Fraunhofer
SIT

FRAUNHOFER-INSTITUT FÜR SICHERE INFORMATIONSTECHNOLOGIE

UNTERSUCHUNG DER SICHERHEIT DES IAAS-ANGEBOTS »FUJITSU CLOUD IN CENTRAL EUROPE«

IRYNA TSVIHUN, MARCEL KULICKE

05/2011

Executive Summary

Cloud Computing bietet neue Chancen und vielfältige Vorteile für Unternehmen und speziell für KMUs. Die Organisationen profitieren von Kostenersparnissen, zunehmender Flexibilität der Unternehmens-IT, aber auch von einem möglichen Zugewinn an Sicherheit, der gerade für kleinere Unternehmen von großem Nutzen sein kann und somit eine höhere Fokussierung auf das eigentliche Kerngeschäft und den Ausbau eigener Wettbewerbsvorteile ermöglicht.

Sicherheitsbedenken sind dabei die größten Hindernisse bei der verbreiteten Nutzung von Cloud-Computing-Angeboten. Da die Sicherheit Vertrauenssache ist und „das Vertrauen auf überprüfbaren und durchgehend sicheren Systemen beruht“[1], ist eine Überprüfung der Umgebung durch unabhängige Dritte von großer Bedeutung, insbesondere unter der Prämisse, dass nicht jeder potenzielle Kunde ausreichende Kenntnisse im Sicherheitsumfeld besitzt und die separate Überprüfung eine größere organisatorische Herausforderung darstellen würde.

Das vorliegende Whitepaper untersucht nach festgelegten Kriterien, die aus den Mindestsicherheitsanforderungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) und der Fraunhofer-Institut SIT München Cloud-Sicherheitsstudie hervorgehen, die Güte der Sicherheitsmaßnahmen des IaaS-Angebots „Fujitsu Cloud in Central Europe“ in den Bereichen Infrastruktur, Administration, sowie Compliance und Audit. Als Basis dienen die dem Fraunhofer-Institut SIT München zur Überprüfung von Fujitsu bereitgestellten Informationen und Interviews mit Verantwortlichen. Im Rahmen dieser Untersuchung wurden keine Penetrationstests und Schwachstellenanalysen durchgeführt und demzufolge können keine Aussagen zur Qualität der technischen Umsetzung der Maßnahmen getroffen werden.

Die Studie erbrachte dabei folgende Ergebnisse: Die Fujitsu Technology Solutions GmbH und ihre Tochter TDS AG stellen Maßnahmen bereit, die den überwiegenden Teil des studienspezifischen Gesamtfragenkatalogs an die IT-Sicherheit der Cloud-Systeme funktional abdecken und teilweise darüber hinaus gehende Schritte beinhalten. Besonders zu bemerken sind die Angaben zu den Sicherheitsvorkehrungen im Bereich der Infrastruktur, wie z.B. physikalische Sicherheit, im Monitoring und Incident Management, sowie die hohe Anzahl an Zertifizierungen. Vom Fraunhofer-Institut SIT München wurden darüber hinaus Verbesserungspotenziale identifiziert, die insbesondere KMUs zugutekommen würden, wie z.B. die Bereitstellung von Security Best Practices zu Konfiguration und Betrieb. Zusammenfassend können viele der von Fujitsu realisierten Sicherheitsmaßnahmen ökonomisch und personell gesehen wahrscheinlich nicht von einem üblichen KMU durchgeführt werden.

Des Weiteren werden über die optionalen Sicherheitsdienste und die Handlungsempfehlungen für Kunden Möglichkeiten zur weiteren Verbesserung der Sicherheit aufgezeigt. Den Abschluss bilden die Sicherheitstrends im Cloud Computing, die vor allem von Tendenzen wie einer Zunahme der Industriespionage, einer Industrialisierung der Hacker und der Consumerization der IT vorangetrieben werden. Dies zeigt deutlich, dass die Erfüllung eines hohen Sicherheitsniveaus ein andauernder Prozess ist, der einen hohen Stellenwert einnehmen sollte und immer wieder beobachtet, überdacht und verbessert werden muss.

[1] Leitgedanke des Bundesministeriums für Bildung und Forschung (BMBF)

Inhaltsverzeichnis

1 Einleitung

Zu den häufigsten Ursachen, die zur Verzögerung der breiten Nutzung von Cloud-Computing-Angeboten führen, zählen Sicherheits- und Datenschutzbedenken. Dahinter verbergen sich unterschiedliche Herausforderungen im Cloud Computing, wie die Erfüllung der klassischen Schutzziele (Vertraulichkeit, Verfügbarkeit, Integrität) sowohl auf der Anwender- als auch auf der Anbieterseite, IT-Governance, Compliance und Datenschutzbestimmungen, sowie Kontrollverlust der Daten, fehlende Standardisierung und Performanz der Cloud-Services.

Diese Bedenken sind oft auf die Informationsasymmetrien zwischen dem Cloud-Anbieter und dem Cloud-Nutzer zurückzuführen. Cloud-Anbieter geben oft nur ein Teil der relevanten Informationen im Bereich der Sicherheitsmaßnahmen an die Cloud-Nutzer weiter. Diese, insbesondere KMUs, können die Sicherheitsvorkehrungen von Seiten des Cloud-Anbieters, sowie das Sicherheitsniveau im eigenen Unternehmen meistens nicht ausreichend beurteilen und bewerten. Dies führt dazu, dass Cloud-Angebote aus der Sicherheitsperspektive oft schwierig zu vergleichen sind. Die vorliegende Sicherheitsuntersuchung möchte diese Informationsasymmetrien verringern.

Das Fraunhofer-Institut für Sichere Informationstechnologie (SIT) München hat anhand seiner Sicherheitstaxonomie [1] und mit Hilfe der Mindestsicherheitsanforderungen an Cloud Computing-Anbieter des Bundesamts für Sicherheit in der Informationstechnik (BSI) [2] das IaaS-Angebot „Fujitsu Cloud in Central Europe“ auf Basis der von Fujitsu bereitgestellten Unterlagen und durchgeführten Interviews untersucht. Das Ergebnis der Studie zeigt, dass Fujitsu umfassende Sicherheitsvorkehrungen zur äußeren und inneren Gefahrenabwehr und zur Herstellung eines gegenseitigen Vertrauensverhältnisses zwischen Cloud-Anbieter und Cloud-Nutzer geplant und nach eigenen Angaben umgesetzt hat.

2 Definition grundlegender Begriffe, Abgrenzung und Untersuchungsgegenstand

2.1 Definition und Abgrenzung grundlegender Begriffe

Da verschiedene Definitionen von Begriffen im Cloud-Computing-Umfeld existieren, ist es notwendig die wichtigsten Begriffe näher zu erläutern, voneinander abzugrenzen und eine einheitliche Terminologie zu entwickeln.

Cloud Computing gemäß NIST Definition [3] ist ein Ansatz, um den bequemen On-Demand Netzwerk-Zugriff auf einen gemeinsamen Pool konfigurierbarer Rechner-Ressourcen (z. B. Netzwerke, Server, Speichersysteme, Anwendungen und Dienstleistungen) zu ermöglichen, die mit geringstem Management-Aufwand oder Eingriff eines Service-Anbieters schnell bereitgestellt und freigegeben werden können [4].

Fujitsu unterscheidet vier Formen von Cloud Computing: Public Cloud, Trusted Cloud, Private Cloud and Hybrid Cloud. Diese werden im Folgenden näher erläutert.

Public Cloud ist eine „öffentliche" IT-Umgebung, die sich eine beliebige Anzahl von Personen und Unternehmen teilen (Multi-Tenancy). Die in dieser Umgebung vorgehaltenen IT-Ressourcen sind standardisiert den Nutzern zur Verfügung gestellt. Aufgrund des gemeinsamen Netzwerkes über verschiedene Rechenzentren hinaus, der Nutzung der Virtualisierungstechnologien und der mit Cloud Computing verbundenen Elastizität wissen die Anwender normalerweise nicht, wo ihre Daten liegen. Public Clouds bieten ein Höchstmaß an Kosteneffizienz, aber nur ein Minimum an Datenschutz und Sicherheit.

Trusted Cloud ist eine Cloud-Umgebung, die eine begrenzte Anzahl von Kunden gemeinsam nutzt. Durch die Nutzung der zur Public Cloud getrennten Netzwerke bietet diese Form der Cloud ein höheres Maß an Sicherheit. Jedes Unternehmen hat hierbei seine eigenen virtuellen Server- und Speichersysteme, auf die es nur über eine virtuelle LAN-Verbindung zugreifen kann.

Fujitsu bietet Managed Trusted Cloud-Services nur aus seinen eigenen Rechenzentren an. Dadurch könnten Kunden von den Skaleneffekten der Services und gleichzeitig von einer hohen Sicherheit profitieren.

Private Cloud ist eine unternehmensspezifische IT-Umgebung mit dedizierten IT-Systemen sowie privatem Zugang und Nutzung ausschließlich durch das Unternehmen. Hierfür können strenge Regeln individuell definiert und implementiert werden. Eine Private Cloud kann sich innerhalb eines Unternehmens befinden oder extern betrieben werden. Fujitsu bietet eine Anbindung zur Trusted Cloud-Umgebung in den Fujitsu-Rechenzentren für zusätzliche „Cloud Burst"-Funktionen an und ermöglicht zudem eine Bereitstellung der für die Private Cloud benötigten Infrastruktur im Unternehmen.

Hybrid Cloud ist eine Kombination aus traditioneller IT (on-Premise), Private, Trusted und/oder Public Cloud. Die Daten und Anwendungen teilen sich entsprechend der definierten Richtlinien oder Geschäfts- und IT-Anforderungen auf. Voraussichtlich werden Hybrid Clouds – meist als Mischform von internen und externen IT-Services – künftig am weitesten verbreitet sein. Mit dem Konzept von Fujitsu können Kunden ihre bestehende IT-Umgebung mit der Cloud verknüpfen. Externe IT-Services aus der Cloud werden von Fujitsu verwaltet, während interne IT-Services vom Kunden bereitgestellt werden. Als Alternative kann der Kunde im Rahmen von Managed Services Fujitsu die volle Verantwortung für die IT-Services übertragen.

Des Weiteren wird es zwischen drei Cloud Computing Service Modellen unterschieden. In jedem Bereich bittet Fujitsu ein eigenes Angebot.

Unter ***Infrastructure-as-a-Service (IaaS)*** wird im Cloud Computing die Bereitstellung virtualisierter IT-Infrastruktur über das Internet verstanden. Beim IaaS nutzt ein Kunde Server, Storage, Netzwerk und die übrige Rechenzentrums-Infrastruktur als abstrakten, virtualisierten Service über das Internet. Hier stellt Fujitsu den Kunden das IaaS-Angebot „Fujitsu Cloud in Central Europe" zur Verfügung.

Im Fall eines ***Platform-as-a-Service (PaaS)*** wird eine Anwendungsinfrastruktur in Form von technischen Frameworks (Datenbanken und Middleware) für Systemarchitekten und Anwendungsentwickler geliefert. So bietet Fujitsu mit seinen Business Enablement Services die Umstellung vorhandener Vor-Ort-Softwareanwendungen (on-Premise) auf eine voll funktionsfähige Online-Anwendung (SaaS) [5] mit offenen Schnittstellen und diversen Services, wie z.B. Account Management, Abonnementverwaltung, Bereitstellung, Rechnungserstellung, Zahlungseinzug und weitere. Die so entwickelten Softwaredienste können entweder selbst benutzt oder auf dem Fujitsu SaaS Marktplatz angeboten werden.

Unter ***Software-as-a-Service (SaaS)*** wird ein Dienstleistungs- und Bereitstellungsmodell verstanden, das Kunden ermöglicht, Standard-Software und Business-Anwendungen über das Internet zu nutzen, ohne sie auf eigenen Rechnern zu installieren. Dafür werden Infrastrukturressourcen und Applikation zu einem Gesamtbündel kombiniert.

2.2 Untersuchungsgegenstand

In der vorliegenden Studie wird die Sicherheit des IaaS-Angebots „Fujitsu Cloud in Central Europe", strukturiert in die drei Bereiche: Infrastruktur, Administration, sowie Compliance und Audit, untersucht. Je Bereich wird die Sicherheitsuntersuchung nach festgelegten Kriterien, die aus den Mindestsicherheitsanforderungen des Bundesamts für Sicherheit in der Informationstechnik (BSI) [2] und der Fraunhofer-Institut SIT Cloud-Sicherheitsstudie [1] hervorgehen, durchgeführt.

Der BSI Katalog der Mindestsicherheitsanforderungen definiert Grundlagen für Basis-, Hochvertraulichkeits- und Hochverfügbarkeitsanwendungen und ist in 16 Bereiche untergliedert. Die Anforderungen sollen in Kooperation mit den Anbietern dynamisch weiterentwickelt werden und einen gemeinsamen Sicherheitsstandard etablieren.

Die Taxonomie des Fraunhofer-Instituts SIT ergänzt den BSI Katalog und stellt ein Rahmenwerk für Sicherheitsprüfungen von Cloud-Angeboten jeglicher Art zur Verfügung. Aufgrund unterschiedlicher Abstraktionsebenen ergänzen sich Taxonomie und BSI Katalog weitgehend. Somit werden beide zur Untersuchung des Angebots „Fujitsu Cloud in Central Europe" (IaaS) herangezogen.

Diese Studie wird basierend auf von Fujitsu für diese Untersuchung bereitgestellten Informationen und Angaben [6] [7] [8] [9] [10] [11], sowie weiterführenden Interviews mit verantwortlichen Stellen zusammengestellt. Anschließend werden die Vorgaben der Mindestsicherheitsanforderungen für Cloud Computing des BSI und der Fraunhofer-Institut SIT Sicherheitsstudie mit den von Fujitsu in den Unterlagen beschriebenen Maßnahmen verglichen. Als Methode zur Untersuchung werden die IaaS- spezifischen Punkte jeweils aus den konkreten Sicherheitsempfehlungen der BSI-Mindestsicherheitsanforderungen der Bereiche „Basis", „Vertraulichkeit hoch" und „Verfügbarkeit hoch", sowie aus den strukturierten Fragestellungen der SIT-Studie zusammengestellt. Anschließend werden diese auf einen Gesamtfragenkatalog zur Abschätzung des Sicherheitsniveaus des IaaS-Angebots abgebildet. Auf Basis der dem Fraunhofer-Institut SIT bereitgestellten Dokumenten wird ein erster Abgleich zum Katalog durchgeführt und folgend offene Punkte in den Interviews besprochen.

Abschließend wird von einer vollständigen Umsetzung der in der Dokumentation beschriebenen Maßnahmen ausgegangen. Sicherheitstests wie z.B. eine praktische Überprüfung der Systemsicherheit mittels Penetrationstests wurden nicht durchgeführt. Die Ergebnisse der Untersuchung stellt das Kapitel 3 dar.

In der Studie wird zwischen den kleinen und mittleren Unternehmen (KMUs) sowie Großkonzernen unterschieden. Diese Studie richtet sich maßgeblich an den Mittelstand.

3 Untersuchung der Sicherheit des IaaS-Angebots „Fujitsu Cloud in Central Europe“

Die in diesem Kapitel vorgenommene Untersuchung ist zusammengesetzt aus den einzelnen Bereichen: Infrastruktur, Administration, Compliance und Audit, wie in der Abbildung 1 dargestellt wird.

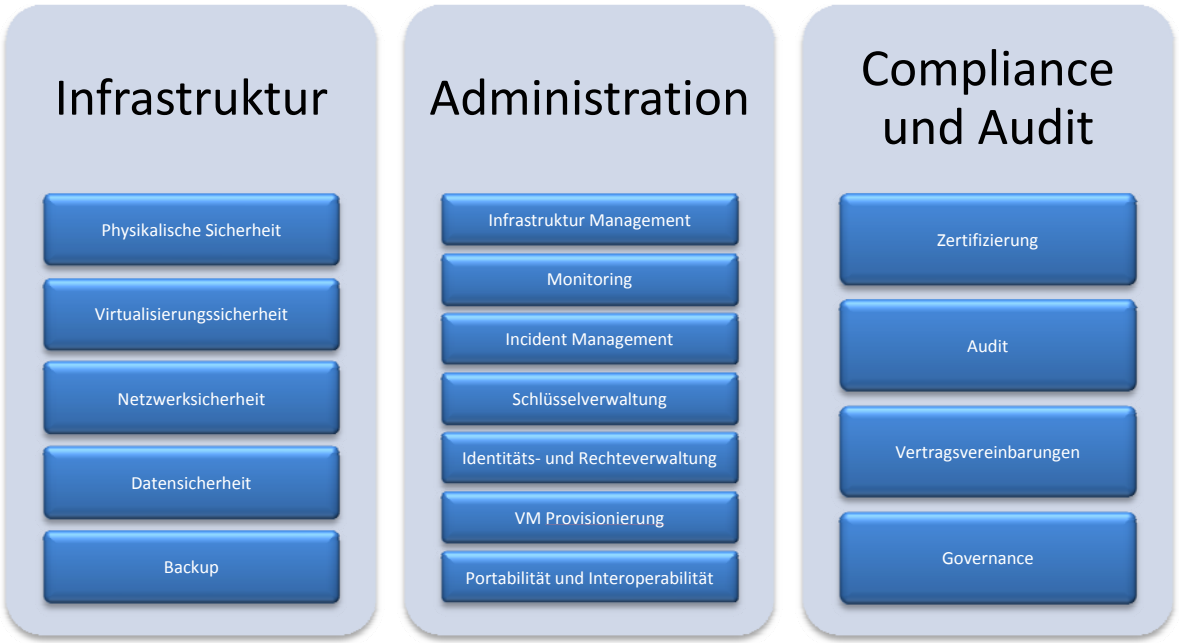

Abbildung 1: Fraunhofer-Institut SIT Taxonomie angepasst auf IaaS-Gegebenheiten

Jedem der Unterpunkte wird ein Unterkapitel gewidmet. Die Kapitel sind folgendermaßen aufgebaut: einer Beschreibung der Kategorie folgt ein Abgleich des Ist-Zustands mit dem im Kapitel 2 beschriebenen Gesamtfragenkatalog, der in einem Fazit resultiert.

3.1 Infrastruktur

Im Bereich Infrastruktur werden die dokumentierten Maßnahmen zur physikalischen Sicherheit, Virtualisierungssicherheit, Netzwerksicherheit, Datensicherheit und Backup untersucht. Dafür werden vor allem die Sicherheitsvorkehrungen im Rechenzentrum sowie in der zugrundeliegenden Architektur der Cloud-Umgebung betrachtet.

3.1.1 Physikalische Sicherheit

Der Bereich der physikalischen Sicherheit umfasst sämtliche Maßnahmen zum Schutz der Rechenzentren vor unbefugtem Zugang und unerwarteten Ausfällen aufgrund externer Faktoren, wie zum Beispiel Stromausfällen, Ausfällen der Anbindung an WAN-Netze und/oder Naturphänomenen. Hierbei werden sowohl reaktive als auch präventive Maßnahmen betrachtet

und insbesondere mögliche Unterschiede zwischen verschiedenen Standorten des Betreibers herausgearbeitet. Mit in diesem Bereich inbegriffen sind z.B. auch nach einem Vorfall stattfindende Prozesse. Das Ziel ist die kontinuierliche Verbesserung der Sicherheitsstrategie. Bei Fujitsu und seinem Partner, der TDS AG, ist ein hohes Maß an physikalischer Sicherheit für ihre Rechenzentren zu beobachten. Als Maßstab dienen hierbei die entsprechenden Punkte im Gesamtfragenkatalog, die von Fujitsu im Einzelnen als erfüllt gesehen werden können und zum Teil im Rahmen der ISO 27001 von unabhängigen Dritten überprüft werden.

Für alle Rechenzentren von Fujitsu gelten nach Aussage von Fujitsu, unabhängig von ihrem tatsächlichen Standort, einheitliche (Sicherheits-)Standards und –Prozesse [7]. Zudem wurde beim Entwurf und Betrieb der Standorte großer Wert auf redundante Strukturen in relevanten Bereichen gelegt. So sind, neben den reinen Versorgungsaspekten, wie z.B. Strom und Netzanbindung über externe Provider, auch weitergehende, mögliche Fehlerpunkte, wie z.B. fehlerhaftes Routing, durch Redundanz abgesichert. Dies kann im Hinblick auf die Gewährleistung eines reibungslosen Betriebs der Rechenzentren [8] positiv bewertet werden. Die Rechenzentren sind zudem redundant ausgelegt, so dass ein Ausfall eines Rechenzentrums, z.B. durch höhere Gewalt, keine oder nur minimale Auswirkungen auf die Serviceleistung haben sollte.

Ebenfalls hervorzuheben sind die Maßnahmen zur Sicherstellung des Zugangs zu Rechenzentren. Dieser ist nur über elektronisch überwachte Zugangsberechtigungen in Verbindung mit einer PIN möglich. Die Legitimität und Notwendigkeit eines Zugangs wird regelmäßig überprüft und ggf. entzogen. Zufallskontrollen beim Verlassen des Rechenzentrums, sowie Sicherheitsrundgänge und eine kontinuierliche Videoüberwachung dienen als weitere Bausteine zur Erhöhung des Sicherheitsniveaus. Besonders die Videoaufnahmen sind im Falle sicherheitsrelevanter Vorfälle wertvoll und werden dem Kunden ggf. zur Verfügung gestellt.

Die physikalische Sicherheit wird zudem in regelmäßigen Audits durch unabhängige Dritte kontinuierlich überprüft. Fujitsu ist hierfür u. a. nach den Normen und Grundsätzen der ISO27001 zertifiziert.

Zusammenfassend und auf Basis der dem Fraunhofer-Institut SIT zur Verfügung stehenden Dokumentation ist der Bereich physikalische Sicherheit bei Fujitsu als wohldurchdacht und in sich schlüssig zu betrachten. Vor allem die zu beobachtenden Aufwände zur Absicherung der Zentren vor unbefugtem Zugang und möglichen Ausfallszenarien führen zu einem positiven Gesamtergebnis.

3.1.2 Virtualisierungssicherheit

Ohne virtualisierte Ressourcen ist eine elastische Bedarfsbedienung, wie sie für Cloud-Computing charakteristisch ist [4], nicht denkbar. Mit den Möglichkeiten dieser Technologie sind allerdings auch Sicherheitsrisiken verbunden, die sich vor allem durch eine stringente Auswahl und Überwachung der Virtualisierungsumgebung minimieren lassen. Hierzu zählt eine Nutzung getesteter Hypervisor-Software genauso wie eine sorgsame Verwaltung der administrativen Zugänge zur Umgebung und eine entsprechend konservative Vergabe von Rechten [1]. Technisch gesehen sollte aber auch der Weg der virtuellen Maschinen von einer Umgebung in eine andere (Live-Migration) und die Art der Kommunikation der virtuellen Maschinen mit ihrem Host betrachtet werden.

Fujitsu hat in diesem Bereich Vorkehrungen auf drei Ebenen zur Sicherstellung der Isolierung der virtuellen Maschinen getroffen:

1. Arbeitsspeicher

   Die unterschiedlichen Speicherbereiche der virtuellen Maschinen werden durch technische Maßnahmen voneinander getrennt.

2. Festplatte

   Es werden virtuelle Festplatten zur Verfügung gestellt, bei denen eine automatische Rücksetzung der Speicherblöcke nach Nutzung bzw. vor einer Neuzuweisung vorgenommen wird. Somit wird ein direkter Zugriff auf die physische Festplatte verhindert.

3. Netzwerk-Schnittstelle

   Von physischen Netzwerkschnittstellen wird in der virtualisierten Umgebung auf Adapterebene abstrahiert. Die Verbindung zwischen den virtuellen Netzwerkkarten und den physischen Adaptern wird zusätzlich durch eine separate Firewall geschützt. Hierdurch werden vor allem Angriffsszenarien wie IP-Spoofing, d.h. das Vortäuschen einer anderen als der eigenen IP-Adresse, und das Abhören anderer als der eigenen (virtuellen) Netzwerkkarte stark erschwert.

Zusätzlich dazu wird auch der Einsatz auf zertifizierte Hypervisor-Software beschränkt. Als Zertifizierungsgrundlage dient dabei die Spezifikation der Common Criteria mit den jeweiligen Evaluation Assurance Level Definitionen für verschiedene Sicherheitsgütestufen. An der Erstellung der Common Criteria Spezifikation arbeitet von deutscher Seite das Bundesamt für Sicherheit in der Informationstechnik mit [12]. Von Fujitsu wird nur zertifizierte Hypervisor-Software eingesetzt. Hierbei werden methodische Tests und Reviews der zugrundeliegenden Implementierung in einem, im Rahmen des Common Criteria Recognition Agreements zertifizierten, Labor vorausgesetzt.

Durch diese Tests und Reviews soll sichergestellt werden, dass der benötigte Reifegrad und damit die erforderliche Hürde zur Kompromittierung der virtuellen Maschinen möglichst hoch liegen. Weiterhin wird durch Intrusion Detection/Prevention Systeme der Datenverkehr jeweils von innen nach außen und von außen nach innen nach auffälligen Mustern und manipulierten Paketen untersucht. Hierbei können kundenseitige Konfigurationswünsche berücksichtigt werden, so dass die zur Verfügung stehenden Maßnahmen auf den Einsatzzweck der virtuellen Maschinen optional individualisiert werden können. Zwar mit entsprechendem Aufwand verbunden, können diese Maßnahmen zu einer spürbaren Reduktion der möglichen Angriffsvektoren führen.

Eine bekannte Schwachstelle aller Systeme ist immer eine unbefugte Nutzung erlaubter Schnittstellen. Als Konsequenz im Kontext der Virtualisierungssicherheit bedeutet dies vor allem eine erweiterte Absicherung der administrativen Zugänge zu den virtuellen Maschinen. Insbesondere deshalb, weil die notwendige Automatisierung im Umfeld des Cloud Computings eine Beschränkung auf Administrationsvorgänge vor Ort praktisch nicht realisierbar macht. Die aus dieser Notwendigkeit geschaffenen Remoteadministrationsmöglichkeiten stellen aus der Sicherheitsperspektive ein besonders lohnenswertes Ziel dar. Ohne Erweiterungen und Konfigurationen würde sich hier ein vielversprechendes Ziel für einen Angriff auf die virtuelle Maschine eröffnen. Nicht zuletzt aus diesen Gründen werden in den Mindestsicherheitsanforderungen des BSI auch Multifaktor-Authentifizierungsmöglichkeiten

nachgefragt [2]. Fujitsu hat diese Möglichkeiten implementiert und stellt sie Kunden optional über einen Software-Token oder die Übermittlung über einen separaten Kommunikationskanal (SMS) zur Verfügung.

Die Virtualisierungssicherheit ist in Cloud-Computing-Umgebungen eine Notwendigkeit. Fujitsu leistet hierbei wichtige Vorarbeiten und liefert schlussendlich ein Rahmenwerk für die Absicherung der Kundenumgebung. Dieses Rahmenwerk kann und sollte der Kunde durch seine eigenen Maßnahmen auf seinen Anwendungsfall zuschneiden. Die Anstrengungen von Fujitsu sind als umfassend zu bewerten.

3.1.3 Netzwerksicherheit

Wie bei allen physisch vom Leistungsnehmer entfernten Systemen spielen Kommunikationsprotokolle und -komponenten eine zentrale Rolle. Deswegen ist eine Cloud-Computing-Umgebung damit definitionsbedingt auf eine funktionierende Netzwerkinfrastruktur angewiesen. Insbesondere IDS/IPS-Systeme, aber auch Firewalls, Verschlüsselung und eine Reaktionsmöglichkeit auf erkannte Angriffe sind hierbei genauer zu betrachten.

Fujitsu setzt zur Absicherung seines Netzwerks auf verschiedene Schutzmechanismen. So besteht die Möglichkeit einer dedizierten Trennung vom eigenen Netzwerk und dem anderer Kunden durch ein Virtuelles Netzwerk (VLAN). Gleiches ist für eine weitergehende Segmentierung des eigenen Netzwerkes in einen öffentlich zugänglichen und einen administrativen Teil möglich, wie beispielhaft die Abbildung 2 zeigt. Neben der herkömmlichen Firewall-Architektur der Fujitsu-Rechenzentren wird darüber hinaus eine virtuelle Firewall für den öffentlichen Teil des Kunden-IaaS-Angebots verwendet. Auch die administrativen Zugänge zur Konfiguration und Verwaltung des IaaS-Angebots werden gesondert durch ein Management VLAN, Firewalls und einen IPS Sensor gesichert. Insbesondere bei der Firewall werden zukünftig Möglichkeiten für den Kunden zur individuellen Konfiguration bestehen. So können spezifische Filterregeln bestimmt werden, die ein zusätzliches Maß an Sicherheit für die dahinterliegende Infrastruktur bieten. Nicht alle verfügbaren Infrastrukturkomponenten sind uneingeschränkt von Endkunden des Cloud-Kunden erreichbar. Nachgelagerte Dienste, wie zum Beispiel die Datenbank, sind gemeinhin nur indirekt über Web-Server zugänglich. Eine Abtrennung von öffentlich zugänglichem und privatem Bereich ist daher auch auf Netzwerkebene anzuraten. Fujitsu wird daher zukünftig auch die Bildung von Subnetzen administrativ unterstützen. Der sicherheitsrelevante Vorteil ergibt sich hierbei aus der Möglichkeit der Anwendung von Filtern und Firewalls auf die Subnetze anstelle vom gesamten Netz.

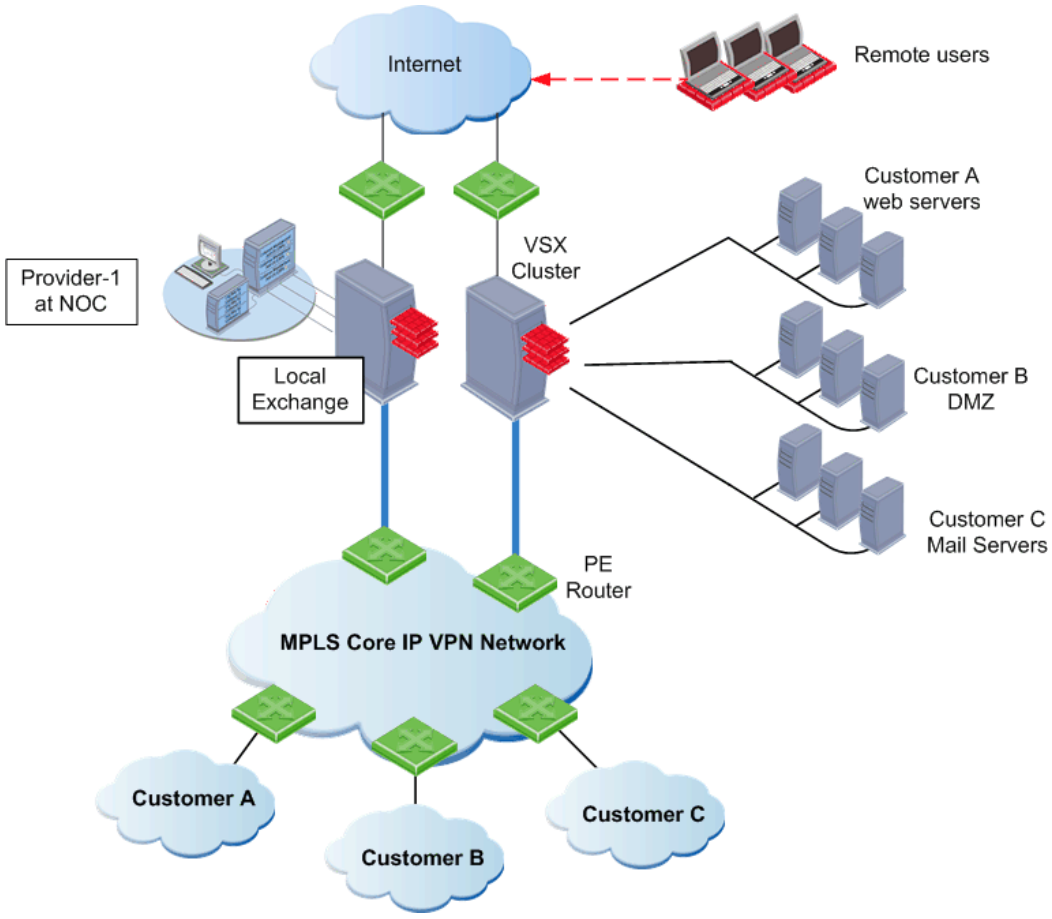

Abbildung 2: Beispiel eines in administrativen und öffentlich zugänglichen Bereich aufgeteilten Netzwerks [8]

Ein gesondert zu adressierendes Sicherheitsproblem sind Angriffe von innen, wie z.B. IP-Spoofing oder Packet Sniffing. Beim IP-Spoofing wird der Netzwerkverkehr mittels einer anderen als eigenen IP- und/oder MAC-Adresse gesendet. Aufgrund der Nutzung ausschließlich virtueller Netzwerkadapter im IaaS-Angebot von Fujitsu und einer zusätzlichen Firewall zwischen physischem und virtuellem Adapter wird diese Angriffsmöglichkeit hier abgefangen, denn nur die tatsächlich zugeordneten Adressen werden weitergeleitet. Beim Packet Sniffing versucht eine Netzwerkkarte durch die Nutzung des Promiscuous-Modus auch nicht an sie gesendete Pakete mitzuempfangen. Dies wird ebenfalls durch die Hypervisor-Schicht verhindert, weil nur ausdrücklich an die virtuelle Netzwerkkarte adressierter Verkehr weitergeleitet wird. Auch bei einer Kompromittierung der virtuellen Maschine sind durch die Konfiguration der Netzwerkknoten und der IPS-Sensoren an anderer Stelle weitere Sicherheitsvorkehrungen gegen Angriffe von innen getroffen worden.

Betrachtet man nun die Sicherungsmaßnahmen auf Netzwerkebene für einen Zugang von außen, so ist hier vor allem eine Nutzung gängiger Verschlüsselungstechnologien von Bedeutung. Die übliche Absicherung erfolgt hier durch Virtuelle Private Netzwerke (VPN). Generell ist die Verbindung vom Kunden in das Fujitsu-Rechenzentrum innerhalb des VPNs IPSec-gesichert. Darüber hinaus besteht auch die Möglichkeit einer weiteren Isolierung der Verbindung durch eine, mittels Multiprotocol Label Switching-Verfahren (MPLS), dedizierte Datenverbindung. Mit Blick auf die Redundanz ist im Cloud-Computing-Umfeld eine Einbindung

mehrerer Rechenzentren und der kontinuierliche Datenabgleich zwischen diesen von Bedeutung. Maßnahmen im Bereich Netzwerksicherheit sollten daher auch die Kommunikation zwischen den Standorten miteinbeziehen. Dies ist im Falle von Fujitsu geschehen. Zwar wird von einer Verschlüsselung der Transferdaten abgesehen, jedoch werden auch ausschließlich private Leitungen zur Übertragung genutzt.

Im Zusammenhang mit dieser Übertragung sind externe Provider involviert. Bei ihnen ist generell Redundanz ein wichtiges Kriterium, um im Falle eines Ausfalls eines Anbieters nicht zwangsläufig einem kompletten Wegfall der Verbindungsfunktionalität ausgesetzt zu sein. Zur Abwendung eines solchen Szenarios wird auf Seiten von Fujitsu eine „Dual Provider"-Strategie angewendet. Mittels Leitungen von zwei voneinander unabhängigen Providers mit Endpunkten ins Fujitsu-eigene Netz wird die Gefahr eines Ausfalls eines Providers relativiert. Die Komponenten des Fujitsu-Netzwerks vom Endpunkt des Providers an sind ebenfalls redundant ausgelegt.

Alle Vorsichtsmaßnahmen zur Erkennung von Gefahren sind wirkungslos, wenn nicht auch eine entsprechende Aufarbeitung und Auswertung der gesammelten Informationen stattfindet und daraus angemessene Reaktionen abgeleitet werden. Für Hochverfügbarkeitsanwendungen über das Internet bedeutet dies eine mögliche Reaktionsfähigkeit im 24/7-Bereich. Der Umstand einer garantierten Verfügbarkeit der Services von Seiten des Anbieters aufgrund eines Service Level Agreements (SLA) als Bestandteil des Vertrages macht die Fähigkeit zur Reaktion umso bedeutender. Der Bereich des System-Monitorings erfährt daher bei Fujitsu besondere Aufmerksamkeit. Mittels einer kontinuierlichen Überwachung aller infrastrukturrelevanten Komponenten und der Server, bzw. auf der Virtualisierungsebene auch des Gastes, werden Abweichungen vom Normalzustand zeitnah festgestellt und im Verdachtsfalle proaktive Maßnahmen zur Sicherstellung/Wiederherstellung des Normalzustandes eingeleitet. Sollte keine solche Maßnahme zur Verfügung stehen, werden entsprechende Schritte im Rahmen des vereinbarten Service Level Agreements unternommen.

Die Maßnahmen von Fujitsu zur Gewährleistung der Netzwerksicherheit sind durchdacht und decken verschiedene Ebenen der vorzufindenden Netzwerke bei Fujitsu und dem Kunden ab. Die in diese Sicht eingebrachten Sicherheitsvorkehrungen sind auf technischer und organisatorischer Ebene aktiv und lassen den Schluss auf eine systematische Sicherheitsarchitektur zu.

3.1.4 Datensicherheit

Datensicherheit konzentriert sich primär auf die Ziele Integrität und Vertraulichkeit der Daten. Zentral ist hierbei in Cloud-Umgebungen die Isolation der Daten eines Kunden von den Daten der anderen Kunden derselben Umgebung sowie der Schutz der Daten vor Verlust, zum Beispiel durch Hardwareversagen. Der Cloud-Kunde profitiert hierbei generell von definierten Sicherungs-/Backupmaßnahmen durch den Anbieter, welche aber bezüglich der Vertraulichkeit hinterfragt werden sollten. Die eigenen Daten können, insbesondere bei Backups, die gesicherte Umgebung, eventuell auch geographisch, verlassen und somit der Gefahr ausgesetzt sein, Dritten zugänglich zu werden. Um dies zu verhindern, sind neben organisatorischen Richtlinien vor allem Verschlüsselungsverfahren dienlich. Nicht zuletzt sollten die Löschvorgänge genauer betrachtet werden. Ein sicheres Löschverfahren ist hier wünschenswert. Wie bei der Frage nach

den Backups ist hier ebenfalls die Frage nach dem Verbleib der Daten auf Sicherungsmedien, gespiegelten Instanzen und eventuellen Zwischenspeichern zu stellen.

Nach vorliegender Betrachtung besitzt Fujitsu umfangreiche Werkzeuge und Verfahren zur Sicherstellung der Datensicherheit. Die Isolierung der eigenen Datenbestände auf virtuellen Maschinen erfolgt auf Basis der (virtualisierten) Betriebssysteme. Neben den bereits im Kapitel 3.1.2 Virtualisierungssicherheit erläuterten Maßnahmen ist im Zusammenhang mit der Datensicherheit vor allem die Sicherung der Festplatten erwähnenswert. Es besteht keine Möglichkeit des direkten Zugriffs auf die physische Festplatte. Stattdessen werden virtuelle Festplatten zur Verfügung gestellt, deren Speicherblöcke bei Neuzuweisung automatisch zurückgesetzt werden, um unbeabsichtigten Zugriff auf Daten anderer Kunden zu vermeiden. Dies hat allerdings keine weiteren Auswirkungen auf die bereits erstellten Snapshots. Eine gemeinsame Nutzung von Daten, z. B. mit anderen Kunden ist ebenfalls nicht direkt möglich, sofern man von der Möglichkeit einer Freigabe über das externe Netz, zugangsgesichert oder nicht, absieht.

Bei jeder Nutzung von Daten stellt sich auch die Frage nach deren sicherer Löschung. Hierfür bestehen im Angebot der Fujitsu mehrere Möglichkeiten. Löschvorgänge können, in Abhängigkeit der jeweils genutzten Art des Dienstes, auf zwei Arten geschehen. Standardmäßig werden die Daten bei Löschvorgängen mehrmalig überschrieben, um die Anforderungen zum sicheren Löschen zu erfüllen. Darüber hinaus hat der Kunde die Möglichkeit eine physikalische Zerstörung der Datenträger in Anspruch zu nehmen. Diese Variante ist aufgrund des Mehraufwandes und der Bedingung der ausschließlichen Nutzung des Datenträgers mit entsprechendem Mehraufwand verbunden, der gegenüber den Vorteilen dieser Löschart abgewogen werden muss. In jedem Fall werden die Daten und Sicherungskopien unwiderruflich von allen Datenträgern und Zwischenspeichern gelöscht.

In diesem Bereich sind vor allem die Möglichkeiten bei der Löschung von Daten bemerkenswert. Die normalerweise vorzufindenden Angebote zur Löschung von Daten in Cloud-Computing-Umgebungen, namentlich das mehrfache Überschreiben von Daten, werden durch die Möglichkeit einer physischen Zerstörung des Datenträgers noch übertroffen. Auch die Vorkehrungen beim Einrichten der Festplatten sind vorausschauend, allerdings bleiben die Verschlüsselung der Daten und das Rechtemanagement in der Verantwortung des Kunden.

3.1.5 Backup

Zur Gewährleistung der Verfügbarkeit von Daten sind regelmäßige Sicherungskopien schlicht eine Notwendigkeit. Neben der bloßen Existenz von Backupstrategien ist allerdings auch der Ablauf der Sicherung von Bedeutung. Daher muss jede Kopie ähnlichen Schutz genießen wie das Original. Wichtig sind in diesem Umfeld die Unterstützungsleistungen des Cloud-Anbieters, weil durch sie ein definierter Rahmen geboten wird, dessen Anwendung auf regelmäßiger Basis stattfindet. Dieser Grad an technologischer Unterstützung ist sonst nur mit Eigenaufwand auf Seiten des Cloud-Kunden zu erreichen, was neben zusätzlichem Aufwand auch Kenntnis der Materie voraussetzt und somit oftmals in der benötigten Güte unterbleibt. Neben den Möglichkeiten einer Sicherung sollten nicht zuletzt auch die Eventualitäten bei der Wiedereinspielung der Daten in das Produktivsystem einer Prüfung unterzogen werden. Wegen der speziellen Anforderungen, die sich aus einer kundenspezifischen Umgebung und Nutzung ergeben, sollte hierbei auf das Mittel der Kundentests zurückgegriffen werden. Notwendig ist

dies, weil viele Systeme nicht einfach wiederhergestellt und angeschaltet werden können, sondern oftmals weitergehende Vorkehrungen, wie z. B. zur Sicherstellung der Integrität von Datenbanksystemen, getroffen werden müssen. Als eine sinnvolle Unterscheidung bietet sich hierbei eine Replikats-basierte Sicherung mittels Fail-Over-Mechanismen und die Frage nach den eingesetzten Methoden zur Sicherstellung der Synchronisation sowie eine Sicherung der gesamten virtuellen Maschine zum Zwecke einer späteren Wiedereinspielung. Aspekte zu rein rechtlich vorgeschriebenen Sicherungen, zum Beispiel für Archivierungspflichten oder zur Erfüllung steuerrechtlicher Vorschriften, werden in diesem Punkt nicht behandelt.

Fujitsu bietet für ihre Server generell eine tägliche Sicherung auf Basis von Snapshots an. Die Aufbewahrungszeit für diese Daten beträgt sieben Tage, kann bei Bedarf allerdings kostenpflichtig verlängert werden. Ein wichtiger Punkt ist hierbei die Granularität der Sicherungen, weil immer nur der gesamte Datenbestand zum Zeitpunkt des Snapshots wiedereingespielt werden kann. Eine Wiederherstellung einzelner Daten(-bestände) ist hierbei nicht möglich.

Als optionale Erweiterung ist auch eine kontinuierliche Sicherung des Inhalts der virtuellen Maschinen möglich. Hierbei wird auf die Softwarelösung eines spezialisierten Drittanbieters vertraut. Eine Wiedereinspielung ist damit sehr viel feingranularer als mit den täglichen Snapshot-Verfahren möglich und bietet daher ein höheres Niveau an Datensicherheit. Neben den Kosten für den optionalen Dienst sind die entsprechenden organisatorischen Prozesse beim Kunden für eine Wiedereinspielung zu definieren. Besondere Sorgfalt sollte auf die, auch bei diesem Sicherungsverfahren bestehende, zeitliche Lücke zwischen dem Ausfall, eventuellem Ersetzen defekter Hardware und der Dauer der Wiedereinspielung gelegt werden. Im Sinne einer möglichst unterbrechungsfreien Dienstebereitstellung sollte zusätzlich für kritische Komponenten ein Replikat bereitgestellt werden, welches im Falle des Ausfalls und bis zur Wiederherstellung der ausgefallenen Komponente(n) die Anfragen übernimmt. Entsprechende Fragen bezüglich der Datenkonsistenz bei Wiedereinspielung und/oder der Übernahme der Verarbeitung durch ein Replikat sind hierbei konzeptionell zu durchdenken und im Rahmen von Tests zu verifizieren.

Das Backup-Konzept im Fujitsu-IaaS-Angebot ist als Basisangebot zu sehen. Die Absicherungen für einen Ausfall sind als ausreichend zu betrachten, weil eine Wiederherstellung der Daten des letzten Tages eine Verbesserung gegenüber keiner Wiederherstellung bietet und für viele Fälle, wie z.B. Webserver ohne eigene Datenbank, akzeptabel ist. Für kritischere Komponenten können die weitergehenden Konzepte für Sicherungsstrategien durch das optionale Erweiterungsangebot zum kontinuierlichen Backup in Betracht gezogen werden. Jedoch ist eine Sicherungsstrategie immer Anwendungs- und Dienste-spezifisch und daher schwer verallgemeinerbar in der Implementierung, so dass diese Aufgabe dem Kunden oftmals selber überlassen werden sollte.

3.2 Administration

Die Möglichkeiten zur Administration der Cloud-Umgebung durch den Anbieter und die möglichen Schnittstellen zu Softwarekomponenten des Kunden entwickeln sich zusammen mit dem Cloud-Computing-Ansatz kontinuierlich weiter und unterliegen damit einer beständigen

Veränderung. Sie sind darüber hinaus noch Gegenstand aktueller Forschungs- und Standardisierungsbemühungen. Nichtsdestotrotz sind die in der Administration existenten Konfigurationen, Prozesse und die geschaffenen Möglichkeiten zur kontinuierlichen Anpassung der Cloud-Umgebung Schlüsselpunkte für weitere Dienste und Verwendungszwecke durch den Kunden.

So lässt sich, gemäß der Fraunhofer-Institut SIT Taxonomie, dieser Themenbereich durch folgende Aspekte: Infrastrukturmanagement, Monitoring, Incident Management, Schlüsselverwaltung, Identitäts- und Rechteverwaltung, Provisionierung der virtuellen Maschinen sowie Portabilität und Interoperabilität näher beschreiben.

3.2.1 Infrastruktur-Management

Die Möglichkeiten zur Verwaltung der Infrastruktur durch den Cloud-Kunden schließen im sicherheitsrelevanten Bereich die Fernadministration der virtuellen Maschinen unter Nutzung gängiger Absicherungsmethoden ein. Zum Zwecke einer Absicherung dieser Zugänge sollte zudem auch die Frage nach spezifischen Richtlinien zur Verhinderung von Brute-Force-Angriffen gestellt werden.

Ferner spielt die (Wieder-)Verwendung von Kundenimages für die virtuellen Maschinen eine Rolle, weil hierbei implizit die Verwendung bereits auf den Anwendungsfall zugeschnittener Images unterstellt werden kann. Auch Möglichkeit der Nutzung von durch den Anbieter vorbereiteter Images ist von großer Bedeutung.

Möglichkeiten zur Konfiguration der Infrastruktur durch den Kunden sind im Rahmen des Infrastruktur-Managements zu überprüfen, weil diese Einstellungsmöglichkeiten die Erfahrungen des Kunden berücksichtigen können und sollen. In der Regel sollte dieser Konfigurationszugriff, wegen dort meist stark reduzierter Konfigurationsmöglichkeiten, nicht ausschließlich auf Portale im Web beschränkt sein.

Sicherheitsrelevant in Bezug auf die Infrastruktur sind ebenfalls Aktualisierungen der Infrastruktur und der virtuellen Maschinen. Zwar ist die sicherheitstechnische Bedeutung ständig aktueller Betriebssystem- und Anwendersoftware unstrittig, allerdings steht der Einspielvorgang selber im Konflikt mit dem Ziel der Verfügbarkeit, so dass hierbei ein Verzug zwischen dem Erscheinen einer Aktualisierung für die Software und deren Anwendung in Produktivsystemen durch nachgelagerte Patch-Wartungsfenster in Kauf genommen werden muss. Im Hinblick auf die Verfügbarkeit als Schutzziel ist auch die Frage nach der Patchverträglichkeit zu stellen, bzw. welche Vorkehrungen getroffen werden, um diese sicherzustellen.

Fujitsu stellt im Bereich Infrastruktur-Management die Fernadministration mittels virtueller, privater Netzwerke zur Verfügung, um das kundenseitige Konfigurationsmanagement zu ermöglichen. Hierbei obliegt die administrative Verantwortung für die virtuelle Maschine dem Kunden, der hierfür auch die vollen Rechte innehat. Alternativ und hauptsächlich für Konfiguration der Infrastruktur des zugrundeliegenden Hosts gedacht, kann das webbasierte IaaS-Portal genutzt werden. Host-Systeme und die Infrastruktur werden von Fujitsu gewartet. Im Regelfall wird diese organisatorische Trennung aufrecht gehalten, die Ausnahmen bilden vom Kunden vorab genehmigte Aktualisierungen und ein notwendiges Eingreifen von Fujitsu im Falle

eines drohenden Datenverlustes. Unkritische Aktualisierungen der Infrastruktur werden dem Kunden zur Genehmigung vorgelegt und erst anschließend durchgeführt.

Auch beim Einspielen der Aktualisierungen wird zwischen dem Infrastrukturteil und den virtuellen Maschinen des Benutzers unterschieden. Für die Aktualisierung der Infrastruktur ist ein Wartungsfenster pro Quartal am Sonntag zwischen 0 Uhr und 18 Uhr vorgesehen, über das der Kunde im Vorfeld informiert wird. Davon abgesehen behält sich Fujitsu allerdings das Recht zur Aktualisierung oder zum Austausch von Hard- oder Software vor, wenn dadurch Verfügbarkeit der Dienste nicht beeinträchtigt wird. Auch besteht das Recht, weitere als die bereits geplanten Wartungsfenster zu planen, sofern diese vorher, in Regel 14 Tage, angekündigt werden. Generell findet eine Überprüfung der Patchverträglichkeit vor dem Einspielen in das Wirksystem im eigens dafür vorhandenen Labor statt.

Die virtuellen Maschinen der Kunden obliegen nicht dem Zugriff durch Fujitsu, allerdings werden die Systemaktualisierung und die Bereitstellung dieser Maschinen von Fujitsu unterstützt. Letzteres hat sicherheitsrelevante Vorteile, weil bereits bewährte Konfigurationseinstellungen verwendet werden können und so die mögliche Angriffsfläche, z.B. durch unbeabsichtigt laufende Dienste, vermindert werden kann. Darüber hinaus können Kunden auch vorgefertigte Abbilder laufender Betriebssysteme erstellen und von Fujitsu einspielen lassen. Dafür muss allerdings das Open Virtualization Format (OVF) als Speicherformat genutzt werden, wobei von einer Unterstützung dieses Formats bei allen gängigen Virtualisierungslösungen ausgegangen werden kann. Durch die Autonomie des Kunden bzgl. seiner virtuellen Maschinen ist eine automatische Aktualisierung der Systeme nicht mehr von vornherein möglich. Sofern vom Kunden explizit gewünscht, wird für die virtuellen Maschinen ein reguläres Wartungsfenster an jedem Donnerstag zwischen 22 Uhr und 2 Uhr eingerichtet. Ohne diese explizite Erlaubnis stehen dem Kunden nur betriebssystemeigene Informationsdienste zur Aktualisierung zur Verfügung.

Das Konzept des Infrastruktur-Managements kann zusammenfassend als ausgereift bezeichnet werden. Sowohl Möglichkeiten zur Fernadministration, ein umfangreiches Portal und die strikte Trennung zwischen Kunden-Infrastruktur und Basis-Infrastruktur sind hervorzuhebende Bestandteile mit Vorteilen für die Fujitsu IaaS-Kunden.

3.2.2 Monitoring

Das Ziel des Monitorings ist die Sicherung von Informationen zur Ad-hoc oder späteren Analyse und/oder der Beweissicherung in allen relevanten Komponenten einer Cloud-Computing-Umgebung. Das Monitoring sollte dabei die allgemeinen Schutzziele als Gegenstand der Überwachung im Auge behalten. Insbesondere das Schutzziel der Verfügbarkeit wird hier durch neue verteilte Angriffsformen, wie zum Beispiel der Distributed Denial of Service-Attacke (DDoS) tangiert. Die gesammelten Daten, bzw. ein Teil davon sollte auch für den Kunden einsehbar sein.

Neben der Frage, ob Operationen im und Informationen über das System aufgezeichnet werden, ist auch die Granularität der gesammelten Informationen von Bedeutung. So wird gemeinhin eine Protokollierung jeder Konfigurationsänderung und jeder Management-Aktion in Cloud-Umgebungen vorausgesetzt. Zusätzlich sollte die Möglichkeit bestehen, eine kundenspezifische Aufzeichnung zusätzlicher Daten zu beauftragen. Speziell in Bezug auf versuchte Verletzungen

des Schutzzieles der Vertraulichkeit sollten auch Daten z.B. über fehlgeschlagene Authentifizierungsversuche mitgespeichert werden.

Über das Fujitsu Systems Management Center (SMC) erfolgt im Bereich des Monitorings eine zentrale Überwachung der verschiedenen Zustände der Hard- und Software. Hierzu zählt unter anderem die Hardwarefunktionalität, Auslastung der Festplatten, Prozessoren und des Arbeitsspeichers, Datensicherungsprotokolle, Anti-Viren-Software, Keep-Alive der physikalischen Systeme und Komponenten und die Sammlung von Systemmeldungen. Die Überwachung durch das Management Center ist dabei kontinuierlich im 24/7-Zeitraum. Im Rahmen der Tätigkeiten von Administratoren an Host-Systemen findet eine Protokollierung der Konfigurationsänderungen und Managementaktionen statt.

Die eigentlichen Daten erhält der Kunde aggregiert im Rahmen seines monatlichen Berichts neben den Daten über die Verfügbarkeit und Finanzinformationen. Zusätzlich bestehen Überwachungseinstellungen über das IaaS-Webportal, wobei die daraus resultierenden Informationen auch mit einem Überwachungswerkzeug des Kunden verbunden werden können. Betriebssystemeigene Log-Daten können über das Windows Event Log File Format oder das Syslog Message Format zur Verfügung gestellt werden. Optimal wäre eine Integration dieser Logdateien in kundeneigene Überwachungssysteme.

Die Vorkehrungen im Bereich Monitoring sind in zwei Bereiche aufgeteilt: einen Basis- und einen angepassten Bereich. Diese Kombination hat aus Sicht des Kunden zwei Vorteile. Zum einen werden die Monitoring-Daten nicht in einer Menge angezeigt, die ein Auffinden relevanter Informationen erschweren würde und zum anderen können die für ihn wirklich interessanten Parameter beauftragt und eingebunden werden. Allerdings kann diese Aufteilung auch den Nachteil eines Wegfalls eventuell relevanter Überwachungsdaten mit sich bringen, der bedacht und ggf. durch weitere Überwachungsaktivitäten ausgeglichen werden sollte. Diese Möglichkeiten und die verfügbaren Monitoring-Parameter ermöglichen eine umfangreiche Basisüberwachung und sind daher in diesem Bereich als sehr gut anzusehen.

3.2.3 Incident Management

Neben der reinen Überwachung von Systemen sollte auch die Reaktionsfähigkeit auf erkannte Ausfälle und Gefahrensituationen betrachtet werden. Zentral hierbei ist die Existenz eines handlungsfähigen Cloud-Managements, welches auch rund um die Uhr erreichbar ist. Nicht zuletzt sollte beim Cloud-Anbieter geprüft werden, ob jedes Vorkommnis auch zeitnah gemeldet wird.

Konkret ist ein Service Desk bei Fujitsu ohne Unterbrechung im Jahr in 26 Sprachen via Telefon, E-Mail oder über das Web-Portal für vom Kunden festgestellte Fehlerzustände erreichbar. In diesem Fall erfolgt die Fehleranalyse nach Übersendung des Incidents. Das daraus entstehende Service-Ticket wird über diesen 1st Level Support gegebenenfalls gelöst und die entsprechenden Schritte dokumentiert. Eine Information für den Kunden wird im entsprechenden System zur Einsicht hinterlegt. Eine Fehleranalyse kann auch an nachgelagerte Support-Stufen (2nd und 3rd Level Support) weitergeleitet werden, wenn eine Behebung durch den Service Desk nicht möglich und eine genauere Untersuchung der Ursachen vonnöten ist oder Supportleistungen von Drittanbietern in Anspruch genommen werden müssen.

Mindestens einmal im Monat erhält der Kunde einen Report mit einer Auflistung der bestellten Dienste von Seiten von Fujitsu. Dieser Bericht enthält auch die abrechnungsrelevanten Informationen, wie die Verfügbarkeit der Services für den Zeitraum des Berichts, sowie eine Liste der aufgetretenen Incidents, bestellten Änderungen und durchgeführten Aktualisierungen.

Der Service Desk des Incident Managements bei Fujitsu bietet einen zentralen Weg zur Abarbeitung von Anfragen im Supportbereich. Die Verfügbarkeit des Service Desks von 24/7/365 ist hierbei positiv hervorzuheben. Eine Weiterleitung der Support-Anfragen in die entsprechenden Kanäle und die dann erfolgende Übersicht über den Status lassen eine positive Einschätzung dieses Bereichs angemessen erscheinen.

3.2.4 Schlüsselverwaltung

Für einen Zugriff auf Verwaltungsschnittstellen im Cloud-Computing-Umfeld sind herkömmliche Verfahren in Form einer Kombination von Benutzername und Passwort aus Sicherheitsgründen nicht empfehlenswert. Hier bietet eine Public/Private Key-Verschlüsselung in Verbindung mit Zertifikaten einen weit höheren Schutz. Sofern diese Methode jedoch verwendet wird, sollte die Verwaltung dieser Schlüssel und Zertifikate genauer geprüft werden. Hilfreich sind hierbei Optionen zur Schlüsselverwaltung von Seiten des Anbieters, weil dadurch mögliche Probleme im Bereich Interoperabilität, zum Beispiel bei den kryptografischen Verfahren, deutlich reduziert werden. Die Verwendung von Schlüsseln und Zertifikaten an sich stellt aber noch keine hinreichende Sicherheit bei der Authentifizierung und Autorisierung sicher, denn auch Schlüssel und Zertifikate können, bei schwachen Algorithmen, gebrochen werden oder auch schlicht in nicht autorisierte Kanäle gelangen.

Aufgrund der sicherheitstechnischen Relevanz und aus Kompatibilitätsgründen mit eigenen Infrastrukturen werden Belange der Schlüsselverwaltung und Verschlüsselung der Daten bei Fujitsu ausschließlich dem Kunden überlassen. Daher bestehen auch keine Schutzmechanismen gegen einen Verlust des Schlüssels, weil diese eine Hinterlegung bei Fujitsu bedingen würden. Von diesem Vorgehen wird nur im Bereich der Verbindungsverschlüsselung abgesehen. So unterstützt Fujitsu den Kunden in diesem Umfeld insbesondere bei Maßnahmen zur Schlüsselrotation mittels multipler, valider Schlüssel. Hier erfolgt die Verschlüsselung auf der WAN-Strecke bis zum Fujitsu Rechenzentrum. Für die entsprechende IPSec-Verbindung ist eine Konfiguration der Kunden-Firewall durch den Kunden erforderlich. Im Bedarfsfall kann dieser Schritt auch über vorkonfigurierte Router von Fujitsu erfolgen, die dem Kunden zur Verfügung gestellt werden.

Der Bereich der Schlüsselverwaltung kann als sehr positiv betrachtet werden, wenn kundenseitig eine entsprechende Nutzung der vorgeschlagenen Maßnahmen erfolgt. Die Unterstützung beim notwendigen Austausch von Schlüsselmaterial und der Einrichtung der Firewalls zur Verbindungsverschlüsselung sind die ausschlaggebenden Punkte für diese Einschätzung.

3.2.5 Identitäts- und Rechteverwaltung

Im Bereich der Identitäts- und Rechteverwaltung ist vor allem die Zuordnung einer virtuellen auf eine reale Identität von Bedeutung, weil letztendlich die Nachweisbarkeit von Operationen und Zugriffen dadurch tangiert wird. Die Zugänge zum System sollten durch starke

Authentifizierungsmechanismen, zum Beispiel eine Zwei-Faktor-Authentisierung, gesichert werden. Idealerweise existiert eine Auswahl an unterschiedlichen Mechanismen für den Systemzugang. Im Bereich der Konfiguration der Identitäts- und Rechteverwaltung ist hierfür eine zentrale Anlaufstelle vorhanden. Über Zugriffskontrolllisten wird festgelegt, welche Mitarbeiter des Anbieters und des Kunden auf welchen Konfigurationsabschnitten Rechte besitzen. Nach dem Least-Privilege-Model sollte der Umfang der Zugriffsrechte eingeschränkt werden. Hierbei ist, regelmäßig, eine Anpassung der vergebenen Rechte vorzunehmen, damit zum Beispiel versetzte oder ausgeschiedene Mitarbeiter auf beiden Seiten auch der Zugang zum System entzogen wird. Die allgemeine Betriebssicherheit wird auch durch Maßnahmen wie das Vier-Augen-Prinzip für kritische Administrationstätigkeiten, zum Beispiel das sichere Löschen einer virtuellen Maschine im Rahmen der Dekommissionierung, erhöht und Fehlerfälle reduziert. Generell sind für die Rechtevergabe, auch die des Anbieters, transparente Regeln aufzustellen. Des Weiteren kann eine Unterstützung bestehender Identitäts- und Rechteverwaltungsstandards und APIs die Integration des Cloud-Computing-Angebots in die Kundenmanagement-infrastruktur verbessern.

Im konkreten Fall ist bei Fujitsu die sichere Zuordnung der Konten zu den entsprechenden Cloud-Nutzern gegeben. Standardmäßig ist das Anlegen und Nutzen von Gruppen- oder Sammelkonten zum Zwecke einer besseren Identifizierbarkeit für Monitoring- und Audit-Aktivitäten untersagt. Die Konfiguration der Benutzerkonten und –rechte erfolgt zentral über das IaaS-Portal in einem Self-Service-Bereich. An dieser Stelle können über privilegierte Benutzerkonten zusätzliche Benutzer und Rechte eingestellt werden. Eine Freischaltung der Konten erfolgt dabei über Einmalpasswörter zur Aktivierung. Nachfolgend ist die Nutzung komplexer Passwörter für den Kontenzugang erforderlich. Eine Zwei-Faktor-Authentifizierung ist für Kunden ebenfalls möglich, wenn auch nur im Rahmen eines optionalen Angebots. Zum Einsatz kommen hier spezielle Tokens oder SMS-Nachrichten mit den entsprechenden Codes. Die vergebenen Rechte sind dabei an die kundeneigene Domäne geknüpft, d.h. nur in dieser gültig. Als mögliche Integrations-schnittstellen werden das Lightweight Directory Access Protocol (LDAP) sowie die Active Directory-Schnittstellen (AD) der Windows-Betriebssysteme zur Verfügung gestellt, wobei sich in beiden Fällen die entsprechenden Server im privaten Subnetz des Kunden befinden. Eine Bereitstellung von dedizierten Programmierschnittstellen für eine weitergehende Integration der Benutzerkonten- und Rechtevergabe in die kundeneigenen Systeme ist von Fujitsu nicht vorgesehen.

Die Verwaltung des Zugriffs durch Mitarbeiter von Fujitsu und seinen Dienstleistern ist strikt geregelt. Die Rechte werden nach dem Least-Privilege-Prinzip vergeben, so dass jeder Administrator nur die Rechte hat, die er für die Durchführung von Aktionen in seinem Bereich benötigt. Vor allem die regelmäßige Kontrolle der Notwendigkeit dieser Rechte ist der Sicherheit zuträglich. Zwar wird kein Vier-Augen-Prinzip bei der Durchführung von Administrations-tätigkeiten angewandt, also die exklusive Durchführung von Aktionen nur durch mindestens zwei Berechtigte, allerdings sind die Aktionen vorher geplant und terminiert, so dass im Prinzip keine ungeplanten Aktionen durchgeführt werden und damit eine ähnliche Sicherheit wie beim Vier-Augen-Prinzip erreicht wird.

Die Einrichtungen im Bereich Identitäts- und Rechteverwaltung sind solide und bieten durch die Unterstützung von SMS- und Token-basierter Zwei-Faktor-Authentifizierung zudem den (optionalen) Vorteil einer sicheren Schnittstelle. Die Integration in LDAP- und AD-

Verzeichnisdienste ist zudem eine sinnvolle Erweiterung für die nahtlose Nutzung der eigenen und der IaaS-Infrastruktur für Kunden.

3.2.6 VM Provisionierung

Unterstützungsleistungen bei der Einrichtung von virtuellen Maschinen von Seiten der Anbieter sind sinnvolle Hilfen, weil die Absicherung der Maschinen nicht nur durch die Infrastruktur, z.B. Firewalls, erfolgt, sondern auch die Maschinen selber in einem gehärteten Zustand ausgeliefert werden. Dieser Zustand müsste ansonsten vom Kunden selber hergestellt werden. In diesem Fall wäre eine Unterstützung seitens des Anbieters mittels Werkzeugen zur Provisionierung wünschenswert.

Im Rahmen der Bereitstellung von Servern ohne vorkonfiguriertes Betriebssystem bietet Fujitsu als Dienstleistung die Bereitstellung eines Installationsimages an. In dieses Image integriert sind bereits Antivirensoftware, Virtualisierungstreiber/-software und die benötigten Einstellungen für die Betriebssystemaktualisierungen. Weiterhin sind die Abbilder jeweils auf die verwendete Infrastruktur zugeschnitten. Der Kunde kann bestimmte Werkzeuge ebenfalls über das IaaS-Portal der Fujitsu nutzen. Hierbei können die virtuellen Maschinen verwaltet werden.

Die Unterstützung durch vorbereitete Betriebssysteme ist positiv für den Kunden. Hier besteht das Potenzial für eine einfache Bereitstellung und Erweiterung der eigenen Infrastruktur, die dem Kunden zusätzlichen Aufwand und damit Kosten abnehmen könnte.

3.2.7 Portabilität und Interoperabilität

Im Bereich Portabilität und Interoperabilität werden vor allem Gefahren eines Vendor-Lock-Ins untersucht. Ein Mangel an Portabilität würde z.B. die Möglichkeiten des Kunden für einen Wechsel hin zu einem Angebot eines anderen Anbieters unmöglich machen oder zumindest nur mit hohem Aufwand ermöglichen. Daher ist dieses Thema auch Kern neuerer Standardisierungsbemühungen, z. B. der IEEE [13]. Speziell im Sinne der Investitionssicherheit für den Kunden ist dieser Abschnitt von Bedeutung.

Hilfreich bei Fragen der Portabilität und Interoperabilität sind Standards. Diese existieren seit der jüngeren Vergangenheit auch für die Speicherformate der virtuellen Maschinen. Neben dem Microsoft-eigenen VHD-Standard und dem VMWare-spezifischen VMDK-Standard hat das OVF-Format eine breite Unterstützung erfahren. Daneben sollte ein Blick auf vom Anbieter zur Verfügung gestellte APIs zur Integration nicht fehlen. Im Zuge der weiteren Standardisierung des Cloud-Computing-Umfeldes existieren Bestrebungen zur Vereinheitlichung der genutzten Technologie-Stacks, wie zum Beispiel OpenStack. Auch das Open Cloud Manifesto (OCM) [14], bzw. die Befolgung seiner Grundsätze, kann hier von Interesse sein. Das OCM ist eine Zusammenstellung von Prinzipien, u.a. im Bereich Sicherheit, ohne den Anspruch einer finalen Taxonomie. Kernpunkte sind vor allem eine geforderte Zusammenarbeit von Anbietern zur Adressierung der im Cloud-Umfeld existenten Herausforderungen (z. B. Sicherheit, Integration, Portabilität und Monitoring), einer Verhinderung von Vendor Lock-Ins, einer Verwendung anerkannter Standards und einer Kundenorientierung bei der Etablierung von Standards.

Sollte ein solcher Standard beim Anbieter implementiert sein, wäre dies ein großer Vorteil bei der Portabilität hin zu alternativen Angeboten, z.B. im Falle einer Insolvenz eines Anbieters.

Diesen Punkt ergänzend sind Migrationsmöglichkeiten des Anbieters selber interessant, um die Kompatibilität eines Formats zu einem anderen Format auch ohne eine gemeinsame Basis herzustellen. Bei Nutzung eines Backup-Angebots sollten die zugrundeliegenden Speicherformate und –medien auf Konformität zu Standards und anbieterunabhängige Formate untersucht werden. Dies gilt insbesondere für die Langzeitarchivierung, die viele Cloud-Anbieter als Angebot über den Zeitraum normaler Backups hinaus unterstützen.

Die Interoperabilität bei Fujitsu wird durch eine Vielzahl von Möglichkeiten unterstützt. So können zum Beispiel anstelle von vorkonfigurierten Betriebssystem-Images auch eigens vom Kunden angefertigte oder zuvor exportierte Images verwendet werden. Hierzu müsste allerdings die entsprechende Option hinzugebucht werden und die Images müssten im Open Virtualization Format (OVF) vorliegen. Eine weitere Nutzung von Images über die Dauer des Vertragsverhältnisses bei Fujitsu hinaus ist ebenfalls mit Einschränkungen möglich. Die Treiberkomponenten und damit die Lauffähigkeit des Systems ist auf den Hersteller VMWare zugeschnitten und würde, dem entsprechend, auch eine ähnliche Umgebung des gleichen Herstellers für einen erfolgreichen Ex- und Import benötigen. Darüber hinaus gehende Migrationsmöglichkeiten sind aufwandsbezogen möglich und werden im Bedarfsfall auch abweichend von den Standardvorgehensweisen realisiert. Zur Steuerung der IaaS-Infrastruktur wird ferner eine eigene API von Fujitsu zur Verfügung gestellt.

Die Bereitstellung von Betriebssystem-Abbildern im OVF-Format ist positiv zu bewerten, weil es sich um einen sich abzeichnenden Industrie-Standard handelt. Allerdings sollte der Kunde beachten, dass der Inhalt des Abbilds auf die VMWare Umgebung zugeschnitten ist, wie z.B. Treiberkomponenten und Hardware-Abstraktionsschicht.

Im Bereich Portabilität und Interoperabilität setzt Fujitsu seinen Kunden wenig Grenzen und ist daher positiv zu bewerten, jedoch erfolgt eine projektspezifische Abrechnung des Migrations-Aufwands. Die Möglichkeiten für einen flexiblen Einsatz der Infrastruktur inklusive einer Verschiebung der Maschinen on- und off-Premise sind gegeben und die Einrichtung der Steuerungs-API ist abhängig von ihrer Implementierung ein weiterer Vorteil für den Kunden.

3.3 Compliance und Audit

In diesem Bereich erfolgt die Zusammenfassung der regulatorischen Themen, die durch die Gesetzgebung und diverse Richtlinien vorgegeben sind und gegebenenfalls sicherheitsrelevante Auswirkungen haben. Dies beinhaltet sowohl mögliche Zertifizierungen durch unabhängige Dritte, wie auch die Fragen nach regelmäßigen Audits und den Vertragsvereinbarungen. Der Bereich Governance umfasst zusätzlich noch wichtige Sicherheitsrichtlinien und Normen, deren Erfüllung den Schutzzielen zugutekommt.

3.3.1 Zertifizierung

Mittels der Zertifizierungen der Vorgehensmodelle und des Notfallmanagements kann vom Anbieter der Nachweis einer Implementierung notwendiger sicherer Prozesse erbracht werden. Die gängige Zertifizierung ist die ISO-Norm 27001 für den Betrieb, die Überwachung, die Wartung, und die Verbesserung von Informationssicherheits-Managementsystemen. Darüber

hinaus gibt die Norm ISO 27002 Empfehlungen für das Informations-Sicherheitsmanagement, die allerdings nicht zertifizierbar sind. Des Weiteren dient die ISO/IEC 20000 als messbarer Qualitätsstandard für das IT Service Management. Dazu werden in der ISO/IEC 20000 die notwendigen Mindestanforderungen an Prozesse spezifiziert und dargestellt, die eine Organisation etablieren muss, um IT-Services in definierter Qualität bereitstellen und managen zu können.

Statement on Auditing Standards Nr. 70 (SAS 70) ist ein international anerkannter und gezielt für die Prüfung von Outsourcing-Geschäften angelegter Standard, durch den eine Berichterstattung über die implementierten Kontrollen beim Service-Anbieter erfolgt. Grundsätzlich bescheinigt ein solcher Bericht, dass ein Unternehmen über ein funktionierendes Kontrollsystem verfügt. Der SAS 70 Standard unterscheidet zwei Typen von Prüfungen. SAS 70 Typ I bestätigt die Beschreibung des internen Kontrollsystems des Dienstleisters zu einem bestimmten Zeitpunkt und enthält die zusammengefassten Ergebnisse einer unabhängigen Prüfungsgesellschaft. SAS 70 Typ II zielt darauf ab, das interne Kontrollsystem – zusätzlich zur reinen Beschreibung des Kontrollsystems – umfassend zu testen und es insbesondere hinsichtlich seiner Effektivität im Detail zu bewerten. Die Prüfung erfolgt über einen Zeitraum von sechs Monaten.

Fujitsu verfügen über eine Vielzahl von verschiedenen Zertifizierungen. Darunter fällt sowohl der ISO-Standard 20000 für ein IT Service Management auf Basis der ITIL, als auch die Zertifizierungen nach ISO-Standard 27001. Darüber hinaus hat Fujitsu Technology Solutions einen Bericht nach SAS-70 Typ II durch einen unabhängigen Prüfer erstellen lassen.

Bei Fujitsu und TDS sind Kundenorientierung und Kundenzufriedenheit, sowie ein ständiges Streben nach einer Verbesserung ihrer Qualitätssysteme und Lieferantenbeziehungen von großer Bedeutung. Aus diesem Grund haben sie sich den Anforderungen an ein Qualitätsmanagementsystem (QM-System) ISO 9001 unterzogen. Diese Zertifizierung steht für kundenorientierte, geregelte und prozessorientierte Abläufe im gesamten Bereich Application Hosting und sichert Kunden somit eine hohe Qualität der durch TDS erbrachten Dienstleistungen zu.

Die Zertifizierungshistorien von Fujitsu und TDS zeugen von einem großen Maß an Konformität zu den zugrundeliegenden Standards der Zertifizierungsstellen. Auch ist hier der Aufwand für die externen Prüfungen und kontinuierlichen Verbesserungen zu würdigen, so dass dieser Bereich als Fazit positiv bewertet werden kann.

3.3.2 Audit

Obschon Cloud Computing eine relativ junge Ausprägung der IT-Infrastruktur ist, ist die Verwaltung von Rechenzentren, die ebenfalls beim Cloud Computing genutzt werden, dies nicht. Daher existiert in diesem Bereich eine signifikante Anzahl von prozessualen und formalen Werkzeugen zur Sicherstellung eines reibungslosen Betriebs in Form von Überprüfungen. Die Art und Weise und auch die Frequenz dieser Überprüfungen wurde daher näher untersucht. Speziell Fragen zu Überprüfungen in den Bereichen Ausfallsicherheit und regelmäßigen Sicherheitsübungen, formale Rahmenwerke für Sicherheitstest, zum Beispiel in Form von Penetrationstest – auch für beteiligte Subunternehmen, unabhängige Sicherheitsrevisionen,

Berichte an den Kunden über die in der Vergangenheit erreichten Service Levels und die Möglichkeit für Kunden auch eigene Penetrationstests durchzuführen werden hier gestellt.

Zur Gewährleistung eines kontinuierlich hohen Sicherheitslevels werden bei Fujitsu in regelmäßigen Abständen Sicherheitsübungen und –revisionen durchgeführt. Diese Übungen simulieren beispielsweise den Ausfall eines Cloud-Computing-Standorts zur Verbesserung der Reaktionsfähigkeit des Personals und zur Optimierung der Prozesse. Sofern notwendig, würden auch Subunternehmen in diese Maßnahmen miteinbezogen.

Fujitsu bietet den Kunden, nach vorheriger Absprache, die Möglichkeit zur Durchführung eigener Penetrationstests. Dem Kunden werden in monatlichen Intervallen Berichte über die erreichte Qualität des IaaS-Service elektronisch zugesendet. Speziell im Bereich der Verfügbarkeit haben diese Berichte auch abrechnungstechnische Relevanz. Des Weiteren beinhalten die Reports Abschnitte zu Trends und speziellen Aktivitäten, mit denen Fujitsu Auskunft über die Maßnahmen zur weiteren Verbesserung der Services gibt. Nicht zuletzt wird auch ein Überblick über die Aktualisierungen im System und eine Übersicht der im Berichtszeitraum aufgelaufenen Support-Calls gegeben. Die Berichte können darüber hinaus kundenspezifisch angepasst werden und zusätzliche Informationen enthalten.

Neben den Vereinbarungen zu Service Levels zeugt die Bereitschaft zur Durchführung eigener Tests der Kunden von Vertrauen in die eigene Infrastruktur. Dabei ist die generelle Möglichkeit von kundeneigenen Sicherheitstests positiv zu bewerten, jedoch wären klarere Richtlinien über den durchführbaren Test-Umfang und –Grenzen wünschenswert. Zudem ist eine Nutzung dieses Angebots durch den Kunden anzuraten.

3.3.3 Vertragsvereinbarungen

Die Vertragsvereinbarungen stellen die Grundlage der Dienstleistung zwischen dem Cloud-Computing-Anbieter und dem Kunden dar. Insbesondere bei zusätzlichen Anforderungen an die Dienstleistungen existieren Sonderregelungen und –Berechtigungen für Anbieter, die ein Kunde im Vorwege beachten sollte. So ist Fujitsu mit den Prinzipien Good Manufactoring Practice (GMP) konform. GMP beschreibt Verfahren, Prozesse, Ausrüstungs- und Betriebsmittel sowie Regeln für die Herstellung von Produkten der Pharma-, Kosmetik- und teilweise der Lebensmittel- und Futtermittelindustrie.

Die Bedeutung der Sicherheit von IT-Infrastrukturen auf nationaler Ebene ist aufgrund der zunehmenden Vernetzung kontinuierlich gestiegen. Dieser Bedeutung geschuldet ist die Einrichtung von Koordinierungsstellen auf internationaler und nationaler Ebene zur Sicherstellung der Funktion dieser Infrastrukturen, wie z.B. diverse CERT – Computer Emergency Response Team - Organisationseinheiten. Hierbei wird Wert auf die Verringerung der Reaktionszeiten bei sicherheitsrelevanten Vorfällen gelegt. Für die Bundesrepublik Deutschland übernimmt diese Aufgabe der Information und Koordination zukünftig das nationale IT-Krisenmanagement [15]. Eine Einbindung des Anbieters in diese Strukturen ist für die Kunden eine zusätzliche Versicherung für die Robustheit der angebotenen Dienste.

Fujitsu verfügt, nachgewiesen durch diverse Zertifizierungen Dritter, über ausgewiesene Kapazitäten z. B. zur Verarbeitung von schützenswerten Daten aus der Automobil- und Lebensmittelindustrie, dem Bankengewerbe und der Pharmabranche. Des Weiteren wird eine

eigene, zentrale Organisationseinheit in Form eines CERT im Bereich der Cloud-Computing-Sicherheit unterhalten.

Die Einbindung in die CERT-Infrastrukturen und der Nachweis der Erfüllung spezieller branchenspezifischer Sonderreglements sind aus Kundensicht vorteilhaft zu bewerten.

3.3.4 Governance

Die Governance definiert sich im Allgemeinen als Steuerungs- und Regelungssystem für Organisationen. In Bezug auf die Informationssicherheit ist sie ein Ansatz auf Prozessebene zur Etablierung dieser Systeme. Hierbei ist eine Abwägung zwischen dem Aufwand und den Kosten zur Durchsetzung der Prozesse, der Sammlung der Daten, der Bestimmung der zu nutzenden Metriken und dem Wert eines Rahmenwerks zur Informationssicherheit für die Bezugs- und Nutzungsmodelle des Cloud-Computing-Systems zu treffen. In diesem Zusammenhang kann die Verantwortung für die Steuerungs- und Regelungssysteme nicht singulär beim Cloud-Computing-Anbieter liegen, sondern erfordert die Einbeziehung der Kundensicht in ähnlichem Maße. Bei den zu beachtenden Richtlinien für die Informationssicherheit sei angemerkt, dass diese auf etablierten Standards basieren sollten. Als Beispiele hierfür können die einschlägigen Veröffentlichungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI), der European Network and Information Security Agency (ENISA) oder auch die verschiedenen Standards im Bereich Sicherheit des National Institute of Standards and Technology (NIST) dienen.

Das Cloud-Computing-Angebot von Fujitsu umfasst ein Notfallmanagement, wie es auch in der ISO 27001 vorgeschrieben wird. Obwohl auf zahlreichen einzelnen Maßnahmezielen beruhend, bezieht sich das Notfallmanagement zusammengefasst auf:

- eine Übernahme der Gesamtverantwortung im Falle eines Notfalls durch die Leitungsebene,
- einer Bereitstellung angemessener Ressourcen zur Bewältigung der Notlage und
- einer Integration der Mitarbeiter in organisationsweite Abläufe.

Zudem sind vorbeugende Tests und Sicherheitsübungen genauso Teil des Notfallmanagements wie eine nachgeordnete Prozessverbesserung.

Neben dem Notfallmanagement, welches bedeutungsgemäß erst im Falle eines Notfalls greift, trifft Fujitsu schon im Vorwege zahlreiche Maßnahmen zur Sicherstellung der Sensibilisierung der Mitarbeiter für Themen wie Datenschutz, Betriebssicherheit und Vertraulichkeit von Daten. So werden, im Rahmen des gesetzlich Zulässigen, Überprüfungen des Personals auf deren Vertrauenswürdigkeit durchgeführt. Regelmäßige, verpflichtende Schulungen für alle relevanten Mitarbeiter dienen darüber hinaus einer weiteren Vorbeugung vermeidbarer Vorfälle.

Zur Sicherstellung eines einheitlichen gesetzlichen Rahmens in Bezug auf staatliche Zugriffsmöglichkeiten und Datenschutz besteht die Möglichkeit einer Beschränkung der in die Datenverarbeitung involvierten Rechenzentren auf Regionen. Für einen Kunden aus Deutschland bedeutet dies die mögliche Einschränkung auf eine Datenverarbeitung in einem der zwei deutschen Rechenzentren in Neckarsulm und Neuenstadt.

Die Aufteilung von Dienstleistungen für den Kunden auf verschiedene Sub-Unternehmen ist keine Besonderheit des Cloud Computings, hat in diesem Bereich allerdings eine ähnlich hohe, wenn nicht höhere Bedeutung. Begründet liegt dies in der zunehmenden Spezialisierung von Teilbereichen, wie zum Beispiel der Bewachung der Rechenzentren oder der Überprüfung der Daten auf Viren. Unternehmen setzen hierbei nicht auf eigene Lösungen, sondern bedienen sich aus diversen Angeboten von spezialisierten Unternehmen. Von Bedeutung ist dann wiederum die Offenlegung dieser Dienstleistungsbeziehungen durch den Anbieter gegenüber dem Kunden. Fujitsu kommt diesem Wunsch nach Transparenz nach. So werden bspw. für den Betrieb der Rechenzentren Dienstleistungen der TDS AG, einer über 80 prozentigen Tochter der Fujitsu genutzt. Für technische Dienstleistungen, speziell auf dem Sicherheitsbereich, werden Software und Angebote der Symantec Corporation, zum Beispiel zur Erkennung von Spam und Viren im Mail Security Bereich benutzt. Service Level Agreements der Sub-Dienstleister werden, soweit anwendbar, in das Agreement zwischen Fujitsu und dem Kunden mit aufgenommen.

Aufklärung und Transparenz wird auch beim Einsatz der eigenen Software beim Kunden betrieben. Welche Soft- und Hardwarekomponenten, zum Beispiel beim Hybrid-Cloud-Betrieb, von Fujitsu beim Kunden benutzt werden, wird vor deren Einsatz kommuniziert.

Im Bereich der eingesetzten Softwarelösungen und –Dienste werden vor Inbetriebnahme auf einer eigenen Laborplattform interne Sicherheitstests durchgeführt, um die korrekte Funktion der Lösungen sicherzustellen. Erst nach einem erfolgreichen Bestehen dieser Tests erfolgt eine Einspielung in die Produktivumgebung.

Der Bereich Governance bietet einen Überblick über die umfangreichen und damit positiv zu bewertenden Maßnahmen von Fujitsu. Neben dem Nachweis über das implementierte Notfallmanagement und der Sensibilisierung der Mitarbeiter gewährleisten auch die Testbedingungen eine funktionierende Gesamtumgebung. Nichtsdestotrotz wäre eine Erweiterung der regelmäßigen Kundeninformation auf aktuelle und bevorstehende Veränderungen organisatorischer Natur wünschenswert.

4 Optionale Security-as-a-Service Erweiterungen zum IaaS-Angebot

Eine spezielle Art von Software-as-a-Service Angeboten stellt die Security-as-a-Service-Kategorie dar. Hierbei werden die Dienste ebenfalls auf Cloud-basierten Systemen angeboten, allerdings handelt es sich ausschließlich um Sicherheitsfunktionalitäten, deren kundenseitige Realisierung auf gleichem Niveau mit entsprechendem Mehraufwand verbunden wäre. Typischerweise betrifft dies Sicherheitsfunktionalitäten unter Anderem zur Auslagerung von E-Mail-Schutz, Verschlüsselung von E-Mails, Filterung ein- und ausgehender Verbindungen, sowie Authentifizierung. Oftmals werden diese Dienste nicht ausschließlich online in einer Cloud-Umgebung erbracht, sondern über Appliances lokal zur Verfügung gestellt oder über separate Hardware realisiert (Managed Security Services). Die Vorteile des Kunden ergeben sich vor allem aus einer besseren Planbarkeit der Finanzierung durch ein Abonnement-Modell anstelle von Anschaffungsinvestitionen mit folgend variablen Kosten beim Eigenbetrieb sowie einem stark verminderten Administrationsaufwand, speziell in Bezug auf die bei Sicherheitssoftware notwendigen Aktualisierungen. Die Nachteile sind hierbei die relative Abhängigkeit von einem

Anbieter für eine sicherheitsrelevante Leistung in Verbindung mit oft eingeschränkten Konfigurationsmöglichkeiten im Vergleich zu einer unabhängigen Lösung, sowie langfristig eventuell höhere Kosten durch das Abonnement. Speziell der Abhängigkeitsaspekt kann im Bereich des Patchings, durch eine mögliche zeitliche Verzögerung bei der Auslieferung der Aktualisierungen, Auswirkungen auf die Sicherheit haben.

Fujitsu unterstützt die Einbindung von Sicherheitsdiensten als Ergänzung zum eigenen IaaS-Angebot. Hierzu werden Dienste im sicherheitsrelevanten Bereich angeboten, die die Notwendigkeit des Vorhaltens kundeneigener Ressourcen weiter beschränken können.

Eine zentrale Komponente sind die Schutzmaßnahmen für die Bereiche E-Mail, Web und Instant-Messaging. Mittels eines Rückgriffs auf Produkte verschiedener externer Anbieter wird ein grundsätzlicher Schutz vor Viren und Spam in den genannten Bereichen erreicht. Dies beinhaltet erwartungsgemäß auch die feingranulare Konfiguration von der Erkennung dienlichen Informationen, wie z.B. Schlüsselwörter und URL-Listen, als auch der im Nachgang einer Erkennung durchzuführenden Aktionen. In der Erweiterung dieser Dienste für die E-Mail-Kommunikation werden kundenseitige Kontrollmöglichkeiten eröffnet, die eine Filterung der Inhalte auf Basis von Richtlinien zulassen und die Verschlüsselung der ausgehenden Kommunikation ermöglichen. Besondere Aufmerksamkeit erfährt die Verarbeitung von in E-Mails enthaltenen Bildern.

Als weiteren Bereich für einen zusätzlichen Security-as-a-Service-Dienst ist die bereits an anderer Stelle erwähnte Authentifizierung für Administratoren des Kunden zu nennen. Die herkömmliche Absicherung durch Kombinationen von einem Benutzernamen und einem Passwort greifen hier wegen der weitreichenden Berechtigungen der Konten oftmals zu kurz. Eine zusätzliche Absicherung durch das bekannte One-Time-Password-Verfahren mittels eines Software-Tokens erhöht den Schutz der Administrationskonten erheblich, sofern das Betriebssystem, auf dem Software-Token ausgeführt wird, entsprechend gesichert ist und nicht kompromittiert wurde.

Sicherheit im Sinne von Security-as-a-Service beinhaltet auch die Sicherheit der Daten. Diese muss auch in virtualisierten Umgebungen gewährleistet sein. Mittels einer Software eines Drittanbieters bietet Fujitsu eine Erweiterung seines eigenen Backup-Konzeptes an. Im Normalfall werden von jeder Kundeninstanz einmal am Tag Momentaufnahmen, so genannte Snapshots gezogen, die zu einem beliebigen späteren Zeitpunkt wiedereingespielt werden können. Der Nachteil einer solchen Lösung liegt im mit jeder Wiedereinspielung verbundenen Datenverlust der seit dem letzten Snapshot hinzugekommenen oder veränderten Daten. Sofern es sich beim gesicherten System um ein System mit geringen Datenveränderungen, wie z.B. fest konfigurierte Front-End-Webserver handelt, dann ist ein solcher Verlust eventuell vernachlässigbar und das Snapshot-Verfahren damit ausreichend. Handelt es sich jedoch um sich verändernde Systeme, wie beispielweise Datenbankserver, so ist höchstwahrscheinlich eine andere Sicherungsstrategie zielführender. Für diesen Fall wird eine häufigere oder kontinuierliche Sicherung der Daten empfohlen. Aufgrund des damit verbundenen Aufwands und seiner nicht immer notwendigen Anwendung wird dieses Angebot optional gehalten.

5 Handlungsempfehlungen für Kunden

Cloud Computing ändert nichts an der unternehmerischen Verantwortung für den Datenschutz. Das Unternehmen ist und bleibt der „Herr der Daten“ genauso wie im Fall des Outsourcings, Application Service Provider (ASP) oder Einsatz von Managed Services. Es ist somit für die Authentizität, Integrität, Verfügbarkeit und Vertraulichkeit der Daten voll verantwortlich. Diese Verantwortung kann das Unternehmen vertraglich nicht auf einen Dienstleister abwälzen. Das Bundesdatenschutzgesetz (BDSG) verpflichtet die Unternehmen per se zur "sorgfältigen Auswahl" des Cloud-Providers, sowie zur Überprüfung der von ihm durchgeführten Datenschutzmaßnahmen.

Die an Cloud-Services interessierten Unternehmen müssen ihre Daten analysieren und ihre Schutzbedarfe festlegen. Diese Anforderungen müssen sie mit den Gegebenheiten der Cloud-Lösungen abgleichen. Ausgehend vom ausgewählten Cloud Service Modell (IaaS, PaaS, SaaS) variieren die Rechten und Pflichten der Kunden in der Cloud-Infrastruktur. Da dieses Whitepaper das Fujitsu-IaaS-Angebot untersucht und IaaS die größten Freiheiten den Kunden anbietet, bedingt dies gewisse Rahmenbedingungen. Im Folgenden werden die Eckpunkte dieser Pflichten in Form von Empfehlungen an die Kunden betrachtet.

Verschlüsselung der Daten

Personenbezogene, finanz- und steuerrelevante, sowie andere Daten mit besonderem Schutzbedarf sollen von Kunden verschlüsselt auf den angemieteten Ressourcen abgelegt und gespeichert werden. Dies schützt auch im Falle eines unberechtigten Zugriffs, einer Kompromittierung spezieller Dienste und Anwendungen oder gar des Hypervisors der virtuellen Maschine um im schlimmsten Fall keinen Datenverlust erfahren zu müssen.

Schlüsselverwaltung

Die Verantwortung des Kunden für die Schlüsselverwaltung innerhalb des IaaS-Angebots bietet ihm ein höheres Maß an Flexibilität und letztendlich auch Sicherheit, weil so zum Beispiel Schlüsselmaterial verwendet werden kann, welches bereits in die Infrastruktur des Kunden eingebunden ist und somit in definierte Prozesse zum Anlegen, Verwalten und Löschen eingebettet ist.

Genau wie bei jedem Passwortschutz ist auch bei einer Absicherung durch Schlüssel ein Wechsel der Schlüssel in gewissen Zeiträumen angeraten. Unterstützungsleistungen des Anbieters zum reibungslosen Austausch von Schlüsseln wären dabei sinnvoll, um während des Austauschs nicht die Möglichkeit eines Zugangs zum System zu verlieren oder es durch andere unsicherere Zugangsmechanismen zu gefährden. In diesem Zusammenhang sollte das Szenario des Schlüsselverlustes durchdacht werden:

- Wie sind die Prozesse zu gestalten, um die mögliche Zeit nach dem Bekanntwerden eines Verlustes bis zur Deaktivierung des betroffenen Schlüssels möglichst klein zu halten?
- Wie kann dennoch ein reibungsloser Zugang zum System während dieser Zeit gewährleistet werden?

- Existieren von Seiten des Anbieters Möglichkeiten, die im Falle eines Verlustes von Schlüsseln greifen?

Rollen- und Berechtigungskonzept

Eine umfassende Sicherheitsstrategie für die eigenen Dienste und Anwendungen mit der Berücksichtigung von Mitarbeiter-Rollen soll durchgehend konzipiert und umgesetzt werden. So können Unternehmen mit Rollen- und Berechtigungskonzepten gezielt festlegen, wer auf welche Informationen in der Cloud zugreifen darf. Ein Berechtigungskonzept dient dem Schutz von Ressourcen vor Veränderung oder Zerstörung und unterstützt die Datensicherheit im Unternehmen. Darüber hinaus verhindert die Implementierung eines solchen Konzeptes auch den unrechtmäßigen Gebrauch der Informationen und dient dem Zweck des Datenschutzes. So werden die Daten über Authentisierungs- und Autorisierungsmethoden in der Cloud geschützt.

Härtung der Browser

Speziell im Kontext der Sicherung von Zugängen wird die Verwundbarkeit von Browsern oft vernachlässigt. Vor allem bei webbasierten Administrationszugängen ist diese Sicherung aber von großer Bedeutung. Zwar ist die Anzahl der Sicherheitslücken in Browsern seit Jahren relativ stabil im mittleren dreistelligen Bereich [16], allerdings mit zunehmender Tendenz. Darüber hinaus ist das Gefährdungspotenzial durch browserspezifische Sicherheitslücken sehr viel höher, weil diese Softwareart einsatzbedingt besonders exponiert ist. So ist es für einen Angreifer im Vergleich sehr viel schwerer Sicherheitslücken in Anwendungen innerhalb eines geschützten Netzwerks auszunutzen, als eine bekannte Lücke in einem Browser auszunutzen, der naturgemäß mit Stellen außerhalb des eigenen Netzwerks kommuniziert.

Generell und speziell für die Zugänge und Zugangsdaten zur Administrationsplattform ist daher die Nutzung von stets aktuellen und darüber hinaus gesicherten/gehärteten Browsern zu empfehlen.

Anbindung von Kunden-Netzwerken an Fujitsu-Rechenzentren

Da die Cloud-Dienste über das Internet bezogen werden, ist eine zuverlässige und performante Netzwerkanbindung von überragender Bedeutung. Deswegen ist es sehr wichtig sich Gedanken über die benötigte Bandbreite, Antwortzeiten und Verfügbarkeiten der Anbindung, sowie über die sichere Übertragung der Daten zu machen. Dafür stellt Fujitsu mehrere technische Möglichkeiten, wie z.B. IPSec VPN über das Internet, VPN über MPLS oder dedizierte Punkt-zu-Punkt-Verbindung, zur Verfügung. Bei der ersten Variante wird der vorhandene Anschluss des Kunden genutzt. Dabei soll auf die Auswahl eines passenden Telekommunikations-Carriers geachtet werden.

Sicherungs- und Wiederherstellungskonzept

Fujitsu bietet Sicherungsdienste für virtuelle Instanzen an. Sollte ein Kunde eine dedizierte Instanz für sein Cloud-Angebot nutzen, so obliegt auch ihm selber die Pflicht zur Etablierung eines Sicherungskonzeptes. Ein weiterer Punkt ist die Möglichkeit der Wiedereinspielung. Diese ist im konkreten Fall nicht durch den Kunden selber möglich, sondern muss von diesem bei Fujitsu in Auftrag gegeben werden. Die Erfüllung einer solchen Anfrage dauert von Seiten des Anbieters einen Arbeitstag. Diese Verzögerung kann dabei unter Umständen zu inkonsistenten

Zuständen oder einer Unterbrechung des durch den Kunden beim Anbieter gehosteten Service bedeuten.

Eine Empfehlung ist es daher, den Umstand eines Ausfalls der Systeme konzeptionell zu bedenken. Sollten die von Fujitsu bereits etablierten Möglichkeiten zur Sicherung und Wiederherstellung der Instanzen für einen Betrieb der Dienste nicht ausreichen, so sind entsprechende Reserve-Kapazitäten in Erwägung zu ziehen. Speziell die Dauer der Wiedereinspielung von Backups ist hier zu bedenken. In diesem Fall können auch eigene Sicherungsdienste Anwendung finden, um im Fall der Fälle eine Wiederherstellung einer Sicherung in Eigenregie in kürzerer Zeit durchführen zu können. Die Granularität der Datensicherung sollten ebenfalls Gegenstand weiterer Überlegungen sein. Aufgrund der erwähnten Trennung zwischen Fujitsu-Infrastruktur und Kundeninfrastruktur kann Fujitsu als kleinstmögliche Einheit nur die virtuellen Instanzen sichern. Alles andere würde eine nicht gewünschte Kenntnis der Inhalte der Instanz erfordern. Oft ist aber eine Sicherung nur bestimmter Teile einer Instanz notwendig. Dies würde wiederum die Wiedereinspielungszeiten dramatisch senken.

Gesetzliche Bestimmungen

Für eine Vielzahl von Branchen, Unternehmen und/oder Geschäftsbereichen existieren gesonderte, gesetzliche Bestimmungen zur Datenhaltung, Datenverarbeitung und zum Datenschutz. Einige spezielle Bereiche sind von Fujitsu bereits über Zertifizierungen abgedeckt, für alle andere muss eine separate Prüfung der Bestimmungen durch den Kunden erfolgen. Bei der Nutzung von Cloud-Computing-Angeboten ist daher eine genauere Betrachtung der eigenen Regelungswerke notwendig und empfehlenswert. Der Kunde ist in letzter Instanz selbst für die korrekte Einhaltung der für ihn geltenden Gesetze verantwortlich und kann sich dieser Pflicht auch nicht über eine Beauftragung, z.B. von Fujitsu, entledigen.

Es ist daher in jedem Fall eine entsprechende rechtliche Beratung zu diesen Punkten einzuholen. In einigen Bereichen, z.B. der Sozialdatenverarbeitung, bestehen generell höhere Anforderungen, so dass hierbei expliziter rechtlicher Rat notwendig ist.

Fujitsu Zusatzsicherheitsdienste für IaaS

Fujitsu bemüht sich sehr den Kunden das höchste Sicherheitsstandard anbieten zu können. Da diverse Kunden über unterschiedliches Schutzniveau und unterschiedliche Geschäfts-anforderungen verfügen, bietet Fujitsu ein Set an vorkonfigurierten Sicherheitsservices an. Somit bekommt ein Kunde ein flexibles und umfassendes Angebot, das er sich nach seinen Anforderungen zusammenstellen könnte.

6 Zusammenfassung der Ergebnisse

Nach einer Untersuchung der Dokumentation und Interviews mit Verantwortlichen in Bezug auf die Sicherheit des Angebots „Fujitsu Cloud in Central Europe“ (IaaS) und Abgleich mit dem Gesamtfragenkatalog, basierend auf den BSI-Mindestsicherheitsanforderungen für Cloud Computing und Studien des Fraunhofer-Instituts SIT lässt sich zusammenfassen, dass Fujitsu den überwiegenden Teil der betrachteten Vorgaben erfüllt oder sogar übertrifft. Besonders hervorzuheben ist die Sicherheit im Infrastruktur Bereich, dem Monitoring und dem Incident Management, sowie die hohe Zahl an Zertifizierungen als Nachweis der Konformität zu anerkannten Standards. Im Bereich Datensicherheit und Backup liegt der Aufwand auf der Kundenseite, weil der Kunde der „Herr der Daten“ ist und Fujitsu ihm lediglich Unterstützungsleistungen zur Verfügung stellt. Verbesserungspotenziale hingegen bestünden in der weiteren Unterstützung der Kunden, insbesondere KMUs, z.B. mit Security Best Practices zu Konfiguration und Betrieb, sowie im Berichtswesen mit einer klareren Kommunikation organisatorischer Gegebenheiten und bevorstehender Änderungen.

Insgesamt gesehen wäre eine vergleichbare Sicherheitsausstattung für KMUs nur mit erheblichem finanziellem Aufwand möglich und ökonomisch höchstwahrscheinlich nicht mehr im Verhältnis zum Schutzwert der Daten. Hierbei sind die notwendigen Kosten für Ausbildung und/oder Einstellung von Personal mit dem notwendigen Know-How nicht mit einberechnet. Ein kontinuierliches, professionelles Monitoring, wie es von Fujitsu kommuniziert wird, könnte ebenfalls ein großes Hindernis bei der Etablierung eigener IT-Leistungen sein. Neben der bloßen Infrastruktur wären hierfür auch Vorkehrungen für die Überwachung der eingehenden Daten notwendig, was schon rein personell erst ab einer gewissen Größenordnung Sinn macht. Die erweiterten Möglichkeiten für ein Monitoring über das Fujitsu Systems Management Center (SMC) verstärken diesen Fakt noch weiter. Viele der Maßnahmen ließen sich auch bei einigen größeren Unternehmen mangels mindestens zwei getrennter Rechenzentrumsstandorte nicht realisieren. Insbesondere im Fall von komplexen Desaster Recovery Szenarien könnten diese Unternehmen von der Nutzung der Cloud Angebote überdurchschnittlich profitieren.

Die strukturierte Vorgehensweise der durchgeführten Sicherheitsuntersuchung anhand des Gesamtfragenkatalogs diente dem Abbau der Informationsasymmetrien zwischen Fujitsu und Kunden. Somit besteht die Hoffnung, dass ein Großteil der Sicherheitsbedenken durch die zusätzlichen Informationen zu den getroffenen Sicherheitsvorkehrungen von Fujitsu in dieser Studie ausgeräumt werden konnten. Dessen ungeachtet bestehen natürlich weitergehende Sicherheitsbedürfnisse, die sich aus dem individuellen Anwendungsfall ergeben. Die Umsetzung der dafür notwendigen, erweiterten Sicherheitsmaßnahmen liegt in der Verantwortung des Kunden. Diese Maßnahmen müssen allerdings von ihm im Rahmen eines Sicherheitsprozesses durchdacht, beobachtet und kontinuierlich verbessert werden.

7 Sicherheitstrends im Cloud Computing

Der IT-Markt entwickelt sich sehr rasant und IT-Systeme werden immer komplexer. Hinzu kommen eine Reihe neuer IT-Bedrohungen. Industriespionage und Angriffe auf die IT-Infrastrukturen werden stets professioneller. Die angespannte wirtschaftliche Situation durch die neuste Wirtschaftskrise verstärkt die Nachfrage nach Cloud-basierenden Lösungen und den damit einhergehenden Vorteilen wie Kosteneffizienz, flexible Anpassung der IT an aktuelle Erfordernisse sowie Hochverfügbarkeit und Sicherheit.

Zu den wichtigsten Wendepunkten in den Unternehmen im Rahmen der Informations- und Kommunikationstechnologien zählen somit:

- Virtualisierung
- Cloudifikation
- Mobilität
- Industrialisierung von Hackern
- Externalisierung und Kollaboration
- Consumerization der IT [17].

Diese Tendenzen führen zu den neuen Herausforderungen im Sicherheitsbereich. Nicht zuletzt hat die Bundesregierung die IT-Sicherheit auf ihre Agenda gesetzt. Demgemäß hat das Ministerium für Bildung und Forschung (BMBF) die folgenden Schwerpunkte in der IT-Sicherheitsforschung und damit die Richtung für die neuen Entwicklungen vorgegeben:

- Sicherheit in unsicheren Umgebungen, insbesondere mit dem Einsatz von mobilen Geräten,
- Schutz von Internet-Infrastrukturen und Eingebaute (Embedded) Sicherheit,
- Intrinsisch sichere Systeme,
- Durchgehender Schutz von IT-Systemen und
- Identifikation von Schwachstellen.

Cloud-Systeme werden als unsichere Umgebungen eingestuft. Dies führt zum mangelnden Vertrauen und somit einem verzögerten Einsatz in Unternehmen, insbesondere im Mittelstand. Um dies zu ändern müssen die Cloud-Anbieter ihr Augenmerk besonders auf die IT-Sicherheit richten. Dafür sollte unter anderem den Sicherheitstrends im Cloud Computing gefolgt werden, die im Folgenden näher beschrieben sind.

Security Dashboard

Das Bedrohungsniveau des Unternehmens steigt nicht nur durch neue Angriffstechniken, sondern vielmehr durch die zunehmende Komplexität und Anzahl von IT-Sicherheitssystemen, gesetzlicher Vorgaben und anzuwendender Standards. Immer öfter wird klar, dass eine weitere Firewall oder eine neue Verschlüsselung das Sicherheitsproblem in einem Unternehmen oder einer IT-Umgebung nicht lösen können. Deswegen sind viele Sicherheitsexperten sich einig, dass die IT-Sicherheit durch mehr Transparenz erhöht werden sollte. Eine unentbehrliche Komponente dafür ist ein Security Dashboard, in dem das aktuelle Sicherheitsniveau sowie der Status der Erfüllung der Compliance Vorgaben anhand der Aggregation, Normalisierung/Normierung und aussagekräftiger Aufbereitung der Informationen aus den

verteilten Sicherheitslösungen jederzeit zeitnah angezeigt wird. Dies wird mit dem Einsatz von Cloud-Computing-Lösung noch aktueller als den je.

Die Transparenz in Bezug auf den Status der Sicherheitssysteme (Security Level Management), die durch ein Security Dashboard geschaffen werden kann, sowie der kontinuierliche Abgleich der tatsächlichen Leistungen der Schutzsysteme mit Zielvorgaben ist ein Schlüssel zu deren kontinuierlichen Verbesserung der IT-Sicherheit im Unternehmen. Des Weiteren unterstützt das Security Dashboard auch den Leitgedanken des BMBF: „Das Vertrauen in die Informations- und Kommunikationstechnik beruht auf überprüfbaren und durchgehend sichereren Systemen", weil dies zur besserer Überprüfbarkeit der IT-Systeme und somit mehr Sicherheit beiträgt.

Sicheres Data und Software Development Lifecycle Management

Sicherheit soll im ganzen Lebenszyklus der Softwareentwicklung wie auch des Datenmanagements berücksichtigt werden. Dafür müssen in den Unternehmen entsprechende Sicherheitsregelwerke (Security Policies) vereinbart und durchgehend genutzt werden. Die Einhaltung dieser Regeln soll auch in jedem Stadium geprüft und die Maßnahmen beim Nichteintreten eingeleitet werden.

Hybrid Cloud Management Plattform

Nach der Meinung von Cloud-Experten werden sich in der nächsten Zeit eher hybride Clouds durchsetzen, weil die Mehrheit der Unternehmen bereits über eine IT-Infrastruktur verfügt. Eine Hybrid Cloud Management Plattform wird den Unternehmen ein Überblick über die genutzten Ressourcen: on- und off-Premise, und über das Patch-, Kapazitäts-, und Bereitstellungs-Management, sowie ihre Steuerung erleichtern. So ist z.B. Single Sign On (SSO) aus der Cloud und in der Cloud denkbar.

Interoperabilität und Portabilität

Interoperabilität und Portabilität von Cloud-Services ist essentiell für die erleichterte Migration der Daten zwischen den Cloud-Anbietern. Die ist gegeben, wenn die Standards z.B. auf der Schnittstellen oder Protokollebene unterstützt werden, sowie die Daten in den standardisierten Formaten, z.B. als CSV mit verfügbaren Metadaten den Kunden zur Verfügung gestellt werden. Für bessere Kommunikation zwischen unterschiedlichen Cloud-Umgebungen sollten noch Standards für den Austausch der Kontext-Informationen etabliert und verwendet werden.

Cloud Identity Layer

Identity Layer in der Cloud stellt einen abstrakten ID-Layer dar, der alle Identity- and Access-Management Aspekte an einer Stelle kapselt. So können Identitäten einfach integriert, eingesetzt und verwaltet werden und beim Anwender das Vertrauen in die Cloud schaffen, dass sie kontrollieren können, wer Zugang zu welchen Services hat.

Zusätzlich können noch Intermediärlösungen für sichere vertrauenswürdige Identitäten, wie z.B. eID-Brokern eingesetzt werden. Es ist denkbar, dass die eIDs wie z.B. neuer Personalausweis in Deutschland weitere Verbreitung finden werden, sowie Biometrics wie Bio-IDs verstärkt für die Cloud verwendet werden.

„Versiegelte“ Cloud-Infrastruktur

Die „versiegelte“ Cloud-Infrastruktur funktioniert auf der Basis von Trusted Platform Modules (TPMs), in der der Betreiber nicht auf die Daten seiner Kunden zugreifen kann. Durch den HW-basierten Vertrauensanker sollte letztlich durchgängiger Schutz der Daten durch den Ausschluss des Zugriffs auf die Daten von der Seite des Betreibers der Cloud, seines Personals sowie externer Dritten gewährleistet werden.

Kombination von Kryptographie und Steganographie

Durch eine Kombination von Kryptographie und Steganographie sollten die kritischen Daten in den Cloud-Computing-Systemen abgesichert werden, so dass niemand anders als der Eigentümer die Einsichten in die Daten versteht.

Verstärkung von Compliance Vorgaben

Ein grundsätzlicher Trend, der ebenfalls auf Cloud Computing auswirkt, ist die Verstärkung von Compliance Vorgaben. Die Unternehmen sind gezwungen einen hohen Maß an Governance und Compliance vorweisen zu müssen. Die Pflicht der externen Audits nimmt zu. Dies effektiv zu gestalten, ist oft schwierig für viele KMUs. Diese Last können die hochqualifizierten Cloud-Anbieter ihnen abnehmen. Der Trend geht dahin, dass die Cloud-Anbieter sich auf die Sicherheitsthemen spezialisieren und leistungsstärkere und fortschrittlichere Sicherheitsoptionen, die als Cloud-Services zur Verfügung stehen, ihren Kunden anbieten. Damit wird ein Level an Sicherheit geliefert, den die meisten Unternehmen eigenständig mit vertretbarem Aufwand so nicht erreichen können.

Literaturverzeichnis

1. **Dr. Werner Streitberger, Angelika Ruppel.** Cloud Computing Sicherheit: Schutzziele.Taxonomie.Marktübersicht. *Fraunhofer Institut für Sicherheit in der Informationstechnik.* [Online] 25. September 2009. [Zitat vom: 9. März 2011.] http://www.sit.fraunhofer.de/presse/texte-studien/Cloud-Security-Studie.jsp.

2. **Bundesamt für Sicherheit in der Informationstechnik.** Cloud Computing: Eckpunktepapier Mindestsicherheitsanforderungen an Anbieter von Cloud-Lösungen. *Bundesamt für Sicherheit in der Informationstechnik.* [Online] 28. September 2010. [Zitat vom: 9. März 2011.] https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Sonstige/Cloud_Computing_Mindestsicherheitsanforderungen.pdf.

3. **National Institute of Standards and Technology.** Computer Security Division. *Computer Security Resource Center.* [Online] 17. August 2010. [Zitat vom: 15. April 2011.] http://csrc.nist.gov/groups/SNS/cloud-computing/.

4. **National Institute of Standards and Technology.** Information Technology Laboratory. *The NIST Definition of Cloud Computing.* [Online] 10. Oktober 2009. [Zitat vom: 15. April 2011.] http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc.

5. **Fujitsu Technology Solutions GmbH.** Fujitsu Business Enablement Services. *Fujitsu Technology Solutions GmbH.* [Online] 19. November 2010. [Zitat vom: 23. Mai 2011.] https://globalsp.ts.fujitsu.com/dmsp/docs/ds-business-enablement-services-de.pdf.

6. **Fujitsu Technology Solutions GmbH.** *Additional Services for IaaS.* München : Fujitsu Technology Solutions GmbH, 2010.

7. **Fujitsu Technology Solutions GmbH.** *Fujitsu im Sicherheitsvergleich - BSI-Sicherheitsanforderungen.* München : Fujitsu Technology Solutions GmbH, 2011.

8. **Fujitsu Technology Solutions GmbH.** *IaaS Security.* München : Fujitsu Technology Solutions GmbH, 2011.

9. **Fujitsu Technology Solutions GmbH.** *Infrastructure as a Service Security.* München : Fujitsu Technology Solutions GmbH, 2011.

10. **Fujitsu Technology Solutions GmbH.** *Leistungsbeschreibung Infrastructure as a Service.* München : Fujitsu Technology Solutions GmbH, 2011.

11. **Fujitsu Technology Solutions GmbH.** *The Cloud Security Strategy.* München, Bayern, Deutschland : Fujitsu Technology Solutions GmbH.

12. **Common Criteria Recognition Agreement.** Common Criteria for Information Technology Security Evaluation. *Common Criteria: The Common Criteria Portal.* [Online] [Zitat vom: 24. März 2011.] http://www.commoncriteriaportal.org/cc/.

13. **Institute of Electrical and Electronics Engineers.** IEEE Standards Association. *P2301 - Guide for Cloud Portability and Interoperability Profiles (CPIP).* [Online] IEEE Standards Association, 2. Februar 2011. [Zitat vom: 15. April 2011.] http://standards.ieee.org/develop/project/2301.html. P2301.

14. **Open Cloud Manifesto.** Open Cloud Manifesto. *Introduction.* [Online] Open Cloud Manifesto, 1. September 2009. [Zitat vom: 15. April 2011.] http://www.opencloudmanifesto.org/opencloudmanifesto1.htm.

15. **Bundesamt für Sicherheit in der Informationstechnik.** CERT Bund. *Computer Emergency Response Team der Bundesverwaltung.* [Online] Bundesamt für Sicherheit in der Informationstechnik. [Zitat vom: 15. April 2011.] https://www.cert-bund.de/.

16. **Microsoft Corporation.** Microsoft Security Intelligence Report. *Microsoft Corporation Safety and Security Center.* [Online] 1. Mai 2011. [Zitat vom: 16. Mai 2011.] http://www.microsoft.com/security/sir/.

17. **MacDonald, Neil.** Gartner Incorporated. *Six Trends That Will Further Reshape Information Security in 2010.* [Online] 4. Januar 2010. [Zitat vom: 15. April 2011.] http://www.gartner.com/it/content/1552000/1552016/march_10_future_security_trends_nmacdonald.pdf.

18. **National Institute of Standards and Technology.** Cloud Computing Definition v15. [Online] 12. Juli 2010. [Zitat vom: 15. Mai 2011.] http://csrc.nist.gov/groups/SNS/cloud-computing/cloud-def-v15.doc.

19. **Europäische Kommission.** Generaldirektion Unternehmen und Industrie. *Die neue KMU-Definition.* [Online] 1. Januar 2005. [Zitat vom: 15. April 2011.] http://ec.europa.eu/enterprise/policies/sme/files/sme_definition/sme_user_guide_de.pdf .

20. **Hans-Bernd Kittlaus, Prof. Dr. Dirk Schreiber.** SaaS - wie können KMU profitieren? *Wirtschaftsinformatik & Management.* 2010, 2:36-42.

21. **Common Criteria.** Common Criteria Portal. *Official CC/CEM versions.* [Online] 1. Juli 2009. [Zitat vom: 5. Mai 2011.] http://www.commoncriteriaportal.org/files/ccfiles/CCPART3V3.1R3.pdf. CCMB-2009-07-003.

Kontaktdaten

Fraunhofer-Institut für Sichere Informationstechnologie (SIT)

Parkring 4

D 85748 Garching bei München

Tel.: +49 (0)89 322 9986 0

Fax.: +49 (0)89 322 9986 299

http://www.sit.fraunhofer.de

Planung und Durchführung der Studie

Iryna Tsvihun

Tel.: +49 (0)89 322 9986 157

iryna.tsvihun@sit.fraunhofer.de

Marcel Kulicke

Tel.: +49 (0)89 322 9986 138

marcel.kulicke@sit.fraunhofer.de

Forschungsbereich „Sichere Services und Qualitätstests“

Mario Hoffmann

Tel.: +49 (0)89 322 9986 177

mario.hoffmann@sit.fraunhofer.de

Presse und Öffentlichkeitsarbeit

Oliver Küch

Tel.: +49 (0)615 1869 213

oliver.kuech@sit.fraunhofer.de

Stand des Whitepapers: Mai 2011