Konzept Cloud-Technologie winMedio

1. Vorwort

Predata AG betreibt die für die eigenen Cloud-Dienste (auch SaaS - Software as a Service genannt) eigene Server in einem externen Rechenzentrum (Co-Locating). Betreiber des Rechenzentrums ist die Firma nts Workspace ag, Bern

Bei der Konzeption der Architektur standen immer folgende Eigenschaften im Vordergrund:
- Verfügbarkeit
- Zuverlässigkeit
- Sicherheit

1.1. swiss hosting

swiss hosting

«swiss hosting» steht für zwei Versprechen:
1. Die Daten bleiben in der Schweiz
2. Der Zugang zu diesen Daten ist für Dritte nur via Schweizer Behörden möglich

Quelle: swissmadesoftware.org

Für die Wartung und den Unterhalt der Infrastruktur wird Predata AG durch folgende Firma unterstützt:
smart dynamic ag
Burgstrasse 4
3600 Thun
www.smartdynamic.ch

1.2. Verfügbarkeit

Die Verfügbarkeit wird wie folgt sichergestellt:
- Architektur der Server (RAID, redundante Power Supply, Prozessor, usw.).
- Ausfallsicherheit durch redundante Netzwerkkomponenten.
- Daten werden auf mehrere Server gespiegelt.
- Unterschiedliche Stromkreise für die Server.
- Redundanter Internet-Zugang.
- Überbrückung von Stromausfällen mittels Batterien und Diesel-Aggregat.

1.3. Zuverlässigkeit

Die Server sind so konzipiert, dass sowohl geplante Wartungsarbeiten (z.B. für Installation von Patches und Security-Updates oder Ersatz von einzelnen Servern) wie auch ungeplante Systemausfälle überbrückt werden können. Ein Load-Balancing sorgt zudem dafür, dass die verfügbaren Server gleichmässig und optimal ausgelastet sind.

Die Serverinfrastruktur wird mit effizienten Tools überwacht. Bei Unregelmässigkeiten (bevorstehender Ausfall von Festplatten, Leistungsabfall, Serverausfall, ungewöhnliche Netzwerklast, usw.) wird eine entsprechende Alarmierung ausgelöst (SMS und Email).

1.4. Sicherheit

Für ein Höchstmass an Sicherheit ist der Zugang zum Rechenzentrum nur für berechtigte Personen über Badge bzw. Fingerprint und PIN möglich. Die einzelnen Racks sind zudem mit Schlüsseln individuell gesichert. Das nts Rechenzentrum ist mit modernen Feuer- und Rauchmeldern ausgerüstet.

2. Datensicherung

Jede Nacht erfolgt ein Full-Backup der Kundendatenbanken. Die erzeugten Backupdateien sind verschlüsselt und können ohne passenden Schlüssel nicht wiederhergestellt werden. Die erstellten Backups werden auf einem netzwerkgetrennten und passwortgeschützten WORM(*)-Laufwerk im Rechenzentrum gespeichert. Ausserdem wird zusätzlich eine Kopie der Datensicherung auf ein NAS (WORM(*), RAID 1) am Standort von Predata AG übertragen (geografische Trennung).

(*)*WORM: Write Once Read Many = Hardware-Schreibgeschützt*

2.1. Datenaufbewahrung und Archivierung

Predata AG bewahrt standardmässig folgende Backup-Generationen auf:

Im RZ Bern	Auf NAS in Thun
Tägliche Backups: Letzte zehn Tage.	Tägliche Backups: Letzte zehn Tage. Wöchentliche Backups: Letzte sieben Wochen (Stand jeweils Sonntag)

Predata AG bietet die Einrichtung einer auf Kundenwunsch abgestimmten Archivierung an.

2.2. Datenverlustzeit und Wiederherstellung

Die Wiederherstellung ab Datenbanksicherung erfolgt innerhalb von 4 Std. (offizielle Öffnungszeiten Predata AG).

Die maximale Datenverlustzeit beträgt 24 Std.

2.3. Besondere Vorkehrungen

Falls es zu Support-Zwecken erforderlich ist, kann Predata AG die Datenbank des Kunden auf der Predata-eigenen Infrastruktur wiederherstellen. In diesem Fall werden die Benutzerdaten anonymisiert, so dass kein Rückschluss auf echte Personen mehr möglich ist.

Alle Mitarbeiter:innen von Predata AG sind über die Anstellungsdauer hinaus vertraglich zur absoluten Verschwiegenheit, hinsichtlich Tatsachen, Verfahren, Konzepten, Unterlagen und allen betrieblich relevanten Themen mit welchen sie während ihrer Arbeit in Berührung kommen, verpflichtet.

3. Notfallsituationen

Risiken, welche zu Notfallsituationen führen könnten, werden laufend beurteilt und beim Aufsetzen und Erweitern der Serverarchitektur berücksichtigt. So sind die Server und die Switches inkl. Firewall redundant ausgelegt und für eine verbesserte Performance mit Load Balancing-Mechanismen ausgestattet. Ausserdem werden alle Server regelmässig (min. monatlich) gewartet und mit den aktuellsten Sicherheitspatches aktualisiert. Für eine Unterbruchsfreie Wartung werden die Server einzeln und nacheinander gewartet. Damit wird auch der Ausfall eines Servers simuliert.

Allen Massnahmen zum Trotz ist es möglich, dass die Server nicht erreichbar sind. So kann ein Ausfall der Netzwerk- oder Internet-Infrastuktur kundenseitig zu einer Notfallsituation führen.

3.1. Notausleihe

Für die Überbrückung von Verbindungsausfällen mit der Datenbank wird kundenseitig ein oder mehrere PCs für die Notausleihe konfiguriert. Dafür wird bei jedem Start von winMedio ein Snapshot der wichtigsten Tabellen der Datenbank auf die lokale Festplatte gespeichert (Benutzer, offene Ausleihen und Reservationen).

Die Notausleihe wird automatisch gestartet, wenn winMedio keine Verbindung zur Datenbank herstellen kann. Die Notausleihe erlaubt die Ausführung der wichtigsten Arbeiten (Ausleihen und Rücknahmen) an der Theke im Falle eines Wegfalls der Verbindung mit der Datenbank. Die aktuellen Snapshots der Datenbank ermöglichen eine benutzerfreundliche Verarbeitung durch die Anwender.

Sobald die Verbindung zur Datenbank wieder hergestellt werden kann, werden die mit der Notausleihe registrierten Transaktionen automatisch in die Datenbank übertragen.

4. Detailangaben zum Anbieter des externen Betriebes

Predata AG betreibt die eigenen Server in Form eines Housings bei

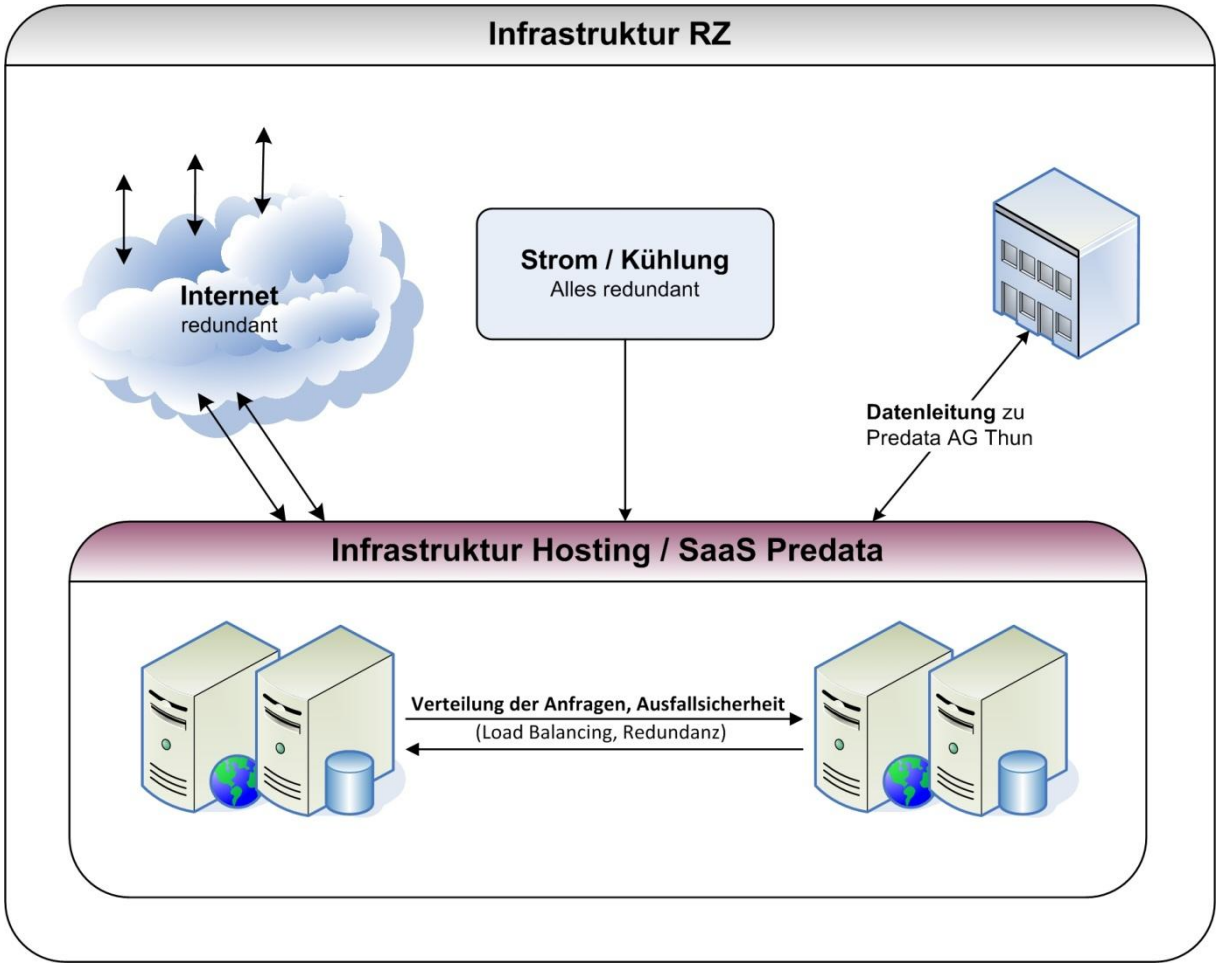
nts workspace AG
Wölflistrasse 1d
3006 Bern
www.nts.ch
www.colobern.ch

5. Schematische Darstellung der Architektur

Bei den Servern handelt es sich um physisch getrennte Hardware. Jeder Server ist grundsätzlich autonom, wobei die Datenbank- und die Webserver untereinander über Load Balancing-Mechanismen verbunden sind.

Jeder Kunde verfügt über eine eigene unabhängige Datenbank. Diese ist auf allen Datenbankservern abgelegt und wird in Echtzeit synchronisiert. Damit wird auch beim Ausfall eines Servers eine unterbruchsfreie Verfügbarkeit sichergestellt.

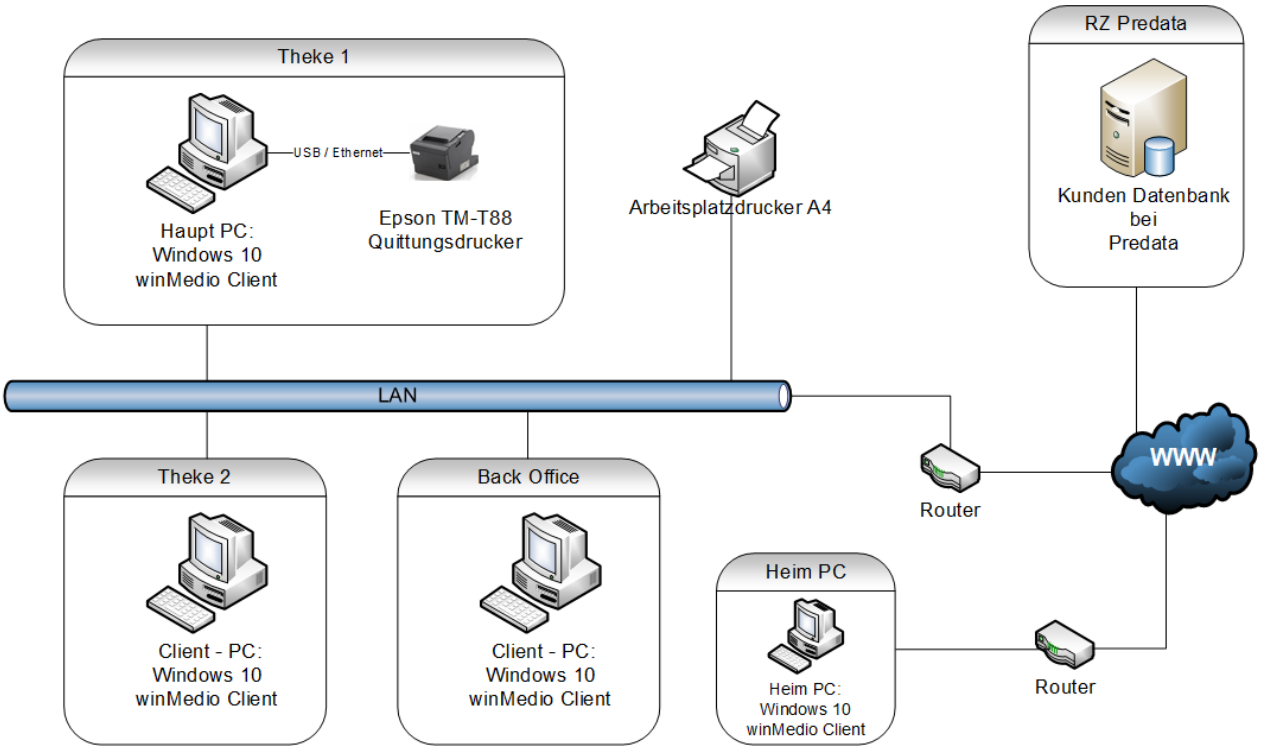
Für den Online-Katalog webOpac wird auf den Webservern für jeden Kunden ein ElasticSearch-Index angelegt, welcher die Daten der SQL-Datenbank beinhaltet. Die Aktualisierung des ElasticSearch-Index erfolgt jeweils in Echtzeit.



6. Übersicht über die konzeptionelle Anbindung der Kunden

Die folgende Darstellung zeigt, wie die Infrastruktur des Kunden beim externen Betrieb an das RZ von Predata angebunden wird.

Für die Kommunikation mit dem RZ wird ein Internet-Zugang (Port 80) benötigt.



7. Schematische Darstellung des Verschlüsselungsverfahrens

Die Kommunikation zwischen dem Client und der Datenbank wird verschlüsselt und komprimiert.

1. *winMedio.net hat ein „Zertifikat" integriert*

2. *Der Client erstellt einen Random-Key (Session Key)*
3. *Der Session Key wird mit einem Public Key verschlüsselt*
   Asymmetrische Public/Private Key Verschlüsselung: 384 Bit RSA

4. *Der neue Session-Key wird zum Server gesandt*

5. *Der Server entschlüsselt den Session Key mit dem nur bei Predata AG bekannten Private Key. Jetzt haben Client und Server den gleichen Session Key*

6. *Die Kommunikation erfolgt mit dem neuen Session Key*
   Symmetrischer Session Key: 256 Bit AES oder Rijndael