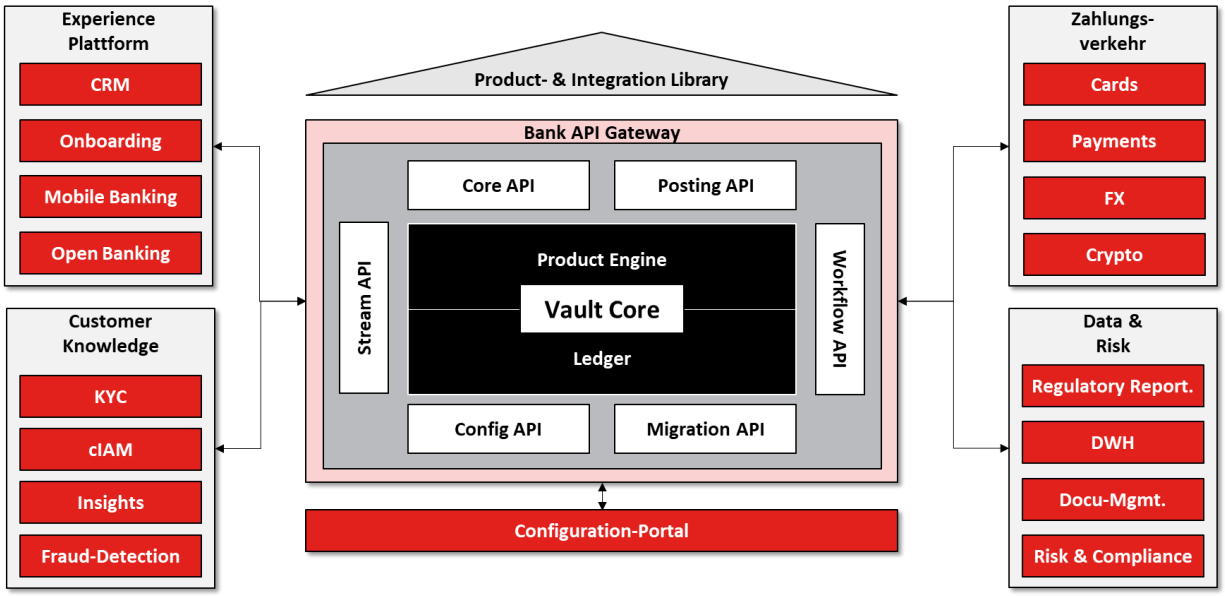


Abbildung 9: Architektur eines Neo-Core-Systems

Fazit

Die Business-Plattform von Banken und Krankenversicherungen ist in Bewegung. Die laufende Modernisierung der Kernsysteme wird in den kommenden Jahren bedeutende Investitionen im gesamten Ökosystem binden. Es bleibt offen, ob die derzeitigen Lösungen inklusive Umbau den funktionalen und nicht-funktionalen Anforderungen und hinsichtlich Kosten und Innovationsfähigkeit der Geschäftsmodellentwicklung gerecht werden. Wir empfehlen deshalb die IT-Architektur im Kontext der gesamten Anwendungslandschaft auf unterschiedliche Szenarien auszurichten. Dazu empfehlen wir, die folgenden Prinzipien in der IT-Strategie zu verankern:

- **Decoupling:** Die Applikationslandschaft muss systematisch entkoppelt werden, ohne den Lock-in zu vertiefen.
- **Unabhängigkeit:** Der Betrieb der Anwendungslandschaft soll möglichst unabhängig von der Cloud-Plattform sein.
- **Organische Modernisierung:** Technische Schulden sind im Rahmen von Releases aktiv abzubauen bzw. bei neuen Anwendungsintegrationen zu verhindern.
- **Kostenstrukturen:** Die Kostenstrukturen sind zu variabilisieren und an transparente, verbrauchsorientierte Metriken zu knüpfen.
- **Applikationslandschaft:** Die Weiterentwicklung der IT-Architektur ist nicht ans Kernsystem gebunden, sondern auf Basis der Gesamtanwendungslandschaft und der Cloud-Plattform-Strategie auszugestalten.
- **Zero Trust**: Die Sicherheitsarchitektur wird konsequent auf Zero Trust ausgerichtet.
- **Datenzentriert**: Den Datenaustausch zwischen den Anwendungen direkt (real-time) und indirekt über die Datenplattform systematisch trennen.

Decoupling-Plattform: Dreh- und Angelpunkt der IT-Strategie

Die Komplexität und die grossen Abhängigkeiten innerhalb der Anwendungslandschaft machen den Betrieb, die Wartung und auch die Umsetzung von Innovationsprojekten zunehmend anspruchsvoll und zäh. Die Sicherstellung des Betriebs und die fortlaufenden Technologie-Erneuerungen (Tech-Refresh) beanspruchen einen Grossteil der finanziellen und personellen Ressourcen in der IT. Es erfordert überdies einen hohen Koordinationsaufwand mit zahlreichen Partnern und Software-Herstellern, welche einen massgeblichen Einfluss auf den gesamten Technologieeinsatz haben. Die freien Kapazitäten für Innovationen gegenüber Kunden und Fachbereichen wird dadurch signifikant eingeschränkt. Um die IT-Architektur auf unterschiedliche Optionen der Zukunft auszurichten, ist die Entkopplung der Anwendungslandschaft ein Imperativ. Beleuchten wir nun also die Decoupling-Plattform, welche als zentrale Drehscheibe in der Integration von verteilten Systemen unerlässlich ist.

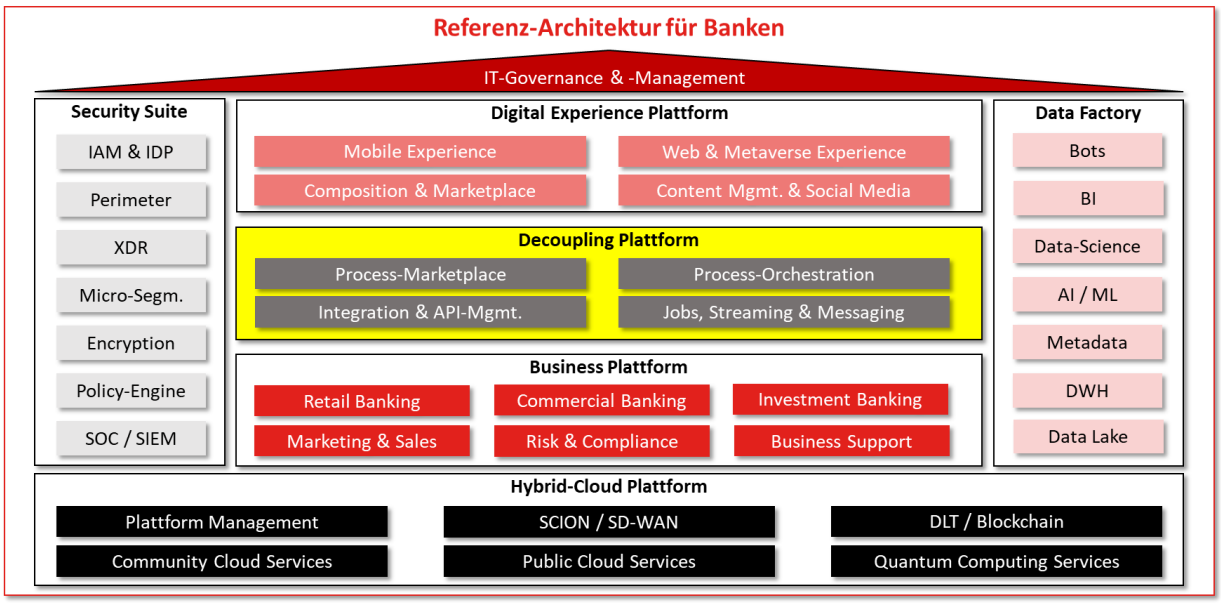


Abbildung 10: Decoupling-Plattform

Grundlagen: synchroner vs. asynchroner Datenaustausch

Mit dem Schritt, die hostbasierten Universal-Anwendungen mit unterschiedlichen Applikationen (Best-of-Breed-Strategie) abzulösen, kam der Integration von IT-Anwendungen eine wichtige Rolle zu, um die Daten nicht redundant pflegen zu müssen. Dieser Datenaustausch wurde früher mit proprietären und üblicherweise synchronen Schnittstellen realisiert. Der Begriff API – also Anwendungsprogrammier-schnittstelle – wurde erstmals 1974 von C.J. Date benutzt. Eine API ist ein Regelwerk, das festlegt, wie zwei Programme miteinander kommunizieren sollen. Mit den aufkommenden Webtechnologien und den damit verbundenen IT-Architekturen (Distributed Systems) wurden die API zum Standard der Anwendungsintegration. Besonders bekannt sind die so genannten REST- und SOAP-API. Diese Webservices basieren auf HTTP und dienen dazu, standardisierte Operationen wie «get» oder «delete»

ohne Zeitverzug auszuführen. Im Gegenzug werden die Daten des angefragten Systems in verschiedenen Formaten (xml, json etc.) bereitgestellt. Obwohl API und synchroner Datenaustausch in modernen IT-Anwendungen weit verbreitet und in vielen Szenarien äusserst nützlich sind, gibt es auch signifikante Nachteile. Denn bei einem synchronen Datenaustausch muss das Empfänger-System auf die Antwort des Senders warten, bevor die Verarbeitung stattfinden kann. Wir alle kennen das Phänomen des Timeouts eines Servers bei der Nutzung einer Webanwendung. Um diesen Nachteil und weitere Schwächen wie bspw. Latenz oder Single Point of Failure zu vermeiden, werden in der Anwendungsintegration auch sogenannte asynchrone Verfahren eingesetzt. In Umgebungen mit hoher Last, niedriger Latenz oder komplexen, ereignisgesteuerten Transaktionen – wie sie in der Finanzindustrie oft anzutreffen sind – sollten deshalb asynchrone Verfahren wie Message Queues oder event-basierte Verfahren genutzt werden, um die Flexibilität, Skalierbarkeit und Resilienz der Anwendungslandschaft zu verbessern. Natürlich mit dem Hauptunterschied, dass keine Real-Time-Daten zur Verfügung stehen. In unseren IT-Architektur-Konzepten sprechen wir bewusst von Decoupling. Denn mit der Decoupling-Plattform fassen wir wichtige, zentrale Funktionen für die Anwendungsintegration zusammen und bedienen den Bedarf nach synchronem und asynchronem Datenaustausch für die gesamte Anwendungslandschaft. Zudem möchten wir damit auch zum Ausdruck bringen, dass die Entkopplung nicht nur technisch, sondern auch organisatorische Abhängigkeiten adressiert.

Anspruchsvolle Anforderungen

Die Decoupling-Plattform ist das zentrale Bindeglied zwischen den so genannten Systems of Record resp. dem Kernsystem in der Business-Plattform und den Umsystemen, insbesondere den Applikationen in der Digital-Experience-Plattform und der Data Factory. Die Bedeutung dieser zentralen Vermittlungsfunktion ist enorm, wenn wir uns vor Augen führen, dass eine Bank bzw. Versicherung 150 und mehr unterschiedliche IT-Anwendungen für die Abwicklung ihres Geschäftsmodells nutzt.

Betrachten wir nun zuerst die funktionalen Anforderungen, welche an die Decoupling-Plattform in einer modernen IT-Architektur gestellt werden:

- **Prozesskoordination**: Integrieren, gestalten und automatisieren von anwendungsübergreifenden Prozessen.
- **Datenintegration**: Synchroner bzw. asynchroner Austausch von Daten inkl. Aufbereitung und Transformation (CDC/ETL).
- **Kommunikation**: Austausch von Nachrichten, Ereignissen und Transaktionen.
- **Sicherheit**: Verwaltung der Sicherheit im Datenzugriff mit Authentifizierung, Autorisierung und Consent Management.
- **Interoperabilität**: Übersetzung für heterogene Services, Protokolle und Technologien in einer Multi-Cloud-Architektur.
- **Management**: Überwachung und Protokollierung der Datenflüsse und Kommunikation inkl. einfacher Störungsbehebung.

Die nicht-funktionalen Anforderungen an die Decoupling-Plattform sind sehr hoch, denn ohne diese zentrale Drehscheibe funktioniert die Anwendungslandschaft in der Gesamtheit nur fehlerhaft. Neben einer hohen Performance muss die Plattform hochverfügbar ausgestaltet sein und eine skalierbare

Architektur aufweisen. Da auch kritische Geschäftsdaten unter den Anwendungen ausgetauscht werden, liegen höchste Anforderungen an die IT-Security vor – gerade, wenn wir von Hybrid-Cloud-Architekturen ausgehen. Ferner ist ein effizienter Betrieb, eine einfache Wartung, minimale Downtimes bei automatisiertem Release Management und der Einsatz von weit verbreiteten Technologien gewünscht.

Die Hauptfunktion der Decoupling-Plattform ist es, die Kommunikation und den Datenaustausch innerhalb einer komplexen Anwendungslandschaft zu erleichtern, ohne dass die einzelnen Applikationen direkt miteinander verbunden werden.

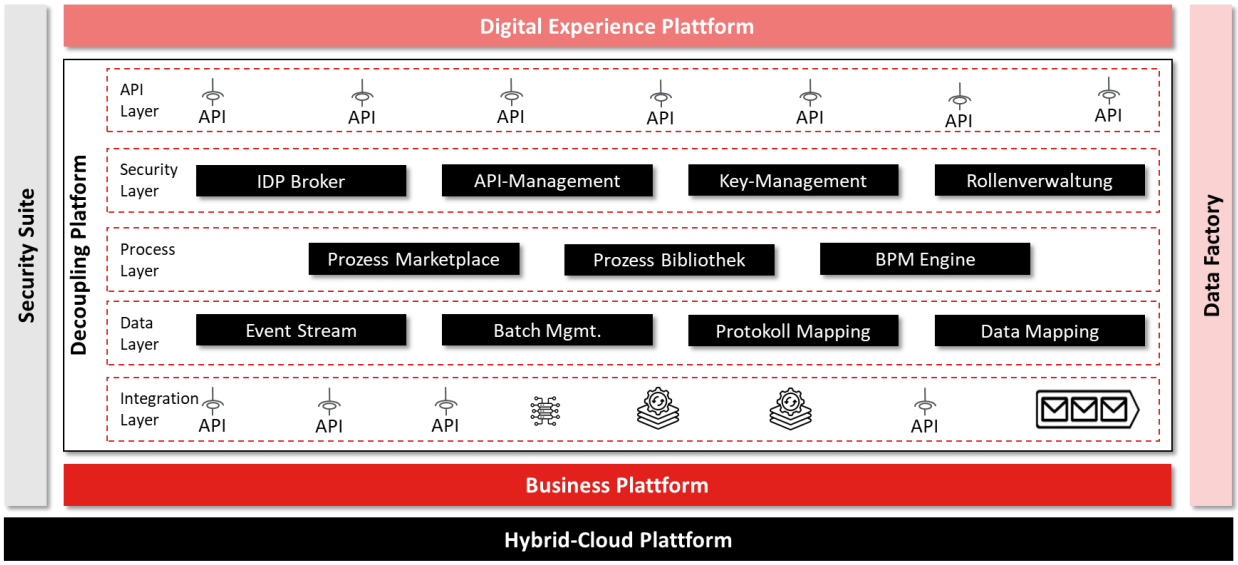


Abbildung 11: Funktionen der Decoupling-Plattform

Wir segmentieren die Decoupling-Plattform in einzelne Schichten, welche die funktionalen Leistungen wie folgt zusammenfassen:

- **Integration Layer:** Über den Integration Layer werden die Quellsysteme an die Plattform angebunden. Neben modernen Anwendungen, welche auf API beruhen, sind auch andere Verfahren abzudecken wie File Transfer, Event Streaming oder Messages.
- **Data Layer**: Im Data Layer werden die Daten so aufbereitet, damit sie vom Zielsystem genutzt werden können. Dies beinhaltet auch die Übersetzung für unterschiedliche Technologien.
- **Process Layer**: In diesem Bereich werden die Prozesse verwaltet. Neben eigenen Prozessen, welche aus den bestehenden Anwendungen in einer Bibliothek zusammengefasst werden, sind auch Marketplaces für Prozesse zu berücksichtigen, welche von Cloud-Plattformen zur Verfügung gestellt werden. Ferner werden für die Steigerung der Effizienz unterschiedliche Business-Prozesse in einer Process Engine abgebildet, wenn die Anwendungslandschaft Lücken im Prozesssystem aufweist.
- **Security Layer**: Dieser Teil der Decoupling-Plattform stellt sicher, dass nur erlaubte Kommunikationen und Datentransfers unterstützt werden. Ebenso werden die APIs für insb. die public-adressierten Webanwendungen verwaltet und die Verschlüsselung für den Datentransfer

(Data in Motion) sichergestellt. Eine sehr wichtige Funktion, wenn wir uns die zunehmende Exposition im Internet oder Open Finance vor Augen führen.

- **API Layer**: In dieser Schicht werden die APIs für die eingehenden Anfragen bereitgestellt.

Beispiel für eine solche Entkopplung könnte der interne Austausch von Zahlungsinformationen zwischen verschiedenen Systemen einer Bank sein. Eine Decoupling-Plattform sorgt dafür, dass die Zahlungsanwendung nicht direkt mit anderen Systemen wie der Buchhaltung oder dem Risikomanagement-System kommunizieren muss. Stattdessen können die Systeme über die zentrale Decoupling-Plattform die definierten Daten senden bzw. empfangen, ohne dass eine direkte Kopplung erforderlich ist. Dies reduziert die technische und betriebliche Komplexität und ermöglicht eine einfachere und unabhängige Weiterentwicklung der bestehenden Anwendungslandschaft. Ein weiterer Vorteil der Decoupling-Plattform ist die Erhöhung der Resilienz, was bekanntlich auch ein grosses Bedürfnis des Regulators ist. In einer hochverfügbaren IT-Architektur sind die Systeme weniger anfällig für Ausfälle, da sie nicht in einer starren Abhängigkeit voneinander agieren. Sollte ein System ausfallen oder Änderungen (Change Management) erfahren, können die anderen Systeme weiterhin – allenfalls mit reduziertem Funktionsumfang – über die Plattform miteinander kommunizieren, wobei die Integrität der gesamten Architektur erhalten bleibt. Auch die Integration neuer Anwendungen im Rahmen der fortschreitenden Digitalstrategie wird erheblich vereinfacht, da sie nur minimierten Einfluss auf die bestehende IT-Landschaft hat.

Für Banken und Versicherungen ist eine solche IT-Architektur besonders wichtig, da häufig mit sensiblen Daten und komplexen Transaktionen gearbeitet wird. Die Decoupling-Plattform hilft, die Sicherheit zu gewährleisten, indem Sicherheitsmechanismen wie Verschlüsselung und Authentifizierung in die Kommunikationsprozesse integriert werden. Darüber hinaus ist es entscheidend, dass die IT-Systeme schnell auf Änderungen reagieren können, sei es aufgrund regulatorischer Anforderungen, neuer Kundenbedürfnisse oder neuer Marktbedingungen. Durch die Entkopplung der Systeme muss nicht die gesamte IT-Infrastruktur angepasst werden, wenn zum Beispiel neue SaaS-Anwendungen eingebunden werden. Bei all den skizzierten Vorteilen zeigt sich, dass moderne Ansätze der Geschäftsstrategie wie «Data Driven Business» oder «Open Finance» ohne eine funktionierende Decoupling-Plattform in der Praxis nicht realisiert werden können. So könnte beispielsweise die Data Factory ihre angedachte Funktion mangels Datenzufluss gar nicht erfüllen.

Nachteile des Decouplings

Eine entkoppelte Anwendungslandschaft hat jedoch auch Nachteile. Eine Abwägung unter Einbezug der Stärken ist deshalb unumgänglich. Deshalb wollen wir die wichtigsten Schwächen des Decouplings ebenfalls beleuchten:

- **Kosten**: Die Integration einer Decoupling-Plattform, der entsprechende Aufbau von Wissen, die Erneuerung der bestehenden Anwendungsintegration sowie Betrieb und Weiterentwicklung der Plattform bedeuten zusätzliche Kosten.
- **Komplexität**: Die Decoupling-Plattform führt zu einer zusätzlichen Abstraktionsebene. Sie führt zudem zu einer höheren Anzahl von IT-Komponenten, die wiederum betrieben und gewartet werden müssen. Kurzfristig zusätzliche Komplexität für langfristig weniger Komplexität resp. Sicherstellung der Handlungsfähigkeit.

- **Datenkonsistenz**: In einer entkoppelten Architektur wird die Verantwortung für Daten im Vergleich zum Monolithen über mehrere Systeme verteilt. Dabei können Fehler im Datenaustausch zu Inkonsistenzen führen, die oft nur schwer zu diagnostizieren sind.
- **Störungsprozesse**: Fehler in einem System können Auswirkungen auf andere Teile der IT-Landschaft haben, was zu einer komplexeren Fehlerbehandlung führt. Der Verlust einer einzelnen Komponente oder das Fehlen einer Verbindung zwischen Systemen kann die Fehlerbehebung erschweren, da die Ursache des Problems oft nur schwer zu isolieren ist.

Fazit

Die Decoupling-Plattform spielt eine zentrale Rolle in der modernen und hoch-integrierten IT-Architektur. Für Banken und Versicherungen ganz besonders, wo Flexibilität, Skalierbarkeit, Sicherheit und kontinuierliche Innovation höchste Priorität haben. In der typischen Anwendungslandschaft existieren zahlreiche Anwendungen, die in unterschiedlichen und teils veralteten Technologien entwickelt wurden und unterschiedliche Geschäftsfunktionen, Architekturen, Datenklassen und Betriebsmodelle aufweisen. Die Systeme sind eng miteinander verbunden und erzeugen dadurch ein hohes Mass an Komplexität und Abhängigkeiten. Änderungen an einem System können schnell Auswirkungen auf andere Systeme haben, was die Wartung und Weiterentwicklung massiv erschwert. Die Decoupling-Plattform ermöglicht es, die Systemlandschaft technisch und betrieblich zu entkoppeln und gleichzeitig den Austausch von Daten und Informationen zu erleichtern, ohne dass die einzelnen Anwendungen direkt voneinander abhängen. Die strategische Rolle der Decoupling-Plattform für die IT kann gar nicht überschätzt werden. Denn die Handlungsfähigkeit, die Anwendungslandschaft weiterzuentwickeln und auf die Business-Anforderungen der Zukunft auszurichten, hängt direkt mit ihr zusammen. Es gilt also die Entkopplung der Anwendungslandschaft fest in der IT-Strategie zu verankern, eine holistische Perspektive auf die Decoupling-Plattform zu erzeugen und insbesondere einen Lock-in in Bezug auf die Technologie-Wahl zu vermeiden.

Digital-Experience-Plattform: Schlüssel zu moderner Customer Experience

Mit der Experience-Plattform rückt ein weiterer, zentraler Baustein der modularen IT-Architektur ins Zentrum unserer «Composable Architecture». Wir widmen uns nun der Frage, wie Banken und Krankenversicherungen digitale Erlebnisse schaffen können, die nicht nur überzeugen, sondern Vertrauen und Relevanz nachhaltig stärken.

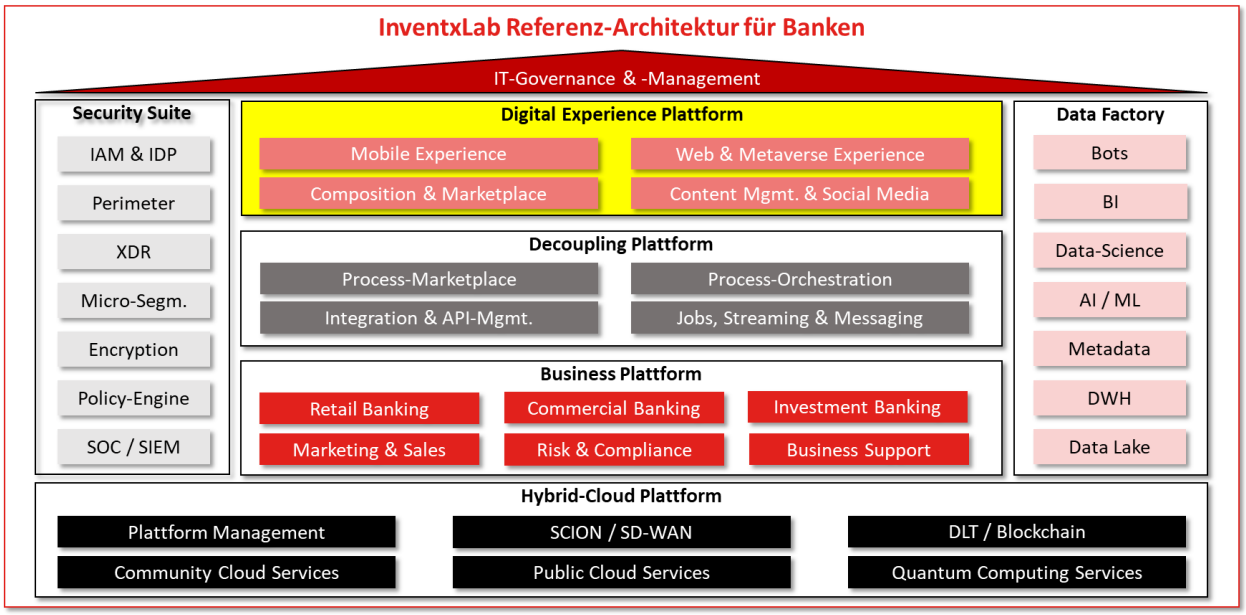


Abbildung 12: Experience-Plattform

Immer mehr definieren sich Banken und Krankenversicherungen nicht mehr über ihre Produkte, sondern über das gebotene Kundenerlebnis. Der Wettbewerb um loyale Kunden, effiziente Interaktionen und langfristiges Vertrauen entscheidet sich zunehmend über digitale Plattformen, die Erlebnisse individuell und konsistent gestalten können. Aber nicht nur die Endkunden sind relevant – denn Mitarbeitende sind genauso eine wichtige Zielgruppe oder, je nach Absatzkonzept, auch Zwischenhändler. Nachfolgend fokussieren wir uns primär auf die Perspektive der Endkunden, wobei sich die Insights problemlos auf andere Zielgruppen übertragen lassen. Auf die Integration in Ökosysteme gehen wir in diesem Teil bewusst nicht fundiert ein, da die Ausgestaltung der Experience bei einer Drittpartei stattfindet. Kommt hinzu, dass der technische Leistungsschnitt für Open Finance bei der «Decoupling-Plattform» liegt.

Die Art und Weise, wie Menschen mit Banken und Versicherungen interagieren, verändert sich grundlegend. Diese sieben Trends prägen diese Entwicklung aus unserer Sicht:

1. **Hyperpersonalisierung**: Kunden erwarten Angebote und Dienstleistungen, die exakt auf ihre individuelle Situation zugeschnitten sind. Und dies in Echtzeit und kanalübergreifend – generative KI und Machine Learning machen dies möglich.

2. **Omnichannel**: Der Bruch zwischen digitalen, telefonischen und persönlichen Kanälen wird verschwinden. Kunden erwarten ein nahtloses Erlebnis, bei dem Informationen und Kontext übergreifend zur Verfügung stehen.
3. **Digitales Vertrauen**: Sichere Authentifizierung, transparente Consent-Mechanismen und Self-Sovereign Identity (SSI, wie sie in der Schweizer eID implementiert wird) sind zentrale Voraussetzungen für vertrauensvolle Interaktionen.
4. **Open Finance**: Kunden erwarten integrierte Erlebnisse über Branchengrenzen hinweg. Offenheit gegenüber Ökosystemen wird zur Voraussetzung für Relevanz in den Customer Journeys der Zukunft.
5. **Employee Experience**: Mitarbeitende mit fragmentierten Anwendungen und Sichten auf die Zielgruppen können keine konsistente Kundenerfahrung bieten. Intuitive Oberflächen und Self-Service-Funktionen sind essenziell und steigern die Attraktivität am Arbeitsmarkt.
6. **Demografischer Wandel**: Experience Design muss generationenübergreifend funktionieren und technologische Innovation darf nicht auf Kosten der Zugänglichkeit gehen.
7. **Effizienz**: Moderne Customer Experience zielt auch auf Kosteneffizienz. Automatisierung und Self-Services entlasten Ressourcen und steigern die Wirtschaftlichkeit.

Designprinzipien der modernen Customer Experience

Eine zukunftsfähige Experience-Plattform folgt klaren Prinzipien und ist entscheidend für den Geschäftserfolg. Sie stellt alle Touchpoints eines Kunden mit der Marke ins Zentrum des Geschehens und soll barrierefreie, personalisierte Interaktionen entlang der Customer Journey ermöglichen. Sechs Designprinzipien spielen dabei eine besonders wichtige Rolle:

Kundenzentriert	Bedürfniserfüllung, Prozessabdeckung (Customer Journey), Personalisierung, einfache Benutzung, Barrierefreiheit
Modularisiert	Offene Architektur, Omni-Channel mit nahtlosen Übergängen, Modularisiert, Composable
Datenzentriert	Unified Customer Profile, Echtzeit-Verarbeitung, Datensicherheit, Datenkontrolle durch Kunden
Performant	Speed ist Key, mobiler Zugriff, sinkende Geduld bei User, Impact auf Conversion-Rate, Vorteile für SEO
Resilient	Security by Design, Zuverlässigkeit, High-Available, effiziente Wartung ohne Downtime
Zukunftsfähig	Skalierbar, hoher Automationsgrad, einfache Integration (API-first), Nutzung von ML/KI, cloud-agnostisch

Abbildung 13: Design Prinzipien der Experience-Plattform

Bekanntlich entwickeln sich die so genannten Systems of Engagement bzw. Systems of Record in unterschiedlichen Geschwindigkeiten weiter (Stichwort: 2-Speed-IT). Wie man diesem Umstand in der Praxis begegnen kann, beleuchten wir nun im folgenden Abschnitt.

Headless als Grundlage

In der klassischen IT-Architektur sind Frontend und Backend eng miteinander verknüpft, so z. B. bei Legacy-Kernsystemen. Bei der modernen Headless-Architektur dagegen stellt das Backend Inhalte, Funktionen und Logik über APIs bereit. Das Frontend (z. B. Mobile-App, Website, Chatbot) ruft diese Inhalte via Decoupling-Plattform ab und steuert selbst, wie und wann sie dem Benutzer angezeigt werden. Es gibt also keine Kopplung an ein bestimmtes Ausgabegerät oder User-Interface mehr. Diese Trennung ist für die moderne Customer Experience unerlässlich und bringt wichtige Nutzen:

- Inhalte und Services lassen sich konsistent über Website, App, Callcenter, Chatbot, Smartwatch usw. ausspielen (Omnichannel-Strategie).
- Die Frontends können unabhängig vom Backend entwickelt und modernisiert werden, was die Innovation beschleunigt und den dynamischen Kundenbedürfnissen gerecht wird. Einmal entwickelte Services (z. B. Preisrechner, Fragebogen etc.) können mehrfach verwendet werden.
- Die UI kann zudem je nach Kanal, Zielgruppe oder Nutzungskontext dynamisch angepasst werden – was letztlich auch Zukunftssicherheit ergibt.

Headless ist also die technische Grundlage für eine wirklich kanalübergreifende, modulare und zukunftsfähige Customer Experience. Insbesondere für Banken und Versicherer, die viele unterschiedliche Zielgruppen und Touchpoints bedienen, ist Headless die Antwort auf Flexibilität, Agilität und Wiederverwendbarkeit für eine erfolgreiche Zukunft. Ferner ergibt sich durch diese Entkopplung ein geringeres Lock-in-Risiko gegenüber Kernsystemen.

Zielbild

Die Experience-Plattform aggregiert digitale und klassische Kanäle, orchestriert Inhalte und Interaktionen und stellt zentrale Services von Tracking & Analytics über Consent Management bis hin zu Customer IAM bereit. Sie ist damit nicht nur technologische Plattform, sondern strategisches Steuerungsinstrument für kanalübergreifende, kontextuelle und hochgradig personalisierte Erlebnisse.

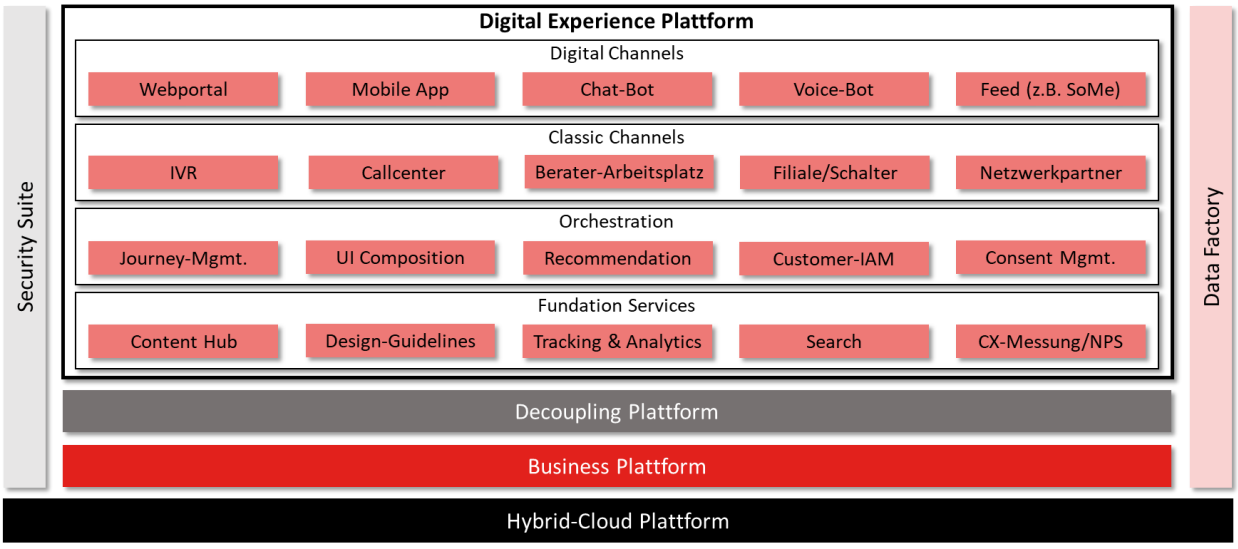


Abbildung 14: Funktionen der Experience-Plattform

Fazit: CX ist kein Projekt, sondern ein strategisches Paradigma

Die Experience-Plattform der Zukunft ist kein Monolith, sondern ein dynamisches, digitales Ökosystem von IT-Anwendungen. Wer heute die Grundlagen für eine kanalübergreifende, kontextuelle und hochgradig personalisierte Customer Experience schafft, sichert seinem Unternehmen den entscheidenden Vorsprung im Wettbewerb um Vertrauen, Relevanz und Wachstum. Deshalb gehört CX aus unserer Sicht zwingend auf die Agenda der Geschäftsstrategie. Denn eines ist sicher: In Zukunft wird Customer Experience nicht nur das Frontend der Marke sein – sondern der Katalysator des Geschäftsmodells.

Security Suite: Fundament für digitale Resilienz

In einer zunehmend digitalisierten Finanzwelt sind Banken und Krankenversicherungen mehr denn je gefordert, ihre Informations- und Cybersicherheit auf dem neuesten Stand zu halten. Cyberbedrohungen entwickeln sich rasant weiter. Und zwar sowohl in ihrer technischen Komplexität als auch in der Häufigkeit. Gleichzeitig fordern neue Geschäftsmodelle, steigende Kundenerwartungen und regulatorische Anforderungen von Banken und Krankenversicherungen ein Höchstmass an Agilität – und Sicherheit. Denn je stärker Prozesse digitalisiert und Systeme vernetzt werden, desto grösser wird die Angriffsfläche für Cyberbedrohungen. Mit der Security Suite zeigen wir ein funktionales Zielbild auf und begründen, warum die Bewältigung dieser Risiken über die Zukunftsfähigkeit ganzer Unternehmen entscheidet. Wo aber liegen nun die grössten Herausforderungen der Cybersicherheit? Wir haben zahlreiche Aspekte in die folgenden acht Schlüsselthemen konsolidiert:

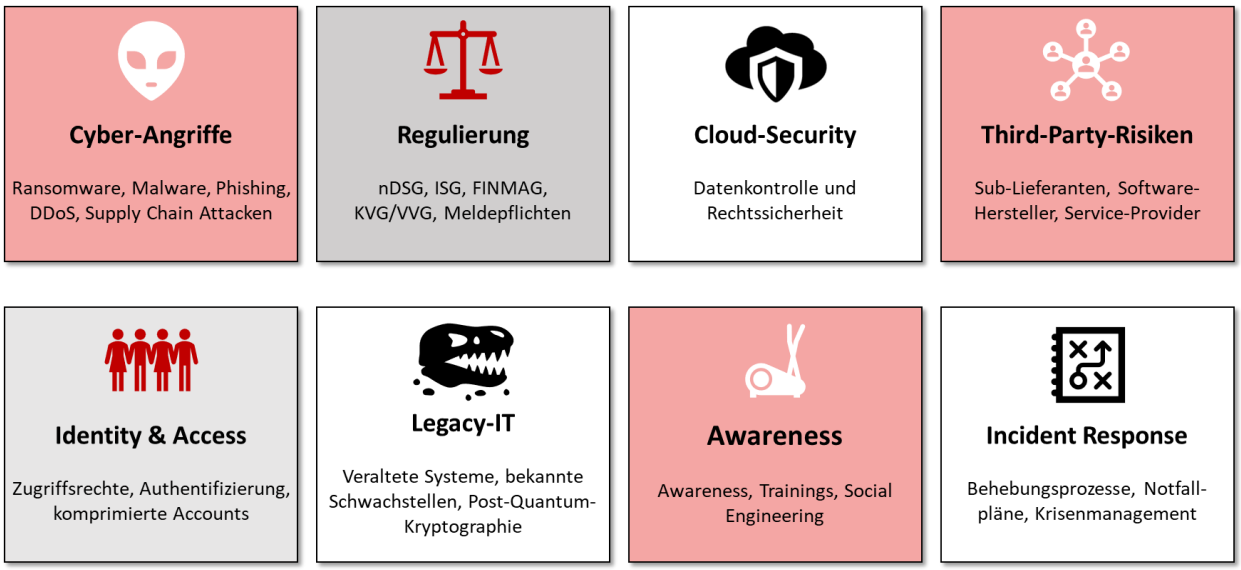


Abbildung 15: Herausforderungen der Cybersicherheit

Informationssicherheit im Spannungsfeld von Komplexität und Geschwindigkeit

Die Herausforderungen im Bereich der Cybersicherheit sind vielfältig und sie wachsen stetig an. Ransomware, Phishing, DDoS oder Supply-Chain-Attacken gehören längst zum Alltag. Angreifer nutzen zunehmend automatisierte, schwer erkennbare Methoden, um Zugang zu Daten und IT-Infrastrukturen zu erlangen – oft über kompromittierte Drittanbieter und, leider sehr erfolgreich, durch Social Engineering. Gleichzeitig steigen die regulatorischen Anforderungen: Das revidierte Datenschutzgesetz (nDSG), das Informationssicherheitsgesetz (ISG), FINMAG oder KVG/VVG verlangen ein hohes Mass an Transparenz, Nachvollziehbarkeit und Reaktionsfähigkeit. Hinzu kommen neue Herausforderungen durch die Cloud-Nutzung: Wer ist für was verantwortlich? Wie lassen sich Zugriff und Datenfluss kontrollieren? Und wie steht es um die Rechtssicherheit bei Hyperscalern (z. B. CloudAct)? Auch die zunehmende Vernetzung mit Drittanbietern – von FinTechs über SaaS-Anbieter bis hin zu Payment-Providern – erhöht die Komplexität und das Risiko. Ein Schwachpunkt bei einem Dritten kann schnell zur Eintrittspforte für einen grossangelegten Angriff werden.

Gleichzeitig bleibt der Mensch ein kritischer Faktor: Awareness, Schulungen und eine gelebte Sicherheitskultur sind essenziell, um Risiken wie Social Engineering oder unsicheren Umgang mit Passwörtern zu minimieren. Und schliesslich ist auch die Reaktionsfähigkeit entscheidend: Ein Sicherheitsvorfall ist keine Frage des Ob, sondern des Wann (Assume Breach). Ein ausgereifter Incident-Response-Plan, regelmässige Notfallübungen und ein klares Krisenkommunikationskonzept sind unerlässlich und müssen bei einem regulatorischen Audit in höchster Qualität vorgelegt werden.

Die Security Suite als Plattform für ganzheitliche Sicherheit

Vor diesem Hintergrund bietet die Security Suite ein funktionales Zielbild für eine moderne, resiliente Sicherheitsarchitektur. Sie aggregiert in einer Service-Perspektive einzelne Komponenten der Informations- und Cybersicherheit in einer zentralen Plattform. Dabei gelten ähnliche Designprinzipien wie für die gesamte IT-Architektur: Modularität, Interoperabilität, Edge-to-Cloud-Abdeckung, Automatisierung, Transparenz und Auditierbarkeit. Die Security Suite strukturiert sich in mehrere Bereiche, die unterschiedliche Aspekte der Sicherheit abdecken und dies von organisatorischen Grundlagen über technische Schutzmechanismen bis hin zu Reaktions- und Wiederherstellungsprozessen. So entsteht eine durchgängige Sicherheitsarchitektur, die sich flexibel an neue Bedrohungen und technologische Entwicklungen anpassen lässt.

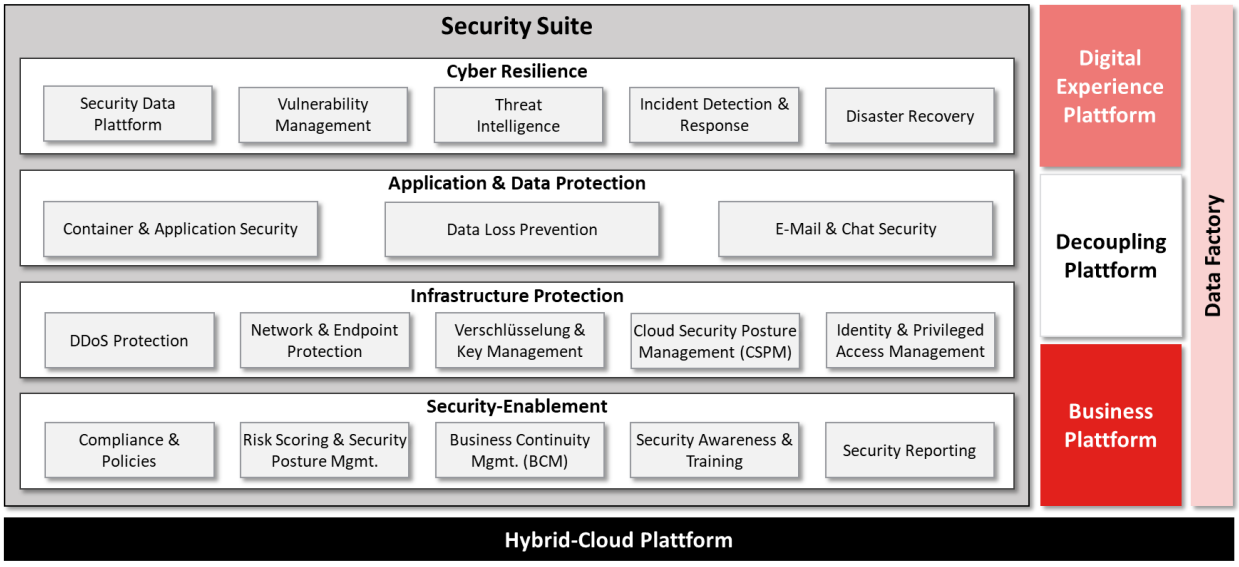


Abbildung 16: Funktionen der Security Suite

Im Bereich «**Security Enablement**» finden sich unterschiedliche Services für die einwandfreie Funktion der Informations- und Cybersecurity. Die Compliance-Vorgaben & Policies bilden die Basis für die Ausgestaltung der Informations- und Cybersicherheit. Zudem sind unterschiedliche kulturell-organisatorische Aspekte zu berücksichtigen.

In der «**Infrastructure Protection**» werden die Cloud-Plattformen geschützt bzw. Systeme und Daten verschlüsselt. CSPM-Lösungen überwachen kontinuierlich hybride Cloud-Infrastrukturen auf Fehlkonfigurationen und Sicherheitslücken, was bei der funktionalen Dynamik der Hyperscaler manuell nur eingeschränkt zu bewerkstelligen ist. Die Verwaltung aller digitalen Identitäten und deren

Zugriffsrechte ist von höchster Relevanz und entsprechende Konzepte wie PAM, RBAC und MFA sind unerlässlich für einen zeitgemässen Schutz.

In der Domäne «**Application & Data Protection**» werden die Anwendungen und Daten geschützt. Der Datenabfluss wird aktiv kontrolliert bzw. ungewollter Datenverlust verhindert. Besonders Rechnung gilt es der steigenden Verbreitung von Containern und den aufkommenden Cloud Functions (FaaS) zu tragen. Ferner werden Informationen und Daten geschützt, die via E-Mail oder Chat-Anwendungen manuell oder automatisiert verteilt werden.

In den «**Cyber Security**» Services werden Schwachstellen und Anomalien entdeckt, protokolliert und priorisiert für die risikobasierte Mitigation aufbereitet. SOAR-Lösungen (Security Orchestration, Automation and Response) automatisieren wiederkehrende Sicherheitsaufgaben und orchestrieren Prozesse zwischen verschiedenen Sicherheitstools. Sie ermöglichen eine schnelle, koordinierte und regelbasierte Reaktion auf Vorfälle. Wie moderne, KI-basierte Methoden helfen, den zunehmenden Cyberrisiken wirksam entgegenzutreten, zeigen wir in den folgenden Zeilen auf.

KI als Schlüsseltechnologie in der Cybersicherheit

Ein zentrales Element einer modernen Security Suite ist der Einsatz von KI. Denn je komplexer die Bedrohungslage, desto wichtiger wird die Fähigkeit, grosse Datenmengen schnell und präzise zu analysieren. Entlang des NIST-Frameworks zeigt sich das Potenzial von KI:

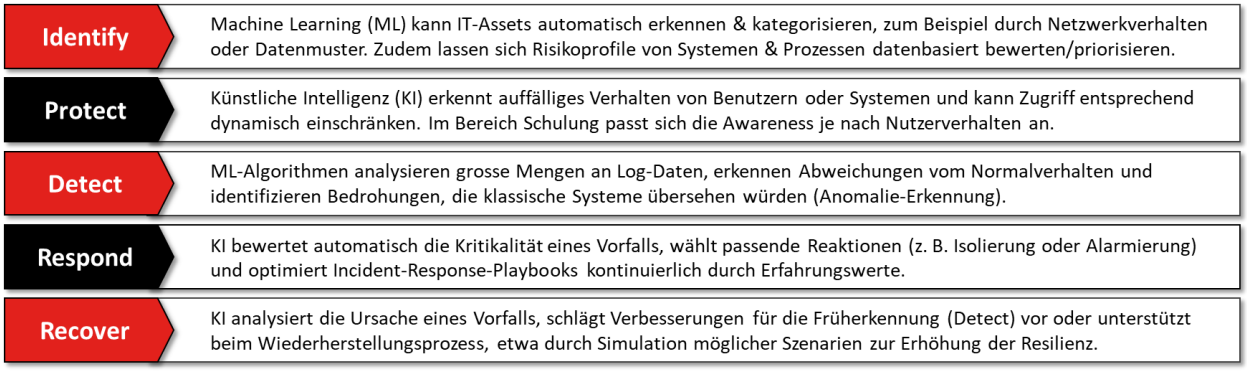


Abbildung 17: Potenziale von KI in der Cybersicherheit

Bereits einzelne KI-Anwendungen sind sehr wirksam. Die Verkettung von einzelnen AI-Agenten zu «Multi-Agenten-Systemen» wird ein Quantensprung in der Bekämpfung von Cyberrisiken sein. Im InventxLab haben wir zusammen mit unserem Cybersecurity-Bereich einen Prototypen im Bereich Threat Intelligence umgesetzt. Dabei werden rund 400 Cyber Threat Reports eingebunden, die Daten aufbereitet und die Informationen mithilfe generativer KI (Sprachmodell) für Cybersecurity-Analysten kompakt und priorisiert darstellt. So können wir grössere Datenmengen nutzen, irrelevante Inhalte («Noise») herausfiltern und nur relevante Informationen zur manuellen Analyse weitergeben. Das verbessert die Qualität und Effizienz deutlich.

Fazit: Sicherheit als strategische Business-Kompetenz denken

Für die Informations- und Cybersicherheit von Banken und Krankenversicherungen sind ganzheitliche, durchdachte Konzepte entscheidend. Die Bedrohungslage wird zunehmend komplexer: Cyberangriffe erfolgen gezielter, schneller und intelligenter. Ein einzelner Vorfall kann selbst für solide Unternehmen existenzbedrohend sein, wie der Fall Travelex im Jahr 2020 beispielhaft gezeigt hat. Um dem wirksam zu begegnen, braucht es mehr als Einzelmassnahmen: Es braucht eine holistische Sicherheitsplattform, die alle relevanten Komponenten integriert, modular aufgebaut und flexibel erweiterbar ist. Nur das Zusammenspiel technischer Bausteine – ergänzt durch KI-gestützte Analysen und Automatisierung – sowie wirksamer organisatorischer Massnahmen schafft eine widerstandsfähige, adaptive Verteidigungslinie. Diese schützt über alle Edge-Devices, Cloud-Plattformen, Systeme, Prozesse, Datenflüsse und Benutzer hinweg.

Unser Blick in die Zukunft ist klar: Informations- und Cybersicherheit wird zur zentralen Business-Kompetenz in der Finanz- und Versicherungsindustrie. Sie muss proaktiv, automatisiert, lernfähig und plattformbasiert gedacht und rund um die Uhr betrieben werden. Jetzt ist der Moment, Sicherheitsarchitekturen und -prozesse neu zu denken, Silos aufzubrechen und eine zentral orchestrierte Plattform zu schaffen, die nicht nur schützt, sondern auch mitwächst, mitlernt und Mitverantwortung übernimmt.

Hybrid-Cloud-Plattform: Rückgrat der Digitalisierung

Die Cloud hat sich vom kontroversen Konzept zur unverzichtbaren Grundlage moderner IT-Architekturen entwickelt. Wir widmen uns in diesem Kapitel der Frage, wie Banken und Krankenversicherungen ihre IT-Landschaft zukunftsfähig, flexibel und regulatorisch konform gestalten können und warum die Cloud dabei nicht nur Infrastruktur, sondern strategischer Enabler ist.

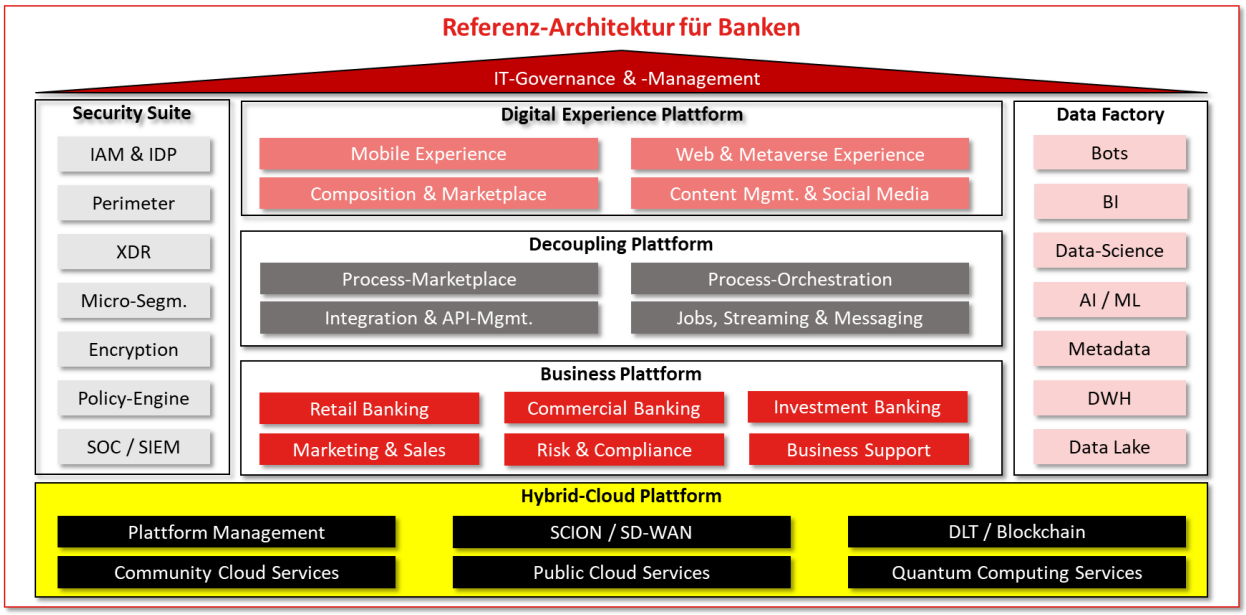


Abbildung 18: Hybrid-Cloud-Plattform

In den letzten zehn Jahren hat sich die Cloud auch in stark regulierten Branchen wie Banken und Krankenversicherungen von einem umstrittenen Thema zur geschäftskritischen Plattform entwickelt. Seit 2015 begleitet Inventx ihre Kunden mit einer systematischen Transformationsmethode in die Hybrid-Cloud und blickt dabei auf über 1'000 modernisierte Anwendungen zurück. Unsere Überzeugung: Hybride Umgebungen bieten den grössten Mehrwert für unsere Kunden. Heute verbinden wir private Infrastrukturen in unseren Schweizer Rechenzentren mit Public-Cloud-Services zu einer integrierten Hybrid-Plattform. Die frühe Skepsis gegenüber hybriden Architekturen ist unterdessen einer breiten Akzeptanz gewichen.

Die technologische Reife von Cloud-Plattformen ist fortgeschritten, Hyperscaler bieten ihre Services in der Schweiz an, und Regulierungsbehörden haben klare Rahmenbedingungen geschaffen (vgl. Cloud-Leitfaden von Swiss Banking). Gleichzeitig steigt der Druck auf IT-Organisationen: steigende Kundenerwartungen, schnellere Innovationszyklen, zunehmende Cyberrisiken und wachsende Betriebskosten machen traditionelle Modelle zunehmend problematisch. Doch viele Organisationen befinden sich noch mitten in der Transformation. Historisch gewachsene Architekturen, Legacy-Systeme, organisatorische Silos und politische Unsicherheiten – etwa rund um den Cloud Act – erschweren die Modernisierung. Die Cloud ist jedoch gekommen, um zu bleiben. Jetzt gilt es, sie strategisch zu denken, technologisch zu verankern und organisatorisch zu beherrschen.

Cloud-Trends und was die Plattform der Zukunft ausmacht

Die Cloud-Plattform der Zukunft ist nicht nur skalierbar und performant, sondern vor allem dynamisch, integriert und geschäftsgetrieben. Für Banken und Krankenversicherungen kristallisieren sich zentrale Trends für die Cloud-Plattform heraus, die den Wandel aus unserer Sicht massgeblich prägen werden:

1. **Hybrid-Cloud als Standard**: Multi-Cloud-Strategien setzen sich durch. Workloads werden je nach Risiko und Nutzen der optimalen Plattform zugeordnet. Die Fähigkeit zur plattformübergreifenden Orchestrierung wird zur Kernkompetenz.
2. **Cloud-native Technologien**: Container-Plattformen, Microservices und serverlose Architekturen ermöglichen modulare, automatisierte und skalierbare Anwendungen.
3. **Zero Trust by Design**: Sicherheitsarchitekturen basieren nicht mehr auf Perimetern, sondern auf konsequenter Prüfung jeder Anfrage – mit integrierten Sicherheits- und Compliance-Funktionen.
4. **KI & Automatisierung**: Die Cloud wird zur Basis für datengetriebene Automatisierung und KI, vorausgesetzt, die Datenplattform ist entsprechend modernisiert.
5. **Regulierung als Innovationsmotor**: Compliance wird zur strategischen Disziplin. Moderne Plattformen integrieren Audit-Funktionen, Logging und Richtlinienmanagement nativ.

Für Banken und Krankenversicherungen können wir auf Basis der Trends und bewährten Praxis die Anforderungen an die zukünftige Cloud-Plattform ableiten. Diese sind nicht isoliert zu betrachten – sie bedingen sich gegenseitig. Nur wer funktionale Leistungsfähigkeit mit nicht-funktionaler Exzellenz verbindet, kann das volle Potenzial der Cloud sicher, effizient und regeltreu ausschöpfen.

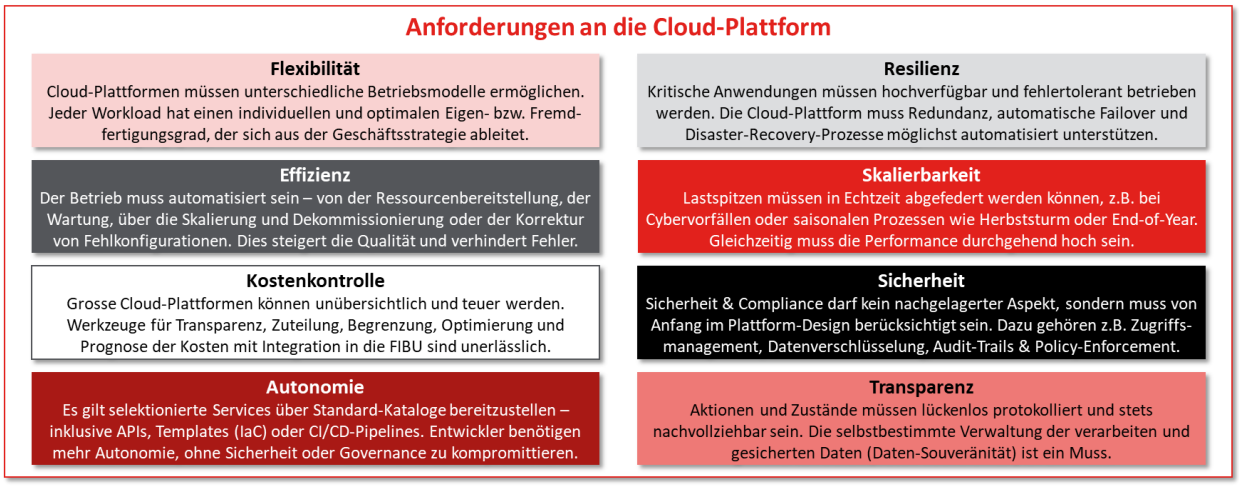


Abbildung 19: Anforderungen an die Cloud

Die moderne Hybrid-Cloud-Plattform und ihre Funktionen

Die Hybrid-Cloud-Plattform der Zukunft ist die zentrale Drehscheibe der digitalen Transformation: Sie orchestriert Infrastruktur, Daten, Prozesse, Sicherheit und Innovation über mehrere Cloud-Provider und Standorte hinweg. Sie ermöglicht den flexiblen Einsatz von Public- und Private-Cloud-Komponenten wie

unserer ix.Cloud und stellt zentrale Funktionen bereit, die unternehmensweit einheitlich und sicher genutzt werden können.

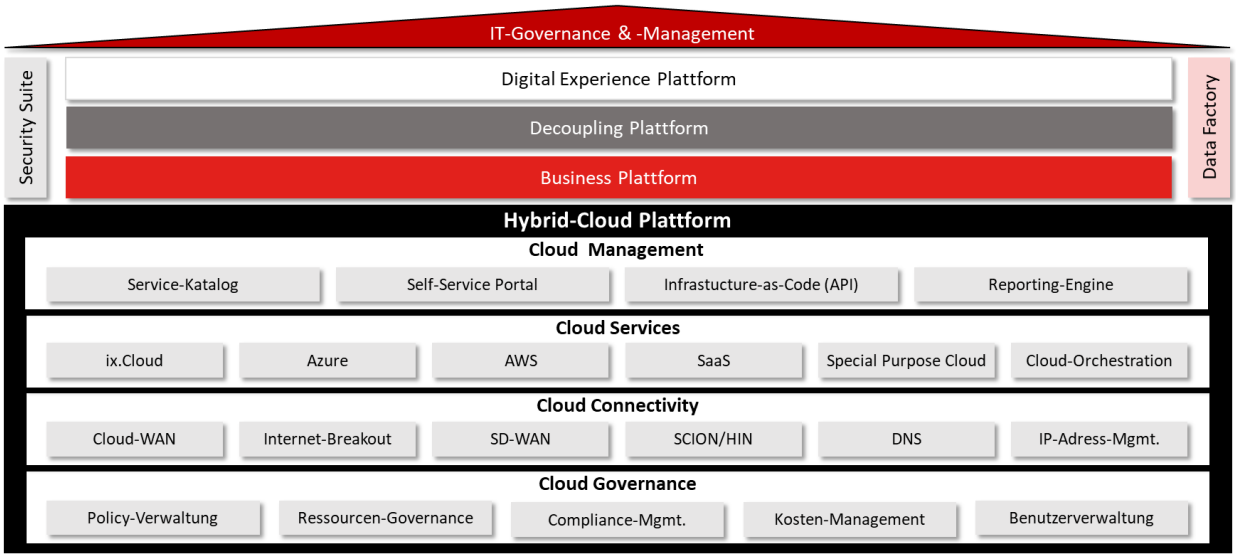


Abbildung 20: Funktionalität der Hybrid-Cloud-Plattform

Die Funktionen des «**Cloud Management**» Layers stellen sicher, dass Fachbereiche, Entwickler und Applikationsmanager effizient und möglichst eigenständig (Self-Services) ihren Bedarf an neuen Cloud-Services bzw. den Betrieb der deployten Services umsetzen können. Die gewährte Autonomie auf Basis eines standardisierten und zentral gepflegten Service-Katalogs entlastet die Cloud-Administratoren und sorgt für rasche Innovationszyklen. Natürlich gilt es in regelmässigen Schulungen die Neuigkeiten des Servicekatalogs zu schulen – regelmässige Information ist Key!

Im Bereich der «**Cloud Services**» werden die Service Offerings der selektionierten Cloud Provider bereitgestellt. Der Bedarf für «Special Purpose»-Infrastrukturen wie z. B. Quantencomputing, Public Blockchains oder souveränen KI-Clouds ist je nach Bedarf individuell zu berücksichtigen. Die Multi-Cloud-Orchestration sorgt dafür, dass Workloads zwischen den Clouds nach Bedarf möglichst einfach verschoben werden können, was jedoch hohe Anforderungen an die spezifische Anwendung mit sich bringt (z. B. Exit-Strategie, siehe nachfolgendes Kapitel zu PaaS).

Mittels «**Cloud Connectivity**» werden die Cloud-Standorte standortübergreifend verbunden, die Geschäftsräumlichkeiten und Filialen an die Cloud-Plattform mit modernen Technologien angeschlossen sowie die Edge-Devices in die Gesamtarchitektur integriert. Dabei sind nach Bedarf auch Spezial-Verbindungen wie SSFN (SCION) oder HIN bereitzustellen, welche die Branche und das Ökosystem erfordern. Ferner wird der Internetzugang für den In- und Outbound Traffic ermöglicht und kontrolliert (vgl. Security Suite).

Im Layer «**Cloud Governance**» wird die zentrale Verwaltung über die gesamte Cloud-Plattform – wenn immer möglich – als Code (GitOps) sichergestellt (z. B. Namenkonvention, Tags, Deployment-Standorte etc.). Ebenso wichtig ist die Benutzerverwaltung für die Cloud-Administratoren resp. deren Integration mit den zentralen IAM-Systemen der Security Suite. Denn jede Cloud hat eine eigene Berechtigungslogik, welche bedarfsgerecht integriert werden muss. Immer wichtiger wird die Kostenkontrolle (FinOps). Aus unserer Sicht wird unerlässlich, dass die Kosten auf das Business

aufgeschlüsselt werden können, damit Kostenbewusstsein, aber auch Messbarkeit von Digitalisierung in den Business-Prozessen und Fachbereichen erhöht wird.

PaaS als strategischer Imperativ

In einer hybriden Cloud-Architektur ist die Fähigkeit, Anwendungen flexibel zwischen Cloud-Anbietern zu verschieben, ein strategischer Imperativ, nicht zuletzt aufgrund regulatorischer Anforderungen wie der FINMA-Richtlinie RS 2023/1 (Operationelle Risiken und Resilienz). Der Schlüssel dazu liegt im Einsatz von Platform-as-a-Service (PaaS). Containerisierte Anwendungen, idealerweise auf Basis von Open-Source-Technologien, ermöglichen eine hohe Portabilität, Skalierbarkeit und Automatisierung. Doch nicht jeder Container ist automatisch cloud-native: Wird Legacy-Software lediglich neu als Container verpackt, ohne sie zu modernisieren, bleibt die gewünschte Flexibilität aus. Orientierungsrahmen soll dabei unbedingt die Twelve-Factor-Methode sein. Viele Kernsystem-Hersteller bringen eigene PaaS-Stacks mit, was zu Mehraufwand, reduzierter Skalierbarkeit der Container-Plattform und – aus unserer Sicht unterschätzten und zusätzlichen – Lock-in-Risiken führt. Eine duale Strategie ist daher oft unumgänglich. Wer langfristig unabhängig bleiben will, sollte auf offene Open-Source-Standards und containerbasierte Architekturen setzen – für mehr Resilienz, regulatorische Konformität und strategische Beweglichkeit.

Kriterien	IaaS	PaaS	FaaS	SaaS
Applikationsmobilität	Mittel	Hoch	Gering	Sehr gering
Technische Mittel	VM/OS-Image	Container	Stark anbieter-abhängig	Stark anbieter-abhängig
Lock-in	Mittel	Tief (v.a. mit OpenSource)	Hoch	Sehr hoch

Abbildung 21: Vergleich der Service-Modelle in der Cloud

Fazit: Die Hybrid-Cloud ist die Basis für nachhaltige Wettbewerbsfähigkeit

Die CIOs von Banken und Krankenversicherungen stehen an einem Wendepunkt. Die Hybrid-Cloud ist nicht optional, sie ist essenziell. Die Cloud ist nicht als Infrastruktur-Plattform zu betrachten, sondern als unerlässlicher Enabler der Innovation. Um wettbewerbsfähig zu bleiben, müssen Banken und Krankenversicherungen ihre IT-Architektur jetzt proaktiv weiterentwickeln. Die Modernisierung der Gesamtarchitektur lässt sich optimal mit der systematischen Nutzung einer modernen Hybrid-Cloud-Plattform kombinieren. Basis dazu bildet eine individuelle Cloud-Strategie mit Fokus auf die Entwicklung der Anwendungslandschaft, der Transformation hin zum gewünschten Betriebskonzept auf Basis einer strategischen Capability-Perspektive, der IT-Security und der erforderlichen Regulatory Compliance.

Der Bau der Hybrid-Cloud-Plattform kann schrittweise erfolgen und mit dem Zielbild und dem anvisierten Eigen- und Fremdfertigungsgrad im Blick (Present-, Transition- und Future Mode of Operation). Die neue Plattform soll von Beginn an die Fachbereiche befähigen statt einschränken und damit schnell und sichtbar Mehrwert im Business-Alltag bringen. Es gilt eine moderne Governance-Struktur zu etablieren und gemeinsam mit strategischen Partnern in Cloud-Kompetenzen zu investieren – technologisch, organisatorisch und kulturell (vgl. Kapitel zu IT-Governance & -Management). Der Weg ist anspruchsvoll – aber unerlässlich. Die Hybrid-Cloud-Plattform per se ist nicht das Ziel. Sie ist das Fundament für die Innovationsfähigkeit im Wettbewerbsumfeld der Zukunft.

IT-Governance & ITSM: Steuerzentrale für digitale Exzellenz

Eine zukunftsorientierte, businessnahe IT-Governance und ein effizientes IT Service Management (ITSM) sind entscheidend, um die Herausforderungen in den IT-Organisationen zu meistern. Denn der IT-Betrieb erfolgt in der Regel in einem Multi-Provider-Setup – selbstverständlich komplementär zur bewusst gewählten Eigenfertigung. Die Steuerung der heutigen Gesamt-IT erfolgt jedoch nicht selten fragmentiert und reaktiv. Gleichzeitig steigen die Anforderungen durch Regulatorik, IT-Security und letztlich aufgrund der dynamischen Kundenerwartungen und dem Wettbewerbsumfeld rasant an. Die IT ist daher mit einem Spannungsfeld aus Innovationsdruck, Kosteneffizienz und regulatorischer Sicherheit konfrontiert.

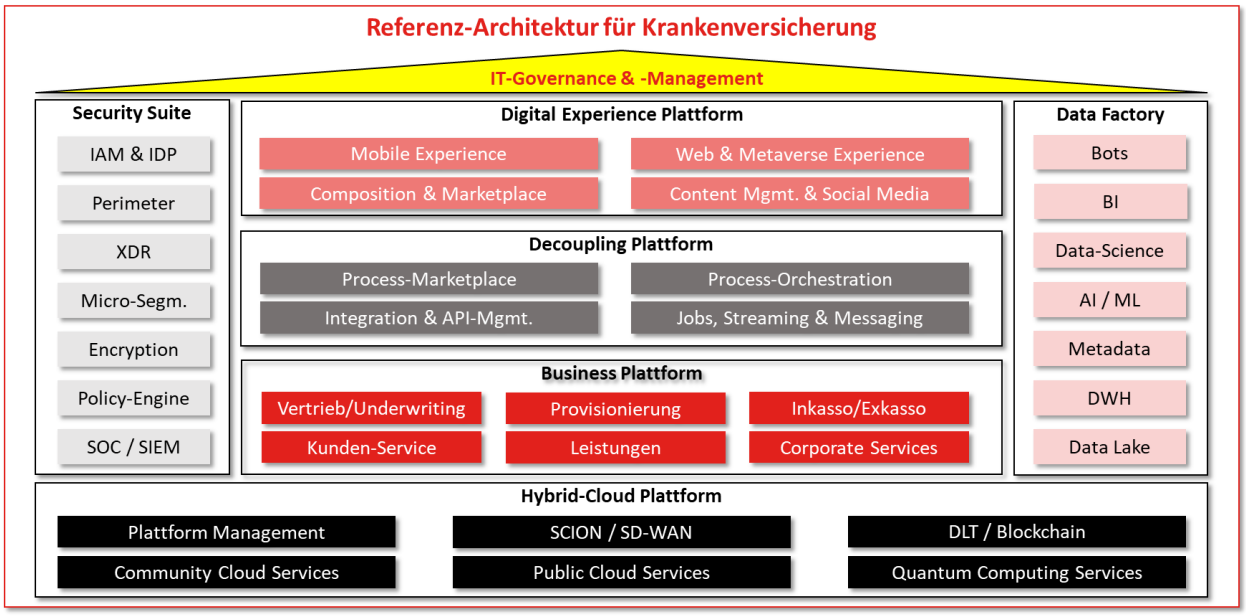


Abbildung 22: IT-Governance &-Management

Die Idee einer vollständig in der Public Cloud betriebenen IT-Infrastruktur ist in der Finanz- oder Versicherungsindustrie aus unserer Sicht mit den heute betriebenen Anwendungen nicht optimal umsetzbar – sei es aufgrund von Datenhoheit, Latenzanforderungen, Risikoüberlegungen, Kosten oder regulatorischer Vorgaben. Stattdessen hat sich eine Hybrid-Cloud-Architektur etabliert, in der wichtige Systeme wie das Kernsystem weiterhin in einer Private Cloud betrieben werden, während beispielsweise neue Anwendungen ohne kritische Daten entkoppelt in der Public Cloud angesiedelt sind. Darüber hinaus setzen viele Organisationen auf Multi-Cloud-Strategien, um Abhängigkeiten von einzelnen Hyperscalern zu reduzieren und die besten Services für unterschiedliche Anforderungen zu nutzen. Dies führt jedoch zu einer neuen Komplexität in Bezug auf IT-Architektur, Sicherheit, Datenmanagement und operativer Steuerung – die nicht ohne eine starke, zentrale IT-Governance bewältigt werden kann.

Immer mehr Softwarehersteller entwickeln neue Anwendungen cloud-native, also unter Nutzung von Microservices, Containern und PaaS. Dies erlaubt eine höhere Skalierbarkeit, bessere Resilienz und schnellere Release-Zyklen. Parallel dazu verbreiten sich DevOps-Prozesse, bei denen Entwicklung und Betrieb eng verzahnt zusammenarbeiten, um eine kontinuierliche Lieferung und Verbesserung von Software zu ermöglichen. Für die IT-Organisation bedeutet dies einen Paradigmenwechsel: Weg von klassischem Change- und Release-Management und hin zu automatisierten, CI/CD-basierten Prozessen mit Self-Services für Applikationsmanager und Entwickler, die sich über die gesamte Supply Chain der IT hinweg erstrecken muss. Die IT-Governance muss dies ermöglichen, ohne dabei Kontrolle, Sicherheit oder Compliance zu vernachlässigen.

Klassische Sicherheitskonzepte mit klar definierten Netzwerkgrenzen (Perimeter) reichen in der heutigen dezentralisierten IT nicht mehr aus. Mit der zunehmenden Mobilität bzw. dem Arbeiten im Homeoffice, modernen Anwendungen mit public-adressiertem Cloud-Zugriff und dem Einsatz zahlreicher externer Supplier gewinnt das Zero-Trust-Konzept an Bedeutung. Dieses Modell basiert auf dem Grundsatz «Never trust, always verify» und setzt u. a. auf starke Identitäts- und Zugriffskontrollen, Mikrosegmentierung und kontinuierliche Risikobewertungen – unabhängig vom Standort, dem Benutzer oder den eingesetzten Devices. Die IT-Governance muss diese Prinzipien nicht nur technologisch abbilden, sondern auch organisatorisch zuverlässig verankern.

Die Menge an Daten, Events, Alerts und Incidents im IT-Betrieb wächst exponentiell. Klassische, manuelle Prozesse stossen an ihre Grenzen. Automatisierung wird zum zentralen Enabler für einen proaktiven, stabilen und resilienten IT-Betrieb. AIOps-Lösungen analysieren Betriebsdaten in Echtzeit, erkennen Muster, korrelieren Vorfälle und leiten automatisierte Massnahmen ein. Dadurch können Störungen schneller identifiziert und gelöst werden, bevor sie den Nutzer erreichen. Gleichzeitig lassen sich Betriebskosten durch Skalierung von Routineaufgaben senken. Die Governance-Strukturen der IT müssen solche Technologien nicht nur zulassen, sondern strategisch fördern.

Best Practice

Um sich auf die Zukunft vorzubereiten, genügt es nicht, punktuelle Initiativen zu starten. Gefragt ist eine systematische, strategisch verankerte Transformation, die sowohl technologische als auch organisatorische Veränderungen umfasst. Die folgenden Best Practices sind zentral, um die IT-Governance und das IT Service Management fit für die Zukunft zu machen:

Capability-Zielbild: Die Transformation sollte mit einer systematischen Maturitätsanalyse der IT-Governance beginnen. Dabei werden Prozesse, Rollen, Steuerungsmechanismen und die Zusammenarbeit mit den Fachbereichen betrachtet. Ziel ist es, ein fähigkeitsbasiertes Zielbild zu definieren und anschliessend eine Gap-Analyse abzuleiten: Welche Governance- und Managementfähigkeiten in der IT werden benötigt, um den Anforderungen im Business – unter Berücksichtigung der Compliance – gerecht zu werden?

Multi-Provider-Setup: In einer Welt mit zahlreichen IT-Providern, Cloud-Plattformen und externen Dienstleistern ist es entscheidend, das Zusammenspiel der gesamten IT Supply Chain strukturiert zu orchestrieren. Das Konzept des Service Integration and Management (SIAM) etabliert sich zusehend als wirksame Methode, um Verantwortung klar zu regeln, Servicequalität zu messen und Risiken im Gesamtsystem zu minimieren. SIAM unterscheidet sich von traditionellem IT Service Management und Frameworks wie ITIL, indem es ITSM-Prozesse erweitert und an die Anforderungen einer Multi-Provider-

Umgebung anpasst. Während ITSM sich auf das Management einzelner IT-Services konzentriert, legt SIAM den Fokus auf die Integration und Orchestrierung aller Services aus verschiedenen Quellen und Betriebsmodellen, um eine ganzheitliche Dienstleistung für das Business zu gewährleisten.

Cloud Governance: Die zunehmende Nutzung von Cloud-Diensten erfordert ein stringentes Cloud-Governance-Modell, das klare Richtlinien für Kostenkontrolle (z. B. FinOps), Sicherheitsstandards, Datenmanagement und Provider-Steuerung definiert. Moderne Governance-Modelle setzen auf Policy-as-Code, wobei die Compliance direkt in der Cloud-Infrastruktur mit Code verankert wird (vgl. unseren Beitrag zur Hybrid-Cloud-Plattform). Die Kosten können in der Cloud rasch ansteigen – die Transparenz über Cloud-Kosten und deren Verursacher ist deshalb elementar. Selbstverständlich bleibt, dass alle Änderungen an Systemen lückenlos und nachvollziehbar protokolliert werden müssen.

Observability: Als entscheidende Ergänzung zu SIAM erweist sich die moderne Observability. Sie geht über das traditionelle Telemetrie-Monitoring hinaus, indem sie ein tiefes Verständnis des Systemzustands basierend auf Daten (Logs, Metriken, Traces) ermöglicht. Für SIAM ist Observability unerlässlich, da sie eine ganzheitliche End-to-End-Sicht über alle Service-Anbieter hinweg schafft, damit Silos aufbricht und die Faktenbasis für systematische Verbesserungen legt. Diese Transparenz führt zu einer schnelleren Fehlerbehebung, da detaillierte Einblicke die Ursachen von Störungen in komplexen Multi-Provider-Umgebungen schnell offenlegen. Zudem unterstützt sie ein proaktives Management, indem sie die Erkennung von Trends und potenziellen Problemen ermöglicht, bevor diese die IT-Benutzer beeinträchtigen.

Funktionsübersicht

Um eine effektive IT-Governance sowie ITSM in einer komplexen Multi-Provider-Landschaft zu gewährleisten, bedarf es einer integrierten Lösung mit zahlreichen Funktionen. Die einzelnen Elemente führen wir in folgende Plattform mit einer Service-Perspektive zusammen:

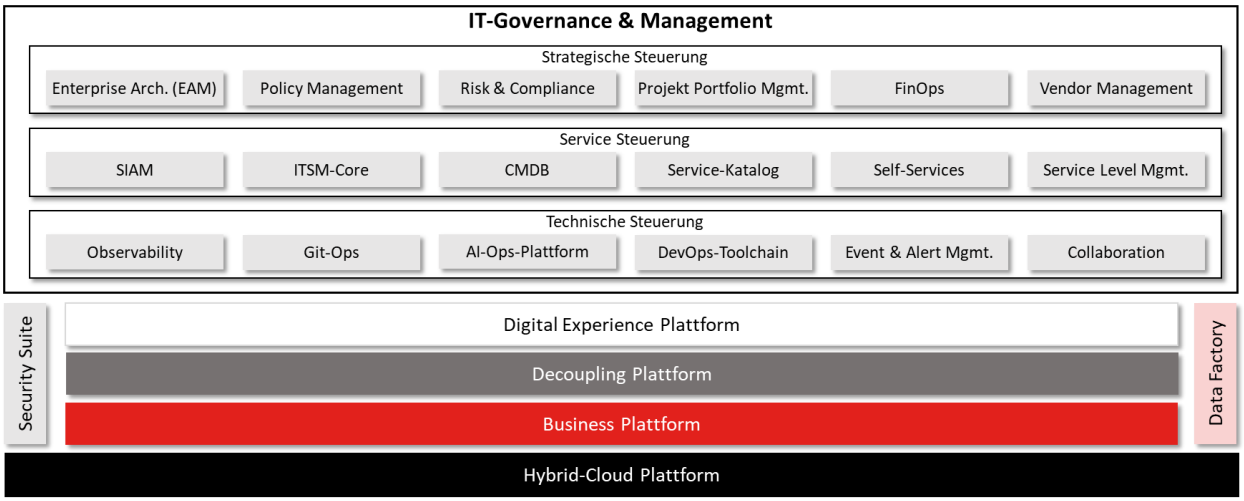


Abbildung 23: Funktionen moderner IT-Governance & -Management

Business IT Alignment neu denken

Die zunehmende Dynamik im Wettbewerb, der Regulierung und den anspruchsvollen Kundenerwartungen zwingt Banken und Krankenversicherungen, schneller auf Veränderungen zu reagieren. Klassische IT-Strukturen – mit langen Planungszyklen, starren Gremien und indirekten Kommunikationswegen – geraten dabei an ihre Grenzen. Ein zeitgemässes Business IT Alignment muss deutlich agiler, datengetriebener und kollaborativer werden. Die zentrale Veränderung: Die IT wird vom Dienstleister zum strategischen Innovationspartner für das Business. Sie agiert nicht mehr reaktiv auf Anforderungen des Fachbereichs, sondern gestaltet aktiv mit. Das gelingt nur, wenn beide Seiten sich auf gemeinsame Value Streams, Ziele und Metriken ausrichten.

Wesentliche Elemente des modernen Business IT Alignments sind:

- **Value-Stream-Organisationen**: IT-Teams sind nicht mehr nach Technologien oder Systemen, sondern entlang von Geschäftsprozessen bzw. fachlichen Domänen organisiert. Business und IT arbeiten gemeinsam als cross-funktionale Teams – stets die Anforderungen der Kunden im Fokus. Aus unserer Sicht eignet sich diese Organisationsform nicht für alle Bereiche gleichermassen. Allenfalls kann es zweckmässig sein, einzelne Bereiche mit einem traditionellen IT-Modell zu bedienen (vgl. 2-Speed-IT).
- **Business-IT-Architekten**: Neue Rollen überbrücken die «Sprachbarriere» zwischen Geschäftsstrategie, Prozessen und IT-Architektur – als Brückenbauer für Priorisierung, Investitionen und Roadmaps. In einer zunehmend komplexen IT-Umgebung ist das Verständnis zwischen Business und IT ein wichtiger Erfolgsfaktor.
- **Continuous Aligment**: Statt starrer Jahresbudgets und IT-Projektportfolios setzen moderne Organisationen auf rollierende Forecasts, agiles Projektportfolio-Management und kontinuierliche Priorisierung auf Basis des erwarteten Geschäftswerts. Dazu gehört auch, dass die Kosten nicht en-bloc bei der IT «parkiert» werden, sondern diese verursachungsgerecht auf Kostenträger im Business umgelegt werden.
- **Neue Kennzahlen**: Der Erfolg wird nicht ausschliesslich an Verfügbarkeiten, Anzahl Tickets oder Anzahl abgeschlossener Tasks gemessen, sondern am Wertbeitrag für das Geschäft – etwa Kundenzufriedenheit, Time-to-Market oder Prozesskosten.
- **Komponenten-Mentalität**: Die IT bietet digitale Enabler (IT-Services, Daten etc.) als standardisierte Komponenten in einem Service-Katalog an. Die Fachbereiche können darauf aufsetzen, ohne jedes Mal neu zu entwickeln (Composable Architecture).

Ein modernes Business IT Alignment bedeutet nicht nur bessere Kommunikation – sondern gemeinsame Ziele, vereinbarte Prioritäten, integrierte Strukturen und Prozesse sowie geteilte Verantwortung und Transparenz für die Wertschöpfung. Die IT-Governance und das IT Service Management müssen diese neue Realität organisatorisch und technisch abbilden und befähigen. Nicht nur auf operativer Ebene, sondern mit gleicher Systematik auch in der Geschäftsleitung und im Verwaltungsrat bzw. Stiftungs- oder Bankrat (strategische Ebene).

Fazit: Wichtigkeit von IT-Governance und ITSM

Die Modernisierung der IT-Plattform erfordert klare Governance-Strukturen und ein modernes Management der IT-Services über Plattformen und Provider hinweg. Nur mit modernen Instrumenten und Prozessen behalten CIOs die Kontrolle über komplexe Hybrid-Cloud-Umgebungen, stellen die Einhaltung regulatorischer Anforderungen sicher und schaffen die Voraussetzungen für eine zuverlässige, sichere und innovationsfähige IT. Die Funktionen der IT-Governance und des gesamtheitlichen IT Service Managements sind nicht mehr «Backoffice-Themen», sondern wichtiger Faktor für effiziente und kundenorientierte Digitalisierung. Ganz besonders bei Banken und Krankenversicherungen mit ihrem bereits heute sehr hohen Digitalisierungsgrad. CIOs sollten bereits heute eine ganzheitliche IT-Governance-Strategie definieren, ihre Service-Management-Prozesse parallel zum Technologie-Stack modernisieren und mit intelligenten Plattform-Lösungen aufstellen. Wer frühzeitig handelt, sichert sich operative Exzellenz und Innovationsfähigkeit – und wird zum aktiven Gestalter der digitalen Zukunft mit greifbarem Mehrwert für das Business.

Digital Workplace: Am Puls der modernen Arbeit

Für Banken und Krankenversicherungen hat sich der digitale Arbeitsplatz zu einem strategischen Nervenzentrum und einem unverzichtbaren Erfolgsfaktor im Alltag der gesamten Organisation entwickelt. Die Ursache dafür liegt in den branchenspezifischen Rahmenbedingungen: das Umfeld der Banken und Krankenversicherungen ist geprägt von regulatorischen Anforderungen, steigenden Kundenerwartungen und immer kürzeren Innovationszyklen. Nicht zu vergessen die grossen Herausforderungen in der IT-Security – denn der digitale Arbeitsplatz ist das kritische Glied der Sicherheitskette. Diesen Challenges erfolgreich zu begegnen, erfordert einen modernen digitalen Arbeitsplatz, der nicht nur Effizienzgewinne bietet, sondern auch die Chance, neue Formen der Zusammenarbeit und Wertschöpfung zu realisieren. Der Wandel des Digital Workplace von einer Plattform für IT-Applikationen zu einem integrierten, intelligenten und hochgradig personalisierten Arbeitsinstrument, das höchste Anforderungen an Sicherheit und Compliance erfüllt, setzt sich auch in den kommenden Jahren weiter fort. Diese Transformation erfordert von den Unternehmen strategisches Denken, technologische Weitsicht und mutige Entscheidungen.

Workplace-Trends

Werfen wir zuerst einen Blick in die Zukunft. Die folgenden Trends beeinflussen aus unserer Sicht den Digital Workplace massgeblich mit:

1. **Künstliche Intelligenz**: KI-gestützte Assistenten – wie bspw. der Copilot von Microsoft oder eingebettete Agenten in Beratungstools – werden zum Standard im digitalen Arbeitsplatz gehören. Sie unterstützen auf sehr individuelle Weise die Mitarbeitenden bei der Priorisierung ihrer Aufgaben, übernehmen Routineprozesse und ermöglichen kontextbasierte Informationsbereitstellung in Echtzeit.
2. **Automatisierung**: Mit Workflows wird die Effizienz weiter gesteigert – auch in Bereichen, die bisher nicht abgedeckt werden. Workflows werden intelligent und adaptiv (z. B. ein Beschaffungsantrag) und mit No-Code-Anwendungen (im Self-Service für Fachabteilungen) zum Kinderspiel. Sie passen sich auf Basis von real-time Daten und KI dynamisch an Nutzerverhalten und Geschäftsanforderungen an.
3. **Zero Trust by Design**: Die Arbeitswelt wird weiterhin stark hybrid bleiben – die Absicherung dezentralisierter Arbeitsplätze ist daher essenziell. Sicherheitsarchitekturen müssen vollständig auf Zero-Trust-Prinzipien basieren, kombiniert mit kontinuierlicher Authentifizierung, Endpoint-Überwachung und kontextsensitiven Zugriffsmodellen.
4. **Edge Computing:** Die dezentrale Verarbeitung von Daten direkt am Entstehungsort (Edge) in Verbindung mit extrem schneller und latenzarmer Konnektivität (6G) sowie sehr leistungsfähigen Clients wird die Performance von cloud-basierten Anwendungen massiv verbessern und ganz neue Anwendungen für den lokalen Betrieb auf dem Workplace schaffen.
5. **Immersive Erlebnisse:** Obwohl noch in den Kinderschuhen, werden erweiterte & virtuelle Realität (Mixed Reality) erste praktische Anwendungen im Workplace finden. Denkbar sind z. B. virtuelle Meetingräume, Schulungen für neue Produkte und virtuelle Trainings für Beratungsgespräche.

6. **Employee Experience**: Die Grenzen zwischen physischem und virtuellem Arbeitsplatz verschwimmen. Die Erwartungen an Selbstbestimmung, Flexibilität und sinnstiftende Arbeit steigen. Der Arbeitsplatz der Zukunft muss die individuelle Employee Experience (EX) priorisieren – mit intuitiven Interfaces, kollaborativen Tools und personalisierten Lernangeboten. Das bringt mit sich, dass die User ihr Feedback kontinuierlich an die IT senden und zusammen mit den User-Daten als Basis für die Optimierung genutzt werden.
7. **Lebenslanges Lernen:** Angesichts des rasanten Wandels wird der digitale Workplace zur Lernplattform. Dabei werden Wissensdatenbanken und Microlearning-Angebote nahtlos integriert. Der moderne Workplace muss Mitarbeitende proaktiv auf neue Kompetenz-Anforderungen hinweisen und passende Schulungsinhalte vorschlagen.
8. **Nachhaltigkeit**: Konsequente Ausrichtung auf den Einsatz ressourcenschonender Technologien, effiziente Collaboration-Tools und eine umweltbewusste Nutzung digitaler Arbeitsmittel mitsamt Darstellung des Footprints.
9. **Digital Wellbeing**: Förderung einer gesunden Balance zwischen Erreichbarkeit und Erholung durch bewusste Nutzung digitaler Tools, klare Kommunikationsregeln und unterstützende Technologien (z. B. konfigurierte Fokus-Zeiten, Workload-Management etc.).

Wandel in der Workforce-Struktur

Neben den zuvor beschriebenen Trends wird sich auch die soziodemographische Struktur der Bevölkerung stark verändern. Dieser Wandel wird die Arbeit massgeblich prägen. Die klassische Organisation mit fest angestellten Mitarbeitenden, in definierten Organisationsstrukturen, an festen Arbeitsplätzen und an den definierten Standorten verliert zunehmend an Relevanz. Welche Tendenzen lassen sich am Markt beobachten und welchen Einfluss hat dies auf den digitalen Arbeitsplatz?

Abbildung 24: Soziodemographischer Wandel

Impact von KI auf die Wissensarbeit

Der Einsatz von künstlicher Intelligenz (KI) verändert die Wissensarbeit fundamental – und mit ihr die Anforderungen an den digitalen Arbeitsplatz der Zukunft. Wo heute Fachkräfte etliche Stunden mit der Recherche, Analyse und Dokumentation verbringen, übernimmt KI zunehmend die Rolle eines

intelligenten Assistenten, der Informationen kontextbasiert aufbereitet, Prozesse automatisiert und Entscheidungen vorbereitet und künftig vermehrt auch trifft. Im Digital Workplace der Zukunft ist KI nahtlos in die Applikationen integriert – nicht als separates Tool, sondern als intelligente Funktion als Teil der Prozesse. Knowledge Worker erhalten Informationen genau dann, wenn sie gebraucht werden: durch KI-gestützte Suchfunktionen, smarte Dokumentenanalyse und automatische Empfehlungen. Die klassische Navigation durch Dokumente, File-Ablagen, Datenbanken und Kundendossiers wird ersetzt durch eine dialogorientierte Interaktion: Per Sprache oder Texteingabe stellen Mitarbeitende ihre Fragen und erhalten strukturierte, nachvollziehbare Antworten. Darüber hinaus fördert KI die kollaborative Intelligenz: Sie erkennt ähnliche Fälle (z. B. Kundenbeschwerden), schlägt Experten oder Lösungen vor oder zeigt potenzielle Risiken auf – über Teams und Abteilungen hinweg. Besonders bei komplexen Aufgaben wirkt KI als Coach, der Mitarbeitende gezielt unterstützt. Der Lernbedarf wird automatisch identifiziert und passende Inhalte direkt präsentiert. Wissensarbeit wird dadurch dynamischer, entlastender und hoch-individualisiert.

Diese Entwicklung bringt jedoch neue Herausforderungen in der Compliance mit sich. Banken und Versicherungen müssen sicherstellen, dass KI-Systeme erklärbar, ethisch vertretbar und technisch mit den bestehenden Geschäftsinformationen integriert sind. Der Umgang mit sensiblen Daten und regulatorischen Anforderungen erfordert eine klare Governance und robuste, nachvollziehbare Kontrollmechanismen. Gleichzeitig gilt es, Mitarbeitende für den souveränen Umgang mit KI zu befähigen – nicht nur als Anwender, sondern als kritische Mitgestalter der neuen Arbeitsrealität – und zwar über alle Generationen hinweg. Bei all diesen Möglichkeiten und Änderungen – diese bringen ein grosses, soziales Spannungsfeld mit: Je mehr Routine- und Analyseaufgaben durch KI übernommen werden, desto mehr geraten klassische Wissensarbeitsplätze unter Druck. Die Effizienz im Unternehmen steigt zwar, aber der Impact auf den Arbeitsmarkt und die Gesellschaft kann enorm sein. Bestehende Rollenprofile verändern sich, manche Tätigkeiten entfallen ganz.

Workplace der Zukunft

Ein zukunftsgerichteter digitaler Arbeitsplatz muss aus unserer Sicht folgende Kernfunktionen bieten:

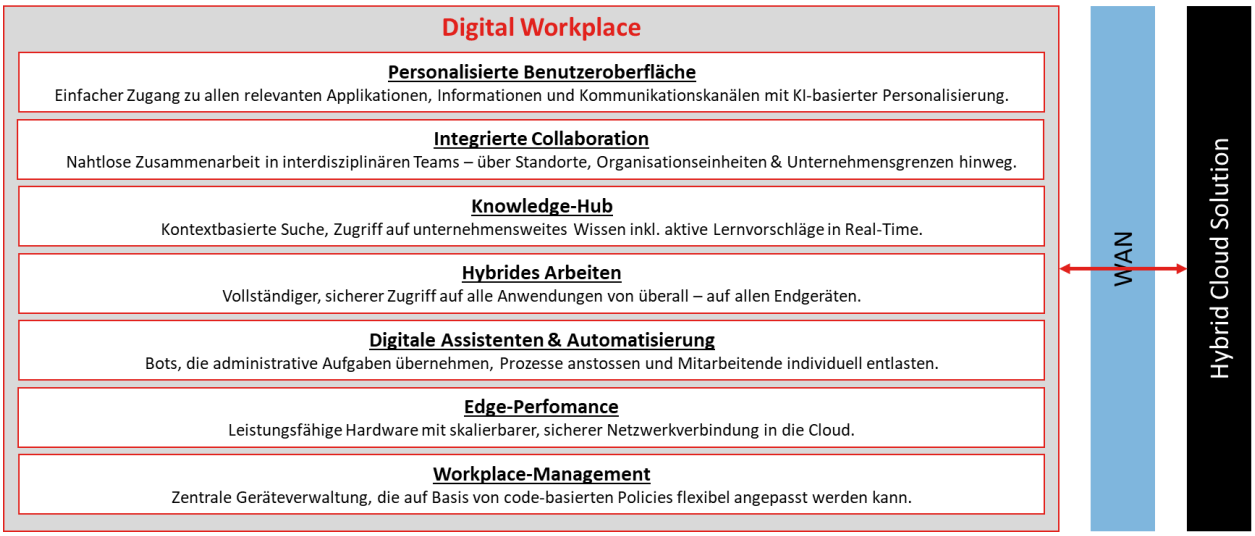


Abbildung 25: Moderner Workplace

Fazit

Der Digital Workplace der Zukunft entsteht heute. Banken und Krankenversicherungen stehen vor der Aufgabe, nicht nur technologische Weichen zu stellen, sondern eine Digitalisierungsstrategie mitzugestalten, die die Arbeitswelt grundlegend verändert. Dabei geht es nicht nur um Software und IT-Architektur, sondern um Zusammenarbeit, Kultur, Prozesse und soziale Verantwortung für die Mitarbeitenden. Der moderne Digital Workplace ermöglicht hybrides, grenzüberschreitendes Arbeiten und Kollaborieren, von dem kontinuierliches und bedarfsgerechtes Lernen integraler Bestandteil ist. Die klassische Grenze zwischen intern und extern verschwimmt – und genau dafür braucht es Konzepte auf Basis von Zero Trust, neue Architekturen, Prozesse und Mindsets. Der digitale Arbeitsplatz muss deshalb nicht nur technologisch neu konzipiert werden, sondern als Effizienz-Plattform für die sichere Nutzung von IT-Applikationen, den geschützten Zugang auf Unternehmensdaten und als «Hub» für Kollaboration und Wissensmanagement, Weiterentwicklung und Qualifizierung der Mitarbeitenden gedacht werden.

Schlusswort

Die Transformation der IT-Architektur im Schweizer Finanz- und Versicherungssektor ist mehr als eine technische Erneuerung – sie ist ein strategischer Schritt in Richtung Zukunftsfähigkeit. Composable Architecture bietet dabei einen vielversprechenden Ansatz, um Komplexität zu reduzieren, Agilität zu steigern und Innovation gezielt zu fördern. Doch der Wandel gelingt nur, wenn Technologie, Organisation, Sourcing und Kultur gemeinsam weiterentwickelt werden.

Mit diesem Booklet möchten wir einen Beitrag leisten, mehr Klarheit in ein dynamisches und komplexes Thema zu bringen und eine bessere Orientierung für anstehende Entscheidungen zu schaffen. Die skizzierten Konzepte, Einschätzungen und Empfehlungen sollen dazu ermutigen, neue Wege zu gehen und bestehende Paradigmen kritisch zu hinterfragen. Gleichzeitig verstehen wir diese Arbeit als Einladung zu einem fortlaufenden Dialog – über Chancen, Herausforderungen und die gemeinsame Gestaltung einer modernen, resilienten und innovationsfähigen Enterprise-IT.

Wir hoffen, dass die vorangehenden Seiten inspiriert haben, Denkanstösse vermitteln konnten und dazu beigetragen haben, die zukünftige IT-Landschaft im Banking und Versicherungswesen aktiv und erfolgreich zu formen.

Wir freuen uns auf den persönlichen Dialog – ganz getreu unserer Werte Innovation, Interaktion und Swissness!

Urs Rhyner
Head of Business Development
Business Development
urs.rhyner@inventx.ch
T +41 81 287 18 96