SWANcloud

Security Aspekte

SSC-Services GmbH
Herrenberger Straße 56
71034 Böblingen
Deutschland

Dokument: SWANcloud Security Aspekte

Stand: V4_DE_07.08.2014
Autor: SSC-Services GmbH

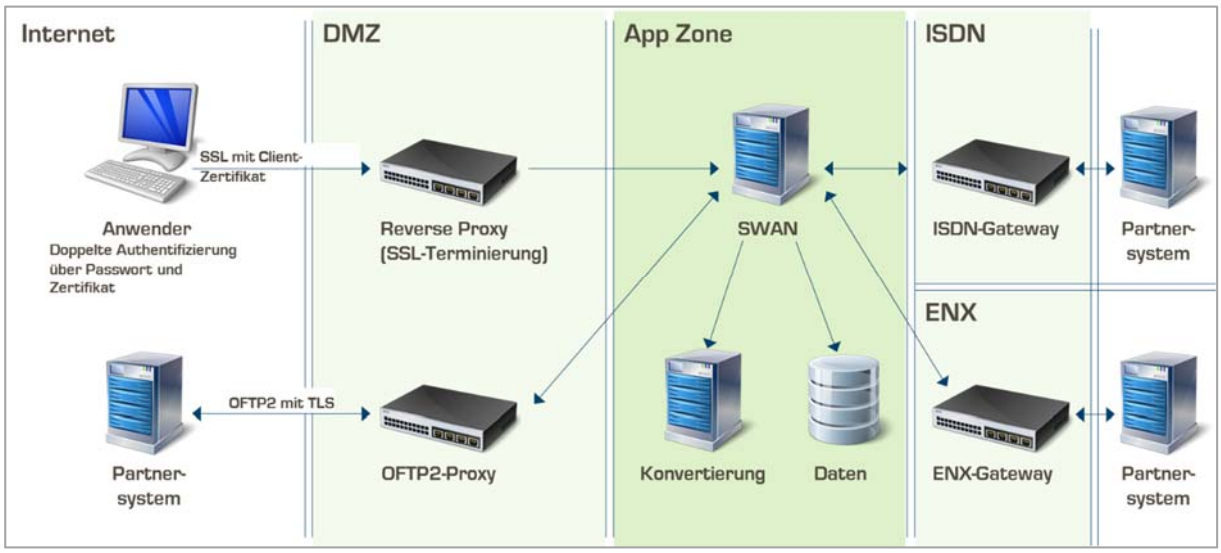
SSC-Services GmbH
Herrenberger Straße 56
71034 Böblingen
Deutschland

Telefon: +49 (0) 70 31/49 13 - 0
Telefax: +49 (0) 70 31/49 13 55
E Mail: kontakt@ssc-services.de
Internet: http://www.ssc-services.de

Geschäftsführer: Matthias Stroezel
Sitz: Böblingen
Registergericht: Stuttgart
HRB-Nr.: 21439

Inhaltsverzeichnis

SWANcloud Security Aspekte



Hosting im SSC-Rechenzentrum

Die gesamte SWANcloud-Infrastruktur wird im SSC-Rechenzentrum (Böblingen, Germany) betrieben. Das Rechenzentrum erfüllt unter anderem die nachfolgenden Kriterien:

» Anbindungsvarianten: Internet (OFTP2, VPN), ENX (OFTP), ISDN

» Redundante Firewall-Systeme

» Redundante Server-Farm (Virtualisierte Server-Umgebung)

» Redundante Stromversorgung

» Mehrstufige Backup-Strategie (Backup-to-disk / Disaster Recovery in ein zweites Rechenzentrum)

» Vorbeugender Brandschutz (Brandschutzwände, Rauchmelder, Gaslöschanlage)

Basis für SWANcloud - Software-as-a-Service-Model (SaaS)

Die Kunden von SWANcloud greifen über das Internet auf die im SSC-Rechenzentrum gehostete SWAN-Installation zu. SWAN ist eine unter Java entwickelte, webbasierte Lösung, welche keine speziellen Software-Anforderungen an die Clients stellt (Internet Explorer oder Firefox, Java Runtime Environment). SWANcloud als SaaS bietet denselben Komfort wie die „Inhouse-Lösung“ SWANenterprise.

Verschlüsselte Kommunikation zwischen Anwender und SWANcloud

Die Kommunikation zwischen dem Anwender und SWANcloud erfolgt über den Web-Browser. Zur Verschlüsselung der Kommunikation wird das HTTPS-Protokoll verwendet. Die HTTPS-

Verschlüsselung besteht aus einem öffentlichen und einem privaten Schlüssel. Der öffentliche Schlüssel ist in SWANcloud hinterlegt, der private Schlüssel wird auf dem Client des SWANcloud-Anwenders hinterlegt.

Beim privaten Schlüssel handelt es sich um ein persönliches SSL-Zertifikat mit einer 2048-Bit-RSA-Verschlüsselung, welches individuell für jeden SWANcloud-Anwender ausgestellt wird. Anonyme Zugriffe sind technisch unterbunden. Somit ist der Zugriff auf SWANcloud ausschließlich über ein gültiges persönliches SSL-Zertifikat möglich.

Leitungsverschlüsselung während der Datenübertragung

Damit die Sicherheit während des Datenübertragungsprozesses gewährleistet werden kann, wird die Leitung zwischen SWANcloud und dem Kommunikationspartner durch standardisierte Verfahren abgesichert. SWANcloud nutzt hierbei die nachfolgenden Leitungsarten:

» ISDN mit OFTP

Bei der Verbindung mittels ISDN handelt es sich um eine direkte Verbindung (1:1) zwischen zwei Kommunikationspartnern. Die elektronische Datenübertragung erfolgt mittels des OFTP-Protokolls. Da es sich in diesem Fall um eine 1:1 Verbindung handelt ist diese Verbindung nicht verschlüsselt.

» ENX mit OFTP

Das ENX-Netzwerk ist ein spezielles Netzwerk für Automobilhersteller und deren Zulieferer. Technisch gesehen handelt es sich hierbei um ein verschlüsseltes VPN-Netzwerk, welches ausschließlich durch zertifizierte Dienstleister der ENX-Association betrieben wird. Die elektronische Datenübertragung erfolgt, wie bei ISDN, mittels des OFTP-Protokolls.

» Internet mit OFTP2

Die Basis für die Datenübertragung über OFTP2 ist ein Standard-Internetanschluss mit einer öffentlichen IP-Adresse. Dies bietet gegenüber dem ENX-Anschluss den Vorteil, dass eine bereits vorhandene Leitung genutzt werden kann. Zudem sind Internet-Anschlüsse in der Regel kostengünstiger als ENX-Anschlüsse. Gegenüber der ISDN-Leitung hat der Internet-Anschluss heutzutage enorme Geschwindigkeitsvorteile. Die elektronische Datenübertragung erfolgt mittels des OFTP2-Protokolls, welches einen TLS-verschlüsselten Kommunikationskanal mit X.509-Zertifikaten nutzt. Während des Datenübertragungsprozesses zwischen SWANcloud und dem Kommunikationspartner via OFTP2 werden die Nutzdaten zusätzlich zur Leitungsverschlüsselung mit X.509-Zertifikaten verschlüsselt.

Mehrstufiges Authentifizierungskonzept

Die Authentifizierung eines Anwenders an SWANcloud erfolgt mittels der zwei Faktoren "individuelles SSL-User-Zertifikat" + "personifizierte Anmeldung mit Benutzername und Passwort". Der Datenzugriff auf die Anwendung SWAN wird anhand eines fein granularen Rechte- und Rollenkonzepts gezielt gesteuert.

Nachvollziehbarkeit der Empfangs- und Versandhistorie

Anhand einer detaillierten Protokollierung in der SWAN-Historie existiert jederzeit ein Überblick über alle versendeten und empfangenen Aufträge.

Serverseitige Protokollierung der einzelnen Prozessschritte

Anhand der Server-Logfiles sind die einzelnen Prozessschritte (Versand, Empfang, Übermittlungsprozess, etc.) des SWAN-Servers durch unser Support-Personal stets nachvollziehbar.

Penetration-Tests zur Überprüfung der Applikationssicherheit

Ein fester Bestandteil der Release-Zyklen des Software-Entwicklungsprozesses ist der sogenannte Penetration-Test (die Sicherheitsüberprüfung).

Ein von uns beauftragter externer Dienstleister übernimmt die Rolle eines potentiellen Angreifers (ugs. "Hacker") und versucht einen unautorisierten Zugriff auf das SWAN-System (die Applikation SWAN oder die Middleware-Komponenten) zu erlangen. Hierzu setzt der externe Dienstleister bekannte Methoden und Tools (Skripte, Software-Pakete) der "Hacker-Szene" sowie sein spezielles IT-Know-how im Bereich der Software-Entwicklung und Netzwerktechnik ein.

Für den Fall, dass es möglich ist über eine dieser Methoden einen unautorisierten Zugriff auf das System zu erlangen, werden diese Sicherheitslücken untersucht und beseitigt. Daraufhin erfolgt ein weiterer Penetration-Test zur Qualitätssicherung.

Update- und Patch-Management

Das zeitnahe Einspielen von sicherheitsrelevanten Updates und Patches ist heutzutage für ein IT-System unerlässlich. Darum werden bei SSC alle Komponenten unseres Rechenzentrums (Firewalls, Betriebssystem, Applikationsserver, Datenbank,...) anhand eines von uns definierten Prozessablaufes regelmäßig überprüft und aktuell gehalten.