IT-Strategie

Für den neuen Geschäftsbereich Cashless

von Julian Nischler
und Kjartan Ferstl

1 MANAGEMENT SUMMARY

1.1 ALLGEMEINES

Die Geschäftsführung plant aktuell den neuen Cashless-Geschäftszweig, dessen Ziel es ist, ein bargeldloses Bezahlsystem zu entwickeln und anzubieten. Neben dem Produkt als On-Premise Installation, soll auch ein Cloud-Service angeboten werden. Bei beiden Varianten ist wegen der direkten Verbindung zu Konten und Kreditkarten ein besonderer Fokus auf die Sicherheit gegen Angriffe zu richten.

Diese IT-Strategie wurde von der IT-Leitung für den oben erwähnten neuen Geschäftszweig entwickelt und gibt die Rahmenbedingungen, sowie die Ziele der internen IT vor. Als Grundlage dient die aktuelle IT-Unternehmensstrategie, dieses Dokument richtet den Fokus auf die zusätzlichen Anforderungen durch die spezifischen Risiken und Ziele aus diesem Geschäftszweig.

2 BUSINESSZIELE UND ANFORDERUNGEN

Das wichtigste Businessziel die Stellung als Marktführer im noch sehr jungen Geschäftsbereich. Hauptverantwortlich dafür soll neben der wirtschaftlichen Aufstellung des Unternehmens besonders die die Leistungen der F&E Abteilung im BI-Bereich sein. Wichtigstes Asset hierfür sind wiederrum die Kundendaten und die Protokollierung jeder Transaktion.

2.1 KONTEXTANALYSE

Der Geschäftszweig bietet eine On-Premise sowie eine Clould-basierte Lösung an. Beide Lösungen speichern jede Transaktion mit allen verfügbaren aktuellen Kunden- und Betriebsdaten und sind daher entsprechend zu schützen.

Die zu schützenden Daten werden in zwei Klassen kategorisiert:

Klasse A — Direkt sicherheitsrelevante Daten

- Kreditkartendaten
- Kontoinformationen

Klasse B — Persönliche Daten

- Transaktionen
- Kundendaten
- BI-Erkenntnisse und Entscheidungen

Zur Minimierung der Risikostellen sollen Daten nur dort, und nur in dem Umfang verfügbar sein wo und wie sie tatsächlich benötigt werden. Die zu schützenden Betriebsdatenbanken von On-Premise und Cloud-Installationen dürfen nur für den Betrieb verfügbar, so treffen die Anforderungen an Informationssicherheit der Klasse A und Klasse B nur die Betriebsabteilung.

Backupfunktionen und andere Zugriffmöglichkeiten auf größere Datenmengen erfordern spezielle Berechtigungen, die nur für befristete Zeitfenster von wenigen Stunden ausgestellt werden.

Das Betriebs-Team stellt eine Arbeitsgruppe zur Anonymisierung von Betriebsdaten. Ziel dieser Arbeitsgruppe ist es, automatisiert in Intervallen von zwei Wochen Daten für das BI-Team und die Entwicklung zur Verfügung zu stellen. Dabei muss jeder Datensatz manuell eingesehen und freigegeben werden, sodass keine Daten der Klasse A oder der Klasse B die Betriebsabteilung verlassen.

2.2 INTERESSENSGRUPPEN

Stakeholder	Anforderungen
Kunden	• Hohe Qualität und Verfügbarkeit der angebotenen Leistungen. Guten Service und Analysen durch das Betriebsteam.
Betriebsteam	• Verfügbarkeit und Ausfallssicherheit der Betriebsdatenbanken und Applikationen • Berechtigungsmanagement zur Gewährleistung der Sicherheitsrichtlinien.
Produkt-Entwicklungsteam	• Verfügbarkeit der Entwicklungs- und Testsysteme • Lizenzmanagement für Entwicklungstools
Forschung & Entwicklung	• Verfügbarkeit und Performance der BI-Datenbanken und Tools
Vertrieb	• VPN-Zugang und Testsysteme für Demos

2.3 ANFORDERUNGEN / RISIKEN

2.3.1 Sicherheit von Betriebsdaten

Risikominimierung bei Verlust oder Entwendung von Betriebsdaten. Um das Sicherheitsrisiko zu minimieren sollen alle Dienste für den täglichen Betrieb in ein dafür zertifiziertes Datencenter ausgelagert werden. Die Installation der Systeme wird dabei von unseren Mitarbeitern in Zusammenarbeit mit externen Consultants durchgeführt.

Die gesamte Sicherheitsinfrastruktur soll vielschichtig aufgebaut werden, so dass ein Angreifer mehrere Hürden überwinden müsste um einen Schaden anrichten zu können.

Risiko	Maßnahme
Mitarbeiter bevorzugen Einfachheit gegenüber Sicherheit	Externe Consultants bei der Inbetriebnahme neuer Systeme. Sie sollen helfen Normen und Richtlinien einzuhalten sowie sicherzustellen dass Sicherheitsrichtlinien feingranular erstellt werden und keine Notwendigkeit für Super-Administratoren gibt.
Mitarbeiter verlieren den Sicherheitsgedanken mit	Externe Audits in halbjährlichen Intervallen. Eventuelle ISO Zertifizierung der Betriebsabteilung.

fortschreitender Zeit wenn keine Probleme auftreten.	
Hackerangriffe	Das Datencenter kümmert sich auf Netzwerkebene um Firewalls sowie die VPN-Zugriffe und eventuelle. Die Systeme erlauben per Definition kein Auslesen von größeren Datenmengen und schlagen für sich Alarm wenn Anomalitäten auftreten. Daten werden wöchentlich mit den Kunden abgerechnet, ein erfolgreicher Angriff auf die Daten kann nur Statistiken verfälschen oder Daten veruntreuen aber keinen unmittelbaren relevanten Schaden anrichten. Gegen übrige Risiken wird eine Versicherung abgeschlossen.
Veruntreuung durch Mitarbeiter aus dem Betrieb	Mitarbeiter erhalten zu relevanten Betriebsdaten nur lesenden Zugriff. Werden große Datenmengen, z.B. für ein außertourliches Backup benötigt, so müssen dafür separat Berechtigungen für ein begrenztes Zeitfenster angefordert werden.
Veruntreuung durch Mitarbeiter aus der Entwicklung	Neue Softwarekomponenten müssen Langzeittests über mehrere Rechnungsintervalle hinweg bestehen bevor sie ausgerollt werden. Außerdem wird jeder Netzwerkzugriff im Betrieb protokolliert, wodurch Manipulationen schnell sichtbar werden sollten.

2.3.2 Ausfallsicherheit des Produktivsystems

Die Ausfallssicherheit hat höchste Priorität für die Kundenzufriedenheit, die Cloud-Dienste müssen 24/7 verfügbar sein und SLAs an unsere Kunden einhalten.

Risiko	Maßnahme
Ausfall eines Dienstes	Unsere Systeme basieren auf Messagequeues und arbeiten, eine einzelne Aufgabe wird dabei immer von mindestens zwei Instanzen durchgeführt. Fällt eine aus oder liefert andere Ergebnisse so wird umgehend das Betriebsteam informiert um die Fehlfunktion zu beheben.
Ausfall von Servern	Durch die oben erwähnte Parallelisierung der einzelnen Dienste muss nur sichergestellt werden, dass Dienste vom gleichen Typ nicht auf den gleichen Maschinen laufen.
Ausfall des Datencenters	Alle Dienste müssen in zwei oder mehr örtlich getrennten Datencentern verfügbar sein. Je nach Verfügbarkeit vom Dienstleister muss hier evtl. auf mehrere Dienstleister zurückgegriffen werden.
DDOS-Attacke	Ausfallsicherheit vor DDOS-Attacken soll vor allem durch Security trough diffusion gewährleistet werden. Durch die Parallelisierung in der Softwarearchitektur sollen immer unausgelastete Services auf anderen Adresse zur Verfügung stehen. Ein Angreifer müsste so alle Komponenten einer Art kennen und gleichzeitig angreifen. Ein Angriff kann dadurch nicht ausgeschlossen aber sehr viel schwieriger gestaltet werden.

2.3.3 Flexibles Testumfeld der F&E-Abteilung

Risiko	Maßnahme
Starke Einschränkung der Forschungsinfrastruktur durch Sicherheitsmaßnahmen	Durch die klare Trennung von Betriebsdaten und anonymisierten Forschungsdaten treffen hier diesbezüglich keine Richtlinien. Die F&E Abteilung darf sich lokal Systeme installieren und ist selbst dafür verantwortlich. Werden Neuerungen in die Produktentwicklung übernommen, so werden auch die Komponenten von der IT übernommen.
Fehlende IT-Kenntnisse der Forschungsabteilung	Die Forschungsabteilung sollte über genügend Know-How im IT Bereich verfügen. Ist anders der Fall, darf die unternehmensweite IT unterstützend wirken, die Systeme müssen dabei aber getrennt von den produktiven Datencentern installiert werden.

2.3.4 Wartung der Entwicklungsinfrastruktur

Risiko	Maßnahme
Starke Einschränkung der Entwicklungsinfrastruktur durch Sicherheitsmaßnahmen	Durch die klare Trennung von Betriebsdaten und anonymisierten Entwicklungsdaten treffen hier diesbezüglich keine Richtlinien.
Fehlende IT-Kenntnisse der Forschungsabteilung	Die unternehmensweite IT organisiert und installiert alle benötigten Softwarekomponenten. Die installierten Systeme dürfen nicht auf den gleichen Systemen wie das Produktivsystem installiert werden oder darauf zugreifen können. Die Entwicklungssysteme dürfen aber in den gleichen Rechenzentren wie die Produktivsysteme laufen.

3 IT ASSESSMENT

IST-Zustand: Für die Verwaltung soll soweit möglich die Software sowie die Infrastruktur des Mutterkonzerns genutzt werden. Spezifische Systeme wie in etwa die Entwicklungsumgebung, die F&E Infrastruktur oder das Produktivsystem sind noch nicht vorhanden.

SOLL-Zustande: Es soll eine klare Richtlinie geben wie mit Informationen, besonders in der Betriebsabteilung, umgegangen werden muss. Hierbei werden Verantwortlichkeiten genauso wie Sicherheitseinschränkungen festgelegt.

GAP: Festlegung der Sicherheit-Barrieren, Suche nach passenden Datencentern.

4 IT STRATEGIE

4.1 SICHERHEIT VON BETRIEBSDATEN

Strategisches Ziel	Auswahl von geeigneten Datencenter.
Ist-Zustand und derzeitige Mängel	Noch nichts unternommen.
Maßnahme	Datencenter mit entsprechendem Sicherheitsstandard finden
Beschreibung	Sollte ggf. Zertifizierungen aufweisen um die Versicherungspauschalen gering zu halten.
Mehrwert	Sicherheit vor Angriffen.
Erfolgsmessgröße	Preis inklusive Versicherungsprämien.

Strategisches Ziel	Offene Rechnungsbeträge mit Kunden gering halten.
Ist-Zustand und derzeitige Mängel	Noch nichts unternommen.
Maßnahme	Abrechnung in möglichst kurzen Intervallen
Beschreibung	Es sollen möglichst wenig offene / noch nicht abgerechnete Transaktionen mit den Kunden bestehen.
Mehrwert	Reduzierung des momentanen Risikopotentials und damit den Versicherungsprämien.
Erfolgsmessgröße	Mittlerer offener Transaktionswert pro Monat.

4.2 AUSFALLSICHERHEIT DES PRODUKTIVSYSTEMS

Strategisches Ziel	Auswahl von geeigneten Datencenter.
Ist-Zustand und derzeitige Mängel	Noch nichts unternommen.
Maßnahme	Datencenter mit entsprechender Verfügbarkeit finden
Beschreibung	Sollte ggf. Zertifizierungen aufweisen um die Versicherungspauschalen gering zu halten.
Mehrwert	Sicherheit vor Ausfällen.

Erfolgsmessgröße	Verfügbarkeit, SLAs
Maßnahme	Redundante Datencenter.
Beschreibung	Mehrere Datencenter mit entsprechender Verfügbarkeit finden.
Mehrwert	Sicherheit vor Ausfällen.
Erfolgsmessgröße	Akkumulierte Verfügbarkeit, min. 200%
Strategisches Ziel	Ausfallsicherheit der Applikation
Ist-Zustand und derzeitige Mängel	Noch nichts unternommen.
Maßnahme	Parallelisierung der Komponenten
Beschreibung	Die Entwicklung der Softwarekomponenten soll es ermöglichen mehrere Instanzen die den gleichen Datensatz bearbeiten parallel laufen zu lassen.
Mehrwert	Sicherheit vor Angriffen, Sicherheit vor Ausfällen
Erfolgsmessgröße	Komplexität der Single-Point-Of-Failure Software-Komponenten, analysiert mit Code-Analyse-Tools
Maßnahme	Alte Versionen verfügbar halten
Beschreibung	Im Falle eines totalen Ausfalls sollen alter Versionen der Softwarekomponenten die Arbeit wieder aufnehmen können.
Mehrwert	Sicherheit vor Angriffen, Sicherheit vor Ausfällen
Erfolgsmessgröße	Mittlere Dauer der Wiederaufnahme der Arbeit nach testweisen offline-Schalten einzelner Systeme, Tests im quartal-Intervall.

4.3 Flexibles Testumfeld der F&E-Abteilung

Strategisches Ziel	Gute IT-Infrastruktur der F&E, ohne direkte Wartung der IT-Abteilung
Ist-Zustand und derzeitige Mängel	Noch nichts unternommen.
Maßnahme	Reviews
Beschreibung	Monatliche Reviews der Infrastruktur und ggf. Beratung durch die IT.
Mehrwert	Produktivitätssteigerung der F&E

Erfolgsmessgröße	Benötigte IT-Support-Stunden der F&E abseits des Reviews.

4.4 Wartung der Entwicklungsinfrastruktur

Strategisches Ziel	Gute IT-Infrastruktur der Entwicklungsabteilung.
Ist-Zustand und derzeitige Mängel	Noch nichts unternommen.
Maßnahme	Telefon und Ticket-Support
Beschreibung	Rascher Support, bewertet nach Wichtigkeit und Dringlichkeit aktueller Projekte.
Mehrwert	Produktivitätssteigerung der Entwicklungsabteilung.
Erfolgsmessgröße	Benötigte IT-Support-Stunden zur Lösung von Problemen.
Maßnahme	Lizenzen zu Versuchszwecken
Beschreibung	Sollen Produkte auf eine Dauer getestet werden, so dürfen Software-Lizenzen für Entwicklungszwecke beantragt werden.
Mehrwert	Einfaches erproben neuer/alternativer Technologien und Möglichkeiten.
Erfolgsmessgröße	Durchschnittliche Dauer der Lizenzausstellung neuer Softwarekomponenten.

5 Umsetzung des Planes

5.1 Kommunikation der Ergebnisse

Die Ergebnisse der IT-Strategie werden allen Mitarbeitern in einer Quartalsbesprechung des Geschäftszweiges mitgeteilt. Jene Kollegen, welche in die Umsetzungs- und Planungsprojekte involviert sind, werden zusätzlich in einer weiteren Runde über die Details der IT-Strategie und deren Umsetzung informiert. Wichtig ist hierbei sämtlichen Kollegen zu vermitteln, dass ihre Mitarbeit an der Umsetzung essentiell ist und der Erfolg dieses Projektes zu einem wesentlichen Teil von ihnen abhängt.

5.2 Schlüsselindikatoren

Für die oben genannten Themen müssen Projektleiter definiert werden, die sich in monatlichen Intervallen über die Einhaltung der Ziele austauschen und an das Management berichten. Für die

Umsetzungsbezogenen Projekte wie die Auswahl der Rechenzentren ist außerdem ein Projektplan mit konkreten Meilensteinen bis zur kompletten Umsetzung zu erstellen und zu überwachen.

5.3 VERANTWORTLICHKEITEN

Projekt	Verantwortlich	Fertigstellung
Auswahl von geeigneten Rechenzentren für das Produktivsystem	Leitung der Unternehmensweiten IT Max Machtdas	2015/06
Auswahl von geeigneten Rechenzentren für das Entwicklungssystem	Leitung der Unternehmensweiten IT Max Machtdas	2015/06
Kurze Abrechnungsintervalle	Leitung des bisherigen Finanzwesens Herbert Kostetwas	Dauerprojekt
Flexibles Testumfeld der F&E	Leitung des BI-Teams, später Leitung der F&E Abteilung Maria Findetwas	Dauerprojekt
Entwicklungsinfrastruktur	Leitung des der bisherigen Entwicklungsabteilung, später die eigene Entwicklungsabteilung Siglinde Codetwas	Dauerprojekt
Organisieren externer Audits	Leitung des Testteams Franz Ärgerwen	2016/01

5.4 ÜBERPRÜFUNG UND KORREKTUR

Alle zwei Monate wird der Projektfortschritt von dem Strategiekremium überprüft, mit dem Management abgestimmt und falls notwendig werden Korrekturen eingeleitet.

Halbjährlich werden die Ziele- und Strategien der einzelnen Punkte erneut überprüft und gegebenenfalls an einen geänderten Kontext angepasst.

Jedes zweite Jahr wird die gesamte IT-Strategie überarbeitet und neu an der Unternehmensstrategie ausgerichtet, beziehungsweise dem geänderten Kontext angepasst.