

HS 07

Unternehmensweite IT-Architekturen

Fallstudie

Derendinger

Raphael Blatter 02-430-015

Stefan Hutter 03-919-487

Inhaltsverzeichnis

Inhaltsverzeichnis	2
Management Summary	3
Die aktuelle IT-Umgebung	4
Nicht funktionale Anforderungen	5
Verantwortlichkeiten.....	5
Systemzugriffe.....	5
HelpDesk und Support	5
Infrastruktur.....	5
Monitoring.....	5
Storage.....	6
Backup/Recovery	6
Netzwerk	6
Verfügbarkeit	6
Performance	6
Die zukünftige IT-Umgebung	7
Wechsel von IST zu SOLL.....	10
Zusammenfassung	10

Management Summary

Die Derendinger-Gruppe erweitert ihr Einzugsgebiet in die Märkte Spanien, Deutschland und Österreich. Mit der Erweiterung des Kundenstammes steigen auch die Anforderungen an die IT-Architektur bezüglich Skalierbarkeit, Verfügbarkeit und Sicherheit.

Um den sich ändernden Anforderungen gerecht werden zu können, soll ein weiteres Rechenzentrum, nebst jenem in Dietlikon, in Innsbruck aufgebaut werden.

30'000 Kunden erwarten von Derendinger eine schnelle und zuverlässige Bestellabwicklung. Dies wird über einen medienbruchfreien Webkanal gewährleistet. Als Schnittstelle zwischen Webserver und Datenbankserver verwendet Derendinger Oracle Forms. Der Lebenszyklus dieser Applikation hat das Ende erreicht und wird nicht länger von Oracle unterstützt. Als Ersatz fiel im Voraus die Wahl auf Java Enterprise Edition. Im Zuge der Migration soll nun zusätzlich die IT-Architektur optimiert werden. Ziel ist es auch zukünftig zu den Spitzenzeiten den Kunden einen reibungslosen Bestellvorgang zu ermöglichen.

Der Betrieb des Webshops ist eine zwingende Voraussetzung beim Wechsel auf eine neue Architektur. Dieser hat deshalb in kürzest möglicher Zeit, ohne nennenswerte Downzeit des Angebotes zu erfolgen. Nach einer ausführlichen Testphase des Umbaus mit ausgewählten Kunden und Filialen soll das neue System auf einen Schlag unternehmensweit übernommen werden.

Anstatt die Verwaltungssoftware weiterhin auf Citrix-Servern zu betreiben, soll jeglicher administrative Zugriff auf Bestellabwicklung und Teileverwaltung über das Web-Frontend geschehen. Für die Kunden wird sich am Erscheinungsbild nichts ändern, jedoch müssen die Mitarbeiter auf das neue Verwaltungssystem geschult werden.

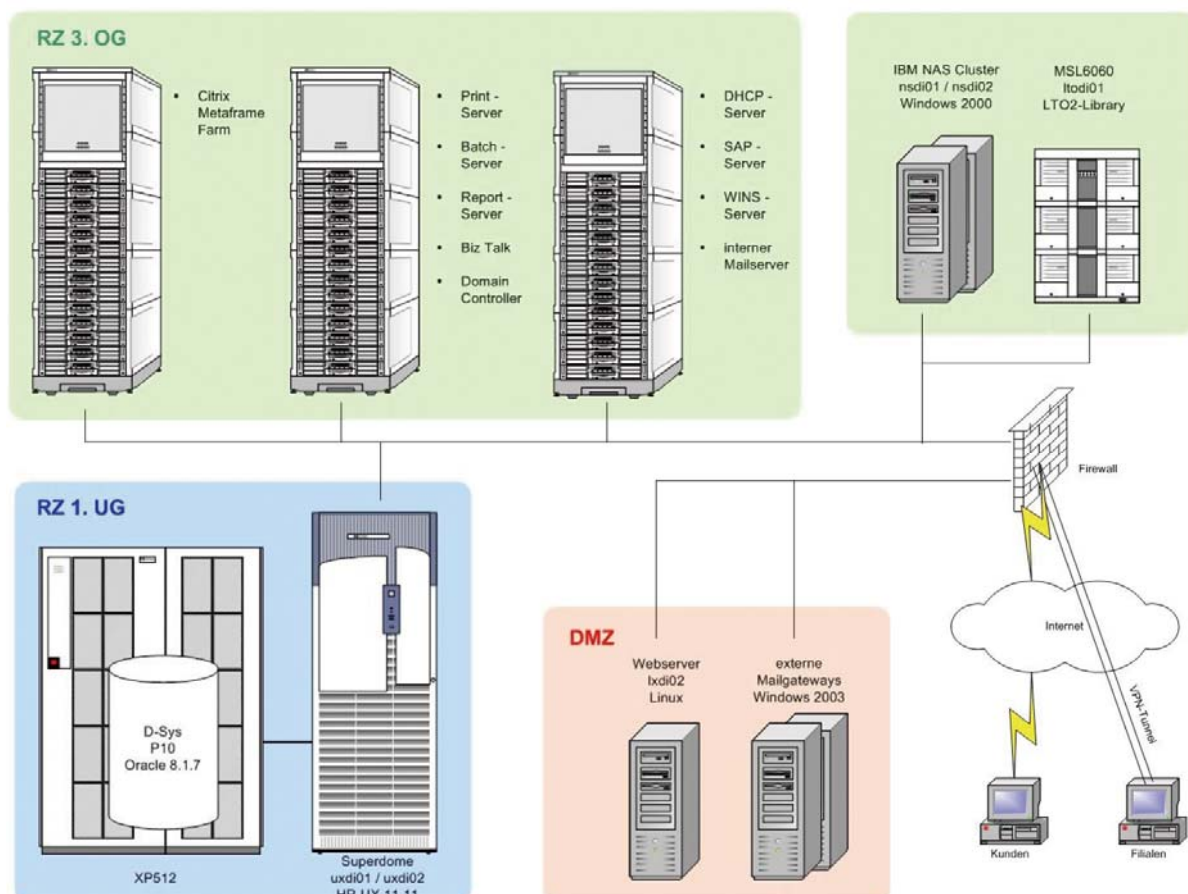
Die aktuelle IT-Umgebung

Die momentan verwendete Architektur genügt den steigenden Anforderungen in mehreren Bereichen nicht mehr. Das vorhandene System verfügt über einen geringen Schutz gegen Angriffe von aussen. Eine einzige Firewall ist für die Trennung zwischen Internet und Intranet zuständig. Der Zugang zur öffentlichen Webseite geschieht über die gleiche Firewall wie der Zugang zu internen Diensten aus dem Intranet heraus.

Dem Rechenzentrum in Dietlikon fehlt die geografische Redundanz, welche auch einen Betrieb bei Strom- oder Netzausfällen längerfristig sicherstellen würde. Derendinger ist auf einen zuverlässigen Betrieb auch in Ausnahmesituation angewiesen und somit vollständig von einer funktionierenden Serverinfrastruktur abhängig.

Auf Applikationsebene werden etwa 600 Oracle Forms für den Zugriff auf die Datenbank eingesetzt. Oracle Forms erschien 1980 und auch wenn die Firma Oracle den Support weiterhin gewährleisten möchte, stellen sie die Weiterentwicklung in näherer Zukunft ein.

Momentan greifen die Filialen und Partner über Citrix-Clients auf die internen Dienste, also vor allem die Oracle Forms, zu.



Nicht funktionale Anforderungen

Die Derendinger-Gruppe bedient mit über 70 Filialen in drei Ländern über 30'000 aktive Kunden. Zusätzlich betreibt sie einen Versandhandel in Deutschland. Im Sortiment werden 200'000 Artikel verwaltet, inklusive dem Wissen, zu welchen Fahrzeugen sie passen, wie sie eingebaut werden und ihre technischen Datenblätter. Zusammen mit Partnern werden weitere Dienstleistungen rund um Fahrzeugbau und -handel angeboten. Auch bei wachsendem Markt sollen wie bisher 96 Prozent der Aufträge innerhalb von 3 Stunden abgewickelt werden können.

Die meisten Bestellungen gehen zwischen 7 bis 14 Uhr ein. Zu diesen Zeiten hat das System hochverfügbar zu sein und der Kunde soll keinen Unterschied im Bestellvorgang zwischen den Hochlaststunden und Randzeiten spüren.

Verantwortlichkeiten

Systemzugriffe

Das IT-Personal des jeweiligen Rechenzentrums hat physischen Zugang zu den Serverräumen. Andere Firmenangestellte, sowie Externe können die Räumlichkeiten nur in Begleitung von IT-Mitarbeitern betreten. Jeglicher Zutritt wird auf einer Liste dokumentiert.

Fernzugriff, d.h. Root-Zugriff auf die Server, hat das IT-Kader und spezielle Zugriffe, je nach Funktion, die einzelnen IT-Mitarbeiter sowie ihre Vertreter.

Die Filialen sollen weiterhin über VPN mit dem Netzwerk verbunden sein und Authentifizieren sich mit ihren persönlichen Login-Daten am System.

HelpDesk und Support

Der Support muss 24/7 in kürzester Zeit Vorort gewährleistet sein. Da das Hauptgeschäft in den Morgenstunden abgewickelt wird, muss auch nachts der Support für die kritischen Systeme sichergestellt sein. Die IT-Abteilungen der Standorte verfügen über einen Bereitschaftsdienstplan mit an die Situation angepassten Erreichbarkeitsdaten.

Infrastruktur

Monitoring

IBM Tivoli Monitoring wird zur Überwachung der Webserver, Netzwerkkomponenten und der Datenbank, sowie der einzelnen Dienste eingesetzt. Falls auch Windows-Systeme benutzt werden, ist eine Überwachungslösung mit Microsoft System Center Operations Manager sinnvoll, um möglichst alle Dienste und alle Hardware von zentraler Stelle überwachen zu können. Es ist sicherlich auch ein Managementpack von IBM wie auch von HP vorhanden, um die Überwachung dieser Systeme auch einzubinden.

Storage

Eine dynamisch erweiterbare und redundante NAS-Lösung soll sowohl den ansteigenden anfallenden Datenmengen gerecht werden, wie auch einen punktuellen Ausfall verkraften könne, ohne dass der laufende Betrieb gestört wird.

Backup/Recovery

Ein inkrementelles Backup wird häufig mit TSM Tivoli Backup Tool erstellt. Die komplette Datenbank soll mindestens 100 Kilometer weit entfernt gesichert werden. Das Backup darf sich nicht in Fluss-/Seenähe, auf der gleichen Verwerfung, Überschwemmungsgebietes des gleichen Stausees oder am Fuss des gleichen Hügel/Berges der beiden Rechenzentren befinden.

Regelmässige Komplettbackups werden auf Tapes erstellt und in einem feuerfesten Safe aufbewahrt.

Netzwerk

Gigabit-Lan wird zwischen den einzelnen Server und HUBS eingesetzt. Switches und Router sollen über 10 Gigabit-Interfaces verfügen. Überwacht wird mit Hilfe von SNMP und anderen von der Hardware unterstützten Möglichkeiten.

Der Backbone zwischen den Switches und Routern ist nicht linear, sondern mit Zyklen aufgebaut, um bei Ausfall eines Switches oder Routers die negativen Folgen zu minimieren.

Verfügbarkeit

Die Bestellseiten sollen zu den Geschäftszeiten über 99,9% verfügbar sein. Pönalen werden mit den verantwortlichen Unternehmen verhandelt (Netzwerk, Server, Software usw.), um die Verluste bei Ausfall abzudecken.

Im Minimum wöchentliche Wartungsslots von wenigen Stunden werden aus der SLA ausgenommen. Diese finden in der Nacht statt und werden auf der Bestellwebseite kommuniziert, sollten beide Rechenzentren davon betroffen sein.

Bei einem kritischen Ausfall der Webserver wird über ein Drittsystem auf Bestellmöglichkeiten per Telefon oder Fax aufmerksam gemacht.

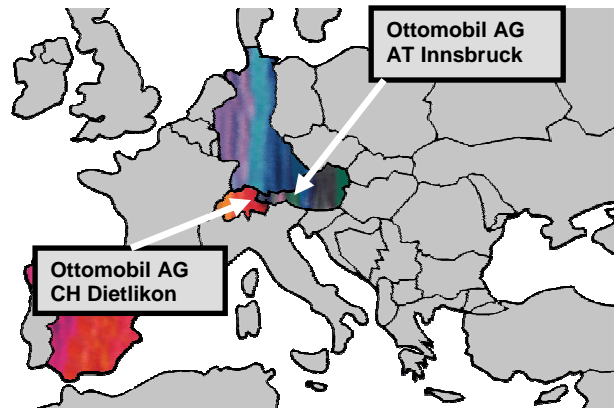
Performance

Auch zu Peakzeiten soll die Ladezeit einer Webanfrage sehr kurz sein, da die Bestellung als Wizzard durchgeführt wird und entsprechend rund ein halb Dutzend Anfragen bis zur Bestellung anfallen.

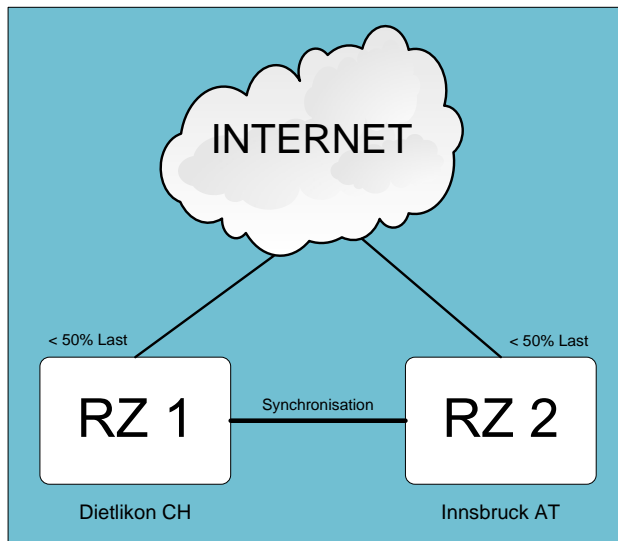
Die Last wird auf die beiden Rechenzentren verteilt. Die Performance wird regelmässig getestet und gespeichert. Wird die Performancegrenze erreicht müssen die entsprechenden Serveranlagen erweitert werden können, was eine gewisse Skalierbarkeit voraussetzt.

Die zukünftige IT-Umgebung

Für die Lastverteilung und Redundanz wird eine Kopie des Rechenzentrums Dietlikon ins Innsbruck (Österreich) aufgebaut. Damit können mehrere Schwachstellen auf einen Schlag behoben werden. Jedes der beiden Rechenzentren darf zu zur Peakzeit nicht über 50% ausgelastet sein. Damit kann der Ausfall eines Rechenzentrums komplett verkraftet werden, indem die gesamte Last vom verbleibenden übernommen wird.



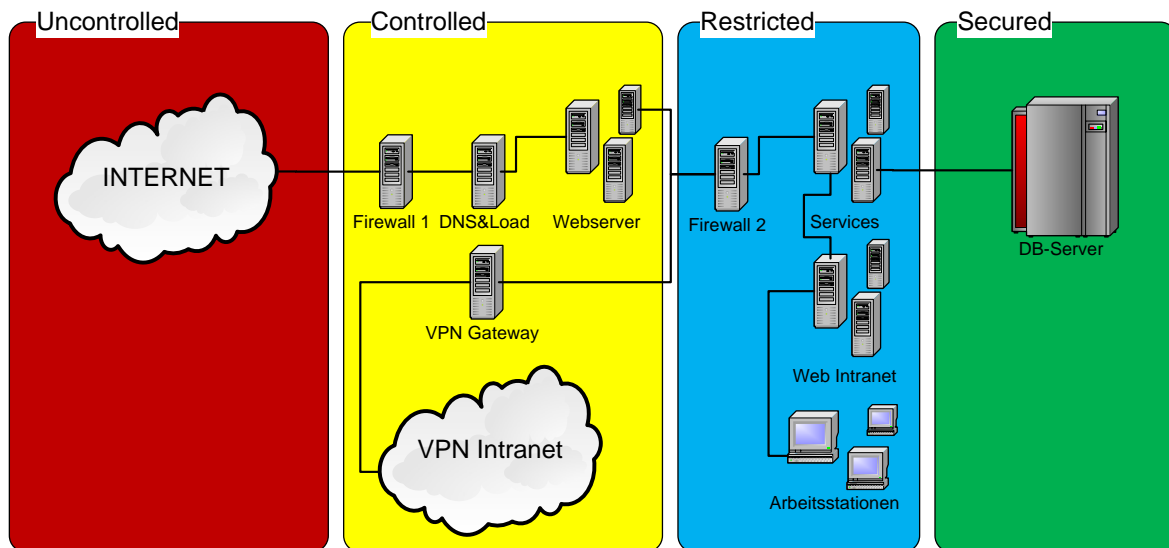
Die gesamten anfallenden Daten werden zwischen den Rechenzentren synchronisiert.



Dazu steht eine Standleitung zwischen Innsbruck und Dietlikon zur Verfügung. Falls die Synchronisation nicht mehr möglich ist wird ein Rechenzentrum vom Netz genommen und vom verbleibenden getragen. Die laufenden Sessions werden wenn möglich übers Internet ans Aktive übertragen, mit dem Ziel, dass der Kunde keinen Unterbruch im Bestellvorgang mitkriegt. Sobald die Standleitung wieder zur Verfügung steht wird das System synchronisiert und zum Normalzustand zurückgekehrt.

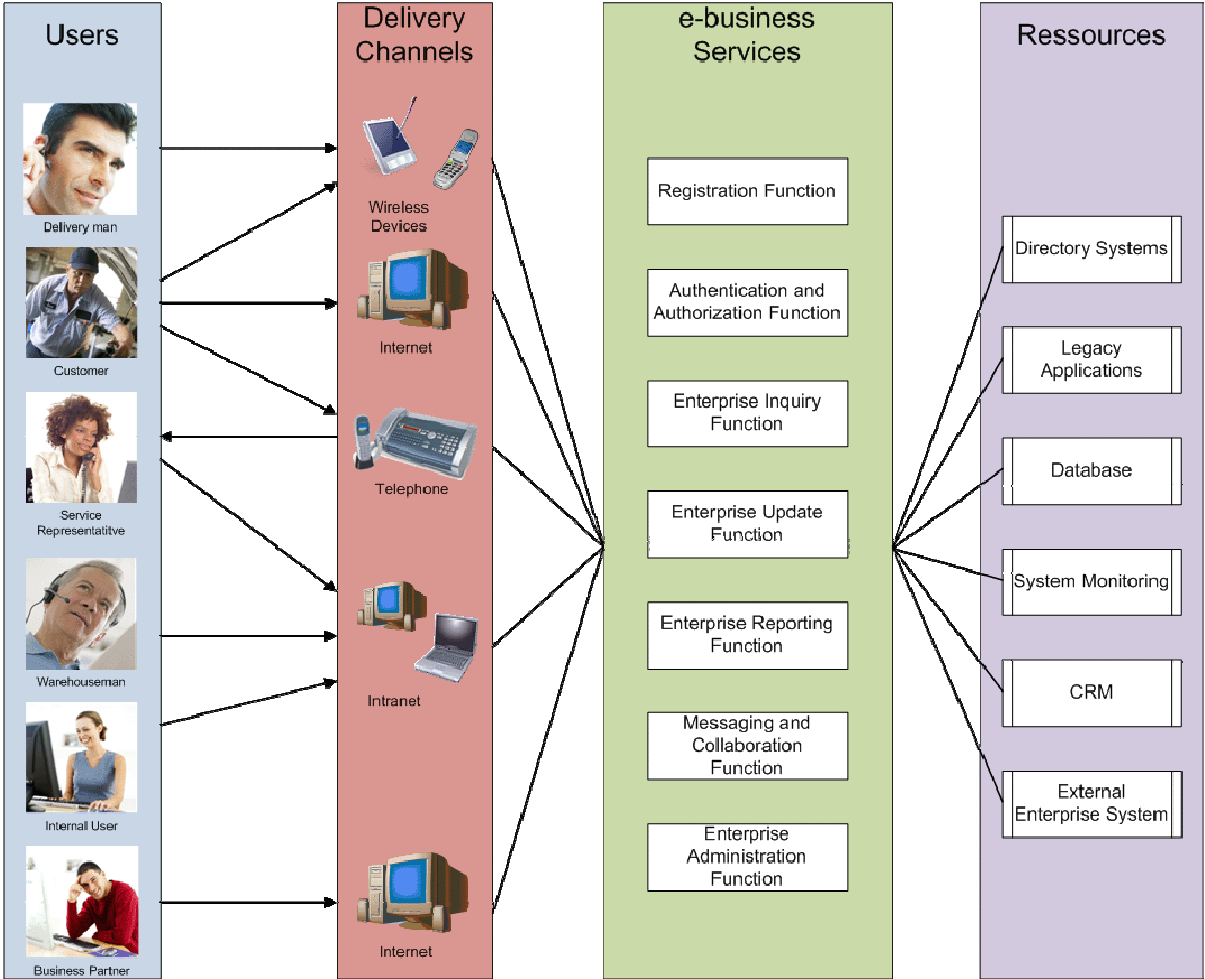
Ein Dispatcher regelt die Lastverteilung zwischen den Rechenzentren. Für die Zuweisung ist die Auslastung der einzelnen Rechenzentren, so wie der Herkunftsort der Anfrage ausschlaggebend. Der Dispatcher holt sich die Auslastung von den Monitoringservern der Rechenzentren. Folglich haben diese Dienste hochverfügbar zu sein. Sie stehen in beiden Rechenzentren zur Verfügung, auch wenn nur einer aktiv ist. Sie kontrollieren sich gegenseitig mit Heartbeat um gegebenenfalls die DNS-Server anpassen zu können, wie auch die Synchronisation auszusetzen, je nach dem welche Dienste im Rechenzentrum des ausgefallenen Dispatchers noch zur Verfügung stehen. Die DNS-Server sind bzgl. Primary und Secondary DNS auf die Rechenzentren verteilt. Alle Dienste laufen auf virtuellen Servern auf Bladesystemen um die notwendige Redundanz und Verfügbarkeit gewährleisten zu können. Beim Ausfall einzelner Basisservern kann die Hardware ohne Betriebsunterbruch manuell ausgewechselt werden.

Die Serverarchitektur wird um eine weitere Firewall erweitert, die zwischen externen Zugriffen auf die öffentlichen Webserver in der DMZ und den internen auf die internen Webserver mit erweiterter Funktionalität unterscheidet. Diese Architektur erhöht die Sicherheit des Intranets beträchtlich, da eine eigene Firewall für das Intranet zuständig ist und diese nicht mit der DMZ geteilt wird. Über das VPN Intranet wird aber genauso, wie über die internen Arbeitsstationen an den zwei Standorten Dietlikon und Innsbruck, der direkte Zugriff auf das Web Intranet ermöglicht. Mitarbeiter in den Filialen greifen so auf die Dienste zu.



Neu sollen die Mitarbeiter nicht mehr direkt über die Oracle-Forms auf den Citrix-Servern ihre Arbeiten an Bestellungen und der Datenbank vornehmen. Die Funktionalität der Oracle-Forms soll in die Web-Applikation integriert werden. Um dies zu bewerkstelligen werden die ca. 600 Oracle-Forms mit JDeveloper auf eine Webapplikation umgeschrieben.

Für die Administration stehen eigene Webserver in der Restricted Zone zur Verfügung. Diese sind unabhängig von den Webservern in der DMZ, auf welche die Kunden zugreifen. Die Applikationsserver bieten den Webservern in der DMZ nur die Bestellmöglichkeiten und Profilverwaltung der Kunden zur Verfügung. Administrationsdienste werden nur den Webservern im Intranet angeboten.



Wechsel von IST zu SOLL

Es wird sofort mit dem Bau des neuen Rechenzentrums bei der Filiale Innsbruck begonnen. Für Innsbruck wird anstatt eines neuen Superdome Datenbankservers direkt ein zeitgemässer Server der IBM pSerie für die gleiche Funktionalität angeschafft.

Die Oracle-Forms werden in einem Schwung auf Java umgeschrieben, damit die Umstellung einerseits zügig vorangebracht werden muss, und andererseits nicht ewig die Altlasten mitgeschleppt werden. Nach Möglichkeit wird diese Arbeit nach China oder Indien gegeben, sollte dies nicht möglich sein werden freie Programmierer angestellt, die während ca. 4 Monaten die 600 Forms umschreiben.

Nach einer ausführlichen internen Testphase der JDeveloper Forms werden sie einem Produktionstest mit ausgewählten Filialen und Kunden ausgesetzt, parallel zur Legacy Applikation.

Während der Umstellungsphase wird erst das eine Rechenzentrum umgestellt, während das andere als Backuplösung fungiert. Treten keine Komplikationen auf wird auch das verbleibende Rechenzentrum auf das neue System umgeschaltet.

Zusammenfassung

Aufgrund des Wachstums von Derendinger ist ein Ausbau der IT-Infrastruktur sowohl im Hardware- wie auch im Softwarebereich unabdingbar. Die neue IT-Infrastruktur muss vor allem eine sehr hohe Verfügbarkeit sicherstellen. Zudem müssen mittelfristig die alten Anwendungen, welche auf Oracle Forms basieren, durch Java Applikationen ersetzt werden.

Die IT-Architektur ist für Derendinger missionskritisch. Deshalb soll nicht an finanziellen Mitteln gespart werden. Die hohe Verfügbarkeit wird durch ein zweites RZ sichergestellt, wobei nur eines davon die Gesamtlast auch zu Spitzenzeiten tragen könnte. Für die Kunden wird sich optisch nichts ändern, bloss von den Filialen aus wird der Zugang neu mithilfe VPN über eine Webfront hergestellt.

Die Umstellung erfolgt in einem Schritt, um unsere IT-Infrastruktur schnell an die neuen Anforderungen anpassen zu können.