PHO-Consulting
CEO Advisory & IT Governance.

Where Business Shapes IT

STRATEGIE
ARCHITEKTUR
RESILIENZ
SOUVERÄNITÄT
ZUKUNFT

Komplexität beherrschen. Chancen nutzen.

WHITEPAPER

Von Business Capabilities zur resilienten, souveränen und zukunftsfähigen Organisation

Enterprise Architecture als strategisches Steuerungsinstrument



Strategie verbindet Möglichkeiten.
Peter Hofmann

Peter Hofmann
Inhaber
PHO-Consulting

- STRATEGIE AUSRICHTEN
- KOMPLEXITÄT REDUZIEREN
- RESILIENZ STÄRKEN
- SOUVERÄNITÄT SICHERN
- ZUKUNFT GESTALTEN



- Effizient
- Transparent
- Sicher
- Resilient
- Souverän
- Zukunftsfähig

EINBLICKE aus der Praxis

KONKRETE ANSÄTZE für Ihre Organisation

NACHHALTIGE WIRKUNG für heute und morgen

MANAGEMENT-PERSPEKTIVE

Executive Summary: Fähigkeiten statt Systeme steuern

Die Ausgangslage

Viele Organisationen kennen ihre Anwendungen, Verträge und technischen Plattformen. Weniger transparent ist, welche geschäftlichen Fähigkeiten davon abhängen und welche Wirkung ein Ausfall, eine Vertragsänderung oder ein Anbieterwechsel auf die Leistungserbringung hat. Genau diese Lücke schließt ein capability-basierter Enterprise-Architecture-Ansatz.

Business Capabilities beschreiben, was eine Organisation dauerhaft beherrschen muss, um Auftrag, Strategie und Leistung zu erfüllen. Prozesse, Organisationseinheiten und Technologien beschreiben dagegen, wie diese Fähigkeit aktuell umgesetzt wird.

Kernaussage

Enterprise Architecture ist kein Dokumentationsprojekt. Sie verbindet Geschäftswirkung, Risiken, Kontrollmöglichkeiten und Technologieentscheidungen zu einem steuerbaren Gesamtmodell.

Der Nutzen

- strategische Transparenz über geschäftskritische Fähigkeiten
- sichtbare Abhängigkeiten zwischen Business, Daten, Anwendungen und Anbietern
- fachlich priorisierte Resilienz- und Wiederanlaufentscheidungen
- bewusste Steuerung von Portabilität, Exit und digitaler Souveränität
- belastbare Zielarchitekturen und priorisierte Transformationsroadmaps

Der durchgängige Use Case



Business Capabilities werden mit Prozessen, Daten, Anwendungen, Technologien und Partnern verbunden.

Eine Organisation nutzt eine zentrale Cloud- und Plattformlösung für Kundenportal, Dokumentenmanagement, Zusammenarbeit, Identitäten und Genehmigungsworkflows. Der Anbieter kündigt eine wesentliche Vertragsänderung an. Gleichzeitig tritt eine mehrstündige Störung auf.

Das Whitepaper zeigt, wie aus einer scheinbar technischen Störung eine strategische Architekturfrage wird: Welche Fähigkeiten sind betroffen? Welche Abhängigkeiten teilen sie? Welche Mindestleistungen müssen erhalten bleiben? Welche Daten, Identitäten, Workflows und Betriebsinformationen sind tatsächlich portabel?

Ergebnis

Statt unmittelbar eine vollständige Migration zu starten, entsteht eine abgestufte Agenda aus Transparenz, Kontrollfähigkeit und modularer Zielarchitektur.

BUSINESS ARCHITECTURE

Business Capabilities als gemeinsame Sprache

Was eine Capability beschreibt

Eine Business Capability beschreibt ein dauerhaft benötigtes geschäftliches Können. „Digitale Kundeninteraktion“ bleibt relevant, unabhängig davon, ob die Leistung über Portal, App, Telefon, E-Mail oder einen persönlichen Kontakt erbracht wird. Die konkrete Umsetzung kann sich ändern, die Fähigkeit bleibt bestehen.

Damit eignen sich Capabilities als relativ stabile Verbindung zwischen Strategie, Fachbereichen und IT. Sie lassen sich nach strategischer Bedeutung, Zeitkritikalität, Datenkritikalität, Reifegrad, Kosten, Risiko und Veränderungsbedarf bewerten.

Abgrenzung

Capability = Was müssen wir können? Prozess = Wie arbeiten wir? Organisation = Wer trägt Verantwortung? Anwendung = Welche Software unterstützt? Technologie = Worauf läuft die Lösung?

Capability Map des Use Cases

- digitale Interaktion
- Identität und Zugriff
- Dokumentenführung
- Fallbearbeitung
- Genehmigungen
- Partnerintegration

Warum die Perspektive wichtig ist

Im Use Case trifft die Plattformstörung fast alle sechs Fähigkeiten gleichzeitig. Auf Anwendungsebene könnte die Organisation mehrere Systeme sehen und vermeintliche Redundanz annehmen. Auf Capability-Ebene wird jedoch sichtbar, dass dieselbe Plattform, derselbe Identitätsdienst und dieselbe Integrationsschicht mehrere Leistungen gemeinsam tragen.

Besonders kritisch sind Identität und Zugriff, weil ohne Authentisierung auch alternative Anwendungen nicht genutzt werden können. Dokumentenführung ist kritisch, weil Entscheidungen ohne vollständige Akten, Versionen und Berechtigungen fachlich und regulatorisch riskant werden.

Praxisdialog

Service Owner: „Alle sechs Fähigkeiten hängen an derselben Plattform.“ BCM: „Dann planen wir nicht sechs isolierte Ausfälle, sondern behandeln die gemeinsame Abhängigkeit.“ Enterprise Architecture: „Genau dafür brauchen wir die Capability Map.“

Owner und Verantwortung

Für kritische Capabilities sollten fachliche Owner benannt werden. Der Capability Owner verantwortet nicht die gesamte Technik, sondern die geschäftliche Wirkung, Mindestleistung, Kritikalität und priorisierte Veränderungsbedarfe. Damit erhält Architekturarbeit eine klare fachliche Verankerung.

ABHÄNGIGKEITEN TRANSPARENT MACHEN

Von der Capability zur End-to-End-Architektur

Die Architektur-Ebenen



Mehrere Geschäftsservices teilen Plattform, Identität, Workflows und Anbieter.

- Geschäftsziele und Leistungsversprechen
- Business Capabilities und Business Services
- Prozesse, Rollen und Organisation
- Informationen, Daten und Geschäftsregeln
- Anwendungen, Schnittstellen und Identitäten
- Technologien, Plattformen und Infrastruktur
- Anbieter, Subdienstleister und Verträge

Konzentrationsrisiken erkennen

Der Use Case zeigt eine typische Täuschung: Mehrere Anwendungen vermitteln den Eindruck von Redundanz. Tatsächlich verwenden alle Lösungen denselben Identitätsdienst, dieselbe Cloud-Plattform oder dieselbe Integrationskomponente. Ein einzelner Fehler kann deshalb mehrere vermeintlich unabhängige Leistungen gleichzeitig beeinträchtigen.

Zusätzlich liegen Workflows, Berechtigungsmodelle und Betriebswissen überwiegend beim Anbieter. Ein einfacher Export von Dateien schafft noch keine Wechseloption. Erst die End-to-End-Sicht zeigt, welche fachlichen, technischen, operativen und vertraglichen Bausteine gemeinsam benötigt werden.

Managementfragen

Welche Komponenten werden von mehreren kritischen Capabilities gemeinsam genutzt? Welche Abhängigkeit ist nicht kurzfristig ersetzbar? Welche Informationen müssen bei einem Wechsel mitgenommen werden? Wer besitzt das notwendige Betriebswissen?

Architektur als Entscheidungsinstrument

Enterprise Architecture übersetzt Geschäftswirkung in Technologieentscheidungen. Die Architektur zeigt nicht nur, was vorhanden ist, sondern welche Optionen existieren, welche Risiken akzeptiert werden und welche Veränderungen den größten geschäftlichen Nutzen erzeugen.

Kritikalität, Zeitwirkung und resiliente Leistungserbringung

Zeitwirkung im Use Case



Die Wirkung eines Ausfalls verändert sich über die Zeit.

- nach 2 Stunden: Portalstörung und erste Rückfragen; Ersatzkanäle sind noch tragfähig
- nach 8 Stunden: Rückstände, manuelle Übergaben und Priorisierung werden erforderlich
- nach 24 Stunden: Fristen, Zahlungen und Partnerprozesse geraten in Gefahr
- nach 72 Stunden: erhebliche Leistungs-, Compliance- und Reputationsauswirkungen

Resilienz fachlich definieren

Resilienz entsteht nicht allein durch technische Hochverfügbarkeit. Fachbereiche müssen beschreiben, welche Leistung in welchem Mindestumfang nach welcher Zeit verfügbar sein muss. Diese Anforderungen steuern Wiederanlauf, Notbetrieb, Architektur und Investitionen.

Im Use Case werden Identität, Dokumentenzugriff und Kernworkflow früher benötigt als Komfortfunktionen des Portals. Daraus ergibt sich eine fachlich priorisierte Recovery-Reihenfolge.

Kontrollierte Degradation

Eine resiliente Architektur plant einen reduzierten, aber definierten Mindestservice: alternative Kanäle, lokale Referenzinformationen, manuelle Genehmigungen, spätere Nacherfassung und klare Kommunikation.

Fachliche Abnahme

Ein technisch laufender Server ist noch kein wiederhergestellter Business Service. Erst wenn Daten vollständig, Berechtigungen wirksam, Schnittstellen funktionsfähig und fachliche Abläufe nutzbar sind, ist die Leistung wiederhergestellt. Deshalb müssen technische Recovery und fachliche Abnahme getrennt dokumentiert werden.

Praxisdialog

IT: „Der Server läuft wieder.“ Fachbereich: „Akten und Berechtigungen sind unvollständig.“ Krisenleitung: „Der Service gilt erst nach fachlicher Bestätigung als wiederhergestellt.“

KONTROLLIERTE WAHLFÄHIGKEIT

Digitale Souveränität als Architekturqualität

Kontrolle statt Isolation

Digitale Souveränität bedeutet nicht, jede Technologie selbst zu entwickeln oder jeden Dienst selbst zu betreiben. Souverän ist eine Organisation, wenn Abhängigkeiten transparent sind, bewusst akzeptiert werden und angemessene Kontroll- sowie Handlungsoptionen bestehen.

Sechs Kontrollfelder

- Datenkontrolle: Speicherort, Zugriff, Export, Löschung und Nachweise
- Identitätskontrolle: Rollen, Schlüssel, privilegierte Zugriffe und Notfallzugänge
- technologische Kontrolle: Standards, Portabilität und alternative Laufzeitumgebungen
- operative Kontrolle: Monitoring, Support, Änderungen und Incident Response
- vertragliche Kontrolle: Informationsrechte, Subdienstleister, Exit und Unterstützung
- Governance: Accountability, Risikobewertung und prüfbare Entscheidungen

Leitgedanke

Souveränität ist kontrollierte Wahlfähigkeit, nicht Scheinautarkie.

Anwendung auf den Use Case



Von fragmentierten Legacy-Abhängigkeiten zu einer modularen, kontrollierbaren Zielarchitektur.

Die Organisation prüft, ob Daten vollständig exportierbar sind, ob Identitäten und Schlüssel unter eigener Kontrolle bleiben, welche administrativen Zugriffe der Anbieter besitzt und welche Änderungen an Datenstandorten oder Subdienstleistern gemeldet werden müssen.

Darüber hinaus wird bewertet, ob alternative Betriebsmodelle existieren und wie ein Exit praktisch unterstützt wird. Erst wenn Export, Migration, Wiederanlauf und Löschung getestet wurden, ist aus einer Vertragsklausel ein belastbarer Nachweis geworden.

Portabilität: Warum ein Datenexport nicht genügt

Sechs Dimensionen echter Portabilität

- Inhalte: Dokumente, Datensätze und Historien
- Metadaten: Aktenstruktur, Versionen, Fristen und Beziehungen
- Identitäten: Nutzer, Rollen, Gruppen und Berechtigungen
- Konfiguration: Workflows, Regeln, Vorlagen und Parameter
- Integration: APIs, Ereignisse, Zertifikate und Schlüssel
- Betriebswissen: Dokumentation, Runbooks, Monitoring und Support

Im Use Case bestätigt der Anbieter, dass Dokumente als Dateien exportiert werden können. Die Prüfung zeigt jedoch, dass Aktenstruktur, Versionen, Berechtigungen und Workflows nicht vollständig enthalten sind. Damit ist der Export technisch vorhanden, aber fachlich unzureichend.

Praxisdialog

Anbieter: „Alle Dokumente können exportiert werden.“ Fachbereich: „Auch Aktenstruktur, Versionen, Fristen und Berechtigungen?“ Anbieter: „Nicht vollständig.“ Einkauf: „Dann erfüllt der Export unseren fachlichen Exit-Bedarf nicht.“

Exit-Fähigkeit als Designanforderung

Portabilität darf nicht erst am Vertragsende geprüft werden. Anforderungen an Formate, Metadaten, Schnittstellen, Dokumentation, Unterstützung, Fristen und Kosten gehören in Architekturprinzipien, Beschaffung und Verträge. Kritische Exporte sollten regelmäßig in eine Testumgebung importiert werden.

Architekturprinzipien

- Capability first: Geschäftswirkung steuert die Entscheidung
- Modularität: klare Verantwortungs- und Kopplungsgrenzen
- Interoperabilität: offene Schnittstellen und gemeinsame Datenmodelle
- Portabilität: Daten, Konfiguration und Betrieb übertragbar gestalten
- Resilience by Design: Degradation, Recovery und Tests einplanen
- Governance by Design: Kontrollen, Nachweise und Ownership integrieren

Ausnahmen bewusst steuern

Proprietäre Funktionen können legitim sein, wenn der geschäftliche Nutzen die Abhängigkeit rechtfertigt, Kompensationen vorhanden sind und die Ausnahme befristet überprüft wird.

TRANSFORMATION

Zielarchitektur: Vom Plattform-Monolithen zur modularen Servicearchitektur

Gestaltungsziele



Zielbild einer modularen und resilienten Servicearchitektur.

- Identität als klar abgegrenzter und kontrollierter Basisservice
- Dokumente und Metadaten in portablen Formaten
- Workflows über dokumentierte Schnittstellen entkoppeln
- kritische Capabilities mit getesteten Notbetriebsoptionen versehen
- Monitoring und Nachweise serviceübergreifend organisieren
- alternative Anbieter- oder Betriebsoptionen regelmäßig validieren

Keine Big-Bang-Migration

Die Zielarchitektur verlangt nicht, die bestehende Plattform sofort vollständig zu ersetzen. Zunächst werden die kritischsten Kopplungen reduziert. Die Organisation gewinnt schrittweise Kontrolle über Identitäten, Daten, Schnittstellen und Betriebswissen.

Im Use Case bleiben ausgewählte Plattformfunktionen bestehen, während Identität entkoppelt, ein vollständiges Exportmodell geschaffen und der Kernworkflow über standardisierte Schnittstellen angebunden wird. Parallel entsteht ein getesteter Mindestbetrieb für die kritischsten Capabilities.

Investitionslogik

Investiert wird zuerst dort, wo Resilienz, Wahlfähigkeit und geschäftliche Wirkung am stärksten steigen.

Übergangsarchitekturen

Zwischen Ist- und Zielbild liegen Übergangsarchitekturen. Sie beschreiben, welche alten und neuen Komponenten zeitweise parallel betrieben werden, wie Daten synchronisiert werden, welche Risiken befristet akzeptiert werden und wann der nächste Zielzustand erreicht ist.

UMSETZUNG

Roadmap, Governance und messbare Wirkung

Drei Umsetzungshorizonte



Drei Horizonte: Transparenz, Kontrollfähigkeit und Zielarchitektur.

- 0-90 Tage: Capabilities, Owner, Kritikalität und Abhängigkeiten erfassen
- 3-12 Monate: Prinzipien, Portabilitätsanforderungen, Notbetrieb, Verträge und erste Tests
- 12-24 Monate: Modularisierung, Konsolidierung sowie stärkere Daten- und Identitätskontrolle

Im Use Case startet die Organisation nicht mit einer vollständigen Migration. Priorität erhalten Identitätskontrolle, vollständiges Exportmodell, Notbetrieb und ein getesteter alternativer Pfad für den kritischen Service.

Architektur-Governance

- Executive Sponsor: Zielbild, Risikobereitschaft und Investitionen
- Capability Owner: Geschäftswirkung, Kritikalität und Mindestservice
- Enterprise Architecture: Prinzipien, Zielarchitektur und Roadmap
- Security & Resilience: Risiken, Kontrollen, BCM und Recovery
- Procurement & Legal: Anbieteranforderungen, Verträge und Exit
- Delivery Teams: Umsetzung, Nachweise und Architekturentscheidungen

Wirksamkeit messen

- Anteil kritischer Capabilities mit Owner und End-to-End-Modell
- kritische Konzentrations- und Single-Provider-Abhängigkeiten
- getestete Export-, Import- und Wechselfähigkeit
- Mindestservice, Recovery- und Übungsnachweise
- technische Schulden nach Geschäftswirkung
- umgesetzte Roadmap-Maßnahmen und erreichte Zielzustände

Entscheidungsregel

Architektur-Governance genehmigt Ausnahmen nur mit begründetem Nutzen, Kompensation, benanntem Restrisiko und Review-Termin.

FAZIT

Management-Selbstcheck und nächster Schritt

Sechs Fragen für die Organisation

- Sind die strategisch wichtigen Business Capabilities bekannt?
- Ist klar, welche Fähigkeiten nach welcher Zeit ausfallen dürfen?
- Sind Daten, Anwendungen, Plattformen und Anbieter nachvollziehbar zugeordnet?
- Sind Kontrolle, Portabilität und Exit praktisch nachgewiesen?
- Existieren Mindestservice und fachlich priorisierter Wiederanlauf?
- Werden Investitionen anhand von Capability-Nutzen, Risiko und Abhängigkeiten priorisiert?

Interpretation

Jede offene Frage ist kein Vorwurf, sondern ein konkreter Auftrag für Business Architecture, Governance, BCM oder Transformation.

Capability & Architecture Quick Check

Ein pragmatischer Einstieg beginnt mit einem kritischen Geschäftsservice. Die relevanten Capabilities und Owner werden identifiziert, Prozesse, Daten, Anwendungen, Plattformen und Anbieter zugeordnet und anschließend nach Kritikalität, Resilienz, Souveränität und Veränderungsdruck bewertet.

Drei Botschaften zum Mitnehmen

PHO-Consulting — CEO Advisory & IT Governance
Where Business Shapes IT

PHO-Consulting: Strategie, Architektur, Resilienz und Souveränität verbinden.

- Business Capabilities schaffen eine stabile gemeinsame Sprache für Strategie, Fachbereiche und IT.
- Resilienz und Souveränität sind Qualitätsmerkmale der Enterprise Architecture, keine nachträglichen Zusatzkontrollen.
- Transformation wird wirksamer, wenn Investitionen nach geschäftlicher Fähigkeit, Kritikalität und Abhängigkeit priorisiert werden.

Nächster Schritt

Wählen Sie einen kritischen Service und stellen Sie drei Fragen: Welche Fähigkeiten hängen daran? Welche gemeinsamen Abhängigkeiten bestehen? Welche Alternative wurde tatsächlich getestet?

Kontakt

PHO-Consulting · Peter Hofmann
Kontakt@pho-online.net · +49 170 5517343
https://www.pho-online.net
Where Business Shapes IT

Grundlage dieses Whitepapers ist das Webinar „Von Business Capabilities zur resilienten, souveränen und zukunftsfähigen Organisation“.