direktzu®

relevantec GmbH

Übersicht zur Systemarchitektur und Sicherheitskonzept

Stand

Dienstag, 28. Februar 2012

Inhaltsverzeichnis

1. Einleitung 3
1.1. Application Service Providing der Anwendung 3
1.2. Hosting bei Amazon Web Services in der Europäischen Union 3
1.3. Verwendete Technologie und Komponenten 3
1.4. Getrennte Datenverarbeitung und Datenhaltung 3
2. Bausteine des Sicherheitskonzepts 4
2.1. Physische Sicherheit von Gebäuden und Anlagen 4
2.2. Organisatorische Sicherheit 4
2.3. Sicherheit von Daten und Servern 4
2.4. Zugriffsbeschränkung beim Application Service Providing 5
2.5. Zusammenarbeit mit Drittanbietern für Datenhaltung und Datenverarbeitung 5
3. Kommunikationskanäle der Anwendung 6
3.1. Komponenten 6
3.2. Kommunikationsbeziehungen 7
4. Berechtigungs- und Rollenkonzept der Anwendung 9
4.1. Mögliche Zustände eines Besuchers 9
4.2. Benutzerrollen und Berechtigungen 9

1. Einleitung

1.1. Application Service Providing der Anwendung

Die interne Kommunikationsplattform wird als Web-Applikation im Rahmen eines ASP angeboten und außerhalb des Intranets des Unternehmen gehostet und betrieben. Der Zugriff auf die Plattform ist grundsätzlich nur aus dem Intranet des Unternehmens möglich und wird über geeignete Maßnahmen eingeschränkt.

1.2. Hosting bei Amazon Web Services in der Europäischen Union

Beim Hosting der Anwendungen für die interne Unternehmenskommunikation arbeitet direktzu® mit Amazon Web Services zusammen und mietet im europäischen Rechenzentrum in Irland virtualisierte Server-Instanzen an. Diese werden von direktzu® auf Betriebssystemebene vollständig selbst administriert und in einem durch Firewall gesicherten privaten Subnetz betrieben.

1.3. Verwendete Technologie und Komponenten

Die Anwendung wird in Ruby mit Hilfe des Webframeworks „Ruby on Rails“ entwickelt. Für den Betrieb der Plattform ist ein Loadbalancer vorgesehen, der die Anfragen auf die Applikationsserver verteilt und die Zugriffsberechtigung auswertet und durchsetzt. Die Datenhaltung erfolgt auf einem MySQL Datenbankserver.

Alle Komponenten werden auf den gemieteten Server-Instanzen unter Linux (Ubuntu Server Edition) betrieben und durch direktzu® selbst administriert. Die Funktionalität des Loadbalancer und der Applikationsserver werden mit dem Apache HTTP Server und entsprechenden Modulen abgebildet.

1.4. Getrennte Datenverarbeitung und Datenhaltung

Für den Betrieb einer internen Kommunikationsplattform werden Loadbalancer und Applikationsserver auf dedizierten Instanzen, von anderen Kunden getrennt, betrieben. Die Datenhaltung erfolgt in einzelnen Datenbanken, logisch getrennt von Daten anderer Kunden, im MySQL Datenbankserver. Je nach Anforderungsprofil sind auch dedizierte Datenbankserver möglich.

2. Bausteine des Sicherheitskonzepts

2.1. Physische Sicherheit von Gebäuden und Anlagen

Die relevantec GmbH hat langjährige Erfahrung im Umgang mit sensiblen Informationen und Daten ihrer Kunden. Die Absicherung der Büroräume erfolgt mit branchenüblichen Maßnahmen wie bspw. Schließdienst durch Wachschutz, einbruchhemmende Absicherung der Eingänge, Einbruch- und Brandmeldeanlagen sowie Panzerschränke für vertrauliche Dokumente und Datenträger.

Die Server für den Betrieb der internen Kommunikationsplattform sind nicht in den Räumen der relevantec GmbH untergebracht und bei Amazon Web Services u.a. vor physischen Angriffen und Gefahren geschützt.

2.2. Organisatorische Sicherheit

Alle Mitarbeiter werden auf die Verpflichtungen des Bundesdatenschutzgesetzes hingewiesen und durch gesonderte Vertraulichkeitserklärung zur Geheimhaltung verpflichtet. Diese besteht auch nach Beendigung der Tätigkeiten für die relevantec GmbH fort.

2.3. Sicherheit von Daten und Servern

Alle betriebenen Server laufen mit einer Ubuntu Server Edition mit Langzeitunterstützung und werden regelmäßig aktualisiert. Nicht benötigte Dienste werden abgeschaltet, alle nicht genutzten Ports gesperrt und unbenutzte Nutzerkonten gelöscht.

Zugriffsrechte für die Plattformen, deren Verwaltungsschnittstellen, Server und Datenbanken werden individuell, zeitlich beschränkt und aufgabenbezogen an einzelne Mitarbeiter vergeben. Sobald ein Mitarbeiter die Rechte nicht mehr benötigt, werden diese umgehend gelöscht, selbst wenn er weiter bei direktzu® beschäftigt ist.

Zugriff auf das Betriebssystem der Server ist nur über individuell zugeordnete, durch Passwort geschützte SSH-Schlüssel möglich (Public-Key-Authentifizierung). Alle Zugriffe und Kommandos der Administratoren werden aufgezeichnet.

Alle weiteren für die Verwaltung der Plattformen nötigen Zugänge der Mitarbeiter sind durch SSL-Zertifikate oder Passwörter, mit hohen Anforderungen an Komplexität, geschützt.

Backup-Lösungen, mit Verschlüsselung vor Übertragung, sichern die Verfügbarkeit der Nutzer- und Anwendungsdaten.

2.4. Zugriffsbeschränkung beim Application Service Providing

Die Plattformen der internen Unternehmenskommunikation werden auf Servern betrieben, die direktzu® von spezialisierten Dienstleistern mietet. Dabei erfolgt eine strikte Trennung (physisch und logisch) von allen übrigen betriebenen öffentlichen und internen Plattformen.

Der Zugriff auf eine interne Plattform ist grundsätzlich nur aus dem Intranet des Kunden und über eine SSL verschlüsselte Verbindung möglich.

Die Zugriffsbeschränkungen können durch folgende Stufen abgebildet werden (Kombinationen und weitere, individuelle Lösungen möglich):

- Zugriff über einen zentralen Reverse Proxy im Intranet des Kunden, bei dem die Berechtigung auf dem Loadbalancer über ein Client SSL Zertifikate ausgewertet wird
- Beschränkung auf Quell IP Adressen und Bereiche
- Filterung anhand von E-Mail Adressbestandteilen der Nutzer und Double Opt-In bei der Registrierung
- Anbindung an vorhandene Single Sign-On Systeme

2.5. Zusammenarbeit mit Drittanbietern für Datenhaltung und Datenverarbeitung

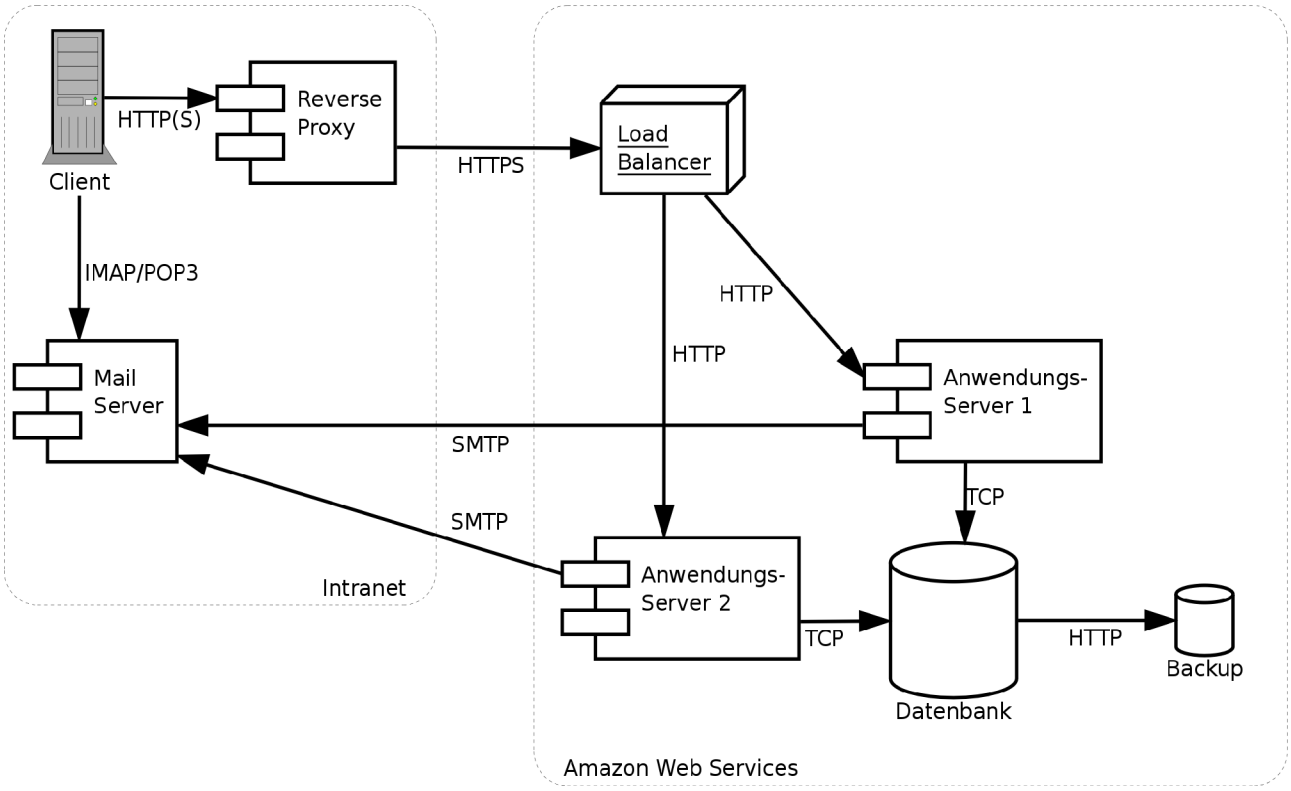
Um eine reibungslose und sichere Leistung zu erbringen, arbeitet direktzu® mit spezialisierten Hosting Dienstleistern zusammen. Diese garantieren für den Schutz, die Vertraulichkeit und die Verfügbarkeit der Datenhaltung und -verarbeitung.

Die Software sowie der erforderliche Speicherplatz für Daten werden in einem Rechenzentrum von Amazon Web Services (AWS) in der Europäischen Union in Irland bereitgehalten. Die Daten werden ausschließlich dort verarbeitet und gespeichert.

Für weitere Informationen über die Sicherheitsverfahren und Absicherungen verweisen wir auf das Dokument „Sicherheitsprozess im Überblick“ bzw. „Overview of Security Processes“ von Amazon Web Services.

3. Kommunikationskanäle der Anwendung

Im Folgenden wird der allgemeine Aufbau der für das Projekt benötigten IT-Komponenten gezeigt. Zusätzlich sind weitere Komponenten dargestellt, um den Zusammenhang und das Zusammenspiel für das projektspezifische Serviceangebot zu verdeutlichen.



3.1. Komponenten

Alle von direktzu® administrierten Server laufen unter Ubuntu Server Edition. Es sind ausschließlich solche Dienste aktiviert und Ports geöffnet, die zum Betrieb der direktzu®-Anwendung notwendig sind.

Der **Loadbalancer** arbeitet mit Apache 2.2.

Die **Anwendungsserver** arbeiten mit Apache 2.2; die E-Mails werden von einem lokal installierten Exim4 an den Mailserver verschickt.

Auf dem **Datenbankserver** läuft MySQL 5.0.

Das **Backup System** ist ein S3-Bucket bei Amazons Simple Storage Service in Irland. Die Daten werden vor der Übertragung verschlüsselt (asymetrisch mit GnuPG).

3.2. Kommunikationsbeziehungen

Nachfolgend erfolgt eine Auflistung über die Verwendung der Schnittstellen der einzelnen Komponenten des Gesamtsystems.

3.2.1. Nutzer ⇄ Reverse Proxy

Verwendung: Dies stellt die Schnittstelle zwischen dem Proxy Server und den Webbrowsern der Mitarbeitern dar. Es werden hierüber Beiträge gelesen, geschrieben oder bewertet bzw. die Videos oder Antworten verfolgt. Die Datenübertragung erfolgt innerhalb des Intranets.

Art: HTTP oder HTTPS

3.2.2. Reverse Proxy ⇄ Loadbalancer

Verwendung: Dies stellt die Schnittstelle zwischen dem Proxy Server im Intranet und dem Loadbalancer bei direktzu® dar. Diese Verbindung ist per SSL Client und SSL Server Zertifikat oder einer anderen geeigneten Maßnahme zur Zugriffsbeschränkung gesichert. Hier werden die Inhalte der Beiträge, Kommentare und Bewertungen übertragen. Die Kommunikation erfolgt über das Internet.

Art: HTTPS

3.2.3. Loadbalancer ⇄ Anwendungsserver

Verwendung: Dies stellt die Schnittstelle zwischen dem Loadbalancer und den Anwendungsservern dar. Hier werden die Inhalte der Beiträge, Kommentare und Bewertungen übertragen. Die Kommunikation findet innerhalb des privaten Subnetzes bei Amazon Web Services statt.

Art: HTTP

3.2.4. Anwendungsserver ⇄ MySQL DB

Verwendung: Dies stellt die Schnittstelle zwischen den Anwendungsservern und der MySQL Datenbank dar. Hier werden die Inhalte der Beiträge, Kommentare und Bewertungen übertragen. Die Kommunikation findet innerhalb des privaten Subnetzes bei Amazon Web Services statt.

Art: TCP/MySQL

3.2.5. MySQL DB ⇄ Backup

Verwendung: Dies stellt die Schnittstelle zwischen der MySQL Datenbank und dem Backup dar. Hier werden sämtliche Inhalte wie Beiträge, Kommentare und Bewertungen übertragen. Backups werden vor Übertragung asymmetrisch verschlüsselt. Die Kommunikation findet innerhalb des Netzwerkes bei Amazon Web Services in Irland statt.

Art: HTTP

3.2.6. Anwendungsserver ⇄ E-Mail Server

Verwendung: Dies stellt die Schnittstelle zwischen den Anwendungsservern und dem E-Mail Server des Unternehmens dar. Sie dient dazu, die Benutzer über bestimmte Ereignisse zu informieren und Aktionen zu bestätigen. Beispielsweise um mitzuteilen, dass Kommentare oder Antworten zu ihren Beiträgen vorliegen. Die Kommunikation erfolgt über das Internet.

Art: SMTP

3.2.7. E-Mail Server ⇄ Benutzer

Verwendung: Dies stellt die Schnittstelle zwischen dem E-Mail-Server des konzerninternen Rechenzentrums und dem Benutzer dar. Die Datenübertragung erfolgt in der Regel innerhalb des Intranets.

Art: IMAP oder POP3

4. Berechtigungs- und Rollenkonzept der Anwendung

Die Anwendung verwendet ein rollenbasiertes Rechtesystem, welches im Folgenden genauer beschrieben wird. Nicht alle der hier beschrieben Rollen müssen in der Anwendung auch vergeben und genutzt werden. Abhängig von der Konfiguration der Plattform und des Konzeptes der internen Unternehmenskommunikation, sind nur bestimmte Rollen überhaupt sinnvoll. Mindestens die Rolle des *Benutzers* muss verwendet werden.

4.1. Mögliche Zustände eines Besuchers

Besucher ist jeder Benutzer, der die Webseite in seinem Webbrowser öffnet.

Jedem nicht angemeldeten Besucher der Webseite wird implizit die Rolle *Gast* zugeordnet. Die Zuordnung eines (wiederkehrenden) Besuchers findet auf der Ebene einer Cookie-basierten Session statt.

Zum Verfassen von Inhalten (Beiträgen oder Kommentaren) muss sich der Besucher an der Anwendung anmelden. Nach der Anmeldung erhält der Besucher die Rolle *Benutzer*.

Alle weiteren Rollen müssen vom Administrator für den jeweiligen *Benutzer* festgelegt werden.

4.2. Benutzerrollen und Berechtigungen

4.2.1. Gast

Jeder Besucher, dem über sein Session-Cookie kein bestehender Nutzer-Account zugeordnet werden kann, ist nicht am System angemeldet.

Gäste können Beiträge und Kommentare anderer Nutzer sowie vorhandene Antworten lesen und für Beiträge abstimmen. Wenn ein Besucher Inhalte verfassen möchte oder aber die Plattformkonfiguration dies für alle Aktionen voraussetzt wird eine Anmeldung verlangt.

4.2.2. Benutzer

Einem Nutzerkonto ist die Rolle *Benutzer* zugeordnet. Sobald sich also ein Besucher an der Anwendung anmeldet, erlangt dieser alle Berechtigungen eines Benutzers und erbt die Rechte eines Gastes.

Benutzer können Beiträge und Kommentare verfassen und zur Veröffentlichung einreichen.

Alle weiteren Rollen erben die Rechte eines *Benutzers*.

4.2.3. Moderator

Das Redaktionsteam überwacht die Einhaltung der Benutzungsregeln und der thematischen Grenzen der eingereichten Beiträge und Kommentare. Dazu wird einem oder mehreren bereits in der Anwendung registrierten Nutzerkonten die Rolle eines *Moderators* zugeordnet.

Moderatoren geben zur Veröffentlichung eingereichte Beiträge und Kommentare nach inhaltlicher Prüfung und ggf. Bearbeitung frei. Zur Überwachung bereits veröffentlichter Inhalte können sie Beiträge und Kommentare bearbeiten, löschen und wiederherstellen.

Ebenfalls von *Moderatoren* gepflegt wird die Themenliste. Dies beinhaltet zum einen die Themen zu denen ein Beitrag geschrieben werden kann und zum anderen das Erstellen und Bearbeiten eines Impulsthemas welches prominent auf der Startseite der Plattform angezeigt wird und den Benutzern als Impuls zum Verfassen neuer Beiträge dienen soll.

Darüber hinaus hat der *Moderator* Einsicht in die Meldungen, die auf der Plattform zu jedem Beitrag abgegeben werden können und auf Spam, Beleidigungen und Ähnliches hinweisen.

4.2.4. Bild-Moderator

Jeder *Benutzer* kann zu seinem Profil ein Portrait hinzufügen. Der *Bild-Moderator* kann diese Bilder freigeben oder ablehnen.

4.2.5. Benutzer-Moderator

Benutzer-Moderatoren haben die Möglichkeit, die E-Mail Adresse des Verfassers eines Beitrages einzusehen um ihn darüber zu kontaktieren.

Außerdem hat er Einsicht in eine Liste aller nicht aktivierten Benutzer (Double Opt-In).

4.2.6. Adressat

Nutzerkonten mit der Rolle *Adressat* können im Namen der Adressaten der Plattform Antworten auf Beiträge verfassen, bearbeiten und löschen.

4.2.7. Übersetzer

Die Plattform kann in verschiedenen Sprachen lokalisiert werden. Ein Nutzer mit der Rolle *Übersetzer* kann die lokalisierbaren Texte auf der Plattform bearbeiten und in andere Sprachen übersetzen.

4.2.8. Plattform-Administrator

Der *Plattform-Administrator* hat die Rechte die plattformweite Konfiguration zu bearbeiten. Dazu gehören u.a. Einstellungen welche Arten von Beiträgen eingestellt werden können, in welchem Intervall die Top-Setzung der Beiträge stattfindet, welche Inhalte moderiert werden sollen, welche Sprachen unterstützt werden, wie die Kontaktdaten des Adressaten aussehen sowie weitere Parameter, die das Kommunikationskonzept beeinflussen.

Zudem kann der *Plattform-Administrator* statische Seiten, bestimmte Links sowie die Seitenleiste verwalten (CMS-Funktionalität).

4.2.9. Analyst

Nutzer mit der Rolle *Analyst* können die vom *Administrator* definierten statistische Auswertungen über die Aktivitäten auf der Plattform einsehen und sich diese per E-Mail-Abonnement zusenden lassen.

4.2.10. Administrator

Administratoren erben die Rechte des *Moderators* und des *Plattform-Administrators*. Zusätzlich können *Administratoren* Rollen an *Benutzer* vergeben oder diese wieder entfernen und *Benutzer* sperren.

Der *Administrator* hat zudem das Recht Statistiken zu erstellen, die auf alle Daten der zugrunde liegenden Datenbank zugreifen können.