

AN DIE KUNDEN

Einkauf | IT | Web-Projektleiter

Kontakt: Alain Martinet
Direktwahl: +41 (0) 34 423 00 08

Kurzbeschreibung für:

- **High-Availability Hosting für Corporate Websites**
- **Hosting von Applikationen mit personenbezogenen Daten**

Inhalt der Dokumentation

- 1) Zweck der Dokumentation
- 2) Rechenzentrum und IT-Architektur
- 3) Datenschutz / Virenschutz
- 4) Notfallszenario
- 5) Backup-Konzept
- 6) Pikettdienst (auch für Publizierung von Geschäftszahlen)

1) Zweck der Dokumentation

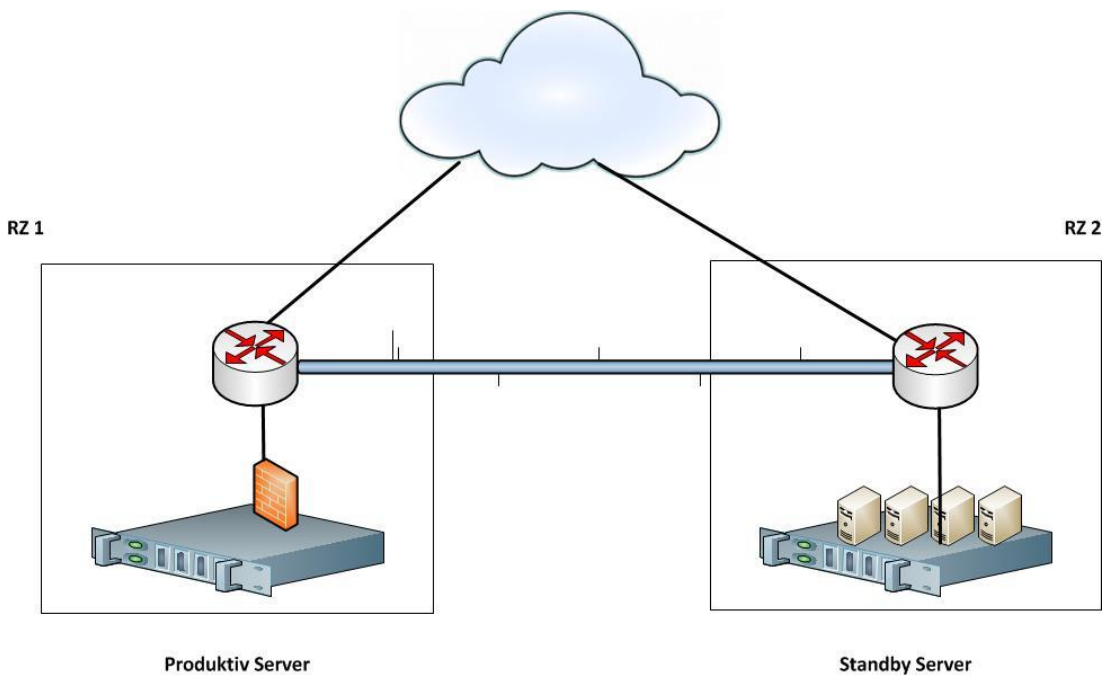
Die Dokumentation vermittelt Informationen zu Prozessen und Massnahmen in Bezug auf die Verfügbarkeit, die Datensicherheit und den Datenschutz bei webstyle.

Sie umschreibt allgemein gültige Bestimmungen, an denen webstyle sich beim Hosting von Daten der erwähnten Kategorie hält. Spezifikationen sind jeweils in den einzelnen Kundenverträgen für das Outsourcing enthalten.

2) Rechenzentrum und IT-Architektur

Standorte der Rechenzentren: Bern | Düringen b. Fribourg (alle in der Schweiz)
Standard Rechenzentren: Tier-3

Schematische und vereinfachte Darstellung der Server einer typischen HA-Hosting Lösung. Die einzelnen Lösungen werden nach Vereinbarung umgesetzt.



Die Rechenzentren sind mit GBit Uplinks an verschiedene Carrier angebunden. Zur Ausrüstung der Rechenzentren gehören:

- Zutrittskontrolle, Sicherheitsschleusen, Kameraüberwachung
- USV, zwei Stromkreise und Dieselgeneratoren (redundant)
- Uplinks mit Cablecom, GroupeE, Swisscom

Hardware

webstyle setzt bei den Servern durchwegs auf die Server der Marke HP.

Eigentumsverhältnisse

Die Rechenzentren sind im Eigentum von Schweizern Colocation-Anbietern (NTS, Senselan)
Alle Server sind im Eigentum der webstyle GmbH. Dazu gehört auch ein eigenes Ersatzteillager.

3) Unsere Grundlagen zum Datenschutz

Zur Sicherstellung des Datenschutzes gelten folgende personalbezogenen- und infrastrukturbezogenen- und Regelungen.

- Alle involvierten Mitarbeiter haben die Rechtsvorschriften zum Bankgeheimnis und Insidergeschäft als Bestandteil des Arbeitsvertrages unterzeichnet.
- Abgestuftes Konzept für den Zugriff auf Systemkennwörter, in der Kompetenz des CEO.
- Einhaltung des Standards gem. Eidg. Banken Kommission Richtlinien 99/2 (CH)
- Einhaltung der Allgemeinen IT Geschäftsbedingungen der Post für die Wartung von Hard- und die Pflege von Software
- Virenschutz: Vulnerability-Scan (Überwachung der Websites auf Hackerangriffe)
- Jährlich mehrere Pentests durch zwei Grossbanken
- Restriktive Beschränkung der physikalischen Zugriffe auf die Server. Betrieb in Rechenzentrum nach Tier3 Standard.
- Arbeitsabläufe in Anlehnung/Übereinstimmung mit ISO27001 (die Zertifizierung wird angestrebt)
- Wartung der Server nach der internen webstyle Server Security Policy [wssp 05/12-1]

Die Aufzählung ist nicht abschliessend. Dazu zählen auch kundenspezifische Massnahmen in Bezug auf die Archivierung von Logfiles.

4) Notfallszenario

Der Ablauf bei ungeplanten Unterbrüchen oder Notfällen in Folge von höheren Gewalten ist bei webstyle wie folgt geregelt:

1. Eingang der Meldung durch automatische Benachrichtigung (Monitoring) oder Kunden.
2. Aufgebot von kompetentem Personal zur Behebung der Störung sowie im Bedarfsfall Aufgebot von involvierten Dienstleistern (z.B. Rechenzentrum-Betreiberin).
3. Intervention gemäss Service-Vertrag. Im Bedarfsfall erfolgt der Wechsel auf den "Standby" Server.
4. Dokumentation, Rückmeldung des Technikers an Kunde und an die webstyle Geschäftsleitung.
5. Einleitung weiterer Massnahmen zur Wiederherstellung des optimalen Zustands. Bei Bedarf Besprechung von notwendigen Optimierungen.

5) Backup-Konzept

Umschreibung eines Standard-Konzeptes wie es in der Regel bei Webservern zur Anwendung kommt.

- Lokal, auf demselben physikalischen Server: RAID 0, separate Festplatte
tägliche, wöchentliche und monatliche Backups, je nach Vereinbarung mit dem Kunden.
Hauptzweck dieser Datensicherung: rasche Wiederherstellung auch älterer Entwicklungsstände.
- Örtlich getrennt auf separatem Standby-Server: Tagesaktuelle Spiegelung von System,
Konfigurationen und Daten, so dass beim Ausfall des produktiven Servers eine raschere
Inbetriebnahme möglich ist. Dies geht weiter als eine simple örtlich getrennte Datensicherung und
dient der Hochverfügbarkeit.

6) Pikettdienst, Bereitschaftsdienst bei Publizierung Halbjahresabschluss

Sofern vertraglich vereinbart ist der Pikettdienst rund um die Uhr und jeden Tag erreichbar. Details dazu werden in einem Service-Vertrag beschrieben. Hierbei wird in der Regel eine Reaktionszeit von 2 Stunden sowie eine Interventionszeit von plus 4 Stunden vereinbart. Während den Betriebszeiten gilt die verkürzte Reaktionszeit von 30 Minuten.

Die Infrastruktur, Systeme und Dienste auf den Systemen werden überwacht (aktives Monitoring). Ausfälle führen in jedem Fall auch ohne Kundenmeldung zu einem Einsatz.

Für börsenkotierte Unternehmen bietet webstyle in Verbindung mit der Publizierung der Geschäftszahlen einen erhöhten Bereitschaftsdienst. webstyle stellt eine umgehende Reaktion und die Intervention innerhalb von maximal 30 Minuten sicher.