TeleTrusT – Bundesverband IT-Sicherheit e.V.
Der IT-Sicherheitsverband.

Sichere Nutzung von Cloud-Anwendungen

am Beispiel des TeleTrusT – Bundesverband IT-Sicherheit e.V. als Praxisleitfaden für Verbände und KMU

Autoren

Oliver Dehning, antispameurope GmbH, Leiter der TeleTrusT-AG "Cloud Computing"
RA Karsten U. Bartels, Bartels Kim Wollenhaupt Rechtsanwälte Partnerschaft
Axel Borchers, Siemens Enterprise Communications GmbH & Co. KG
Michael Gröne, Sirrix AG
Thorsten Humberg, Fraunhofer-Institut für Software- und Systemtechnik ISST
Dr. Holger Mühlbauer, TeleTrusT – Bundesverband IT-Sicherheit e.V.
Christian Senk, Universität Regensburg, Lehrstuhl Management der Informationssicherheit
Dr. Thomas Störtkuhl, TÜV Süd AG
Iryna Tsvihun, Fraunhofer AISEC

Diese Publikation wurde in der Arbeitsgruppe "Cloud Computing" des TeleTrusT - Bundesverband IT-Sicherheit e.V. erarbeitet.

Die in dieser Publikation beschriebenen technisch-organisatorischen Parameter geben den Stand bzw. Kenntnisstand Mai 2012 wieder.

Impressum

Herausgeber:

TeleTrusT – Bundesverband IT-Sicherheit e.V.
Chausseestraße 17
10115 Berlin
Tel.: +49 30 400 54 306
Fax: +49 30 400 54 311
E-Mail: info@ teletrust.de
http://www.TeleTrusT.de

Herstellung:

DATEV eG, Nürnberg

1. Auflage

'*Executive Summary*'

Cloud Computing beginnt Strukturen und Arbeitsabläufe in der Wirtschaft nachhaltig zu verändern. Cloud Computing erschließt Synergieeffekte durch die gemeinsame Nutzung von Ressourcen. Diese Synergieeffekte führen teilweise auch zu einer Verbesserung der IT-Sicherheit gegenüber traditionellen IT-Systemen. Andererseits sind viele Datenschutz- und Sicherheitsfragen beim Cloud Computing zumindest teilweise ungeklärt.

In dieser Publikation wird die sichere Nutzung von Public Cloud-Anwendungen am TeleTrusT - Bundesverband IT-Sicherheit e.V. (TeleTrusT) als Beispiel einer Verbandgeschäftsstelle untersucht. Die Untersuchung kann als Referenz für Vereine und KMU angesehen werden, die sichere Public Cloud Services verwenden wollen.

Untersucht wurden von TeleTrusT benötigte Anwendungen E-Mail, Cloud-Datenspeicher und CRM. Im Rahmen der Publikation wurden verschiedene Marktangebote aus diesem Bereich im Hinblick auf Anforderungen aus funktionaler Sicht, rechtlicher Sicht und aus der Sicht der IT-Sicherheit evaluiert.

Dass Cloud-Angebote hinsichtlich Funktionalität oft mehr bieten als zu vergleichbaren Kosten betriebene interne Lösungen, hat diese Untersuchung bestätigt. Die Untersuchung hat aber auch gezeigt, dass viele Anbieter sich noch immer schwertun, konkrete Aussagen zur Sicherheit und Verfügbarkeit ihrer Services zu treffen, ganz unabhängig von der Größe der Anbieter.

Organisationen mit vereinfachter Infrastruktur können oft keine besonderen Bedingungen und SLAs mit den Anbietern aushandeln, umso mehr müssen sie die Bedingungen der Standardangebote sorgfältig prüfen. Dies besonders dann, wenn es um die Verarbeitung personenbezogener Daten gemäß Bundesdatenschutzgesetz (BDSG) geht. Die Organisation ist und bleibt auch im Cloud Computing der "Herr der Daten" und somit für die Authentizität, Integrität, Verfügbarkeit und Vertraulichkeit der Daten voll verantwortlich. Ob ein Cloud-Angebot die Anforderungen einer Organisation besser erfüllt als eine intern betriebene Lösung, sollte deshalb im Einzelfall geprüft werden.

Inhalt

1 Einleitung

1.1 Zielsetzung und Untersuchungsgegenstand

Cloud Computing beginnt Strukturen und Arbeitsabläufe in der Wirtschaft nachhaltig zu verändern. Wesentliche Treiber sind durch den Einsatz von Cloud Computing erwartete erhebliche Kosteneinsparungen im IT-Bereich sowie der zunehmende Einsatz mobiler Systeme im professionellen Bereich. Cloud-Lösungen bieten in vielen Bereichen auch für kleine Organisationen Leistungsmerkmale, die bisher großen IT-Installationen vorbehalten waren.

Die Realisierung ähnlicher Leistungsmerkmale mit proprietären traditionellen IT-Systemen ist für kleine und mittlere Unternehmen (KMU) und Organisationen schon aus Aufwandsgründen und durch den Mangel von IT-Spezialisten in diesen Organisationen in der Regel unmöglich. Cloud Computing erschließt hingegen Synergieeffekte durch die gemeinsame Nutzung von Ressourcen. Diese Synergieeffekte führen teilweise auch zu einer Verbesserung der IT-Sicherheit gegenüber traditionellen IT-Systemen. Andererseits sind viele Datenschutz- und Sicherheitsfragen beim Cloud Computing zumindest teilweise ungeklärt.

In dieser Publikation wird die sichere Nutzung von Public Cloud-Anwendungen durch einen gemeinnützigen Verein am Beispiel TeleTrusT – Bundesverband IT-Sicherheit e.V. (TeleTrusT) analysiert. Die Untersuchung kann als Referenz für Vereine und KMU angesehen werden, die sichere Public Cloud Services einsetzen wollen. Zudem werden einige Marktangebote für gängige Anwendungen wie E-Mail, Datenablage und CRM vorgestellt und aus Sicht der IT-Sicherheit betrachtet.

1.2 Definition grundlegender Begriffe

Cloud Computing gemäß NIST[1]-Definition ist ein Ansatz, der den bequemen On-Demand Netzwerk-Zugriff auf einen gemeinsamen Pool konfigurierbarer Rechner-Ressourcen (z.B. Netzwerke, Server, Speichersysteme, Anwendungen und Dienstleistungen) ermöglicht, die mit geringstem Management-Aufwand oder Eingriff eines Service-Anbieters schnell bereitgestellt und freigegeben werden können.[2]

Nach der Definition des NIST zeichnet sich Cloud Computing durch die folgenden fünf Kriterien aus[3]:

1. Automatisierte Bereitstellung mit Selbstbedienung
2. Breit verfügbarer Netzwerkzugriff (Ubiquität)
3. Vollständige Elastizität und Skalierbarkeit
4. Nutzungsabhängige Zahlung ("Pay per use"-Prinzip)
5. Mandantenfähigkeit (Multi-Tenancy).

Am Weitesten sind folgende drei Formen von Cloud Computing verbreitet: Public, Private und Hybrid Cloud – auch als Delivery-Modelle bekannt. Ferner wird zwischen drei Cloud Computing Service-Modellen unterschieden:

- *Infrastructure-as-a-Service (IaaS);*
- *Platform-as-a-Service (PaaS);*
- *Software-as-a-Service (SaaS).*

[1] NIST- National Institute of Standards and Technology

[2] National Institute of Standards and Technology (2010): Cloud Computing Definition v15, unter: NIST Definition Version v15, http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc

[3] Dr. Werner Streitberger und Angelika Ruppel. Cloud Computing Sicherheit: Schutzziele. Taxonomie. Marktübersicht. Technical Report, Fraunhofer-Institut für Sichere Informationstechnologie, September 2009

Diese Publikation beschäftigt sich maßgeblich mit SaaS-Lösungen in einer Public Cloud. Informationssicherheit in der Cloud liegt im Fokus der vorliegenden Publikation, daher gilt folgende Definition für Informationssicherheit:

Informationssicherheit wird als die Aufrechterhaltung der Vertraulichkeit, Integrität und Verfügbarkeit von Informationen in ISO 27001 definiert; andere Eigenschaften wie Authentizität, Zurechenbarkeit, Nicht-Abstreitbarkeit und Verlässlichkeit können ebenfalls berücksichtigt werden. Informationssicherheit bezeichnet in diesem Zusammenhang das Ziel, Systeme vor Gefahren bzw. Bedrohungen zu schützen, Schaden zu vermeiden und Risiken zu minimieren[4].

Im Folgenden werden die klassischen ***Schutzziele*** kurz erläutert, weil sie die Grundlage für Anforderungen an Sicherheit darstellen[5]:

1. *Vertraulichkeit* stellt nach ISO 27001 eine Eigenschaft dar, die sicherstellt, dass Informationen unberechtigten Personen, Einheiten oder Prozessen nicht verfügbar gemacht oder enthüllt werden. Das System muss so aufgebaut sein, dass ein Zugriff nur für befugte Personen oder Dienste möglich ist.
2. *Integrität* als Eigenschaft der Absicherung von Richtigkeit und Vollständigkeit von Werten bedeutet, dass die Informationen, Systeme und Netze nicht unbemerkt verändert werden können. Das System muss so beschaffen sein, dass eine Veränderung offensichtlich wird. Die Sicherstellung der Integrität beinhaltet die Komponenten Übereinstimmung, Genauigkeit, Korrektheit und Vollständigkeit.
3. *Verfügbarkeit* ist nach ISO 27001 eine Eigenschaft, einer berechtigten Einheit auf Verlangen zugänglich und nutzbar zu sein. Informationen, Systeme und Netze müssen verfügbar sein. Das System muss bei einem Zugriff in einem definierten Zeitraum antworten bzw. bestimmte Aktionen ausführen. Zum Schutzziel der Verfügbarkeit werden die Komponenten Fehlertoleranz, Zuverlässigkeit, Robustheit und Wiederherstellbarkeit gezählt.

Zur Definition der ***Schutzbedarfskategorien*** bedient sich diese Publikation der Terminologie des Grundschutz-Standards 100-2 des Bundesamtes für Sicherheit in der Informationstechnik (BSI) (Tabelle 1) .

Schutzbedarfskategorien	
"normal"	Die Schadensauswirkungen sind begrenzt und überschaubar.
"hoch"	Die Schadensauswirkungen können beträchtlich sein.
"sehr hoch"	Die Schadensauswirkungen können ein existentiell bedrohliches, katastrophales Ausmaß erreichen.

Tabelle 1: Schutzbedarfskategorien gemäß BSI[6]

Die vorliegende Publikation richtet sich an kleine und mittlere Unternehmen (KMU) und Organisationen. Als KMU bzw. kleine und mittlere Organisation werden in dieser Publikation in Anlehnung an eine Empfehlung der EU-Kommission solche mit weniger als 250 Mitarbeitern angesehen.

[4] Claudia Eckert. IT-Sicherheit: Konzepte - Verfahren – Protokolle. Oldenbourg Wissenschaftsverlag, 2009.
[5] Dr. Werner Streitberger and Angelika Ruppel. Cloud Computing Sicherheit: Schutzziele. Taxonomie. Marktübersicht. Technical Report, Fraunhofer-Institut für Sichere Informationstechnologie, September 2009.
[6] BSI-Standard 100-2, IT-Grundschutz Vorgehensweise, S. 49, https://www.bsi.bund.de/DE/Home/home_node.html

2 Analyse des IST-Zustandes

2.1 IT-Struktur

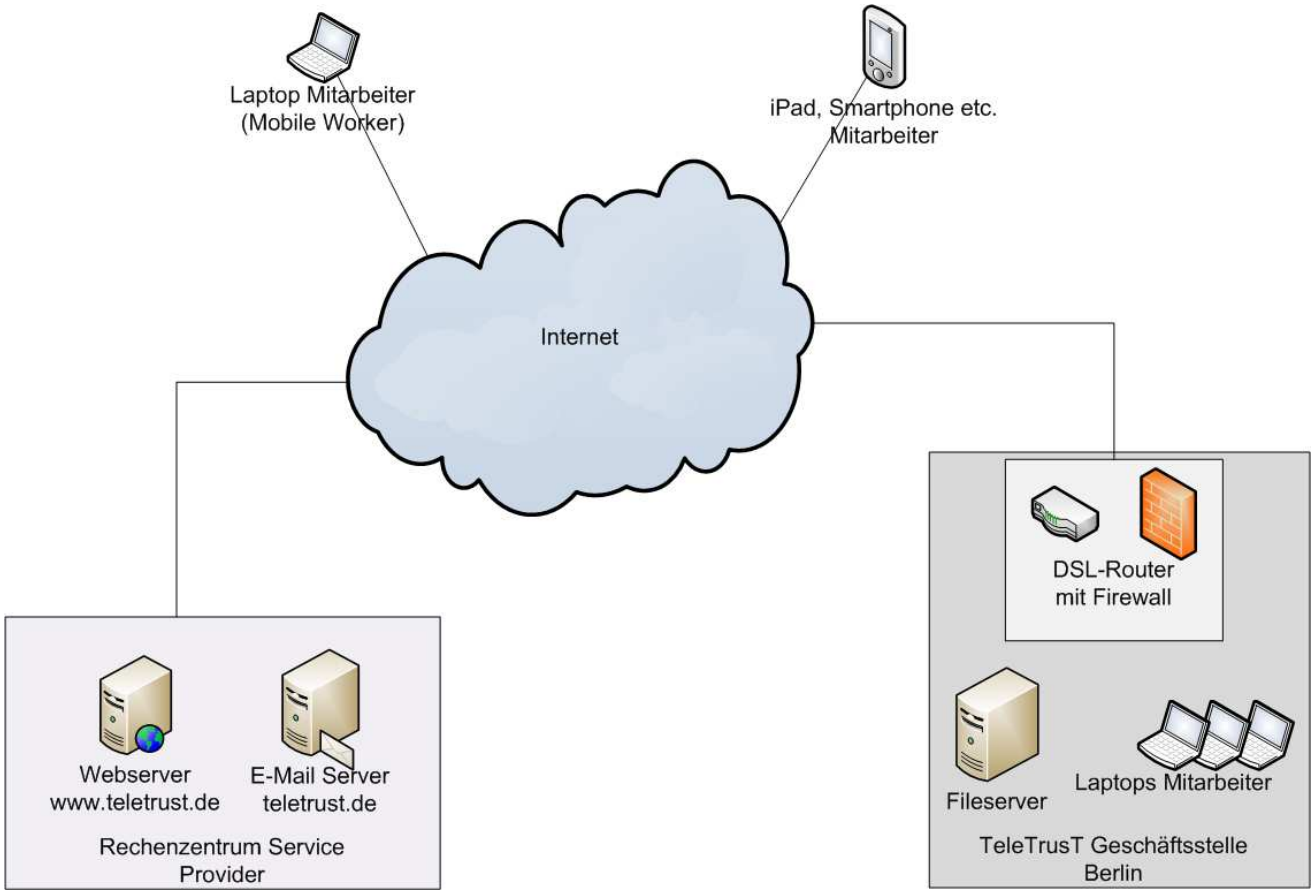

Abbildung 1: Logischer Netzwerkplan für die Anwendungen von TeleTrusT

Die TeleTrusT-Geschäftsstelle hat die in Abbildung 1 gezeigte Infrastruktur:

- Über Arbeitsplätze (Laptops) und mobile Geräte (Laptop, iPad, Smartphone usw.) wird auf genutzte Anwendungen und Daten zugegriffen. Die wichtigsten Anwendungen sind: E-Mail, Datenablage und Kontaktdatenverwaltung.
- TeleTrusT verfügt über einen eigenen Fileserver. Die Verfügbarkeit der Daten wird über eine RAID1-Konfiguration des Fileservers realisiert. Für die Daten des Fileservers ist zudem ein automatisches regelmäßiges Backup implementiert.
- Webserver und E-Mail-Server werden von einem Service Provider über ein zentrales Rechenzentrum bereitgestellt.
- Mobile Geräte von Mitarbeitern können von außerhalb des lokalen Netzes in der Geschäftsstelle zwar auf Webserver und E-Mail-Server zugreifen, nicht jedoch auf Daten im Fileserver.

2.2 Client-Systeme

Für die Nutzung von Cloud-Anwendungen stehen bei TeleTrusT Client-PCs/Laptops mit Netzwerk- und Internetzugang zur Verfügung. Die Clients sind mit Windows 7 und Webbrowser Internet Explorer sowie optional Google Chrome und Firefox ausgestattet.

2.3 Datenkategorien

Tabelle 2 nennt die von TeleTrusT genutzten Datenkategorien:

Nr.	Bezeichnung
D1	E-Mail innerhalb Vorstand und Geschäftsführung
D2	E-Mails (die nicht den Vorstand und die Geschäftsführung betreffen)
D3	(Verteiler)-Adresslisten
D4	Gremienarbeit (z.B. Protokolle, Einladungen)
D5	Öffentlichkeitsarbeit (z.B. Pressemitteilungen, Flyer)
D6	Öffentlichkeitsarbeit (im Vorfeld der Veröffentlichung)
D7	Interne Verwaltung (Mitgliederentwicklungen, Verträge)
D8	Finanzdaten (Rechnungen)
D9	Vorstandsdaten (z.B. Protokolle der Vorstandssitzungen, Planungsdaten)
D10	Projektarbeit (Vergütungsvereinbarungen)
D11	Dokumentenentwürfe/ gemeinsame Dokumente von Arbeitsgruppen

Tabelle 2: Datenkategorien von TeleTrusT

2.4 Genutzte Anwendungen

Die in Tabelle 3 aufgezählten Anwendungen werden derzeit bei TeleTrusT genutzt und fließen in die Betrachtung ein.

Nr.	Bezeichnung
A1	E-Mail
A2	Datenablage
A3	CRM für Kontaktdatenverwaltung (zur Zeit über Office Anwendungen abgedeckt)
A4	Office Applikationen (Textbearbeitung, Tabellenkalkulation usw.)

Tabelle 3: Von TeleTrusT genutzte Anwendungen

2.4.1 E-Mail

E-Mail ist eines der wichtigsten Kommunikationsmittel für TeleTrusT. E-Mail wird unter anderem für Kontakte zu den Mitgliedern und für die Öffentlichkeits- und Gremienarbeit verwendet.

TeleTrusT nutzt bereits einen gehosteten E-Mail-Service. E-Mails können über ein Web-Interface gelesen, bearbeitet und gesendet werden, zudem stehen die E-Mail-Daten per IMAP zur Verfügung. Mitarbeiter im Büro nutzen Microsoft Outlook über IMAP/SMTP zur Bearbeitung bzw. zum Versand von E-Mails. Über IMAP/SMTP ist auch eine Anbindung von mobilen Systemen (Smartphone, Tablet) möglich.

Mitarbeiter speichern Kontakte bzw. Kontaktlisten auf ihren Laptops und melden diese ggf. zur Pflege von Sammelverteilern an die Geschäftsstelle. E-Mailverteiler bzw. Sammel-Mailadressen werden durch die Geschäftsstelle eingerichtet und stehen den TeleTrusT-Mitarbeitern zur Verfügung. Mailadressen und E-Mails werden auf dem E-Mail-Server ge-

halten. Gemeinsame E-Mail-Ordner, Kalender mit Gruppenfunktionen und zentrale Aufgabenlisten werden nicht genutzt.

Neben Mitarbeitern können auch Mitglieder des Vorstandes E-Mail-Adressen von TeleTrusT nutzen. Für diesen Personenkreis sind gleichfalls Mailboxen im gehosteten Mailservice eingerichtet.

Die Postfächer werden technisch von der TeleTrusT-Geschäftsstelle eingerichtet und verwaltet. Es wird ein Initial-Passwort für den Benutzer gesetzt, der dieses dann ändern muss.

2.4.2 Datenablage

Daten der Datengruppen D4-D10 werden derzeit zunächst lokal auf den Laptops der Mitarbeiter gespeichert und dann manuell mit dem zentralen Fileserver synchronisiert. Diese Synchronisierung kann nur während vorhandener LAN-Verbindung erfolgen. Zusätzlich wird ein wöchentliches Backup der Daten des zentralen Fileservers erzeugt. Aktuell stehen 30 GB Speicherplatz auf dem lokalen Fileserver, sowie zusätzlich 11,6 GB bei einem externen Anbieter im Internet zur Verfügung.

Für Dokumente aus Arbeitsgruppen (Datengruppe D11) steht ein spezieller Internet-Service zur Verfügung, der aber nur anlassbezogen genutzt wird. Der Austausch solcher Dokumente zwischen Mitgliedern der Arbeitsgruppe wird regelmäßig intern in der jeweiligen Arbeitsgruppe organisiert, meist per E-Mail.

Mobile, mittels RFID-Token geschützte HDDs zur verschlüsselten Schnelldatensicherung vom Laptop stehen jedem Mitarbeiter zur Verfügung.

2.4.3 CRM

Die Kontaktdatenverwaltung als Kern-CRM-Funktion erfolgt über Office Anwendungen und deckt folgende Funktionalitäten ab:

- Adressverwaltung;
- Informationen zu Personen;
- Funktionen und Verantwortlichkeiten von Personen;
- Finanzdaten.

2.4.4 Office-Applikationen

MS Office ist lokal auf den Laptops der Mitarbeiter installiert. Entsprechende Lizenzen sind vorhanden und sollen weiterhin genutzt werden. Bearbeitete Daten werden lokal auf den Laptops gespeichert (siehe Abschnitt 2.4.2). Ein Austausch von Dateien erfolgt über E-Mail oder die Datenablage.

3 Analyse der SOLL-Anforderungen

Dieses Kapitel beschreibt den Anforderungskatalog für den Einsatz von Cloud Computing-Anwendungen in der Bundesgeschäftsstelle von TeleTrusT – Bundesverband IT-Sicherheit e.V. Die Soll-Analyse ist wie folgt strukturiert: funktionale Anforderungen, IT-Sicherheitsanforderungen, rechtliche und vertragliche Anforderungen sowie die Kosten der in der IST-Analyse definierten relevanten (Geschäfts-)Anwendungen. Neben in Absprache mit Vertretern der Geschäftsstelle von TeleTrusT festgelegten funktionalen Anforderungen stehen dabei insbesondere IT-Sicherheits- und Datenschutzaspekte im Vordergrund.

Es gelten eine Reihe von allgemeingültigen Anforderungen für TeleTrusT:
- Einsatz von Lösungen deutscher Unternehmen, die keine Nischenlösungen darstellen;
- Speicherung der Daten in Deutschland;
- deutschsprachiger Support;
- Software muss komplett in deutscher Sprache vorliegen;
- Abdeckung mindestens aller heute bei TeleTrusT verwendeten Funktionalitäten und Anwendungen (siehe IST-Analyse);
- ein sicherer Zugriff auf aktuelle Datenbestände muss jederzeit und überall möglich sein;
- Gewährleistung der Sicherheit und Kompatibilität;
- die laufenden Kosten dürfen nicht signifikant höher als derzeit ausfallen.

Einige dieser Anforderungen ergeben sich aus der TeleTrusT-Strategie z.B. im Rahmen der Initiative "IT Security made in Germany". Auch datenschutzrechtliche Aspekte (z.B. Bundesdatenschutzgesetz) spielen eine zentrale Rolle.

3.1 Funktionale Anforderungen
Der Funktionsumfang der Anwendungen soll mindestens dem bestehenden, in der IST-Analyse beschriebenen, entsprechen. In den folgenden Abschnitten werden die zusätzlichen Anforderungen aufgeführt.

3.1.1 E-Mail
Für E-Mail soll Microsoft Outlook und ein per Internet Explorer mit kompletter Funktionalität nutzbarer Webmailer unterstützt werden. Ein Adressbuch mit Im- und Exportfunktion, muss vorhanden und einfach benutzbar sein. Auf die E-Mails muss mit Smartphones (z.B. Apple iOS oder Android) von überall zugegriffen werden können. Die Anbindung von E-Mail-Clients kann alternativ per SMTP/IMAP oder über ActiveSync erfolgen.

Postfächer sollen von einem Mitarbeiter von TeleTrusT eingerichtet und verwaltet werden können. Der Zugang muss für alle Schnittstellen zum E-Mail-Server (SMTP, IMAP, Webmail, ggf. ActiveSync) Authentifizierung erfordern. Passwörter müssen durch den Benutzer änderbar sein.

Es sind 10 externe und 5 interne Accounts vorzusehen, jeweils mit einer maximalen Mailboxgröße von derzeit mindestens 5 GByte (nötigenfalls sukzessive Erweiterung vorgesehen).

3.1.2 Datenablage
Es sollen mindestens 50 GB Speicherkapazität vorhanden sein. Daten in der Datenablage (Datengruppen 4-10) sollen lokal in der Geschäftsstelle Berlin vorgehalten werden. Zusätzlich soll auf Daten über einen Cloud-Service aus dem Internet heraus zugegriffen werden können. Der Zugriff soll direkt aus Anwendungen heraus möglich sein, dazu muss der Cloud-Service z.B. als Laufwerk eingebunden werden können. Zugriffe auf diese Daten aus dem Internet erfolgen ausschließlich lesend. Ein Abgleich interner Daten mit dem Cloud-Service einmal pro Woche ist ausreichend, dieser Abgleich kann weiterhin manuell gesteuert erfolgen.

Zusätzlich soll der Cloud Service den gemeinsamen Zugriff auf Daten der Arbeitsgruppen (Datengruppe 11) ermöglichen. Dazu ist eine Berechtigungssteuerung für bis zu 500 Nutzer nötig.

3.1.3 CRM

Die wichtigste Anforderung an das CRM ist die Unterstützung der Adressverwaltung. Darüber hinaus soll CRM für TeleTrusT folgende Funktionen umfassen:

- Verwaltung der Mitgliederkontakte;
- Auswahl von Mitgliedergruppen;
- Individuelle Ansprache der Mitglieder in Serienbriefen und E-Mails;
- Verwaltung von Veranstaltungen;
- Auswertungen & Berichte über diverse Aktivitäten;
- Zentral abgelegte Dokumente.

Das CRM soll eine Doublettenprüfung unterstützen, um die Qualität der Daten durch die Identifikation und Entfernung von doppelten Datensätzen zu sichern. Es sollen maximal fünf Nutzer das CRM nutzen, je nach Lizenzmodell sind auch drei bis vier Nutzerzugänge ausreichend. Mindestens 50 verschiedene Adresslisten müssen verwaltbar sein, mit jeweils bis zu 1.500 Einträgen.

Für die volle Nutzung der CRM-Funktionalitäten, wie z.B. Serien-E-Mails, muss der Mailserver eingebunden werden können.

3.1.4 Office-Anwendungen

Aus Lizenz- und Datenschutzgründen sollen die Office-Anwendungen weiterhin nur lokal, bzw. unter Verwendung der Datenablage genutzt werden. Entsprechend werden im Folgenden auch keine Cloud-Angebote in diesem Bereich evaluiert.

3.2 IT-Sicherheitsanforderungen

3.2.1 Schutzbedarfsklassen

In Zusammenarbeit mit den Verantwortlichen von TeleTrusT wurden die Schutzbedarfsklassen gemäß folgender Tabelle erarbeitet:

Klasse	Erläuterung	
sehr hoch	Vertraulichkeit	Sehr geheime Daten. Diese sind nur einem sehr eingeschränkten Benutzerkreis zugänglich oder werden als besonders vertraulich eingestuft.
	Integrität	Nur ein sehr eingeschränkter Personenkreis darf die Manipulation der Daten veranlassen oder durchführen.
	Verfügbarkeit	Die maximale Ausfallzeit[7] darf 1 Stunde je Ausfall nicht überschreiten. Die definierte max. kumulierte Ausfallzeit: 3 Stunden je Quartal
	Mögliche Folgen eines Verstoßes: - Sehr hohe finanzielle Verluste bis hin zur existentiellen Bedrohung von TeleTrusT, Vertrauensverlust in einer sehr breiten Öffentlichkeit - Grober Verstoß gegen Gesetze	
hoch	Vertraulichkeit	Daten sind geheim und nur einem eingeschränkten Benutzerkreis zugänglich oder werden als vertraulich eingestuft.
	Integrität	Nur ein eingeschränkter Personenkreis darf die Manipulation der Daten veranlassen oder durchführen.
	Verfügbarkeit	Die maximale Ausfallzeit darf 2 Stunden je Ausfall nicht überschreiten. Die definierte max. kumulierte Ausfallzeit: 6 Stunden je Quartal

[7] Die Ausfallzeit ist definiert als die Zeit in der ein Service während der Betriebszeiten nicht zur Verfügung steht. Wartungszeiten sind generell außerhalb der Betriebszeiten.

	Mögliche Folgen eines Verstoßes: - Hohe finanzielle Verluste. Eine existentielle Bedrohung von TeleTrusT ist aber nicht absehbar - Vertrauensverlust bei einer breiten Öffentlichkeit - Verstoß gegen Rechtsvorschriften	
niedrig bis mittel	Vertraulichkeit	Die Daten sind einem breiteren Personenkreis zugänglich
	Integrität	Ein breiterer Personenkreis darf die Manipulation der Daten veranlassen oder durchführen.
	Verfügbarkeit	Die maximale Ausfallzeit darf 8 Stunden je Ausfall nicht überschreiten. Die definierte max. kumulierte Ausfallzeit: 24 Stunden je Quartal
	Mögliche Folgen eines Verstoßes : - Führt nur zu geringen Verlusten - Führt zu einem Vertrauensverlust in einer eingeschränkten Öffentlichkeit - Kein Verstoß gegen Rechtsvorschriften	

Tabelle 4: Beschreibung der Schutzbedarfsklassen

3.2.2 Anforderungen für Datenkategorien

Für die bereits in Tabelle 2 als relevant ermittelten Datenkategorien wurde durch Interview mit der Geschäftsleitung folgender Schutzbedarf ermittelt:

Nr.	Bezeichnung	Vertraulichkeit	Integrität	Verfügbarkeit	Personenbezogene Daten	Aufbewahrung	Löschfristen
D1	E-Mail innerhalb Vorstand	hoch	hoch	hoch	ja	mindestens 10 Jahre	keine
D2	Normale E-Mails	niedrig-mittel	niedrig-mittel	hoch	ja	mindestens 10 Jahre	keine
D3	(Verteiler)-Adresslisten	hoch	hoch	hoch	ja	keine	keine
D4	Gremienarbeit (Berichte, Einladungen)	hoch	hoch	hoch	nein	mindestens 10 Jahre	keine
D5	Öffentlichkeitsarbeit (Pressemitteilungen)	niedrig-mittel	niedrig-mittel	niedrig-mittel	nein	mindestens 10 Jahre	keine
D6	Öffentlichkeitsarbeit (im Vorfeld)	hoch	hoch	niedrig-mittel	nein	mindestens 10 Jahre	keine
D7	interne Verwaltung (Mitgliederentwicklungen, Verträge)	hoch	hoch	hoch	ja	mindestens 10 Jahre	Bewerbungen müssen gelöscht werden
D8	Finanzdaten (Rechnungen)	hoch	hoch	hoch	nein	mindestens 10 Jahre	Keine
D9	Vorstand	hoch	hoch	hoch	ja	mindestens 10 Jahre	Keine
D10	Projektarbeit (Vergütungsvereinbarungen)	hoch	hoch	hoch	ja	mindestens 10 Jahre	Keine
D11	Dokumentenentwürfe, gemeinsame Dokumente von Arbeitsgruppen	hoch	hoch	niedrig-mittel	ja	keine	keine

Tabelle 5: Schutzbedarf der Daten von TeleTrusT

3.2.3 Anforderungen für Anwendungen

Tabelle 6 zeigt den Schutzbedarf der betrachteten Anwendungen. Dieser wird durch Anwendung des ***Maximumprinzips***[8] ermittelt: Demnach ergibt sich der Schutzbedarf eines Systems als das Maximum der Schutzbedarfe der verarbeiteten Daten.

Nr.	Dienst	Vertraulichkeit	Integrität	Verfügbarkeit
A1	E-Mail	Hoch	Hoch	Hoch
A2	Datenablage	Hoch	Hoch	Hoch
A3	CRM	Hoch	Hoch	Hoch

Tabelle 6: Schutzbedarf der betrachteten Anwendungen von TeleTrusT

Tatsächlich sind für alle betrachteten Services im Ergebnis Vertraulichkeits-, Integritäts- und Verfügbarkeitsanforderungen hoch, obwohl für einzelne Datenkategorien niedrigere Anforderungen gelten. Dies liegt daran, dass alle Services zumindest zeitweise Daten mit hohen Anforderungen verarbeiten und bereitstellen.

3.2.3.1 Authentifizierung

Der durch Benutzername und Kennwort bereitgestellte Schutz wird allgemein als unzureichend für hohe Sicherheitsforderungen angesehen. Deshalb ist eigentlich eine starke Authentifizierung vorzusehen. Auch bei der bisherigen Lösung werden die Daten jedoch lediglich durch Benutzername und Kennwort geschützt, die meisten verfügbaren Cloud-Services bieten analog bisher keine starke Authentifizierung an.

Da diese Publikation primär aufzeigen soll, ob und in welcher Form die bisherige Lösung durch Cloud-Services abgebildet werden kann, wird deshalb zunächst auf die Forderung nach einer starken Authentifizierung verzichtet. Starke Authentifizierungsverfahren sollten dennoch baldmöglichst eingesetzt werden.

3.2.3.2 E-Mail

Die Verschlüsselung der Kommunikationskanäle (Webmailer und SMTP/ IMAP, ggf. ActiveSync) mittels SSL muss standardmäßig aktiviert sein. Der Versand und Empfang verschlüsselter und/oder signierter E-Mails alternativ per S/MIME oder GPG/PGP muss möglich sein bzw. vom E-Mail-Server unterstützt werden.

Der eingehende E-Mail-Verkehr muss durch einen Spam- und Virusfilter geschützt sein. Die Erkennungsrate soll mindestens 99% bei Spam und 99,9% bei bekannten Viren betragen. Die Falsch-Positiv-Rate soll unter 0,001% liegen. Als Spam erkannte E-Mails müssen entweder durch Verbindungsabbruch mit Fehlermeldung für den Absender erkennbar abgewiesen oder in eine Quarantäne gestellt werden. Eine Quarantäne muss, soweit vorhanden, durch den Empfänger einsehbar sein. E-Mails in der Quarantäne müssen mindestens 30 Tage aufbewahrt werden.

Alle E-Mails sind mindestens einmal täglich zu sichern und mindestens sieben Tage rückwirkend wiederherstellbar abzuspeichern. Die Funktionsfähigkeit der Wiederherstellung von E-Mails durch das Backup ist sicherzustellen.

Zusätzlich ist eine Langzeitarchivierung von E-Mail entsprechend gesetzlicher Anforderungen (bis zu 10 Jahren) erforderlich. Die Archivierung muss den Nachweis ermöglichen, dass E-Mails im Archiv unverändert abgelegt sind. Die Löschung von im Archiv abgelegten E-

[8] BSI-Standard 100-2: IT-Grundschutz-Vorgehensweise, S. 54

Mails während der vorgesehenen Aufbewahrungsfrist darf nicht möglich sein. Aufbewahrungsfristen sollten einstellbar sein, dürfen aber für bereits archivierte E-Mails nicht nachträglich verändert werden können.

3.2.3.3 Datenablage

Für lokal abgelegte Daten wie für in der Cloud abgelegte Daten müssen Rechtevergabe mittels Rollen (bspw. Geschäftsführung, Arbeitsgruppe, AG-Leitung, Gremien, usw.) und eine Zugriffskontrolle möglich und standardmäßig aktiviert sein. Eine transparente Ver- und Entschlüsselung der Daten muss standardmäßig mittels AES 256 Bit erfolgen. Der Schlüssel darf nur der entsprechenden Stelle bei TeleTrusT bekannt sein.

Eine mobile HDD zur Schnelldatensicherung mit mind. 250 GB Speicherplatz muss lokal am Fileserver in der Geschäftsstelle vorhanden sein. Diese Festplatte muss gemäß aktuellen Standards verschlüsselt werden. Ein Backup aller Daten (Datengruppen 4-11) muss mindestens wöchentlich durchgeführt werden.

3.2.3.4 CRM

Alle Änderungen im System sollen durch Protokollierung nachvollzogen werden können. Rollen und Berechtigungen sollen im CRM umsetzbar sein. Die Übertragung der CRM Daten soll über eine verschlüsselte SSL-Datenverbindung (z.B. z.B. mindestens AES 256 Bit) erfolgen.

Daten im CRM sollen mindestens wöchentlich gesichert werden. Der Export aller Daten im CRM muss über ein allgemein lesbares Format (z.B. CSV) möglich sein.

3.3 Rechtliche und vertragliche Anforderungen

Die rechtlichen Anforderungen, Risiken und sich daraus ergebenden Empfehlungen hängen unmittelbar davon ab, welche Arten von Daten durch welchen Cloud-Dienst verarbeitet werden. Zudem kommt es darauf an, ob die Übermittlung an und Verarbeitung der Daten durch den Cloud-Anbieter innerhalb des Raumes der Europäischen Union bzw. der Vertragsstaaten des Abkommens über den Europäischen Wirtschaftsraum geschehen.

Dabei sind grundsätzlich zwei rechtliche Bereiche zu trennen: Zum einen stellt sich die Frage, ob und bejahendenfalls wie ein Cloud-Dienst datenschutzrechtlich zulässig genutzt werden kann. Zum anderen ist zu klären, welche vertraglichen Regelungen zwischen Cloud-Anbieter und Cloud-Nutzer geschlossen werden sollten.

Die folgenden Ausführungen gelten für Unternehmen und andere verantwortliche Stellen mit deutschem Sitz und einer Datenverarbeitung, die bislang ausschließlich in Deutschland vorgenommen wurde.

3.3.1 Gesetzliche Anforderungen

Soweit sich der Sitz des Cloud-Anbieters und dessen Rechenzentrum in Deutschland befinden, ist deutsches Datenschutzrecht anzuwenden. Die Vorschriften des Bundesdatenschutzgesetzes (BDSG) gelten jedoch nur, wenn es sich bei den betreffenden Daten um personenbezogene oder personenbeziehbare Daten handelt.

Personenbezogene Daten sind jegliche Angaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person (§ 3 Abs. 1 BDSG). Werden durch ein Unternehmen etwa E-Mails von Mitarbeitern oder Kundendaten verwendet, handelt es sich dabei grundsätzlich um Daten mit Personenbezug. Wer solche Daten in der Cloud durch den Cloud-Anbieter erheben, verarbeiten oder nutzen lässt, ist Auftraggeber

einer sog. Auftragsdatenverarbeitung[9] (ADV) und hat gemäß § 11 BDSG folgende Pflichten zu erfüllen:

1. **Sorgfältige Auswahl** des Cloud-Anbieters: Der Cloud-Nutzer hat zumindest zu prüfen, ob der Cloud-Anbieter in der Lage ist, die nach dem Gesetz erforderlichen technischen und organisatorischen Maßnahmen einzuhalten (§ 9 BDSG und Anlage zu § 9 Satz 1 BDSG).
2. **Kontrolle der Umsetzung**: Der Cloud-Nutzer hat sich vor Beginn und regelmäßig während der Nutzung des Cloud-Dienstes von der tatsächlichen Einhaltung der beim Cloud-Anbieter getroffenen technischen und organisatorischen Maßnahmen zu überzeugen. Das Ergebnis ist zu dokumentieren.
3. Abschluss einer **Auftragsdatenverarbeitung-Vereinbarung**: Die Auftragserteilung zur Nutzung des Cloud-Dienstes hat in Schriftform zu erfolgen. Es ist also eine eigenhändige Unterschrift oder der Einsatz einer qualifizierten elektronischen Signatur erforderlich.

Welche Anforderungen an eine sorgfältige Auswahl und die Kontrollen bestehen, hängt insbesondere von den betroffenen Datenarten, den Verarbeitungszwecken, den Betroffenenkreisen sowie dem festzustellenden Risikopotenzial der Auftragsdatenverarbeitung ab. Da es aber grundsätzlich weder faktisch möglich, noch rechtlich erforderlich ist, die Kontrollen persönlich oder vor Ort vorzunehmen, können vielfach Datenschutz-Gütesiegel oder IT-Sicherheitszertifikate von unabhängigen, fachkundigen Stellen anstatt einer eigenen Prüfung herangezogen werden. Ohne Anspruch auf Vollständigkeit sind folgende Zertifikate grundsätzlich geeignet, die Erfüllung der datenschutzrechtlichen Anforderungen an die Auftragsdatenverarbeitung durch den Cloud-Anbieter glaubhaft zu machen:
- Zertifikat zur Auftragsdatenverarbeitung der datenschutz cert GmbH;
- SaaS-Gütesiegel "EuroCloud SaaS Star Audit" des EuroCloud Deutschland_eco e.V.;
- "EuroPriSe" (European Privacy Seal) des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein;
- Zertifizierung nach ISO 27001 auf der Basis von IT-Grundschutz, Bundesamt für Sicherheit in der Informationstechnologie.

Eine "Selbstzertifizierung" gilt nicht als Zertifizierung im obigen Sinne und genügt den gesetzlichen Mindestvoraussetzungen in keinem Falle. Kann der Cloud-Anbieter ein entsprechendes Zertifikat nicht vorweisen, sollte zumindest ein Testat eines unabhängigen und fachkundigen Dritten angefordert werden, das durch ein IT-Sicherheitskonzept des Cloud-Anbieters sowie ein Auditprotokoll des betrieblichen Datenschutzbeauftragten ergänzt wird. Inwieweit solche Unterlagen rechtlich hinreichend sind, sollte eingehend geprüft werden.

Die zu schließende Vereinbarung über die Auftragsdatenverarbeitung hat im Einzelnen festzulegen (§ 11 BDSG):

1. Gegenstand und die Dauer des Auftrags
2. Umfang, Art und Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen
3. Festlegung der technischen und organisatorischen Maßnahmen (gemäß § 9 BDSG),
4. die Berichtigung, Löschung und Sperrung von Daten
5. die gemäß § 11 Absatz 4 BDSG bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen

[9] Ob anstatt einer Auftragsdatenverarbeitung eine sog. Funktionsübertragung vorliegt, ist eine Frage des Einzelfalls. Liegt eine Funktionsübertragung vor, bedarf es für die Verwendung der Daten durch den Cloud-Anbieter einer gesetzlichen Erlaubnis oder einer Einwilligung des Betroffenen. Der Cloud-Anbieter wird dann selbst zur verantwortlichen Stelle für die personenbezogenen Daten des Nutzers und ist gesetzlich nicht privilegiert.

6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Die zur Auftragsdatenverarbeitung zudem zu regelnden technischen und organisatorischen Maßnahmen ("TOM", § 9 BDSG, Anlage zu § 9 BDSG) müssen ebenfalls vereinbart werden, i.d.R. als Anlage zur ADV-Vereinbarung.

"TOM" (Anlage zu § 9 BDSG)

- **Zutrittskontrolle**: Zutritt zu Datenverarbeitungsanlagen
- **Zugangskontrolle**: Nutzung der EDV nur von Befugten
- **Zugriffskontrolle**: Wirksamkeit von Zugriffberechtigungen
- **Weitergabekontrolle**: Zulässigkeit und Prüfbarkeit des Datentransportes
- **Eingabekontrolle**: Änderungsnachverfolgung
- **Auftragskontrolle**: Kontrolle der Einhaltung von Weisungen
- **Verfügbarkeitskontrolle**: Schutz vor zufälligem Untergang der Daten
- "**Trennungskontrolle**": Trennung der Daten nach Zwecken

Abbildung 2: Technische und Organisatorische Maßnahmen gemäß §9 BDSG

Zu den genannten Bereichen sind geeignete Maßnahmen zu regeln, soweit sie erforderlich sind. Erforderlich sind Maßnahmen, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht. Auch wenn Fragen der Verhältnismäßigkeit grundsätzlich einer Einzelfallbetrachtung bedürfen, gibt es hier in vielen Bereichen bereits etablierte Maßnahmen, die geeignet und nicht unvertretbar aufwändig sind. Eine erforderliche, wenn auch nicht hinreichende Maßnahme zur Gewährleistung der Zugangskontrolle kann z.B. ein sicheres, dem Stand der Technik entsprechendes Passwort-Management sein.

Es setzt sich erfreulicherweise zunehmend durch, dass die Cloud-Anbieter ihren Kunden sowohl für die Auftragsdatenverarbeitungs-Vereinbarung als auch für die Anlage zu den technischen und organisatorischen Maßnahmen Muster anbieten. Liegen solche Muster vor, sollten diese fachlich geprüft werden. Sind diese Unterlagen durch den Cloud-Nutzer zu entwerfen, kann nicht selten erfolgreich über einen Preisnachlass mit dem Anbieter verhandelt werden.

Sollte sich der Cloud-Anbieter außerhalb der EU/des EWR befinden, lässt sich Cloud Computing datenschutzrechtlich zulässig durch die Verwendung der EU-Standard-Vertragsklauseln oder der Nutzung von Binding Corporate Rules einsetzen. Bei Anbietern aus den USA ist die alleinige Unterwerfung unter die sog. Safe-Harbour-Regelungen nicht ausreichend.

3.3.2 Vertrag über die Nutzung des Cloud-Dienstes

Nicht weniger Sorgfalt ist bei der Gestaltung des eigentlichen Austauschvertrages anzuraten. Die Nutzung von Cloud-Diensten in Form von SaaS (Software as a Service) führt beispielsweise grundsätzlich zur Anwendbarkeit des Mietrechts. Anpassungsleistungen an der Software und Implementierungen hingegen können dem Werkvertragsrecht unterliegen. Kommt die entgeltliche Überlassung von Software dazu, die lokal installiert wird, kann Kaufrecht Anwendung finden.

Folglich liegen beim Cloud-Computing häufig sog. typengemischte Verträge vor. Soweit rechtlich unterschiedliche Leistungen vereinbart werden, sind deshalb stets die unterschiedlichen Rechtsfolgen zu berücksichtigen, z.B. hinsichtlich der Gewährleistung und Haftung. Auch auf die Gestaltung und Verwendung Allgemeiner Geschäftsbedingungen haben die unterschiedlichen Leistungsarten erheblichen Einfluss.

Folgende Bereiche sollten bei Verträgen über die Nutzung von Cloud-Diensten gründlich geregelt werden (Aufzählung nicht abschließend):
- Detaillierte, möglichst abschließende Leistungsbeschreibung;
- Unmissverständliche Vergütungsregelungen;
- Geplante Einbindung von Subunternehmern;
- Exakte Nutzungsrechteinräumung;
- Service-Level-Agreements (SLA) inkl. Datensicherungs- und Verfügbarkeitsregelungen;
- Regelungen zum Datenschutzrecht und zur Datensicherheit (s.o.);
- Haftung bei Datenverlust;
- Effektives Eskalationsregime;
- Exit-Klauseln/ Vertragsrückbau;
- Rechtswahl und Gerichtsstand.

3.3.3 Fazit zu rechtlichen Anforderungen

Der Cloud-Anbieter ist gründlich und rechtzeitig zu prüfen. Die vertraglichen Gestaltungsmöglichkeiten sollten genutzt werden. Dazu gibt es wider Erwarten häufig Gelegenheit. Die Anforderungen an den Datenschutz und die Datensicherheit sind penibel zu beachten.

3.4 Kostenanforderungen

Migrationskosten, inklusive Einrichtungsgebühren sollen 1.000,00 EURO nicht übersteigen. Die neue IT-Struktur wird Funktionsverbesserungen mit sich bringen, die höhere als derzeit laufende Kosten rechtfertigen. Die laufenden Kosten sollen aber insgesamt 180,00 EURO/ Monat nicht überschreiten.

4 Evaluierte Cloud-Anwendungen

4.1 E-Mail

Im Markt ist eine Fülle von Cloud-E-Mail-Angeboten vorhanden. Viele dieser Angebote richten sich primär an Privatanwender und sind aus verschiedenen Gründen (z.B. Verfügbarkeit, kein Support) für Unternehmensanwender grundsätzlich nicht zu empfehlen.

Angefragt wurden im Rahmen dieser Publikation verschiedene Anbieter von Hosted Exchange, Open Exchange und herkömmlicher Webmail/ IMAP Services. Alle Angebote wurden anhand der im Web zur Verfügung stehenden Informationen des Anbieters bewertet. Zusätzlich wurde allen Anbietern ein kurzer Katalog von Fragen per E-Mail zugeschickt:
- Was ist die vertraglich garantierte Service-Verfügbarkeit (SLA)?
- Gibt es garantierte Leistungswerte zum enthaltenen Spam- und Virenfilter?
- Wie häufig werden E-Mails gesichert, wie lange werden Backups gespeichert?

- Wird E-Mail-Verschlüsselung unterstützt, ggf. in welcher Form?
- Welche Vertragslaufzeiten werden angeboten, Kündigungsfristen?
- Auf welchem Weg können Bestandsdaten übernommen werden?
- Auf welchem Weg können Bestandsdaten exportiert werden, z.B. zum Ende eines Vertrages?

Anhand der Rückmeldungen wurden folgende Produkte in die Bewertung aufgenommen:
- 1&1: Mailexchange und Outlook Exchange;
- antispameurope: antispameurope Secure E-Mail;
- Quality Hosting: QualityExchange;
- Simple ASP: Hosted Exchange Premium.

Bei den Produkten "Outlook Exchange" von 1&1, "QualityExchange" bzw. "StandardExchange" von Quality Hosting und "Hosted Exchange Premium" von Simple ASP handelt es sich jeweils um E-Mail-Postfächer in einer gehosteten Microsoft Exchange Umgebung. Geboten wird der volle Leistungsumfang von Microsoft Exchange, u.a. mit Kalender, Aufgabenlisten, Kontaktverwaltung und öffentlichen Ordnern. Der Zugriff erfolgt über ein Web-Frontend (Outlook Web Access), einem lokal installierten Microsoft Outlook (Lizenz ist jeweils im Paket inbegriffen) oder von mobilen Systeme über SMTP/IMAP oder ActiveSync. Der Zugriff über ActiveSync erlaubt neben der Verarbeitung von E-Mail auch die Synchronisierung von Kontakten, Aufgaben und Terminen und ist derzeit im Standard z.B. von Apple iPad, iPhone und Android Smartphones enthalten.

Bei 1&1 Mailexchange handelt es sich um ein gehostetes Open Exchange, das wie Microsoft Exchange solche Features wie Kontaktverwaltung, Aufgabenlisten und Kalender enthält. Der Zugriff erfolgt gleichfalls über ein Web-Frontend, per SMTP/IMAP oder ActiveSync. Über ActiveSync können auch hier mobile Systeme oder Microsoft Outlook angebunden werden.

antispameurope Secure E-Mail enthält eine gehostete Mailbox mit Zugang über Web-Frontend sowie SMTP/IMAP. Features wie Kalender und Aufgabenlisten sind nicht vorhanden, wohl aber eine Kontaktverwaltung. Ein- und ausgehende E-Mails werden bei antispameurope Secure E-Mail als Schutz gegen Datenverluste zusätzlich zur Mailbox drei Monate lang in einem zusätzlichen "Mini-Archiv" gespeichert, aus dem sie jederzeit wieder abgerufen werden können.

Antworten der Anbieter und veröffentlichten Informationen zu den Produkten wurden getrennt nach den Kriterien "Komfort/Features" und "Sicherheit" bewertet. Hohe Bewertungen bei "Komfort/Features" erhielten die Produkte, die neben reinen E-Mail Services noch weitere Leistungen, z.B. Kalender und Aufgabenverwaltung enthalten. Produkte, die solche Elemente nicht anbieten, wurden entsprechend niedriger bewertet. Im Kriterium Sicherheit wurden Leistungen wie hohe Verfügbarkeit, kurze Backup-Intervalle, Leistungsdaten von Spamfiltern bewertet.

Es zeigt sich, dass vor allem Komfort und Features preistreibend wirken, erhöhte Sicherheit sich hingegen kaum auf den Preis auswirkt.

4.2 Datenablage

Auf dem deutschen Markt für Cloud-basierte Lösungen zur stets verfügbaren Datenspeicherung und/oder zum sicheren Backup von Daten existiert eine Vielzahl von Angeboten.
Angefragt wurden verschiedene Anbieter von Cloud-Lösungen zur Datenspeicherung. Alle Angebote wurden anhand der online zur Verfügung stehenden Informationen der Anbieter

bewertet. Zusätzlich wurde allen Anbietern ein kurzer Fragenkatalog per E-Mail zugeschickt:
- Welche Vertragslaufzeiten werden angeboten, welche Kündigungsfristen existieren?
- Kosten: Welches Angebot ist relevant? Existieren spezielle Angebote für eingetragene Vereine (gem. BGB)?
- Welche vertraglich garantierte Service-Verfügbarkeit bieten Sie an (SLA)?
- Wo werden die Daten gespeichert (Land/Länder in denen sich die Rechenzentren befinden)?
- In welchem Rechenzentrum werden die Daten gespeichert (eigene, selbst betriebene oder durch Dritte bereitgestellte Rechenzentren und Server)?
- Wird Verschlüsselung der Daten unterstützt, ggf. in welcher Form (Standard und Schlüsselstärke)?
- Wird Verschlüsselung des Kommunikationskanals unterstützt, ggf. in welcher Form (Standard und Schlüsselstärke)?
- Auf welchem Weg können Bestandsdaten, inkl. Berechtigungen, übernommen werden?
- Was ist die maximale Anzahl konfigurierbarer Nutzer (Zugriff und Berechtigungen auf Daten/Laufwerke)?
- Auf welchem Weg können Bestandsdaten exportiert werden, z.B. zum Ende eines Vertrags?
- Welche Backupintervalle existieren, wie lange werden Backups gespeichert?
- Über welche Zertifizierungen verfügt ihr Angebot?

Anhand der Rückmeldungen und den zuvor definierten Randbedingungen (insb. Sicherheit, Kompatibilität, dt. Unternehmen, keine Nischenlösungen, Speicherung in der EU, Einhaltung der Kosten) wurden folgende Produkte betrachtet:
- STRATO HiDrive Pro[10];
- CloudSafe[11];
- Deutsche Telekom - Online Backup[12];
- Unicloud UG - Online-Dateiablage[13].

Die Anforderung nach einer starken Authentifizierung lässt sich für die betrachtete geringe Nutzerzahl mit kostengünstigen Anbietern/Lösungen zum heutigen Zeitpunkt nicht realisieren. Dennoch sollen die zwei zuerst genannten Angebote, STRATO und CloudSafe, näher betrachtet werden.

STRATO ist ein in Deutschland etablierter Hosting-Provider. Die Lösung STRATO HiDrive unterstützt folgende Zugriffsprotokolle:
- SMB/CIFS: Einbindung als Festplatte, auch über VPN;
- http/https: Einloggen mit jedem gängigen Internet-Browser;
- Transparent via WebDAV (auch verschlüsselt);
- rsync (auch verschlüsselt): Synchronisation mit vorhandenen Netzwerkspeichern (NAS);
- FTP/FTPS: Übertragung von großen Datenmengen.

STRATO verfügt über eigene dedizierte Server in deutschen Hochsicherheitsrechenzentren, mit vom TÜV Süd geprüfter Datensicherheit nach ISO 27001. Es wird SSL 256 Bit (AES) bei der Datenübertragung verwendet. STRATO gibt in seinen AGB eine Verfügbarkeit von 99% im Jahresmittel für seine Systeme an.

[10] http://www.strato.de/online-speicher/firmen-speicher/
[11] https://secure.cloudsafe.com/
[12] http://geschaeftskunden.telekom.de/tsi/de/1100610/Home/Produkte-und-Loesungen/IT/IT-Anwendungen/Datensicherung/Online-Backup/
[13] http://www.unicloud.de/module/dateien

Das Angebot lässt sich auch mit clientseitiger Verschlüsselung mittels TrueCrypt nutzen. Initial können Festplatten eingesendet werden, jedoch ist fraglich, ob diese auch verschlüsselt eingebunden und vom Kunden entsperrt werden können.

Das Preismodell für STRATO HiDrive Pro mit 1000 GByte und ohne Datenverkehrslimit: Einrichtungsgebühr (einmalig) 9,90 EURO, monatlich 49,90 EURO bei 12 Monaten Vertragslaufzeit. Dies beinhaltet bis zu 25 Nutzer und bis zu 5 Administratoren.

Das Portfolio des jungen Unternehmens CloudSafe (gegründet 2009) bietet eine Datenablage und zugehörige, ergänzende Dienstleistungen an. Jegliche Daten werden verschlüsselt abgelegt. Administratoren von CloudSafe haben keinen Zugriff auf die Inhalte und können auch den Zugang nicht wiederherstellen, falls das Passwort zum Schlüsselspeicher verloren geht. Für diesen Fall ist die Wiederherstellung durch mehrere Personen gemeinsam möglich.

Der Zugriff auf Daten erfolgt per CloudSafe Client (Windows 7, Vista, XP, iPhone, iPad; kostenfrei) oder transparent per WebDAV über SSL, dadurch ist der Zugriff von fast allen Plattformen aus möglich. Dateien können direkt im Online-Speicher bearbeitet werden. Authentifizierung ist lediglich mittels Benutzername/Passwort möglich, die Passwörter werden automatisch generiert. Verschiedene sog. "Safes" lassen sich einrichten und mit individuell abgestimmten Zugriffsrechten für verschiedene Personenkreise versehen.

CloudSafe ist zertifiziert von TRUSTe und speichert die Daten seiner Kunden auf eigenen Systemen in einem ISO27001 konformen Rechenzentrum in Frankfurt. CloudSafe gibt in seinen AGB eine durchschnittliche jährliche Erreichbarkeit von 99,8% an. Ob das gleichzusetzen ist mit der Verfügbarkeit der gespeicherten Daten, wird nicht angegeben.

Das Preismodell für CloudSafe: für jeden Benutzer muss eine Lizenz erworben werden, allerdings können Dritten Zugriffsrechte auf gespeicherte Daten eingeräumt werden. Eine kostenlose Nutzung beinhaltet 2 GB Speicherplatz. Für 5 GB Speicherplatz fallen 29,90 EURO pro Jahr und Benutzer an, 50 GB Speicherplatz kosten 79,90 EURO pro Jahr und Benutzer.

Letztlich erfüllt keines der Angebote die Anforderungen aus Sicherheitssicht vollständig, insbesondere vollständige Ende-zu-Ende-Verschlüsselung und starke Authentifizierung. Auch die Anforderungen hinsichtlich Verfügbarkeit des Services werden von beiden Anbietern nicht gewährleistet. Grundsätzlich bietet CloudSafe ein signifikant höheres Sicherheitsniveau, sowohl hinsichtlich Schutz der Daten als auch hinsichtlich Verfügbarkeit, das geforderte Sicherheitsniveau kann von STRATO HiDrive nur in Verbindung mit TrueCrypt erfüllt werden. Der Einsatz von TrueCrypt reduziert allerdings den Komfort und erschwert den Zugriff in der täglichen Arbeit. Die höhere Sicherheit spiegelt sich im Preis wieder: CloudSafe ist je GB Speicherplatz deutlich teurer als STRATO HiDrive.

4.3 CRM

Angefragt wurden unterschiedliche in Deutschland ansässige CRM-as-a-Service Anbieter. Alle in Frage kommenden Angebote wurden anhand der im Web zur Verfügung stehenden Informationen sowie einer Selbstauskunft bewertet. Dazu wurde den im Vorfeld ausgesuchten Anbietern ein kurzer Katalog von Fragen per E-Mail zugeschickt:

- Wird Veranstaltungs- und Seminarplanung, sowie Beitragsverwaltung und Abrechnung unterstützt?
- Könnten Kontakte, Termine, Aufgaben usw. aus Ihrem CRM System z.B. mit einem mobilen Endgerät synchronisiert und offline genutzt werden?

- Wird die Adressüberprüfung und Dubletten-Erkennung bei der Eingabe der Kontaktdaten durchgeführt?
- Vertraglich garantierte Service-Verfügbarkeit (SLA)?
- Welche Vertragslaufzeiten und Kündigungsfristen werden angeboten?
- In welchem Rechenzentrum werden die Daten gespeichert?
- Backupintervalle, wie lange werden Backups gespeichert?
- Auf welchem Weg können Bestandsdaten exportiert werden, z.B. zum Ende eines Vertrags?

Aufgrund der Rückmeldungen fließen TecArt-CRM Mobile und CAS PIA in die Bewertung ein.

Die grundlegenden Funktionalitäten, wie Kontakt-, Termin und Dokumentenverwaltung sind bei allen untersuchten Angeboten im Grundpreis vorhanden. Standard scheint auch die Adressüberprüfung und Dubletten-Erkennung bei der Eingabe der Kontaktdaten beim Adressimport zu sein.

Weitere von TeleTrusT gewünschte Funktionen wie die Auswahl der Mitgliedergruppen oder Auswertungen und Berichte über diverse Aktivitäten sind z.B. bei TecArt-CRM Mobile mit einem Aufpreis möglich. Die Unterschiede liegen auch bei der Unterstützung der Veranstaltungs- und Seminarplanung – diese werden bei CAS PIA von der Stange (CAS PIA) angeboten.

CAS PIA unterstützt darüber hinaus die Planung und Verwaltung von Veranstaltungen mit einer direkten Einsicht in die Teilnehmerliste und ermöglicht beim Anlegen von Aufgaben diese an weitere Mitarbeiter zu delegieren. Je nachdem wie sensibel die verwalteten Daten sind, besteht die Möglichkeit nur bestimmte Teilinformationen freizugeben.

Die untersuchten Angebote unterscheiden sich bezüglich der Synchronisation mit mobilen Geräten:
- Bei TecArt-CRM Mobile können Kontakte, Termine, Aufgaben usw. aus dem CRM System mit allen gängigen Smartphones durch komplett integrierte Pushdienste synchronisiert und durch den Offlineclient für Windows-Rechner offline genutzt werden.
- CAS PIA erlaubt die Synchronisation der Kontakte, Termine und Aufgaben mit einem mobilen Endgerät über "mobile sync". Die neuen oder geänderten Daten, die auf dem mobilen Gerät eingegeben wurden, werden synchronisiert sobald der Internetzugang zur Verfügung steht.

Die weiteren Unterschiede sind bei den Vertragslaufzeiten, Backups, Zertifizierungen und Exportmöglichkeiten der Bestandsdaten festzustellen:
- TecArt-CRM Mobile garantiert eine Service Verfügbarkeit von 98% im Jahresmittel vertraglich in SLAs. Es werden 1 Monat, 6 Monate oder 12 Monate Vertragslaufzeiten angeboten. Die Daten werden im Rechenzentrum von Lambdanet in Erfurt oder in einem vom Kunden/Partner favorisierten Rechenzentrum verarbeitet. Backup wird täglich durchgeführt, mit Vorhaltung für mindestens 7 Tage. Längere Vorhaltung ist nach separater Vereinbarung möglich. Bestandsdaten können durch Import bspw. via CSV, vorhandene Outlook-Importer, oder direkter Import bei vorhandener Schnittstelle des anderen Systems übernommen werden. Bestandsdaten werden, z.B. zum Ende eines Vertrags auf einer CD oder DVD bereitgestellt.
- Die CAS Software AG gewährleistet im Jahresmittel eine Verfügbarkeit von 99%. Hiervon ausgenommen sind Zeiten, in denen die Server aufgrund von externen Störungen des Internets nicht erreichbar sind. Der Vertrag läuft auf unbestimmte Dauer, kann vom Kunden aber mit einer Frist von 10 Tagen zum Ende eines jeden Kalendermonats ge-

kündigt werden. CAS PIA besitzt Sicherheitsfunktionen wie ein Rechtesystem für Regelung der Zugriffsrechte bis auf Datensatzebene und ein Journal für die Nachverfolgung aller Änderungen bei jeder Aktivität. Die physikalische Sicherheit der Daten wird durch die Verwendung von RAID-Systemen und regelmäßigen, inkrementellen täglichen Backups oder wöchentlichen Voll-Backups der Daten gewährleistet. PIA kann auch Benutzerprofile und Gruppen bilden (z.B. Geschäftsleitung, Assistenz). CAS PIA wird von InterNetX, einer Mehrheitsbeteiligung der United Internet AG, im eigenen nach ISO/IEC 27001, ISO 9001 und BS 7799 zertifizierten Rechenzentrum in München betrieben. Die Übertragung aller Daten erfolgt über eine verschlüsselte SSL-Datenverbindung (128-Bit-Schlüssel). Ein Export der im Programm eingegebenen Daten ist im CSV-Format jederzeit möglich. Das Dokumentenarchiv kann optional mit exportiert werden. TecArt-CRM Mobile wurde mit dem Publikumspreis "CLOUD AWARD 2011" ausgezeichnet. Darüber hinaus hat TecArt-CRM Mobile das Qualitätszertifikat "Trust in Cloud" vom SaaS-EcoSystem e.V. erhalten.

Die Kosten der Lösungen variieren etwas:
- TecArt-CRM bietet die Grundfunktionalitäten (Kontakt-, Termin-, Aufgaben und Dokumentenverwaltung, E-Mail Management) ihrer SaaS Lösung zu einem Grundpreis von 20,00 EURO pro Nutzer und Monat. Zusätzliche Funktionen können dazu gebucht werden, in der Regel zum Preis von 2,50 EURO je Funktion, Nutzer und Monat.
- Das Preismodell für CAS PIA: für jeden Benutzer muss eine Lizenz erworben werden. Preislich liegt eine solche Lizenz bei 19,90EURO pro Benutzer je Monat.

CAS PIA bietet einen kostenlosen 30 Tage-Test der Lösung an.

5 Konzept für Cloud Anwendungen für TeleTrusT

5.1 Konzept für die ausgewählte Lösung

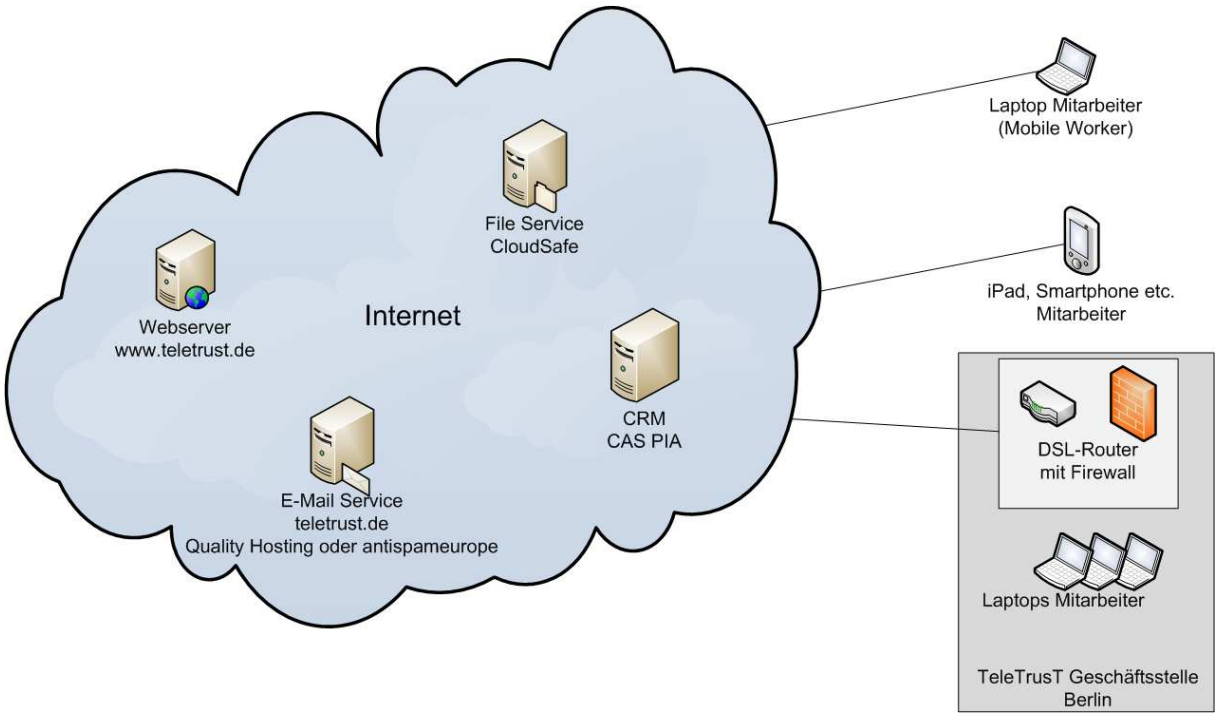

Abbildung 3: IT-Konfiguration von TeleTrusT bei konsequenter Nutzung von Cloud-Services

Bevor auf einzelne Aspekte der gewählten Lösung eingegangen wird, folgende Anmerkungen:

1. Grundsätzlich ist aus Sicherheitssicht eine starke Authentifizierung empfehlenswert. In der Praxis sind die Realisierungsmöglichkeiten aber vor allem für kleine Unternehmen begrenzt, und zwar ganz unabhängig davon, ob die Lösung intern im Unternehmen oder in der Cloud betrieben wird.
2. Die gewählte Lösung sieht eine Speicherung von Daten ausschließlich in Deutschland vor, auch wenn nach aktuellem Stand aus rechtlicher Sicht auch die Speicherung in anderen Ländern der EU möglich wäre.
3. Sicherheitsanforderungen werden höher gewichtet als Anforderungen an den Komfort einer Lösung.

5.1.1 E-Mail

Als Lösungen mit dem höchsten Sicherheitsniveau entsprechend der Bewertung der im Markt verfügbaren Angebote (Abschnitt 4.1) kommen "QualityExchange" von Quality Hosting und antispameurope Secure E-Mail in die Auswahl. Beide Produkte erfüllen die Anforderungen u.a. hinsichtlich Verfügbarkeit, Spamschutz, und Backup. Die Entscheidung für eine dieser beiden Lösungen kann abhängig vom Bedarf nach zusätzlichen Features in Relation zum Preis getroffen werden.

5.1.2 Datenablage

Keines der untersuchten Cloud-Angebote erfüllt vollständig die Anforderungen hinsichtlich Sicherheit und Verfügbarkeit der Daten. Datenablage in der Cloud ist besonders dann empfehlenswert und sinnvoll, wenn die Zugriffe auf diese Daten vorwiegend aus dem Internet, d. h. außerhalb der Büroumgebung bzw. des lokalen Netzes erfolgt. Bei TeleTrusT werden interne Daten vorwiegend in der Geschäftsstelle bearbeitet. Nur gelegentlich erfolgt ein lesender Zugriff aus dem Internet. Mit Blick auf die Sicherheitsanforderungen wird deshalb auch weiterhin die Ablage in einem intern betriebenen Datenspeicher empfohlen. Zusätzlich soll ein regelmäßiger Abgleich der Daten mit einem Cloud-Datenspeicher erfolgen. Der Cloud-Datenspeicher stellt dann die Daten zum einfachen Zugriff aus dem Internet bereit und dient gleichzeitig als Backup.

Der Cloud-Datenspeicher kann gleichzeitig als Ablage für Daten von Arbeitsgruppen genutzt werden. In diesem Fall erfolgt die Ablage direkt im Cloud-Datenspeicher. Da die Anforderungen hinsichtlich Verfügbarkeit bei dieser Nutzung geringer sind, als bei intern genutzten Daten, ist eine zusätzliche Ablage im internen Datenspeicher nicht erforderlich.

Empfohlen wird die Nutzung von CloudSafe als Cloud-Datenspeicher. Die Nutzung von STRATO HiDrive in Verbindung mit TrueCrypt würde als Backup genügen, ein einfacher Zugriff auf die Daten in der Cloud wäre aber deutlich erschwert.

5.1.3 CRM

Alle im Abschnitt 4.3.3 vorgestellten CRM Lösungen garantieren die Anwendbarkeit des Bundesdatenschutzgesetzes (BDSG) durch die Datenspeicherung in Deutschland. CAS PIA läuft in einem nach ISO 27001 zertifiziertem Rechenzentrum. Des Weiteren verfügt CAS PIA über ein granulares Rechtesystem, ein Journal für die Nachverfolgung aller Änderungen und einen "Papierkorb".

CAS PIA und TecArt-CRM erfüllen beide weitgehend die funktionalen TeleTrusT-Soll-Anforderungen. Beide Lösungen decken die Anforderungen hinsichtlich Integrität und Vertraulichkeit ab, nicht jedoch die Anforderungen hinsichtlich Verfügbarkeit. Die vom Anbieter

garantierte Verfügbarkeit beträgt bei CAS PIA 99%, bei TecArt 98%, entsprechend maximalen Ausfallzeiten von ca. 21 Stunden bzw. 42 Stunden im Quartal.

Mit Blick auf den Preis beider Lösungen in Relation zu den angebotenen Features wird mit den o.a. Einschränkungen der Einsatz von CAS PIA empfohlen.

5.1.4 Fazit zu den ausgewählten Lösungen

Die Betrachtung hat gezeigt, dass keine der angebotenen Lösungen alle Sicherheitsanforderungen vollständig erfüllt. Vor allem starke Authentifizierung und durchgängige Verschlüsselung von Daten sind bislang in Cloud-Angeboten praktisch nicht zu akzeptablen Preisen erhältlich. Bei CRM und Datenablage sind auch die von den Anbietern angegebenen Verfügbarkeiten geringer als gefordert. Allerdings wird schon für die bisher genutzten Lösungen keine bestimmte Verfügbarkeit garantiert. Die Ist-Situation in Bezug auf Verfügbarkeit ist also eher schlechter als mit den betrachteten Cloud-Angeboten.

5.2 Migration

Zur Migration bestehender Daten in das neue E-Mail-System wird Outlook eingesetzt. Dazu werden während der Migration beide Mailsysteme parallel betrieben. Die Migration nehmen die Nutzer in Outlook durch einfaches Verschieben bzw. Kopieren von E-Mails von einem in den anderen Server vor. Die gewählten Anbieter unterstützen zwar den Import von E-Mail-Daten per PST-Datei, dieser erzeugt letztlich aber mindestens den gleichen internen Aufwand und höhere Gesamtkosten als das gewählte Verfahren.

Die Übernahme der Daten in den Cloud-Speicher erfolgt durch Abgleich der lokalen Daten mit dem Cloud-Datenspeicher über WebDAV.

CRM Bestandsdaten werden über CSV-Dateien in das neue System eingelesen. Zusammenfassend kann festgestellt werden, dass die Migration in die Cloud mit relativ geringem Aufwand zu bewältigen ist.

5.3 Abschätzung der Kosten und Aufwände

Dienst	**Anbieter/Lösung**	**Kosten für Migration**	**Laufende Kosten (monatlich)**
E-Mail (inkl. Archiv)	Quality Hosting: StandardExchange	---	9,79 EURO/ Benutzer
	antispameurope secure email	---	6,90 EURO/ Benutzer
Datenablage	CloudSafe	---	79,90 EURO (50 GB)
CRM	CAS PIA	---	19,90 EURO/ Benutzer
Summe (3 Benutzer)		**---**	**160,30 - 168,97 EURO**

Tabelle 7: Überblick über Kosten der gewählten Lösungen

Hinzu kommen nicht genau bezifferbare, aber als niedrig eingeschätzte Kosten für interne Aufwände bei der Migration.

6 Restrisikoanalyse

Der Einsatz von Cloud-Anwendungen ist mit spezifischen Risiken verbunden, welche gesondert bewertet werden müssen:

Finanzielle und operative Risiken umfassen insbesondere unerwartet hohe Umstellungs- und Integrationskosten sowie die mangelnde Qualität des erbrachten Cloud-Dienstes. Durch die Vorauswahl von Lösungen mit kompatiblen Schnittstellen zu bestehenden Systemen können unerwartet hohe Kosten weitgehend ausgeschlossen werden. Zudem wurden nur Lösungen von Anbietern betrachtet, welche einen hohen Service Level vertraglich garantieren und für eine Nichteinhaltung haftbar gemacht werden können. Eine weitere Basisanforderung war, dass die laufenden Kosten der eingesetzten Cloud-Anwendungen bisherige Kosten nicht übersteigen. Dies wurde durch eine systematische Kostenbewertung sichergestellt.

Das **strategische Risiko** einer Abhängigkeitsbeziehung zum Cloud-Anbieter (Vendor Lock-In) wird im vorliegenden Fall als gering bewertet. Zum einen wurden keine anbietereigenen Nischenlösungen sondern nur standardisierte Anwendungen betrachtet. Zum anderen wurde bei der Auswahl der Cloud-Anwendungen auf standardisierte Datenexportschnittstellen geachtet, was den Wechsel zu anderen Anbietern deutlich vereinfacht.

Soziale Risiken wie Mitarbeiterwiderstände oder negative Presse aufgrund der Auslagerung einzelner Anwendungen zu Drittanbietern werden aufgrund der Innovatorenfunktion von TeleTrusT im untersuchten Fall nicht erwartet. Abhängig von der jeweils individuellen Organisationskultur ist dies jedoch im Einzelfall zu bewerten.

Desweiteren verbleiben Cloud-spezifische **Sicherheits- und IT-Compliance-Risiken**. Ein wesentliches Problem sind hierbei die Gefahr der mangelnden Datensicherheit sowie mögliche Verstöße gegen geltendes Datenschutzrecht. Die Beschränkung auf deutsche Anbieter mit verpflichtender Datenspeicherung in Deutschland garantiert die Anwendbarkeit des BDSG. Zudem sichern sämtliche ausgewählten Anbieter umfassende Datensicherheit zu, was datenbezogene Risiken weiter reduziert. Als grundsätzliches Problem verbleibt jedoch die Auditierbarkeit der Anbieter der eingesetzten Cloud-Dienste, auf welche bereits in Abschnitt 3.3 hingewiesen wurde. Da die migrierten Anwendungen für Datenhaltung, CRM und Kommunikation essenziell für die Geschäftstätigkeit des Verbandes sind, beinhalten die Service Level-Vereinbarungen entsprechend sehr hohe Verfügbarkeitsanforderungen, denen der jeweilige Anbieter nachkommen muss. Sollten bestimmte Cloud-Dienste dennoch ausfallen, z.B. im Katastrophenfall, so muss zusätzlich ein schnellstmögliches Wiederanlaufen garantiert werden, damit der operative Betrieb fortgesetzt werden kann. Aus diesem Grund wurden ausschließlich Produkte mit integrierten Backup-Lösungen ausgewählt.

Ein hohes Bedrohungspotenzial entsteht durch die internetbasierten Schnittstellen der Cloud-Anwendungen, welche das System so einem potenziell sehr hohen Personenkreis zugänglich machen. Diese Schnittstellen müssen technisch sicher implementiert und um eine effektive Zugriffskontrolle ergänzt sein, um unautorisierte externe oder anbieterinterne Zugriffe oder gar böswillige Angriffe zu unterbinden. Bei fehlenden sicherheitsbezogenen Zertifizierungen der Anbieter muss auf eine technisch hinreichend sichere Implementierung der System- und Benutzerschnittstellen vertraut werden.

Ein weiteres Restrisiko besteht in der fehlenden starken Benutzerauthentifizierung. Da sich der Zugriff auf die Cloud-Anwendungen auf eine passwortbasierte Authentifizierung stützt und eine starke Authentifizierung mit den ausgewählten Lösungen nicht realisiert werden kann, ist die Verwendung von hinreichend komplexen Passwörtern und ein sicherer Um-

gang mit diesen essenziell für eine effektive Zugriffskontrolle und somit insbesondere für die Vertraulichkeit und Integrität der durch die Cloud-Anwendungen verarbeiteten Daten.
Weiterhin muss für den sicheren Einsatz von Cloud-Anwendungen garantiert werden, dass die jeweiligen Client-Systeme selbst sicher sind. Hierfür sind entsprechend Firewall- und Anti-Schadsoftwareanwendungen auf den Client-Systemen bereitzustellen. Diese können selbst wieder als Cloud-Anwendung bezogen werden. In diesem Fall spricht man von Security-as-a-Service. Beispielhaft seien hierzu folgende Lösungen genannt:

- Panda Security Cloud Internet Protection;
- Symantec Web Security.cloud.

Aufgrund des bestehenden Einsatzes lokaler Sicherheitsanwendungen bei TeleTrusT wird allerdings auf die weitere Betrachtung von Security-as-a-Service-Anwendungen verzichtet.

7 Handlungsempfehlungen für Verbände und KMU

Dass Cloud-Angebote hinsichtlich Funktionalität oft mehr bieten, als zu vergleichbaren Kosten betriebene interne Lösungen, hat diese Publikation bestätigt. Die Untersuchung hat aber auch gezeigt, dass viele Anbieter sich noch schwertun, konkrete Aussagen zur Sicherheit und Verfügbarkeit ihrer Services zu machen, übrigens ganz unabhängig von der Größe der Anbieter. Kleine Organisationen können oft keine besonderen Bedingungen und SLAs mit den Anbietern aushandeln, deshalb müssen sie die Bedingungen der Standardangebote sorgfältig prüfen.

Die Nutzung von Cloud Services ändert nämlich nichts an der unternehmerischen Verantwortung für den Datenschutz. Die Organisation ist und bleibt der "Herr der Daten" und somit für die Authentizität, Integrität, Verfügbarkeit und Vertraulichkeit der Daten voll verantwortlich, genauso wie im Fall eines Outsourcings. Diese Verantwortung kann keine Organisation auf einen Cloud-Anbieter übertragen. Das Bundesdatenschutzgesetz (BDSG) verpflichtet Organisationen zur "sorgfältigen Auswahl" des Cloud-Providers, sowie zur Überprüfung der von ihm durchgeführten Datenschutzmaßnahmen. Art und Umfang der übertragenen Aufgaben und Verteilung der Verantwortung muss in einem Vertrag über "Auftragsdatenverarbeitung" geregelt werden. Optimalerweise verfügt der Cloud-Anbieter über ein Zertifikat, das die Einhaltung hinreichender Datenschutzstandards bestätigt. Bisher sind aber nur sehr wenige Anbieter zertifiziert.

Ob ein Cloud-Service tatsächlich höhere oder schlechtere Sicherheit bietet als eine intern betriebene Lösung, muss deshalb im Einzelfall untersucht und abgewogen werden. Die in dieser Publikation verfolgte Vorgehensweise kann als Beispiel dienen:

1. Aufnahme des Ist-Zustands; wichtig sind Informationen über Art und Umfang der derzeitigen Nutzung
2. Analyse der Anforderungen aus funktionaler Sicht, rechtlicher Sicht, Kostensicht und Sicht der IT-Sicherheit, bei letzterer kann die Aufstellung der Schutzbedarfsklassen (entsprechend Tabelle 4 nützlich sein
3. Evaluierung relevanter Cloud-Angebote anhand der Anforderungen aus Schritt 2, die in Kapitel 4 in dieser Publikation genutzten Fragenkataloge können als Anhaltspunkt diesen. Bei der Evaluierung sollte der Ist-Zustand nicht aus den Augen verloren werden. Selbst wenn evaluierte Angebote die Sicherheits-Anforderungen nicht vollständig erfüllen, kann die gebotene Sicherheit dennoch besser sein, als bei der installierten Lösung.
4. Auswahl geeigneter Angebote und Entscheidung

5. Vertragsabschluss mit klaren SLA und Vereinbarung zur Auftragsdatenverarbeitung gemäß BDSG
6. Umsetzung der Lösung
7. Aufnahme der verbleibenden Risiken und Ableitung von Maßnahmen zur Minderung der verbleibenden Risiken.

8 Forderungen an Cloud-Anbieter

Cloud Computing ist den Kinderschuhen entwachsen und beginnt, breite Anwendung zu finden. Die Sicherheit von Cloud-Angeboten ist nicht a priori schlecht, vielmehr ist vielfach eine höhere tatsächliche Sicherheit festzustellen, als bei in KUM intern betriebenen Lösungen. Allerdings gibt es Lücken. Deshalb sind Cloud-Anbieter aufgerufen, die in der Publikation aufgezeigten Mängel bei Cloud-Angeboten zu beheben. Als notwendig werden folgende Verbesserungen der Angebote erachtet:

1. Starke Authentifizierung
2. Ende-zu-Ende Verschlüsselung mit starken Verschlüsselungsverfahren
3. Tatsächlichen Ort der Speicherung (z.B. Deutschland oder EU) mindestens vertraglich festlegen, idealerweise für den Kunden wählbar
4. Verträge nach deutschem Recht anbieten, insbesondere Anlage zur Auftragsdatenverarbeitung gemäß BDSG
5. Klare und leicht auffindbare Leistungsangaben (SLA), z.B. hinsichtlich Verfügbarkeit der Services
6. Unabhängige Prüfung der Einhaltung von Datenschutzbestimmungen, mit Prüfzertifikat.

Abkürzungsverzeichnis

ActiveSync	Protokoll zum Austausch von Daten mit MS Exchange
AES	Advanced Encryption Standard
AG	Arbeitsgruppe
BDSG	Bundesdatenschutzgesetz
BSI	Bundesamt für Sicherheit in der Informationstechnik
COBIT	Control Objectives for Information and Related Technology
CRM	Customer Relationship Management
EU	Europäische Union
GPG	GNU Privacy Guard
IaaS	Infrastructure as a Service
IDS	Intrusion Detection System
IMAP	Internet Message Access Protocol
IPS	Intrusion Protection System
ISO	International Organization for Standardization
ITSMIG	"IT Security made in Germany" (TeleTrusT-Qualitätszeichen)
KMU	Kleine und mittlere Unternehmen
NIST	National Institut of Standards and Technology
PaaS	Platform as a Service
PGP	Pretty Good Privacy
PKI	Public-Key-Infrastruktur
POP3	Post Office Protocol
RAID	Redundant Array of Independent Disks
SaaS	Software as a Service
SLA	Service Level Agreements
S/MIME	Secure/ Multipurpose Internet Mail Extensions
SMTP	Simple Mail Transfer Protocol
SSH	Secure Shell
SSL	Secure Sockets Layer
TLS	Transport Layer Security
VPN	Virtual Private Network

TeleTrusT – Bundesverband IT-Sicherheit e.V.

Der Bundesverband IT-Sicherheit e.V. (TeleTrusT) ist ein Kompetenznetzwerk, das in- und ausländische Mitglieder aus Industrie, Verwaltung und Wissenschaft sowie thematisch verwandte Partnerorganisationen umfasst. TeleTrusT bietet Foren für Experten, organisiert Veranstaltungen bzw. Veranstaltungsbeteiligungen und äußert sich zu aktuellen Fragen der IT-Sicherheit. TeleTrusT ist Träger der "TeleTrusT European Bridge CA" (EBCA; Bereitstellung von Public-Key-Zertifikaten für sichere E-Mailkommunikation), des Expertenzertifikates "TeleTrusT Information Security Professional" (T.I.S.P.) sowie des Qualitätszeichens "IT Security made in Germany". Hauptsitz des Verbandes ist Berlin. TeleTrusT ist Mitglied des European Telecommunications Standards Institute (ETSI).

Kontakt:

TeleTrusT – Bundesverband IT-Sicherheit e.V.
Dr. Holger Mühlbauer
Geschäftsführer
Chausseestraße 17
10115 Berlin
Tel.: +49 30 4005 4306
Fax: +49 30 4005 4311
http://www.teletrust.de

TeleTrusT
Pioneers in IT security.