Odalis Sicherheit

Christoph Siefer,
sym.net

v 1.2 21.02.2012

sym.net

Inhalt

Odalis Sicherheit

Software Odalis

Das verwendete Software-Framework Odalis wurde von Anfang an für die Erfüllung höchster Datenschutz- und Sicherheitsanforderungen konzipiert.

- **Durchgehende HTTPS-Verschlüsselung:**
  Odalis ist so konfiguriert, daß eine unverschlüsselte Verbindung (SSL/HTTPS) nicht möglich ist.

- **Rechte- und Rollensystem:**
  Odalis verfügt über ein granular anpassbares Berechtigungsmanagement.
  - Für lesenden Zugang zum System ist ein berechtigter Account zwingend notwendig (konfigurierbar).
  - Admistrative Zugänge stehen ausschliesslich entsprechend geschultem und verantwortlichem Personal zur Verfügung.
    MoOdalis: Mit Ausnahme des Vorgangs der Buchungsanfrage/Stornierung hat kein Nutzer Zugang zu schreibenden Prozessen im System. Diese Vorgänge sind jeweils durch die Prüfung der eingegebenen Daten auf evtl. Sicheheitsrisiken abgesichert.

- **Logging:**
  Es werden geloggt:
  - MoOdalis: Die Buchungsanfragen und Stornierungen der Teilnehmer
  - Lesende Zugriffe akkreditierter Nutzer auf das Angebot
  - Schreibende Zugriffe des administrativen Personals
  - Vom System versandte eMails inclusive des versandten Texts. Vom System auf Anfrage generierte und versandte Passwörter werden in der archivierten Version unkenntlich gemacht.
  - Aufgezeichnet werden neben der Kennung des Zielprozesses die IP des zugreifenden Geräts, die interne Nutzerkennung im Odalis-System (ID) sowie der Zeitpunkt des Zugriffs.

- Odalis verlangt zwingend eine laufende **Suhosin** Instanz
  Siehe http://www.hardened-php.net/suhosin/
- **Security-Level Object:**
  Entdeckt diverse bekannte Angriffe und Fehlkonfigurationen und reagiert entsprechend

- **Forced GPC-Validation** nach dem Whitelist-Verfahren:
  Konfigurierbare Prüfung/Filterung für eingehende GET-, POST- und COOKIE-Daten. Nur formulierte Prüfungen lassen dabei Daten überhaupt passieren.

- **Formular-IDs:**
  Alle von System generierten Formulare sind mit einer eindeutigen und temporär gültigen IDs versehen, auf diese Art und Weise können unregistrierte Formulare nicht in den Datenraum geladen werden.

- Einsatz des **PHP Intrusion Detection Systems.**
  Siehe www.phpids.org

- LogIn Bereiche mit automatisch erstellten, **starken Passworten**:
  - Die Sicherheit von Authentifizierungsverfahren ist nicht durch Benutzer oder Administratoren kompromittierbar.
  - Die Regeln des Auftraggebers für das Generieren starker Passworte werden angewandt.
  - Passworte werden ausschliesslich verschlüsselt (MD5) gespeichert.
  - Passworte sind für das administrative Personal zu keiner Zeit einsehbar.

- **Dateizugriffe** über das Downloadverfahren werden über das Berechtigungssystem einzeln freigegeben.

- **Regelmäßige Code Audits durch Dritte:**
  Unabhängige, anerkannte Auditore prüfen unsere Software auf Anforderung

- **Lückenlose Daten-Historie** auf Einzelfeld-Ebene:
  - geloggt werde ausgewählte Änderungen am Kursangebot, der Status eingeschriebener Teilnehmer und deren Accounts. Aufgezeichnet werden der Vorstatus des Datenfelds, die IP des zugreifenden Geräts, die interne Nutzerkennung im MoOdalis-System (ID) sowie der Zeitpunkt des Zugriffs.

- **Automatisiertes Backup/Restore Szenario:**
  - Wenn sym.net ihre Applikation hostet, werden täglich um 03:00 Vollsicherungen des Systems gefahren (Amanda-Backup). Diese können bei Bedarf scriptgesteuert wiederhergestellt werden.

Schnittstellen zu anderen Systemen

Es werden Dateiim- und exporte im CSV-, XML- und MS-Excel Format durch Download via Browser unterstützt. Derzeit konfiguriert sind ein CSV-Benutzerdaten-Import sowie diverse Reports (Exporte) in den Formaten MS-Excel, CSV und XML (XHTML). Im- und Exporte können ausschliesslich vom administrativen Personal vorgenommen werden. Andere Schnittstellen sind nicht implementiert.

Zugriff auf Serverebene

Zugriffe können ausschliesslich auf SSH-Ebene erfolgen. Root-Zugriffe über SSH sind nicht erlaubt. Über die geheimen Zugangsdaten für diese Ebene verfügt ausschliesslich der Server Maintainer.

Wenn sym.net Ihre Apllikation hostet, ist der Quellcode der Anwendung gegen das Auslesen durch korrekte Konfiguration des Webservers geschützt.

Zertifiziertes Hosting:

Host Europe GmbH
Welserstraße 14
51149 Köln
Eintragung im Handelsregister.
Registergericht: Amtsgericht Köln
Registernummer: HRB 28495

Datenschutzbeauftragter der Host Europe GmbH:

Eric Drissler, E-Mail: datenschutzbeauftragter@hosteurope.de

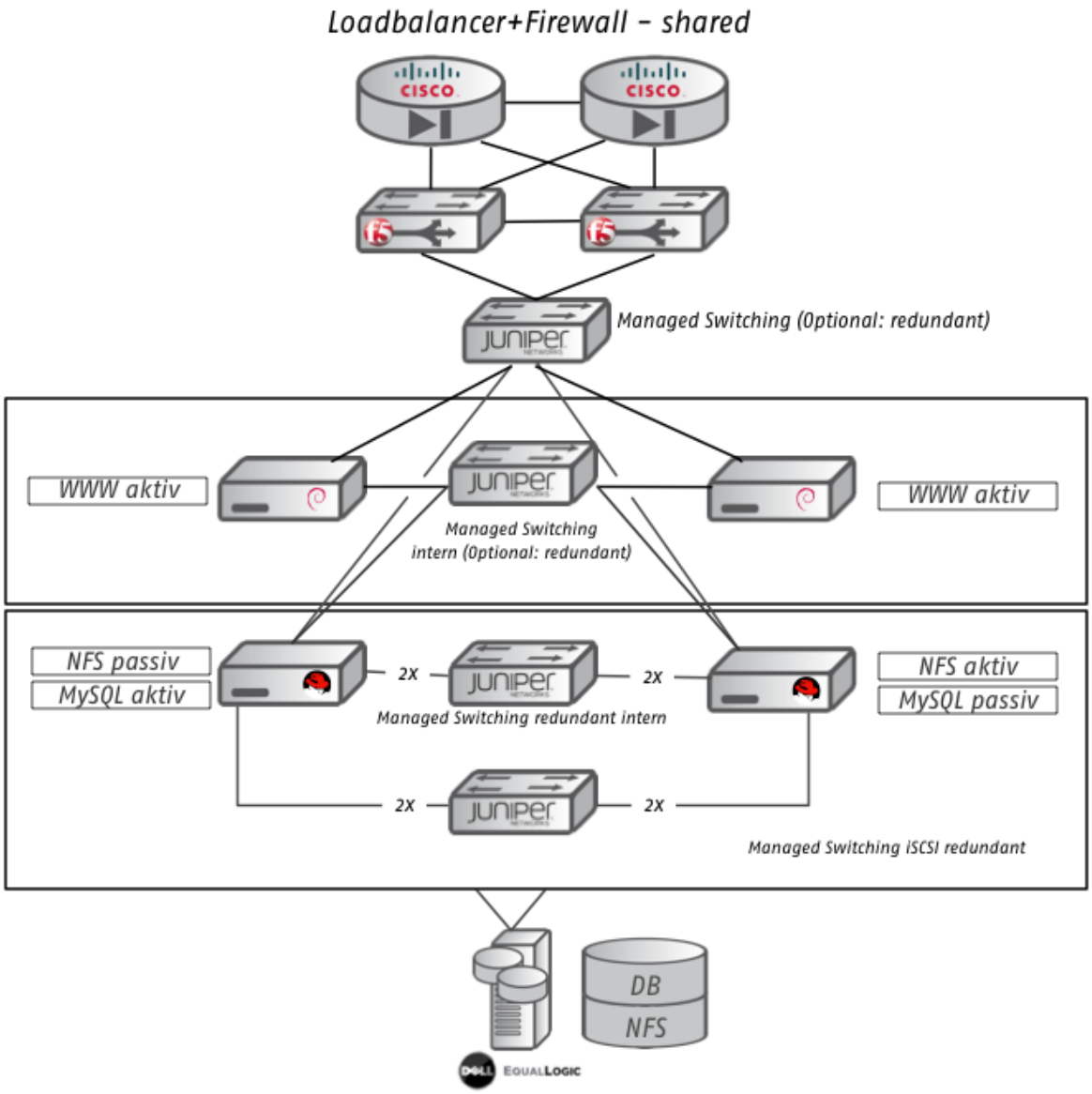
Im Rahmen des eco Datacenter Star Audit wurden beide Rechenzentren der Host Europe GmbH mit Bestnoten ausgezeichnet: hierbei erhielt das Rechenzentrum Welserstrasse die Bestnote von 5 Sternen und das Rechenzentrum Hansestrasse 4 Sterne. Der eco Datacenter Star Audit ist ein Sicherheits- und Qualitätszertifikat für Internet-Datenzentren des Verbands der deutschen Internetwirtschaft. Geprüft und bewertet werden die Hauptkategorien: Gebäude, Personal, Prozesse und Technik.

Siehe hierzu die Seiten des eco Verbands (http://www.eco.de/services/dcsa.htm)

Das Zertifikat kann auf Anfrage eingesehen werden.

Das System - Aufbau siehe unten - wird von der Host Europe GmbH Sicherheitstechnisch gewartet (Managed Hosting).

Beispielhafter Systemaufau



Literatur

[1] ODALIS für Communities, © Christoph Siefer 2005 (www.odls.net)

[2] ODLS – Technische Grundlagen, © Christoph Siefer 2005 (www.odls.net)

Kontakt

sym.net
Christoph Siefer
Gotenring 27

50679 Köln

+49 (0)221 . 376 259 0

siefer@sym.net

Impressum

Verantwortlich i.S.d. § 6 MDStV & 6 TDG

sym.net, Christoph Siefer
Gotenring 27
50669 Köln

Telefon: +49 (0)221 37 62 590

E-Mail: siefer@sym.net
Internet: www.odalis.net, www.sym.net

USt-ID: DE 20558906

Rechtshinweis

sym.net behält sich das Recht vor, Änderungen oder Ergänzungen der bereitgestellten Informationen vorzunehmen. Inhalt und Struktur dieses Dokuments sind urheberrechtlich geschützt. Die Vervielfältigung von Inhalten oder Daten, insbesondere die Verwendung von Texten, Textteilen oder Bildmaterial bedarf der vorherigen schriftlichen Zustimmung der sym.net.

Alle genannten Marken sind Eigentum ihrer Halter.