colada group GmbH
Mühlenstrasse 26
CH – 8200 Schaffhausen

Anlage 2 zum Vertrag „Datenschutz und Datensicherheit“:

Organisation Datensicherheit

colada stellt sicher, dass Daten und Informationen, die in colada verarbeitet werden zu jedem Zeitpunkt sicher sind. Sicherheit hat bei colada einen sehr hohen Stellenwert, weshalb wir ein Sicherheitskonzept auf allen Stufen einsetzen.

Die Eckpfeiler unseres Sicherheitskonzeptes sind:
- Hochqualifizierte Mitarbeiter mit langjähriger Erfahrung im Security, Database und Application-Umfeld
- Laufende Weiterentwicklung und Erweiterung des Sicherheitskonzeptes
- Grösstmögliche Redundanz aller eingesetzten Systeme

Sicherheit auf allen Stufen:

I. colada corporate security

Physische Sicherheit
Unsere Entwicklungs-Umgebung ist an unserem Hauptsitz in Schaffhausen (Schweiz) untergebracht. An diesem Standort haben wir Sicherheitsmassnahmen für Mitarbeiter und Technik realisiert. Diese Systeme werden laufend überprüft und optimiert.
Dieser Schutz umfasst:
- Schutz vor Hochwasser und Feuer
- Schutz vor fremdem Zugriff
- Schutz vor Stromunterbrüchen und Spannungsschwankungen
- Sicherstellung der Verbindung ins Internet

Interne Sicherheit
Unsere Entwicklungsumgebung umfasst Firewalls, Intrusion Detection Systeme, SSL-Verschlüsselung und andere, durch uns selbst entwickelte Sicherheit-Mechanismen.

II. Sichere Rechenzentren

Zusammenarbeit mit zertifizierten Rechenzentren
Durch die Zusammenarbeit mit zertifizierten Rechenzentren bieten wir ein Höchstmass an Service-Qualität und Verfügbarkeit.

Datensicherheit / Backup
Ihre Daten sind bei uns sicher. Sollten Sie doch einmal Ihre Daten verlieren oder löschen, so haben wir mit unserem Backup und Recovery-System vorgesorgt. Unser transaktionsbasiertes Datenbanksystem ermöglicht uns jede Aktion das aktuellen Tages rückgängig zu machen.

Application Security
Das Datenmodell von colada stellt sicher, dass jeder Kunde nur seine eigenen Daten und nicht auch die Daten anderer Kunden einsehen kann. Dieses Modell wird während der gesamten Dauer einer Session mit jeder Server-Anfrage neu überprüft. Zusätzlich hat jeder Kunde seine eigene, physisch getrennte Datenbank.

OS Security / Antivirus
Unsere Hardware befindet sich zu jedem Zeitpunkt auf dem vom Hersteller empfohlenen Patchlevel. Zusätzlich sorgen Antiviren-, IDS und externe Überwachungsprogramme für einen umfassenden Schutz.

Database Security
Der Zugriff auf die Datenbank in colada findet immer über das Framework statt und ist auf eine möglichst geringe Zahl von Access-Points limitiert. Entwicklungs- und Produktiv-Systeme sind vollkommen voneinander getrennt und haben auch keine gemeinsame Passwort-Datenbank.

III. Internet-Sicherheit

Datentransport via SSL
Datenverkehr vollständig SSL-verschlüsselt.

Netzwerk Sicherheit
Durch die redundante Anbindung an nationale und internationale Internet Service Provider garantieren wir eine hohe Verfügbarkeit und kurze Zugriffszeiten

Firewalls
Alle Server befinden sich hinter Firewalls, die den höchsten Ansprüchen genügen. Zusätzlich wird jeder Zugriff auf unsere Systeme von einem Intrusion-Detection-System überwacht und auffällige Datenpakete automatisch abgeblockt

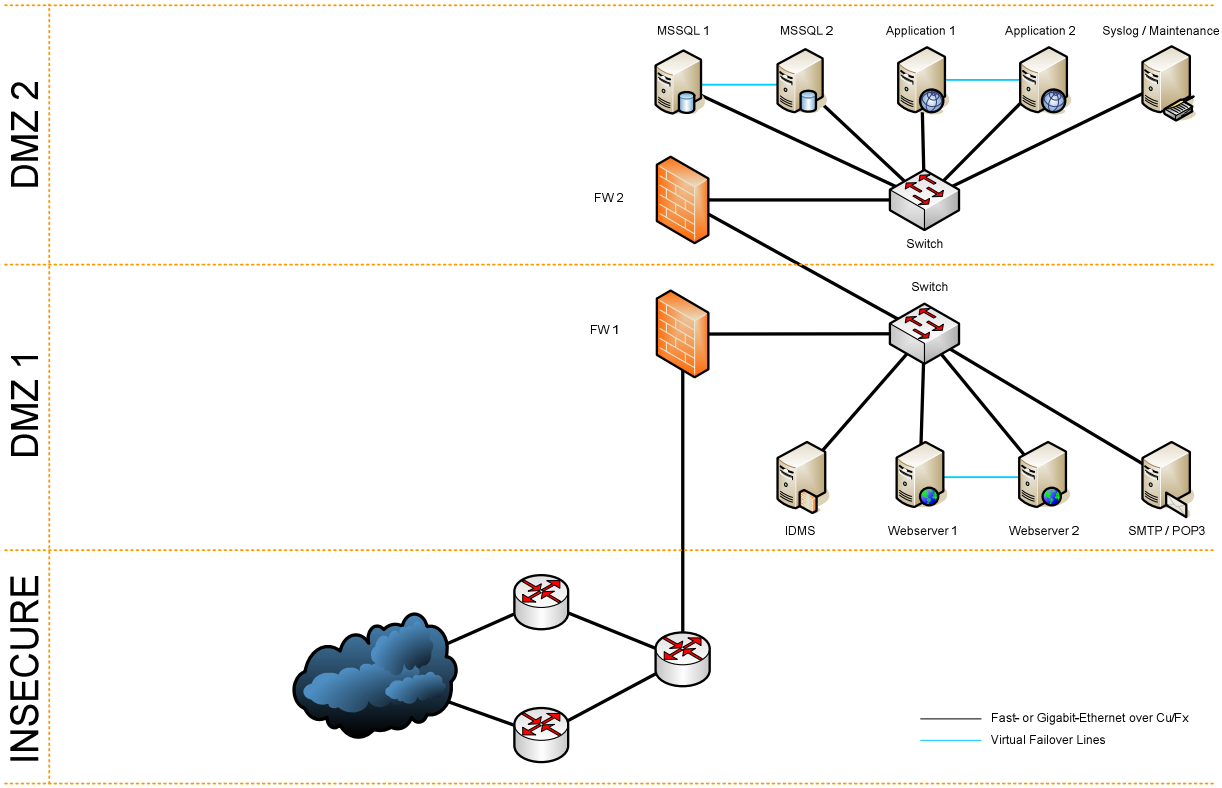
IV. Anwender-Sicherheit

User Authentication
Jeder colada Anwender muss sich in colada authentifizieren. Dies findet in der Regel über Name und Passwort statt. Ein User kann sich nicht mehrmals im System einloggen.

Kundendaten
Alle Daten. die in colada eingegeben und verarbeitet werden gehören vollumfänglich dem jeweiligen Kunden.

colada group GmbH
Mühlenstrasse 26
CH – 8200 Schaffhausen

V. colada Infrastruktur



- Die colada Infrastruktur wird in einem zweistufigen Sicherheitssystem betrieben.
- Dadurch kann eine vollständige Trennung der Datenbank- und Applikationsserver vom unsicheren, öffentlichen Internet gewährleistet werden.
- Restriktive Zugriffsregeln sorgen dafür dass nur autorisierten Systemen der Zugriff gewährt wird.
- Die Remote-Verwaltung der in DMZ 1 platzierten Systeme kann nur von Systemen die über das entsprechende Zertifikat, sowie Benutzern mit gültigem Zertifikat und Passwort erfolgen.
- DMZ 2 Systeme können nur lokal gewartet werden.