Sicherheitsaspekte und -beurteilung von Cloud Lösungen für InvestorFinder

Nutzer Sicherheit:

- Nutzer arbeiten auf Ihrer eigenen geschützten Datenbank, die nur für sie zugänglich ist.
- Nutzer können entscheiden, das System ausschließlich für interne Verwaltungszwecke zu nutzen, so dass kein anderer Teilnehmer Zugang zu seinen Daten erhält.
- Eine Freigabe von Daten für andere Nutzer erfolgt nur dann, wenn der Nutzer dies aktiv so einrichtet.
- Ausnahme sind alle Objektdaten, soweit diese vollkommen anonymisiert dargestellt werden. Anonymisierung schließt aus, dass Objektadresse, Fotos, Mieternamen oder andere Daten angezeigt werden, die auf das individuelle Objekt zurück schließen lassen.
- Der Aufbau von Partnerschaften und Netzwerken ist möglich, muss aber auch aktiv vom Nutzer eingerichtet werden. Hier kann sich der Nutzer vermarkten.
- Der Nutzer profitiert bei Cloud Lösungen von geringen Kosten, die eine Anpassung der Funktionen verursachen. Denn eine Cloud Lösung muss nur einmal angepasst werden, während Software Anpassungen immer auf verschiedenen Versionen und Netzwerkumgebungen angepasst werden müssen.

IT Sicherheit:

- Sichere Kommunikation und Datenübertragung im Internet über SSL
- Schutz vor Fishing durch Identifikation von InvestorFinder über ein Zertifikat. (Analog zu Banking Applikationen)
- Passwort geschützter Bereich
- Daten liegen im professionellen Rechenzentrum
- Sicherung erfolgt im zwei Stunden Takt, Daten älter als 2h gehen damit nicht verloren.
- Export aller Daten in CSV (Excel) Format bei Vertragsende. Export Import Schnittstelle.
- Günstig für mittelgroße Kunden im Vergleich zu eigenen Lösungen
- Multiuserfähigkeit
- Weltweite Verfügbarkeit auf jedem browserfähigen Gerät (PC, iPad, iPhone, Apple, usw.)
- Sparen durch Outsourcing von Administrationsaufwand an den Cloud Anbieter
- Daten lokal vs. Daten bei spezialisiertem Anbieter (Cloud). → Warum hält man Geld bei der Bank und nicht im Unternehmenssafe? → Wegen fehlender Erfahrung und Know how in der Datensicherheit. Cloud Anbieter bieten diese Erfahrung.
- Anbieter kümmert sich um die Anpassungen an die neusten Sicherheitsstandards

Kosten Einsparungen im Einzelnen im Rahmen der IT-Sicherheit:

- Rechenzentrumssicherheit: Sicherheitsservice für Überwachung von Gebäuden, Zutrittskontrolle, Brandschutz, unterbrechungsfreie Stromversorgung (z.B. Stromverteilungsgeräte), Klimatisierung (z.B. Kühlung und Luftfeuchtigkeit),

Notfallmanagement; daraus ergeben sich folgende Kostenkategorien: Anschaffungs-, Betriebs-, Administrations- und Instandhaltungskosten, sowie Kosten für Ausfall und Wartungsfenster und eventuell redundante Auslegung von Rechenzentren
- Datenspeicherung und Versionsverwaltung (Storage): Archivierungskosten, Verwaltungskosten, Kosten für Fehler-, Konfigurations-, Patch- und Änderungsmanagement
- Sicherheitsarchitektur: Kosten für Firewalls, Angriffserkennungssensoren, Intrusion-Detection-Systeme, Antivirensoftware, Monitoring-Systeme; daraus ergeben sich folgende Kostenkategorien: Anschaffungskosten, Lizenzkosten (wenn nicht Open Source), Kosten für Updates, Service- / Wartungsverträge, Kosten aufgrund von Inkompatibilität, Zusatzkosten für Eigenentwicklungen / Umstellungen / Probleme bei Updates, sowie Sicherheitstests
- Kosten für IT-Personal, z.B. Arbeitsaufwand zur Pflege von Soft- und Hardware
- Informationssicherheit und Compliance: etwaige Kosten für Identitätsmanagement (z.B. Überprüfung von Administratoren bei der Anstellung), Schlüsselverwaltung

Ein Wort zur benutzten Programmiersprache: Rails:

- Auf der letzten Konferenz des OWASP 2010 (Open Web Application Security Project) hat Rails als einer der Frameworks mit den sichersten Bordmitteln abgeschnitten.