Bundesamt
für Sicherheit in der
Informationstechnik

Notfallmanagement mit der Cloud für KMUs

Höhere Ausfallsicherheit der IT-gestützten Geschäftsprozesse bei KMUs durch Cloud-Dienste

Bundesamt für Sicherheit in der Informationstechnik
Postfach 20 03 63
53133 Bonn
Tel.: +49 22899 9582-5369
E-Mail: grundschutz@bsi.bund.de
Internet: https://www.bsi.bund.de

Danksagung

Das BSI dankt Herrn Christoph Puppe und Herrn Alexander Papitsch von der HiSolutions AG für die Mitwirkung bei der Erstellung dieser Studie. Ebenso dankt das BSI Herrn Alexander Reichenberger von ACP Solutions für die hilfreichen Kommentare und Diskussionen.

Inhaltsverzeichnis

Abbildungsverzeichnis

Tabellenverzeichnis

1 Einleitung

Aufgrund eines relativ straffen Budgets, welches Klein- und mittelständische Unternehmen (KMUs) in Informationssicherheit investieren können, ist es nicht verwunderlich, dass in vielen KMUs kein umfassender Notfallmanagementprozess etabliert ist. Dies belegt auch die Studie des BSI zur IT-Sicherheit in kleinen und mittleren Unternehmen [BSI_2011a]: Demzufolge „ist das Notfallmanagement bei weniger als der Hälfte der Unternehmen umgesetzt. Dies ist jedoch nicht durch Unwissenheit bedingt, sondern vielmehr durch die Einsparung von Kosten und die mangelhafte Einschätzung des zu tragenden Risikos."

In dieser Studie zum Thema Notfallmanagement für KMUs mit der Cloud, werden heute absehbare Potenziale von Cloud-Techniken für die Absicherung IT-gestützter Geschäftsprozesse in KMUs beleuchtet. Die Zielsetzung ist es, praxisnahe Methoden zur Notfallprävention und Notfallreaktion mit modernen Techniken darzustellen. Daher steht im Fokus eine Betrachtung der Nutzung der auf dem Markt verfügbaren Cloud-Angebote für das Notfallmanagement von KMUs und eine Betrachtung ihres Einsatzes in drei typischen Szenarien. Diese sollen illustrieren, wie der Einsatz von Cloud-Techniken das Notfallmanagement und diverse Kontinuitätsstrategien zum Positiven verändern.

Derzeit wird die Nutzung von Cloud- und Virtualisierungstechniken hauptsächlich unter dem Aspekt der Kostenreduktion vorangetrieben. Es soll verdeutlicht werden, dass durch die Nutzung von Cloud- und Virtualisierungstechniken auch erhöhte Verfügbarkeit und Ausfallsicherheit von Geschäftsprozessen fast automatisch mit erreicht werden kann. Dieses zusätzliche und bisher zu wenig beachtete Potenzial, das gerade für KMUs mit wenigen Ressourcen für ein Notfallmanagement interessant ist, wird hier beleuchtet.

Anhand von realen Praxisbeispielen wird veranschaulicht, wie bei einigen KMUs Virtualisierung bereits Anwendung findet, um die potenziell verheerenden Auswirkungen von Notfällen (Ausfall der Informationstechnik wegen z. B. Feuer oder Wasser) so gering wie möglich zu halten.

Um in das Notfallmanagement einzuführen, gibt dieses Dokument zunächst einen groben Abriss des Notfallmanagements gemäß dem BSI Standard 100-4. Dies soll dem Leser veranschaulichen mit welchen Fragestellungen sich ein Verantwortlicher bei Einführung eines umfassenden Notfallmanagements auseinandersetzen muss.

1.1 Ausgangslage

Notfallmanagement ist ein sehr unterrepräsentiertes Thema in der IT von KMUs. Bisher sind nur wenige Veröffentlichungen und praktische Leitfäden verfügbar, die KMUs unterstützen, ein adäquates Notfallmanagement aufzubauen. Der vom BSI herausgegebene Standard 100-4 für das Notfallmanagement ist umfassend, wird allerdings für diese Unternehmensgröße häufig als zu komplex angesehen. Diese für den Standort Deutschland sehr wichtige Gruppe von Unternehmen verfügt meist weder über das Personal, noch die finanziellen Mittel, um ein umfassendes Notfallmanagement im eigenen Haus umzusetzen.

Gleichzeitig nutzen viele KMUs Virtualisierungstechniken oder bauen eigene Private Cloud Kapazitäten auf oder nutzen Public Cloud Angebote. Eine Studie von Dell und Intel aus 2012 [DI_2012] sagt aus, dass immerhin schon ca. 41 Prozent der KMUs Virtualisierung einsetzen, allerdings nur ca. 17 Prozent aller befragten KMUs die Möglichkeiten des Cloud Computings nutzen. Die mit dem Einsatz von Virtualisierungs- und Cloud-Techniken verbundenen Potenziale zur Absicherung der Geschäftsprozesse vor Ausfall werden jedoch selten genutzt.

Bisherige Ansätze zur Absicherung der IT-gestützten Geschäftsprozesse vor Ausfall beinhalten, entsprechende Hardware doppelt vorzuhalten bzw. schnell nach einem Notfall neu zu beschaffen. Beides ist kosten- und zeitintensiv. Ein Großteil der kleineren KMUs betrachten den Nutzen einer redundanten Auslegung von Komponenten sehr kritisch und würden lieber einen längeren Ausfall eines Systems in Kauf nehmen, als einen weiteren Server zu beschaffen, der dann ohnehin im gleichen Rechenzentrum mit der gleichen Spannungsversorgung stehen würde. Käme es zu einem Stromausfall, wären zumal beide Server davon betroffen. Um Systeme wirklich redundant betreiben zu können, müsste ebenfalls eine redundante

Stromversorgung, sowie eine unterbrechungsfreie Stromversorgung (USV) oder die Aufstellung der Komponenten in geografisch verteilten Rechenzentrum in Betracht gezogen werden, was gerade für kleinere KMUs aus Kostengründen meist nicht praktikabel ist.

Mit der Nutzung von Virtualisierung bzw. Cloud-Techniken können Kosten für die Notfallplanung und die Zeit für den Wiederanlauf deutlich reduziert werden. Damit sind Cloud-Techniken ein Innovationstreiber beim Notfallmanagement. Besonders für kleine und mittlere Unternehmen sind entsprechende Angebote interessant, denn dank dieser Angebote können auch KMU doppelte Kapazitäten wie einen zweiten Standort für die Datenverarbeitung und Redundanzen in der Datenhaltung aufbauen.

1.2 Definition Cloud

Unter Cloud Computing versteht das BSI das dynamisch an den Bedarf angepasste Anbieten, Nutzen und Abrechnen von IT-Dienstleistungen über ein Netz. Angebot und Nutzung dieser Dienstleistungen erfolgen dabei ausschließlich über definierte technische Schnittstellen und Protokolle. Die Spannbreite der im Rahmen von Cloud Computing angebotenen Dienstleistungen umfasst das komplette Spektrum der Informationstechnik und beinhaltet unter anderem Infrastruktur (z. B. Rechenleistung, Speicherplatz), Plattformen und Software.

Hierbei können die Services entweder aus einer Public, Private oder Hybrid Cloud bezogen werden. In einer Public Cloud können die angebotenen Services von jedermann genutzt werden. Von einer Private Cloud spricht man, wenn das Unternehmen sowohl die Services als auch die Infrastruktur selbst betreibt. Werden aus einer Private Cloud heraus Dienste einer Public Cloud genutzt, oder werden mehrere Cloud-Infrastrukturen, die für sich selbst eigenständig sind, über standardisierte Schnittstellen gemeinsam genutzt, wird dies Hybrid Cloud genannt.

Da dieses zumeist auf der Nutzung von Virtualisierungstechniken beruht wird oft auch ein Einsatz einer virtualisierten Umgebung als Private Cloud bezeichnet. In dieser Studie verwenden wir beide Begrifflichkeiten synonym.

Aktuellen Umfragen zufolge wird sich die weltweite Nachfrage nach Cloud-Dienstleistungen in den nächsten Jahren stark erhöhen. Die Gründe für das zunehmende Interesse an Cloud Computing und die steigende Nutzung von Cloud-Diensten sind vielfältig. Cloud Computing verspricht sehr hohe Flexibilität bei der Buchung und Nutzung sowie Stilllegung von Rechenzentrum-Kapazitäten, je nach aktuellem Bedarf. Erwartet wird auch ein hohes Einsparpotenzial im Bereich der sonst lokal vorzuhaltenden, zu wartenden und zu erneuernden IT-Systeme. Ein weiterer Vorteil von Cloud ist die ubiquitäre Verfügbarkeit von Geschäftsanwendungen, auf die dieses Dokument besonders eingeht.

Durch die Nutzung der Public Cloud werden Unternehmen in die Lage versetzt flexibel zu handeln, um somit schnell auf Marktveränderungen zu reagieren. So können z. B. neue Dienstleistungen schneller und ohne den Einkauf teurer Hardware bereitgestellt werden, Leistungskapazitäten können dynamisch an die Nachfrage angepasst werden und passen sich somit besser als starre IT-Infrastrukturen an veränderte Anforderungen an. Es entfallen die Kosten für Anschaffung, Betrieb und Wartung von Hardware. Stattdessen sind nahezu unbegrenzte Ressourcen vorhanden, ohne dass sich IT-Fachpersonal mit der Einrichtung, Konfiguration und Pflege von Hard- und Software auseinandersetzen muss.

Zur Nutzung von Public Cloud hat das BSI ein Eckpunktepapier [BSI_2012a] veröffentlicht. Wird Public Cloud für das eigene Notfallmanagement genutzt, so müssen alle dort genannten Aspekte auf Vereinbarkeit mit den eigenen Anforderungen, z. B. aus der BIA, abgeglichen werden. Public Cloud Angebote zu nutzen, ist in der Regel preiswerter, als eine eigene Infrastruktur zu betreiben. Dennoch ist der Planungsaufwand höher bzw. hat einen veränderten Fokus und es sind zusätzlich vertrags- und datenschutzrechtliche Aspekte zu betrachten, die hier skizziert werden sollen.

1.3 Anwendbarkeit

Diese Studie und die in ihr vorgestellten Szenarien sind auf Unternehmen anwendbar, die zwischen 10 und 500 Mitarbeitern beschäftigen. Auch geht die Studie von einem normalen Schutzbedarf der Daten und der Geschäftsprozesse aus.

1.4 Abgrenzung

Ein Unternehmen, welches besondere Anforderungen an die Verfügbarkeit der Geschäftsprozesse und Daten hat, kann sich an dieser Studie orientieren, ist allerdings angehalten, in einer Schutzbedarfsfestellung für sich zu klären, welche Ziele es sinnvoll im Informationssicherheitsmanagement und Notfallmanagement festlegen sollte.

Eine weitere Einschränkung und Abgrenzung ist der Fokus hinsichtlich der betrachteten Ressourcen. Die Studie legt den Fokus auf der Absicherung der IT-Ressourcen und der benötigten IT-Dienstleister. Die Ressourcenklassen Personal, Gebäude und Nicht-IT Infrastruktur werden in dieser Studie nicht explizit betrachtet, da Cloud- bzw. Virtualisierungs-Techniken diese Ressourcenklassen nicht direkt absichern können.

2 Ausgewählte Aspekte des Notfallmanagements

Notfallmanagement (englisch: Business Continuity Management) ist ein systematischer, an den Geschäftsprozessen einer Institution orientierter Ansatz zur Vorsorge gegen und Bewältigung von Notfällen (und in Teilen auch Krisen). Es zielt darauf ab, solche Ausnahmesituationen, wenn schon nicht zu verhindern, so doch zumindest in ihren Schadenswirkungen zu begrenzen. Dazu gehört es, organisatorische Strukturen aufzubauen sowie Konzepte zu entwickeln und umzusetzen, die eine rasche Reaktion auf Notfälle und die Fortsetzung zumindest der wichtigsten Geschäftsprozesse ermöglichen. Der Begriff "Geschäftsprozess" bezeichnet dabei nicht nur die wirtschaftlichen und produktiven Prozesse von Unternehmen, sondern allgemein alle Prozesse eines Unternehmens oder einer Behörde, mit denen es bzw. sie ihre Dienstleistungen erbringt und die jeweiligen Fachaufgaben erfüllt.

2.1 Überblick

Eine Einführung in das Thema Notfallmanagement vermittelt der Webkurs Notfallmanagement [BSI_2012b], der den BSI-Standard 100-4 erklärt und mit einigen Anwendungsbeispielen die praktische Umsetzung näher bringt. Einige Inhalte dieses Kapitels sind diesem Webkurs oder dem Standard selbst entnommen.

Abbildung 1: Der Notfallmanagementprozess nach BSI-Standard 100-4

Der vom BSI veröffentlichte Standard 100-4 beschreibt eine Methodik zur Etablierung eines Notfallmanagements, welches auf das in BSI-Standard 100-2 beschriebene Vorgehen zur Umsetzung eines Managementsystems für Informationssicherheit aufsetzt und es ergänzt [BSI_2008].

Ziel des Standards 100-4 ist es, geeignete Lösungen aufzuzeigen, um bei Notfällen und Krisen verschiedenen Ursprungs, die zu Geschäftsunterbrechungen führen können, schnell zu reagieren. Größere Institutionen besitzen in der Regel getrennte Notfall- und Krisenmanagementsysteme und trennen strikt zwischen Notfällen und Krisen. Diese Ressourcen besitzen KMUs – um die es hier geht – nicht, weshalb hier beide Fälle durch ein Notfallmanagement adressiert werden sollen. Zusätzlich beschreibt der Standard präventive Methoden und Verfahren damit Notfälle oder Krisen vermieden oder zumindest in ihrer Auswirkung reduziert werden.

Das Notfallmanagement soll Schadensereignisse der Kategorien

- Störung,
- Notfall, und
- in Ansätzen auch einer Krise

betrachten, um angemessen darauf reagieren zu können. Dies bedeutet, darauf hinzuwirken, dass Störungen nicht zu Notfällen und Notfälle nicht zu Krisen eskalieren und bei Krisen die Bewältigung auf der operativen Seite zu unterstützen. Eine zentrale Rolle im Notfallmanagement nach BSI-Standard 100-4 ist der Notfallbeauftragte, der alle Aktivitäten rund um die Notfallvorsorge steuert und bei den damit verbundenen Aktivitäten mitwirkt. Ein KMU wird in der Regel keine Person beschäftigen, die nur die Rolle des Notfallbeauftragten ausfüllt, sondern die Rolle des Notfallbeauftragten wird in Personalunion z. B. mit dem IT-Leiter oder dem IT-Sicherheitsbeauftragten ausgeführt werden. Da diese Studie ohnehin nur von der Absicherung IT-gestützter Geschäftsprozesse handelt, ist diese Personalunion jedoch unkritisch. Erst wenn eine Institution auch nicht IT-gestützte Geschäftsprozesse im Rahmen eines Notfallmanagements absichern möchte, sollte eine solche Personalunion kritisch geprüft werden.

Grundlage eines jeden Notfallmanagementsystems ist die Business Impact Analyse (BIA). In ihr werden Geschäftsprozesse identifiziert, nach Kritikalität priorisiert, zu Prozessketten verbunden, benötigte Ressourcen der Geschäftsprozesse identifiziert und die Betriebsniveaus für den Notbetrieb festgelegt. Als kritisch identifizierte Geschäftsprozesse und Ressourcen werden im Rahmen des Notfallmanagement besonders abgesichert.

Der im BSI-Standard beschriebene Ablauf einer BIA ist aufwändig und wird selten in KMUs in vollem Umfang angewendet. Allerdings gleichen sich erfahrungsgemäß in vielen KMUs die abzusichernden Geschäftsprozesse. Daher ist es gar nicht für jedes KMU nötig, bei Null anzufangen, sondern es kann bei den standardisierten Geschäftsprozessen, Kritikalitäten und Ressourcen aus dieser Studie beginnen und diese nach eigenen Erwägungen abändern. Dies ist deutlich ressourcensparender und effizienter und stellt den Kern des in der Studie dargestellten BIA-Prozesses dar.

Das primäre Ziel eines Notfallmanagements ist es, die Kontinuität von Geschäftsprozessen während oder nach einem Notfall zu gewährleisten. Es müssen daher bestimmte Kontinuitätsstrategien entwickelt werden, welche auf kritische Geschäftsprozesse anzuwenden sind. Hierbei spielen Faktoren wie z.B. Wiederanlaufzeit nach einem Notfall, die Kosten der Umsetzung sowie die Zuverlässigkeit der Lösung eine entscheidende Rolle.

Ein umfassendes Notfallmanagement besteht daher aus diesen Teilen:

- Initiierung des Notfallmanagement-Prozesses
- Konzeption
- Business Impact Analyse (BIA)
- Risikoanalyse (RA)
- Kontinuitätsstrategien
- Notfallvorsorgekonzept
- Notfallbewältigung und Krisenmanagement

- Tests und Übungen
- Aufrechterhaltung und kontinuierliche Verbesserung

Im Rahmen der Erarbeitung einer Lösung zur Sicherstellung der Kontinuität eines Geschäftsprozesses ist es primär eine Frage der Kosten und des Risiko-Appetits, ob eine konzipierte Kontinuitätslösung wirklich umgesetzt werden soll.

Neben diesen Vereinfachungen des Notfallmanagements bei KMUs beeinflussen virtualisierte Umgebungen in allen Institutionen sowohl den Notfallmanagementprozess als Ganzes als auch den Inhalt des Notfallmanagements selbst. Dies soll in den folgenden Unterabschnitten erläutert werden.

2.2 Ziele des Notfallmanagements

Das hauptsächliche Ziel des Notfallmanagements ist immer, das Unternehmen gut auf den Notfall vorzubereiten (Prävention) und die Folgen eines Notfalls auf ein akzeptables Maß zu reduzieren (Reaktion). Der Kern des Notfallmanagements ist, das Unternehmen vor der Geschäftsaufgabe durch zu große Verluste durch einen Notfall zu schützen.

2.3 Notfallprävention

Unter Notfallprävention werden alle Maßnahmen zusammengefasst, die entweder das Eintreten des Schadereignisses verhindern oder dafür sorgen, dass im Falle des Eintretens eines Schadensereignisses der Schaden möglichst gering bleibt.

Ein einfaches Beispiel für eine solche Prävention ist eine doppelt ausgelegte und synchron gespiegelte Serverfarm, die in zwei Gebäudeteilen aufgestellt ist. Wenn ein Wassereinbruch einen der Räume zerstört, können alle Anwendungen weiter laufen und die Anwender können ungehindert weiter arbeiten. Solche Redundanzen konnten früher nur große Unternehmen aufbauen und betreiben, heute ist dies dank Virtualisierungs- und Cloud-Techniken auch einem KMU möglich.

2.4 Abgrenzung Störung, Notfall und Krise

In allen Institutionen gibt es immer wieder kleinere Störungen. Kurzfristige Stromausfälle, Personalengpässe, Dienstleistungen verzögern sich oder Geräte gehen defekt. Für solche Vorfälle gibt es in der Regel einfache Lösungen, die Bestandteil des Alltagsgeschäfts sind. Beispielsweise werden Stromgeneratoren aktiviert, Überstunden geleistet, Produktionszeiten gestreckt oder Ersatzgeräte beschafft. Der mögliche Schaden solcher Ereignisse ist darüber hinaus aus Sicht der betroffenen Institution nur gering.

Erst dann, wenn Störungen oder Ausfälle größere Schäden verursachen und ihre Behebung mit den üblichen Verfahren nicht mehr möglich ist, stellen sie einen Notfall dar und erfordern ein Notfallmanagement.

Mögliche Beispiele für Notfälle:

- Durch Brände können wichtige Betriebsräume (z. B. der Serverraum) nicht mehr genutzt werden.
- Überschwemmungen führen zur tagelangen Sperrung von Zufahrtswegen.
- Lebensmittelkeime in der Kantine führen zu erheblichem Personalausfall.
- Das Stromnetz fällt flächendeckend und über einen längeren Zeitraum hinweg aus.
- Wichtige Kommunikationsnetze (Internet, Telefonnetz) fallen tagelang aus.
- Wichtige Dienstleistungen fallen vollständig aus, weil eine externe Institution Konkurs anmelden musste und auch nicht auf Ersatzdienstleister zurückgegriffen werden kann.

Alle diese Ereignisse können auch zu Krisen oder Katastrophen werden. Krisen werden von Notfällen dadurch abgegrenzt, dass für die Bewältigung von Notfällen konkrete Pläne erstellt werden können, während Krisen meistens unvorhersehbar sind und daher nicht mit konkreten Vorkehrungen und Plänen bewältigt werden können. Obschon hiermit der deutlichste Unterschied zwischen Krisen- und Notfallmanagement angesprochen ist, hängen beide Managementsysteme eng zusammen: Ein Notfallmanagement ist eine gute Vorstufe für das Krisenmanagement einer Institution und je umfangreicher das Notfallmanagement, desto unwahrscheinlicher ist die Eskalation zu einer Krise für die Institution. Außerdem können die konkreten Pläne der Notfallteams die operative Arbeit des Krisenmanagements unterstützen. Aus diesem Grund wurde früher das Notfallmanagement als "operatives Krisenmanagement" bezeichnet.

Die folgende Tabelle erläutert kurz die Unterschiede zwischen Störungen, Notfällen, Krisen und Katastrophen aus Sicht des BSI-Standards 100-4 und fasst zusammen, wann und in welcher Weise das Notfallmanagement für deren Behandlung zuständig ist.

Vorfallsart	Erläuterung	Behandlung
Störung	Kurzzeitiger Ausfall von Prozessen oder Ressourcen mit nur geringem Schaden	Behandlung ist Teil der üblichen Störungsbehebung.
Notfall	Länger andauernder Ausfall von kritischen Prozessen oder Ressourcen mit hohem oder sehr hohem Schaden	Behandlung verlangt besondere Notfallorganisation.
Krise	Im Wesentlichen auf die Institution begrenzter verschärfter Notfall, der die Existenz der Institution bedroht oder die Gesundheit oder das Leben von Personen beeinträchtigt.	Da Krisen nicht großflächig die Umgebung oder das öffentliche Leben beeinträchtigen, können sie, zumindest größtenteils, innerhalb der Institution selbst behoben werden.
Katastrophe	Räumlich und zeitlich nicht begrenztes Großschadensereignis, mit Auswirkungen auf die Umgebung und das öffentliche Leben. Zum Beispiel als Folge einer Leckage eines Chemikalientanks.	Aus Sicht einer Institution stellt sich eine Katastrophe als Krise dar und wird intern durch deren Notfall- und Krisenorganisation in Zusammenarbeit mit den externen Hilfsorganisationen bewältigt.

Tabelle 1: Störungen, Notfälle, Krisen und Katastrophen im Verständnis des BSI-Standards 100-4

2.5 Notfallmanagement-Prozess

Die präventiven Aufgaben im Notfallmanagement werden anhand eines auf stetige Verbesserung abzielenden Prozessmodells beschrieben.

Im BSI-Standard 100-4 werden dazu die folgenden sechs Phasen unterschieden:

- **Initiierung**
  Getragen von der Leitung werden strategische Zielsetzungen festgelegt und grundlegende organisatorische Voraussetzungen für den Notfallmanagement-Prozess in einer Institution geschaffen.
- **Konzeption**
  Die kritischen Geschäftsprozesse und Ressourcen einer Institution werden ermittelt und die Risiken,

denen diese ausgesetzt sind, bewertet. Zu diesen Bewertungen werden präventive und reaktive Notfallstrategien und Maßnahmen entwickelt.

- **Umsetzung des Notfallvorsorgekonzepts**
  Prioritäten für die Umsetzung der Notfallvorsorgekonzepte werden gesetzt, Ressourcen bereitgestellt, Verantwortlichkeiten festgelegt und gegebenenfalls erforderliche begleitende Maßnahmen identifiziert.
- **Notfallbewältigung**
  Verantwortlichkeiten, Pläne und Verhaltensregeln für die Reaktion auf und das Handeln in Notfallsituationen werden in einem Notfallhandbuch geregelt.
- **Tests und Übungen**
  Notfallvorsorgemaßnahmen und Notfallpläne werden getestet und eingeübt, um Funktionsfähigkeiten zu überprüfen, mögliche Mängel zu identifizieren und das Verhalten im Notfall zu trainieren.
- **Aufrechterhaltung und kontinuierliche Verbesserung**
  Angemessenheit und Wirksamkeit der Konzepte und Maßnahmen werden regelmäßig geprüft. Zusammen mit einer Auswertung der Ergebnisse der Tests und Übungen tragen diese Prüfungen zur kontinuierlichen Weiterentwicklung des Notfallmanagement-Prozesses bei.

Der Notfallmanagement-Prozess nach BSI-Standard 100-4 wird im Folgenden noch einmal grafisch dargestellt.

Abbildung 2: Ablauf des Notfallmanagement-Prozesses

2.6 Besonderheiten des Notfallmanagementprozesses in virtualisierten Umgebungen

Virtualisierung hat in allen Bereichen des IT-Betriebs für ein Umdenken gesorgt. Dies trifft auch auf das Notfallmanagement zu. Besonders die Standardisierung der virtuellen Hardware löst viele Probleme. So ist es nicht mehr notwendig, identische Hardware zu beschaffen, um System-Backups wieder einspielen zu können. Auch hat es viel zur Vereinfachung beigetragen, dass es sehr einfach möglich ist, beliebige Server in

einem durch die Virtualisierung aufgebauten Cluster zu betreiben. So ist es nun auch für nicht für Hochverfügbarkeit ausgelegte Dienste möglich, sehr schnelle Produktionsverlagerungen in den zweiten Cluster in einem anderen Raum durchzuführen. Durch Virtualisierung stehen KMUs nun Verfügbarkeitsklassen offen, die noch vor wenigen Jahren nur größeren Unternehmen vorbehalten waren.

Neben der technischen Notfallvorsorge ist auch die Notfallplanung, mit den Prozessen für Wiederherstellung, Geschäftsfortführung, Wiederanlauf und Recovery, vom Umdenken durch Virtualisierung betroffen. So wechselt der Fokus vom Wiederanlauf und seiner Planung zu einer reinen Kontrolle der erfolgreichen Schwenks in den Clustern. Die Planung für den Notbetrieb ist heute eher eine Ressourcen-Planung innerhalb der virtualisierten Umgebung statt einer Standortplanung. Dies gilt zumindest für die Server. Das Notfallmanagement für Clients ist auch vom Umbruch betroffen, da mit der vermehrten Nutzung des Server-Based-Computing und den dafür eingesetzten Thin-Clients der zentrale Terminal-Server wichtiger wird und dieser auch von den Vorteilen der Virtualisierung profitiert.

Mit dem Einzug der Virtualisierung und Cloud-Techniken gelangt der Aspekt Integrität der Informationssicherheit zu einer besonderen Bedeutung. Während ohne Virtualisierung eine verletzte Integrität dazu führen kann, dass einzelne Dateien nicht mehr lesbar sind, bedeutet eine nicht lesbare Image-Datei in virtualisierten Umgebungen, dass die darin enthaltenen Server oder Clients nicht mehr funktionieren. Integrität der Daten und damit vor allem die Sicherstellung der Konsistenz der Replikationen der Images und sonstigen Dateien hat daher in virtualisierten Umgebungen eine deutlich höhere Bedeutung und muss in der Planung und Umsetzung besonders beachtet werden.

2.7 Business Impact Analysen

Die Business Impact Analyse (BIA) hat in der Notfallplanung den Zweck, die Geschäftsprozesse und die diese unterstützenden Ressourcen zu identifizieren, die besonders kritisch für das Unternehmen sind und daher besonders vor Ausfällen und Datenverlust geschützt werden müssen.

In einer BIA wird ausgehend von einem nicht genauer beschriebenen Schadensereignis ermittelt, wie hoch die Schäden für das Unternehmen wären, wenn Geschäftsprozesse durch ein Ereignis unterbrochen werden. Eine vollständige BIA betrachtet die Ausfallszenarien Ausfall von Gebäuden, Infrastruktur (dazu gehört die IT), Personal und Dienstleister. Wir konzentrieren uns hier nur auf die IT, da die Notfallplanung mit Cloud-Techniken nur die IT direkt absichern kann. Daher könnte man hier von einer IT-BIA sprechen. Sie ist jedoch so gestaltet, dass sie nahtlos in eine allgemeine BIA eingebettet werden kann.

Da der im BSI-Standard 100-4 beschriebene Ablauf einer BIA sehr komplex und umfangreich ist, empfiehlt diese Studie ein an die Bedürfnisse eines KMU angepasstes Vorgehen zur Ermittlung der kritischen Ressourcen auf Basis von in allen Unternehmen vorkommenden Geschäftsprozessen.

2.7.1 Geschäftsprozesse und Ressourcen

Im ersten Schritt sind die zu betrachtenden Geschäftsprozesse festzulegen. Zur Vereinfachung sind unten typische Kernprozesse von KMUs dargestellt und festgelegt, welche Auswirkungen ein Ausfall von IT-Komponenten oder IT-Dienstleistern haben würde.

Die hier aufgeführten Prozesse haben erfahrungsgemäß bei KMUs die höchste Priorität und sollten daher im Rahmen eines Notfallmanagements abgesichert werden. Nutzer der Studie zum Thema Cloud und Notfallmanagement müssen nun lediglich diese Priorisierung mit ihren eigenen Anforderungen abgleichen. Ebenso benötigen diese Prozesse bei KMUs oft vergleichbare Ressourcen, also IT-Systeme und IT-Dienstleister. Die betrachteten Kernprozesse sind:

- Finanzbuchhaltung inklusive
  - Lohnbuchhaltung
  - Faktura

  - Steuern, insbesondere Umsatzsteuern
- Vertrieb
  - Verkauf
  - Preisfindung
  - Vertragsabwicklung
  - Marketing
- Produktion
  - Produktionssteuerung / Projektmanagement
  - Kundenkommunikation in Projekten und bei der Fertigung

Ein Unternehmen, das die im Folgenden beschriebenen Vorlagen anwendet, hat damit schon die Grundlagen für eine an KMU angepasste BIA, wenn vorab gegebenenfalls weitere Rahmenbedingungen definiert wurden. Es müssen nur noch gegebenenfalls vorhandene zusätzliche Prozesse mit den dazugehörigen Ressourcen hinzugefügt werden. Diese verkürzte BIA kann dann auch der Rumpf für eine vollständige BIA sein, in der auch die nicht-IT-gestützten Geschäftsprozesse und Ressourcen betrachtet werden.

2.7.2 Schadensszenarien

Die klassischen Schadensszenarien sind: finanzielle Auswirkungen, Beeinträchtigung der Aufgabenerfüllung, Verstoß gegen Gesetze und Verträge, negative Innen- und Außenwirkungen (Imageschaden). Diese dienen dazu, die Auswirkungen eines Ausfalls zielgerichtet einzustufen. Dabei sollten KMUs die jeweils für sich relevanten Schadensszenarien auswählen und in der BIA berücksichtigen. Es ist jedoch zu beachten, dass dabei schwächere Auswirkungen hinter stärkeren Auswirkungen zurücktreten. So ist ein Schaden bei massiven finanziellen Auswirkungen auch dann hoch, wenn damit einhergehende Verstöße gegen Verträge nur geringfügig sind.

2.7.3 Auswirkungsklassen

Die Auswirkungsklassen dienen der Vereinfachung der Bewertung eines Schadens. Diese Studie empfiehlt zur Bewertung, qualitative Auswirkungsklassen festzulegen, da nicht immer ein genauer Schadenswert oder eine Eintrittshäufigkeit vorausgesagt werden kann.

Die nachfolgende Tabelle zeigt eine mögliche Einstufung der Auswirkungsklassen (1 - niedrig, 2 - mittel, 3 - hoch, 4 - sehr hoch). Die dargestellten Werte sind Beispielwerte und sollten von der anwendenden Institution unbedingt an das eigene Verständnis eines niedrigen bis sehr hohen Schadens angepasst werden.

Klasse	Quantitative Beschreibung	Qualitative Beschreibung
1 – niedrig	Der zu erwartende finanzielle Schaden beläuft sich auf bis zu 1% des Jahresumsatzes.	• Die Aufgabenerfüllung ist nicht nennenswert beeinträchtigt • Es besteht keine Gefährdung für das Ansehen / Image • Kein Verstoß gegen Gesetze oder Verträge
2 – mittel	Der zu erwartende finanzielle Schaden beläuft sich auf bis zu 5% des Jahresumsatzes.	• Die Aufgabenerfüllung ist tolerabel und die zu erwartenden Nacharbeiten können im normalen Tagesgeschäft abgearbeitet werden. • Es liegen Verstöße gegen Gesetze oder Verträge mit geringen Konsequenzen vor. Eine Eskalation dieser Verstöße wird nicht erwartet. • Es kommt in Einzelfällen zu einer externen Wahrnehmung des Notfalls. Es sind jedoch keine Konsequenzen aus dieser Wahrnehmung zu erwarten. • Beeinträchtigung wird als tolerabel eingeschätzt
3 – hoch	Der zu erwartende finanzielle Schaden beläuft sich auf bis zu 10% des Jahresumsatzes.	• Die Aufgabenerfüllung ist in einem nicht tolerablen Maße beeinträchtigt und es ist mit Einbußen in der Arbeitsqualität oder der Nichteinhaltung von Fristen zu rechnen. • Die zu erwartenden Nacharbeiten können nicht mehr im normalen Tagesgeschäft abgearbeitet werden. Nacharbeiten können nur mit weiterem Personal oder starker MehrarbKleit abgebaut werden. • Es liegen Verstöße gegen Gesetze oder Verträge mit zu erwartenden Konsequenzen (Vertragsstrafen, Klagen) vor. • Es kommt zu einer externen Wahrnehmung des Notfalls. Der Notfall wird von einem Großteil der Kunden und im

Klasse	Quantitative Beschreibung	Qualitative Beschreibung
		regionalen Umfeld wahrgenommen. • Beeinträchtigung wird als nicht mehr tolerabel eingeschätzt
4 – sehr hoch	Der zu erwartende finanzielle Schaden liegt deutlich über 20% des Jahresumsatzes.	• Die Aufgabenerfüllung ist gravierend unterbrochen. Die Erbringung von Arbeitsleistungen ist nicht mehr möglich. • Die zu erwartenden Nacharbeiten können nicht mehr sinnvoll abgeleistet werden. • Fundamentaler (grob fahrlässiger) Verstoß gegen Gesetze oder Verträge mit schwerwiegenden Konsequenzen. Es können sehr hohe Vertragsstrafen oder zivilrechtliche Klagen gegen einzelne Personen eingeleitet werden. • Ruinöse Auswirkungen auf die gesellschaftliche Stellung oder die wirtschaftlichen Verhältnisse. • Es kommt zu einer deutlichen externen Wahrnehmung des Notfalls. Der Notfall wird von nahezu allen Kunden und im überregionalen Umfeld wahrgenommen.

Tabelle 2: Beispielkriterien der Auswirkungsklassen

2.7.4 Zeithorizonte

Die Bewertung in unterschiedlichen Zeithorizonten dient dazu, die Geschäftsprozesse und dessen benötigten Ressourcen zu identifizieren, die schnell wieder zur Verfügung stehen müssen. Dies ermöglicht es, zielgerichtet Maßnahmen einzuleiten und Priorisierungen durchzuführen. Um den Bewertungsaufwand in Grenzen zu halten, wird empfohlen, nur drei Zeithorizonte festzulegen. In der Praxis haben sich die Zeithorizonte <1d, <3d und >3d bewährt. Kann bereits vorab erkannt werden, dass hohe Schäden entstehen, wenn eine Ressource oder ein Prozess nur wenige Stunden ausfällt, so wird empfohlen einen zusätzlichen Zeithorizont (<4h) hinzuzufügen. Diese Zeithorizonte sind Beispiele und müssen gegebenenfalls von der Institution an die eigenen Bedürfnisse angepasst werden.

2.7.5 Festlegung der Maximal Tolerierbaren Ausfallzeit (MTA)

Die maximal tolerierbare Ausfallzeit, auch MTA genannt, ergibt sich aus den Bewertungen des erwarteten Schadens bei einem Prozessausfall und stellt den Zeitrahmen dar, in der der Wiederanlauf erfolgen muss, um schwerwiegende Schäden zu vermeiden. Wir empfehlen, die MTA an dem Zeitpunkt festzulegen, an dem die Auswirkung die Klasse “hoch” erreicht.

2.7.6 Formular zur Durchführung einer IT-BIA

Die folgende Tabelle stellt beispielhaft das empfohlene Vorgehen zur Durchführung einer kompakten IT-Business Impact Analyse dar. Die angegebene Tabelle ist auf jeden Geschäftsprozess anzuwenden.

<table>
<tr><th>Nr.</th><th>Fragestellung</th></tr>
<tr><td>1</td><td>Welche Auswirkungen (1 - niedrig, 2 - mittel, 3 - hoch, 4 - sehr hoch) hat es auf das Unternehmen, wenn der Kernprozess ausfällt?
<table>
<tr><th>Ausfall <1d</th><th>Ausfall <3d</th><th>Ausfall >3d</th></tr>
<tr><td></td><td></td><td></td></tr>
</table>
Welche Auswirkungen (1 - niedrig, 2 - mittel, 3 - hoch, 4 - sehr hoch) hat ein Datenverlust auf das Unternehmen?
<table>
<tr><th>Geringer Verlust</th><th>Teilweiser Verlust</th><th>Vollständiger Verlust</th></tr>
<tr><td></td><td></td><td></td></tr>
</table>
</td></tr>
<tr><td>2</td><td>Welche IT-Systeme sind für einen Notbetrieb des Prozesses zwingend erforderlich?</td></tr>
<tr><td>3</td><td>Welcher der IT-Systeme enthalten Daten, die bei einem Verlust nicht wiederbeschafft werden können?</td></tr>
<tr><td>4</td><td>Gibt es Alternativen oder alternative Arbeitsabläufe zu diesen IT-Systemen?</td></tr>
<tr><td>5</td><td>Welche IT-Dienstleister sind für einen Notbetrieb des Prozesses zwingend erforderlich?</td></tr>
<tr><td>6</td><td>Gibt es Alternativen oder alternative Arbeitsabläufe zu diesen IT-Dienstleistern?</td></tr>
</table>

Tabelle 3: Formular zur Durchführung der IT-BIA

Stellen Sie sich dafür die Frage, von welchen Ihrer IT-Systeme und IT-Dienstleister die Geschäftsprozesse unmittelbar abhängig sind. Dies erlaubt Ihnen später, die optimale Notfallstrategie zu identifizieren und umzusetzen.

Im Anhang dieser Studie ist ein Beispiel einer BIA, mit typischen Einschätzungen der Auswirkungen und Freifeldern zum Eintragen der IT-Systeme und Dienstleister. Wir empfehlen, diese auszufüllen. Ein Download-Link zu dem Dokument ist unter [BSI_2013] zu finden.

3 Notfallmanagement mit Private-Cloud

Während in der Public- Cloud Dienste und Anwendungen öffentlich zugänglich sind, stehen bei der Nutzung einer Private-Cloud die angebotenen Dienste und Anwendungen nur einem eingeschränkten Nutzerkreis, meistens nur den Mitarbeitern eines Unternehmens, zur Verfügung. Meist gehören die Anbieter von privaten Cloud-Dienstleistungen und die Benutzer der gleichen Organisation an, denn die Private-Cloud wird zumeist von der eigenen IT-Abteilung betrieben. Private Cloud-Dienste haben gegenüber Public-Clouds den Vorteil, dass die Sicherheit, Konfiguration und Betrieb der angebotenen Lösung noch immer in der Hand der Organisation (in der Regel in der Verantwortung der IT-Abteilung) liegen und nicht vollständig an einen Dienstleister abgegeben worden sind. Da sämtliche Komponenten vor Ort im Rechenzentrum des Unternehmens betrieben werden, ist beim Aufbau einer privaten Private-Cloud natürlich mit höheren Investitionen zu rechnen, da die Anschaffung von Hardware, Software und anderen Infrastrukturkomponenten erforderlich ist. Diesen Kosten stehen dem Nutzen durch dynamische Bereitstellung von IT-Ressourcen und, wie in dieser Studie beschrieben, höherer Verfügbarkeit gegenüber. Daher werden diese Kosten vielfach als angemessen bewertet.

3.1 Private-Cloud und Virtualisierung

Unter Private-Cloud wird in diesem Dokument auch die Nutzung von Virtualisierung verstanden, auch wenn es nur um 2 Virtualisierungsserver geht und keine ganze Farm benötigt wird. Software zur Virtualisierung stellt standardisierte Ressourcen (Rechenleistung, Arbeits- und Festplattenspeicher) unabhängig von der realen physischen Ressource (der konkrete Prozessor, Arbeits- oder Festplattenspeicher) bereit. Virtualisierte IT-Systeme sind daher nicht mehr von der konkreten physischen Hardware abhängig. Dies löst viele Probleme, beispielsweise ist es nicht mehr nötig, nach einem Ausfall identische Hardware zu besorgen. Vielfach ist es nicht einmal mehr nötig, die IT-Systeme zur Reparatur auszuschalten, da beispielsweise Festplatten im laufenden Betrieb gewechselt werden können. Auch abseits der Notfallplanung liegen die Vorteile von Virtualisierung, insbesondere der Server, auf der Hand: Durch einen einzelnen leistungsstarken Server besteht die Möglichkeit, mehrere virtuelle Systeme auf nur einer physikalischen Hardware bereitzustellen. Gleichzeitig sollte jedoch nicht vergessen werden, dass die, mit den virtuellen Infrastrukturen einhergehende Replikation Bandbreite im Netz benötigt. Dementsprechend muss das Netz von der Bandbreite her so dimensioniert sein, dass die Replikationen den sonstigen Netzverkehr nicht zu sehr beeinträchtigen.

3.2 Notfallprävention

In einer Umgebung mit physischen Servern, wurden und werden zur Notfallprävention Konzepte nach Cold-, Warm- oder Hot-Standby unterschieden. Dabei wird parallel zu dem produktiven System, ein Identisches aufgebaut und entweder ausgeschaltet (Cold-Standby) oder kurzfristig einschaltbar gehalten, aber nicht eingesetzt (Warm-Standby) oder eingeschaltet und synchron gespiegelt mit Daten versorgt (Hot-Standby). Auch wenn sich an dieser grundlegenden Einteilung, wie Notfallprävention umgesetzt wird, nichts geändert hat, führt der Einzug der Virtualisierung zu einer veränderten Ausgestaltung der Notfallprävention.

Gerade in Anwendungsgebieten, welche hohe Verfügbarkeit von Systemen erfordern, ist Virtualisierung besonders vorteilhaft und wird vielfach eingesetzt. Dadurch, dass virtuelle Maschinen von einem Host auf den anderen im laufenden Betrieb umgezogen werden können, kann mit dieser Technik ein enormes Maß an Verfügbarkeit erzielt werden. Durch Einsatz der High-Availibility Module, ist der bereit gestellte Dienst bei einem Wegfall eines Systems, ohne Unterbrechung für den Benutzer verfügbar. Dabei führt der Hypervisor eine kontinuierliche in-memory Replikation zu einer, auf einem anderen Virtualisierungshost betriebenen Maschine, durch. Dies ist allerdings mit erheblichen Kosten für die Software und das dafür

benötigte SAN verbunden, daher wird in der Regel von einem KMU eher der manuelle Schwenk eines Images von einem Virtualisierungsserver auf einen der verbleibenden praktiziert.

Der Einsatz von Virtualisierung für die Notfallprävention und -reaktion bei KMUs besteht meist darin, zwei oder, bei etwas größeren IT-Landschaften auch mehrere, Virtualisierungsserver zu betreiben. Diese ersetzen sich im Notfall gegenseitig. Wo möglich stehen die Virtualisierungsserver in räumlich abgetrennten Bereichen mit unterschiedlicher Stromversorgung und idealerweise in zwei Brandschutzzonen.

Im Regelbetrieb sind die virtuellen Maschinen auf alle Virtualisierungsserver verteilt und die Images werden auf die jeweilig anderen Virtualisierungsserver repliziert. Durch einfaches Kopieren von virtuellen Maschinen wird der gesamte Zustand des Systems, inklusive Updates und Patches mitgesichert. Virtuelle Maschinen sind letztendlich Dateien und können somit durch einfaches Umkopieren auf einen der anderen Virtualisierungsserver gesichert werden.

In diesen Beschreibungen finden sich die Konzepte Cold-, Warm- und Hot-Standby wieder. Ein Hot-Standby liegt bei synchroner Spiegelung der virtuellen Maschine auf dem anderen Virtualisierungsserver vor. Bei einem Ausfall des einen Servers übernimmt ohne Verlust der andere Server. Wird nur das Image regelmäßig, z. B. stündlich, gesichert und ließe sich auf dem anderen Server starten, läge ein Warm-Standby vor. Wird das Image der virtuellen Maschine lediglich an einem Ort gespeichert, ohne dass es dort hochgefahren werden könnte, liegt ein Cold-Standby vor.

Das tagesaktuelle Backup der gesamten Images, ersetzt nicht das weiterhin erforderliche Backup der Daten im Image, aber es sorgt dafür, dass im Notfall die Gäste auf dem noch zur Verfügung stehenden Virtualisierungserver gestartet werden können. Der Administrator muss bei Erkennen einer Störung die entsprechenden Systeme auf dem verbleibenden Virtualisierungsserver hochfahren, also einen manuellen Schwenk durchführen, was in der Regel binnen weniger Minuten erledigt ist.

Durch Virtualisierung kann somit ohne viel Aufwand und relativ schnell ein ordentliches Wiederherstellungsverfahren für virtuelle Systeme mitsamt den darin gespeicherten Daten aufgebaut werden.

Auch bei Betrachtung der notwendigen Arbeitsaufwände schneidet eine solche Lösung im Vergleich zu einer klassischen Cold-Standby Lösung (ohne Virtualisierung), besser ab, denn auch das nicht virtualisierte Ersatzsystem muss dabei ständig auf dem aktuellen Konfigurations- und Patch-Stand gehalten werden, was selbst bei einer Cold-Standby Lösung mit Virtualisierung automatisch geschieht.

3.3 Mehrfachstandorte

Ein weiterer Betrachtungsgegenstand sind die Möglichkeiten der redundanten Auslegung von Standorten bei KMUs als Notfallvorsorge und die dabei auftretenden Probleme. Sofern ein KMU mehr als einen Standort betreibt, besteht bereits in Bezug auf die Notfallvorsorge eine gute Grundlage der redundanten Datenspeicherung, da sich die Systeme in physisch voneinander getrennten Räumlichkeiten befinden. Die Replizierung von Daten kann über sämtliche Standorte erfolgen, so dass jeder Standort über die gleichen Daten verfügt.

3.3.1 Replikation und Datenmengen

Je nach Gesamtmenge der Daten, welche zwischen allen Standorten untereinander repliziert werden muss, erhöht sich bei einem steigenden Volumen auch die Anforderungen an die Bandbreite. Sind Standorte untereinander nur per ISDN oder einer langsamen DSL-Leitung angebunden, gestaltet sich die Replizierung ganzer Datenbestände als ein langwieriges Unterfangen, insbesondere dann, wenn es sich dabei nicht mehr um nur zwei Standorte handelt. Besteht z. B. die Anforderung die Daten von 5 Standorten synchron zu halten, um Ausfälle einzelner Standorte kompensieren zu können, steigen die Anforderungen an die WAN-Anbindungen der einzelnen Standorte, da eine solch sternförmige Replizierung sehr datenintensiv ist.

Nun gibt es die verschiedensten Gründe, weshalb ein KMU nicht über eine breitbandige Anbindung an das Internet und zu anderen Standorten verfügt. Zum einem sind die Kosten einer dedizierten Anbindung zwischen mehreren Standorten relativ hoch und rechnen sich oftmals nicht für kleinere KMUs. Ein anderer Grund ist, dass KMUs oft nicht in Ballungsgebieten beheimatet sind, sondern oft in ländlicheren Regionen, wo zum Teil die Verfügbarkeit von breitbandigen Internetanschlüssen noch rar ist.

Durch schwache Up- und Downloadraten ist somit eine vernünftige Replizierung von Daten zwischen mehreren Standorten in einem annehmbaren Zeitraum nicht mehr umsetzbar. Hohe Latenzen sorgen dafür, dass eine Synchronität der Datenbestände nicht ohne erhebliche Verzögerungen erreicht wird. Generell muss bei der Planung berücksichtigt werden, dass die Bandbreite nicht nur für die Sicherung, sondern auch für die Wiederherstellung so ausgelegt ist, dass die anvisierte Recovery Time Objective (RTO) auch eingehalten werden kann. Auch die Arbeit von mobilen Mitarbeitern, die z.B. per VPN Verbindung auf Unternehmens- und Geschäftsdaten zugreifen müssen, wäre somit nur eingeschränkt durchführbar, insbesondere dann, wenn die gesamte zur Verfügung gestellte Bandbreite bereits von den implementierten Replizierungsmechanismen aufgebraucht wäre.

Eine Beispielrechnung veranschaulicht die Problematik. In dieser wurden virtuelle Systeme zu einem zentralen Anbieter synchronisiert:

Upload Bandbreite (Mbit)	**Übertragene Daten (GB/h)**	**Durchschnittliche tägliche Replikationsdauer pro VM (Minuten)**	**Durchschnittliche tägliche Replikationsrate (VMs/24h)**
1	0,4	200	7
2	0,8	100	15
5	1,7	40	37
10	4,2	20	74
20	8,4	10	137

Tabelle 4: Erfahrungswerte für Replikationen des Cloud-Dienstleisters ACP Solutions (Mit freundlicher Genehmigung von Thomas Reichenberger von ACP Solutions)

Eine Lösung für dieses Dilemma ist die Nutzung eines virtuellen Standortes, also dem Aufbau von IT-Systemen im Rechenzentrum eines Anbieters. Alle Standorte synchronisieren und replizieren nur noch mit diesem einen, zumal sehr breitbandig angebundenen, virtuellen Standort. So werden die Datenleitungen entlastet, da jeder Standort nur noch die eigenen Daten und nicht auch noch die Daten der anderen Standorte sendet und empfängt. Da hier nicht nur die eigene IT genutzt wird, sondern auch ein externes Angebot, ist dies ein Anwendungsfall der Hybrid-Cloud und wird im nächsten Kapitel näher beschrieben.

3.4 Besonderheiten des Notfallmanagementprozesses

Neben der Bereitstellung standardisierter Ressourcen auf Basis unterschiedlichster Hardware, verändern Virtualisierungs- bzw. Cloud-Techniken auch die Notfallplanung mit den Prozessen für Geschäftsfortführung, Wiederanlauf & Wiederherstellung und Rückkehr in den Normalbetrieb. So wechselt der Fokus vom Wiederanlauf und seiner Planung zu einer Planung des manuellen Schwenks der Gäste von einem Virtualisierungs-Server auf den anderen oder im idealen Fall nur noch der Kontrolle des erfolgreichen automatischen Schwenks. Die Planung für den Notbetrieb ist somit bei Einsatz von Virtualisierung auf eine Ressourcen-Planung innerhalb der virtualisierten Umgebung reduziert bzw. auf die Planung wo in der Liegenschaft, die Hardware für die Private-Cloud aufgestellt wird. Dies gilt zumindest für die Server.

Auch das Notfallmanagement für Clients ist im Umbruch, da der Verbreitung des Server-Based-Computing und den dafür eingesetzten Thin-Clients die gleichen Mechanismen wie bei den Servern greifen. Sofern noch Arbeitsplatzrechner, sogenannte Fat-Clients, im Einsatz sind, ist für diese allerdings auch die Wiederbeschaffung zu bedenken. Die Clients werden in dieser Studie nicht weiter betrachtet.

3.5 Notfallübungen

In virtualisierten Umgebungen können die Notfallpläne viel leichter geübt werden. Die Auswirkungen von dynamischer Ressourcenverteilung können ebenso wie das Umschwenken auf die Hardware in einem anderen Raum oder bei einem externen Cloud-Anbieter, auch im Normalzustand gestestet werden. Es müssen dafür keine neuen Pläne erstellt, sondern es kann auf standardisierten Plänen, z. B. für den Schwenk auf einen anderen Virtualisierungsserver, aufgebaut werden. Der Aufwand für ein Übungswesen in virtualisierten Infrastrukturen im Vergleich zu physischen Infrastrukturen damit viel geringer und somit auch für ein KMU möglich.

4 Notfallmanagement mit Hybrid- und Public-Cloud

Bisher wurde nur der Einfluss von Virtualisierungstechniken, respektive eigenen Cloud-Infrastrukturen auf das Notfallmanagement bei KMUs betrachtet. Wird hingegen die Cloud-Infrastruktur eines öffentlichen Anbieters genutzt, ergeben sich weitere Einflüsse auf die Geschäftsprozesse eines KMU und seines Notfallmanagements. Da in diesem Fall die private und die öffentliche Cloud zusammen genutzt werden, spricht man von einer Hybrid-Cloud.

Auch bei der Nutzung von Public-Cloud-Modellen ergeben sich Vorteile der Standardisierung. Es ist nicht mehr wichtig, nach der konkreten Hardware zu fragen, sondern nur noch, allgemeine Anforderungen wie Rechenleistung, Arbeits- und Festplattenspeicher und Verfügbarkeit zu stellen.

Durch die Auslagerung von Diensten in die Cloud eines professionellen Anbieters, können hohe Verfügbarkeitszeiten und geringe Zeiträume eines Datenverlusts bei einem Ausfall (Recovery Point Objective und Recovery Time Objective) erzielt werden. Gleichzeitig bekommt mit der Nutzung dieser Cloud-Dienste die vertrauliche (verschlüsselte) Anbindung an die Dienste eine vitale bis existenzielle Bedeutung zu.

Betrachtet man die Nutzung von verfügbaren Cloud-Lösungen, so besteht nicht nur die Möglichkeit komplette Server, sondern auch Büroanwendungen (Word, Excel etc.) und andere Anwendungen in die Datenwolke auszulagern. Das bekannteste Beispiel ist die Bereitstellung von E-Mail Diensten. Auch sicherheitstechnische Dienstleistungen wie z. B. Malware Erkennung und Virenscanner lassen sich in die Cloud auslagern. Derzeit ist die vollständige Verlagerung der Dienste in die Public Cloud eher selten. Ein öfter anzutreffendes Szenario ist die Ergänzung der eigenen Dienste um Angebote aus der Public Cloud. So war z. B. ein Backup an einem zweiten Standort für ein Unternehmen mit nur einem Standort ein aufwendiges Unterfangen. Heute kann jedes Unternehmen dafür Cloud-Anbieter nutzen. Es stehen die folgenden Varianten des Cloud-Computings zur Verfügung:

- Infrastructure as a Service (IaaS)
- Plattform as a Service (PaaS)
- Software as a Service (SaaS)
- Security as a Service
- Remote Backup / Backup as a Service (BaaS)
- Disaster Recovery as a Service (DRaaS)

Durch die Nutzung dieser Cloud Architekturen gelingt es einem Unternehmen, den Betrieb vieler zentraler IT-Komponenten zu reduzieren. Nur selten wird es gelingen, sich komplett von solchen Infrastrukturen loszulösen, da in der Regel Switche, Firewalls und insbesondere der VPN-Server für die sichere Verbindung zum Cloud-Anbieter immer noch vorliegen müssen. Der Vorteil einer kompletten Auslagerung von Diensten in die Cloud, sind die enorm hohen Verfügbarkeitszeiten, die dadurch erzielt werden. Diese Aussagen gelten mit der Einschränkung, dass natürlich ein Netz zur Anbindung an die Cloud, Strom, Infrastruktur zur Anbindung an den Cloud-Anbieter und entsprechende Clients in der Institution funktionsbereit sein müssen.

4.1 Software as a Service (Saas) und Plattform as a Service (PaaS)

Software as a Service und Plattform as a Service sind nah verwandte Angebote der Cloud-Anbieter, da in beiden Fällen eine bereits konfigurierte Umgebung angemietet wird. Bei PaaS wird auf dieser eine Anwendungs-Software wie z. B. ein Web-Shop installiert und bei SaaS wird diese Anwendungs-Software durch den Anbieter gestellt. Aus Sicht der Notfallplanung ist hier kein Unterschied, da in beiden Fällen ein Plan vorhanden sein sollte, wie das Unternehmen auch bei Ausfall des Anbieters weiter seine

Geschäftsprozesse aufrecht erhalten kann. Details dazu und der Datensicherung finden sich in den entsprechenden Kapiteln.

Auch aus der Perspektive der Notfall Prävention sind beide Angebote stark vergleichbar. Denn alle technischen Maßnahmen zur Aufrechterhaltung des Dienstes, zum Wiederanlauf und der Wiederherstellung obliegen den Pflichten des Anbieters. Dies entbindet, wie schon betont, die Geschäftsführung des KMU nicht von der Notfallplanung, es ändert nur die Inhalte. Siehe auch hier das Kapitel 5 „Notfallplanung bei Nutzung der Public-Cloud “ auf Seite 34.

4.2 Disaster Recovery as a Service (DRaaS)

Dieses recht junge Angebot auf dem sich ständig weiter entwickelnden Markt ist eine Zusammenfassung mehrerer Techniken. Neben dem Backup-as-a-Service und dem virtuellen Standort enthalten diese Angebote:

- Replizierung der Daten inkl. der Festplatten der virtuellen IT-Systeme
- Vorbereitete Umgebungen für den Betrieb der virtuellen IT-Systeme
- Ersatz-Systeme für die physischen IT-Systeme
- Zugang und Authentisierung für die Mitarbeiter

Im Enterprise-Umfeld bieten die dort eingesetzten Produkte die für die Replikation von Daten und virtuellen IT-Systemen notwendigen Funktionen. So haben alle Anbieter von SAN und auch der Markführer bei Virtualisierungstechniken bereits Funktionen für die Replikation großer Datenmengen auch bei hoher Latenz der Übertragungsleitungen, also weiten Strecken und der im Vergleich zu RZ-Technik geringen Bandbreiten von Weitverkehrsnetzten, eingebaut. Diese Techniken sind zumeist in der Anschaffung nicht im IT-Budget eines KMU abbildbar. Auch da hier nicht nur eine Replizierung der Daten angeboten wird, sondern ein komplettes Konzept, ist die Beauftragung eines DRaaS ein komplexes Projekt, in dem der Auftragnehmer alle Besonderheiten des beauftragenden Unternehmens beachten muss. In den meisten Fällen wird der für diesen Service von den Anbietern geforderte Preis das IT-Budget eines KMU übersteigen.

Für ein KMU ist es dennoch möglich, die Vorteile des technischen Fortschritts zu angemessenen Kosten zu nutzen. So ist bereits ein virtueller Standort mit einem DRaaS vergleichbar, da hier auch die Kapazitäten des Cloud-Anbieters für eine Erhöhung der Ausfallsicherheit und eine Verringerung der Wiederherstellungszeiten genutzt wird. Es wird hierbei dann allerdings keine Recovery der physischen IT-Systeme übernommen. Auch muss sich das KMU selbst um die Replikation der Daten kümmern.

4.3 Virtueller Standort beim Provider

Hierbei mietet das KMU entweder die IT-Systeme beim Provider oder stellt eigene Hardware in dessen Räumen auf. Diese IT-Systeme dienen dann als Backup für den Notfall, oder sie wickeln den täglichen und ständigen Geschäftsbetrieb ab. Wenn die gemieteten Systeme virtuell sind, wird meist von Infrastructure-as-a-Service gesprochen.

Eine besondere Form dieses zusätzlichen Standortes ist es, wenn die IT-Systeme beim Provider als zentrales IT-System für die Replikation zwischen mehreren Standorten dienen. Alle Standorte müssen dann nur mit diesem zumeist sehr viel besser angebundenen Standort replizieren. So werden die Datenleitungen zu den Standorten erheblich entlastet.

Der virtuelle Standort bietet für ein KMU mehrere Vorteile, denn die Datencenter der Anbieter sind vor Elementarschäden wie Feuer, Blitz und Wasser meist besser geschützt, als ein Server-Raum in der eigenen Liegenschaft. Auch ist die Anbindung an die Weitverkehrsnetze bei größeren Anbietern zumeist mehrfach redundant ausgelegt. Die Stromversorgung wird von mehreren Verteilern bezogen und ist mit ausreichender USV-Kapazität und oft auch einer zusätzlichen Stromerzeugung mit Notaggregaten

abgesichert. Die Sicherung der Daten wird beim Aufbau eines solchen Standortes dann auch vom gleichen Anbieter eingekauft. Damit sind schnelle Datentransfers und kurze Wiederanlaufzeiten bei einem Ausfall der IT-Systeme an diesem Standort sichergestellt. All dies ist mit dem typischen Budget für ein KMU in der Regel nicht realisierbar. Mit einem virtuellen Standort geht in der Regel im Vergleich zum lokalen Betrieb eine höhere Latenzzeit für die eigenen Anwendungen einher. Dies sollte in der Planung entsprechend berücksichtigt werden. Sollten die entstehenden Latenzzeiten zu hoch sein müssen weitere Maßnahmen umgesetzt werden, beispielsweise eine eigene Terminal Server Infrastruktur für den Notfall. Zudem sollte auch darauf geachtet werden, dass der Cloud-Anbieter alle Dienste anbietet, die vom eigenen Informationssicherheitsmanagement vorgegeben werden. Werden beispielsweise jeden Tag Datensicherungen gemacht, dann muss dies auch im virtuellen Standort von Cloud-Anbieter angeboten werden.

Wenn die IT-Systeme nicht in den laufenden Betrieb eingebunden sind und nur für den Notfall vorgehalten werden, ist der Wiederanlauf in einem virtuellen Standort ist in der Regel komplexer als im eigenen physischen Standort und sollte sorgfältig geplant und getestet werden. Wird beispielsweise nur ein Teil der IT-Infrastruktur im virtuellen Standort abgesichert und im Notfall dort neu gestartet, müssen in der Regel IP-Adressen und Routing-Tabellen angepasst werden. Eventuell können diese Anpassungen durch Techniken wie „Network Bridging“ vereinfacht oder sogar obsolet werden. Solche Vereinfachungen sollten geprüft und bewertet werden.

4.4 Remote Backup/Backup as a Service

Die Entscheidung, welche Backup-Strategie im Unternehmen gefahren wird, hängt von den internen festgelegten funktionalen und operativen Anforderungen ab. Zusätzlich spielen natürlich auch eine detaillierte Sicherheitsbetrachtung, Datenschutz sowie rechtliche Aspekte bei einer Auslagerung von teilweise sensiblen Geschäftsdaten eine entscheidende Rolle, deren sich die Entscheidungsträger bewusst sein müssen. Wenn diese Risiken und Randbedingungen hinreichend beachtet wurden, können Unternehmen durch die Möglichkeiten der Cloud eine effektive und unkomplizierte Datensicherungsstrategie umsetzen.

Es gilt bei der Auswahl einer Backup Strategie der folgende Grundsatz: Je weiter weg die Daten vom Betriebssystem entfernt sind, umso besser. Die Anforderungen an ein Backup werden durch mehrere Einflussfaktoren (siehe BSI IT-Grundschutz Maßnahme M 6.34 Erhebung der Einflussfaktoren der Datensicherung) bestimmt, nämlich

- Spezifikation der zu sichernden Daten
- Kritikalität der Daten/Verfügbarkeitsanforderungen
- Rekonstruktionsaufwand der Daten ohne Datensicherung
- Datenvolumen
- Änderungsvolumen
- Änderungszeitpunkte der Daten
- Fristen
- Vertraulichkeitsbedarf
- Integritätsbedarf

Klassische Backup-Strategien sehen vor, dass die Speicherung von Daten von Mitarbeitern auf einem zentral bereitgestellten Dateiserver innerhalb des Unternehmens erfolgt. Die auf dem Dateiserver gespeicherten Daten unterliegen einer regelmäßigen Datensicherung, um Daten bei Bedarf wieder herstellen zu können. Ob es sich hierbei um ein inkrementelles Backup oder eine Vollsicherung handelt, ist für diese Betrachtung zunächst unerheblich. Allerdings ist bei einer zentralisierten Backup-Strategie die Kooperation der Mitarbeiter gefragt, damit diese ihre Daten auch wirklich auf dem Dateiserver ablegen, sofern sie sich im

Firmennetzwerk befinden und Zugriff auf den Dateiserver haben. Ist dies nicht der Fall, erfolgt zwangsläufig eine temporäre Speicherung lokal auf dem System. Werden Daten nicht bei nächster Gelegenheit synchronisiert, können Daten verloren gehen, wenn die Festplatte des Clients defekt ist. In Notfällen kann eine Rekonstruktion der Daten von der Festplatte erfolgen, was die finanzielle Investition für solch eine Wiederherstellung nur bei extrem kritischen Daten rechtfertigt.

Das Unternehmen kann bei den am Markt befindlichen Anbietern von Online-Speicher ein Produkt auszuwählen, welches den speziellen Anforderungen des jeweiligen Unternehmens entspricht. Das Preismodell ist abhängig vom jeweiligen Dienstleister und kann nach den folgenden Kriterien oder einer Kombination dieser erfolgen:

- Anzahl der Gesamtdatenmenge, die gesichert wird
- Anzahl der Maschinen, für die ein Backup erfolgt
- Anzahl der Versionen, die pro Datei aufbewahrt werden
- Aufbewahrungszeiten
- Service-Levels und bereitgestellte Funktionalitäten

Der wohl größte Vorteil eines Online-Backups ist, dass der Ansatz, die Daten ausreichend weit entfernt vom Betriebssystem zu speichern, dadurch effektiv umgesetzt wird. Da die Speicherung der Backup-Dateien physisch meist in einer anderen geografischen Region erfolgt, sind sie vor Feuer, Wasser oder anderen Katastrophen, die am eigentlichen Ort der Institution eintreten, sicher. Bezogen auf ein KMU ist dies ein besonders großer Fortschritt zum Status quo, bei dem sich Datei- und Backup Server nur selten in separaten Räumen befinden, sondern die Tendenz zur Aufbewahrung der Systeme in den gleichen Räumlichkeiten geht. Käme es hier zu einem Brand, wären somit Datei- und Backup-Server gleichermaßen betroffen, was im Worst-Case zu einem vollständigen Datenverlust führen könnte.

Da die Rechenzentren der Dienstleister meist bessere Anbindungen als das KMU selbst besitzen, macht es Sinn, dass jede Geschäftsstelle nur die an seinem Standort vorgehaltenen Daten an den Online-Speicher übermittelt. Die Daten werden somit an einer zentralen Stelle konsolidiert, d. h. der Online-Speicher verfügt dann über alle Datenbestände aller Standorte. Durch diesen zentralen Knotenpunkt werden somit die Hürden, die durch eine geringfügige Internetanbindung entstehen können, verringert. Die Bandbreite, die zur Replizierung von Datenbeständen erforderlich ist, reduziert sich um ein Vielfaches im Vergleich zu einer gegenseitigen Replizierung der Standorte.

Die Nutzung eines zentralen Knotenpunktes bringt auch für mobile Mitarbeiter einen enormen Vorteil. Sofern diese den Zugriff auf Daten benötigen, müssen Sie auf diese nicht über den schwach angebundenen Standort zugreifen, sondern können stattdessen den zentralen Knotenpunkt nutzen, der alle Datenbestände konsolidiert zur Verfügung stellt und gleichzeitig eine bessere und vermutlich auch zuverlässigere Anbindung zur Verfügung stellt. Die einzige Beschränkung stellt in so einem Szenario dann die Anbindung der mobilen Mitarbeiter und deren Systeme dar.

4.4.1 Datensicherung auf dem Client

Neben den dedizierten Angeboten für Speicherkapazitäten für Server gibt es auch die Datensicherungen für Clients, die unabhängig von den Servern des Unternehmens die Daten in der Cloud speichert. Bei dieser Lösung installiert das Unternehmen auf den Clients ein Programm des Anbieters des Online-Speichers, das die Synchronisation vornimmt, wann immer ein Internetzugang bereitsteht. Wann immer möglich sollten die Daten vor der Synchronisation verschlüsselt werden. Weitere Hinweise zur sicheren Nutzung von Online-Speicher sind im IT-Grundschutz Überblickspapier zu Online-Speicher [BSI_2012c] zu finden. Ein weiterer Vorteil des Online-Speichers ist die Option, die Daten auch mit anderen Mitarbeitern, Kunden oder dem gesamten Internet zu teilen. Für KMU kann dies den Datei-Server ersetzen, allerdings ist sehr darauf zu achten, dass die Freigabe der Daten auch nur an den gewünschten Personenkreis erfolgt. Untersuchungen

bei großen Cloud-Anbietern haben gezeigt, dass Anwender bis zu 30 % aller Dateien für einen viel zu großen Personenkreis, oft das gesamte Internet, frei geben.

Auch bieten nahezu alle Hersteller von Client-Betriebssystemen einen Cloud-Speicher in ihrem Kernprodukt an. Somit können z. B. Daten jeder Art und oft beliebiger Menge in der Cloud gespeichert werden, was zusätzlich den Zugriff auf diese Daten durch mobile Geräte wie Smartphones ermöglicht. Auch ist es damit möglich, die Daten zwischen den Mitarbeitern auszutauschen, ohne einen eigenen Fileserver zu betreiben.

War bei der traditionellen Methode des Backups stets der Administrator für die Durchführung oder die Wiederherstellung von Backups zuständig, wird dies durch die Nutzung Client-basierter Cloud-Techniken auf den Benutzer übertragen. Der Administrator hat immer weniger Einfluss darauf, welche Daten zum Cloud-Dienstleister übertragen werden. Einfluss darauf nehmen kann lediglich nur noch der Datenbesitzer selbst, da dieser in der Lage ist festzulegen (abhängig vom eingesetzten Produkt), welche Ordner synchronisiert werden müssen und welche Ordner (z. B. hoch vertrauliche Inhalte) von der Synchronisation ausgeschlossen werden. Somit ist der Benutzer im Umkehrschluss für die Wiederherstellung seiner Daten zuständig, da er direkt auf sein Cloud-Konto zugreifen kann.

Der Aspekt der Bedienerfreundlichkeit, der beim Backup in die Cloud erzielt wird, ist dabei erheblich. Dadurch, dass das Backup transparent für den Benutzer ohne sein Zutun (nach einer einmaligen Erstkonfiguration) abläuft, kann sich dieser ganz den Geschäftsabläufen widmen, ohne den Aspekt der Datensicherung dabei berücksichtigen zu müssen. Sofern eine Wiederherstellung einer Datei aus dem Cloud-Speicher erforderlich ist, kann der Anwender sich die benötigte Datei selbst aus dem Online-Speicher herausziehen. Für eine Wiederherstellung muss stattdessen bei einer traditionellen Backup-Methode zunächst der IT-Betrieb dem Anwender die Datei wiederherstellen. Lange Wartezeiten können durch die Möglichkeit der Selbsthilfe vermieden werden.

4.5 Datensicherung bei IaaS und SaaS

Da die Hoster von Cloud Lösungen auch für die Datenspeicherung verantwortlich sind, muss sich der Verantwortliche eines KMUs bei der Nutzung von Diensten in der Public-Cloud nicht mehr um die Erstellung eines Datensicherungsplans und die Durchführung des Backups einzelner Systeme kümmern, da diese Disziplin der Notfallvorsorge an den jeweiligen Hoster der Cloud Lösung ausgelagert wird. Die Schutzbedarfsfeststellung ist aber immer noch nötig, um Anbieter und ihre Angebote auswählen zu können. Die Rechenzentren der großen Anbieter sind häufig mehrfach redundant ausgelegt und unterliegen einer ständigen Synchronisation/Spiegelung, sodass Schadensereignisse selten bemerkenswerten Einfluss auf den Geschäftsprozess eines KMUs haben. Mitarbeiter des KMU können weiter arbeiten, unabhängig von der Tatsache, ob es einen Stromausfall in einem Rechenzentrum des Cloud Anbieters gab.

Kommt es einmal zu einem Datenverlust, so ist der Cloud-Anbieter für die Rücksicherung von Backups verantwortlich und nicht das KMU selbst. Jede durchgeführte Maßnahme des Notfallmanagements ist transparent für das KMU - durch die umgesetzten Kontinuitätsstrategien des Cloud-Anbieters wird die Verfügbarkeit von Systemen und Daten gewährleistet. Dadurch ist das KMU allerdings in einem hohen Grad abhängig vom Funktionieren der Notfallvorsorgemaßnahmen des Cloud-Anbieters, sofern es bei diesem ein konkretes Ausfallszenario eintritt. Scheitern sämtliche umgesetzte Kontinuitätsstrategien ist auch das KMU nicht mehr arbeitsfähig. Da ein Cloud-Dienstleister von SaaS ohnehin meistens nur eine spezielle Dienstleistung zur Verfügung stellt, erfolgt zumindest dabei ein gewisser Grad an Streuung. So ist bei einem Ausfall eines Dienstleister oft immer nur ein Geschäftsprozess ganz oder teilweise von einem Ausfall betroffen. Bei IaaS wird zumeist ein Anbieter für alle Dienste genutzt. Hier führt ein Ausfall dann zu weitreichenden Folgen für die Geschäftsprozesse.

Es sei hier noch einmal erwähnt, dass auch zu Datenverlusten bei Dienstleistern kommen kann, weshalb insbesondere bei sehr geschäftskritischen Daten weitere Sicherheitsmechanismen im Rahmen einer alternativen Backup-Strategie umzusetzen sind. In der Praxis ist dies zumeist ein regelmäßiger, z. B.

wöchentlicher Download der Daten auf einen eigenen Datenträger, die in den Räumen des KMU in einer feuerfesten Datenkassette lagert.

4.6 Fachpersonal mit Cloud-Kompetenzen

Ein weiterer Aspekt, der bei der Nutzung solcher Dienste erwähnt werden muss, ist die Notwendigkeit für spezialisiertes IT-Personal. So ist z. B. die Bereitstellung von E-Mail Diensten via Microsoft Exchange ein komplexes Unterfangen und sollte nur von Personen durchgeführt werden, die sich mit Konfiguration und den Betrieb von Mail Servern auskennen, da es bei Unwissenheit auch so relativ schnell zu Ausfällen des Mail Systems aufgrund von Fehlkonfigurationen kommen würde. Gleiches gilt für die Private- und Public-Cloud. Die Mitarbeiter müssen gerade bei SaaS zwar nicht mehr die Details des Betriebs der Server kennen, aber die Anbindung dieser Dienste an die lokalen IT-Systeme, die Abhängigkeiten zwischen den Diensten und die veränderten Methoden der Fehlersuche sind Herausforderungen, denen sich die mit dem Betrieb der IT betrauten Mitarbeiter stellen müssen. Je nach Grad der gewählten Auslagerung des IT-Betriebs in die Cloud kann das KMU teilweise zwar den Bedarf für IT-Personal reduzieren, muss allerdings bei den Mitarbeitern auf die notwendigen Kompetenzen für komplexe Beziehungen zu Dienstleistern und eventuell auch Partnern achten.

4.7 Internetanbindung der Geschäftsräume

Die Nutzung von Cloud-Diensten setzt eine permanente und schnelle Internetverbindung voraus, um eine flüssige Übertragung von Daten und somit ein adäquates Arbeiten zu ermöglichen. Die Bandbreite vom KMU in das Internet ist als limitierender Faktor immer zu beachten. In Ballungsräumen ist die Anbindung oft schnell und günstig, während es in den kleineren Städten und besonders bei Standorten außerhalb von Ortschaften oft nicht möglich ist, einen ausreichend schnellen Internetanschluss erhalten. Auch kann diese Anbindung jederzeit durch ein Schadensereignis für kurz oder lang unterbrochen werden.

Neben der Verfügbarkeit der Netzverbindung zum Cloud-Dienstleister ist die Vertraulichkeit dieser Verbindung ebenso unverzichtbar. Bei Web-Diensten muss immer eine HTTPS-Verbindung vorliegen. Für sichere Anbindung von Server-Diensten oder Client-Images ist eine verschlüsselte VPN-Verbindung herzustellen. Besonderes Augenmerk muss auf die Schlüssel- und Zertifikatsverwaltung gelegt werden. Weitere Details zu VPN sind im gleichnamigen IT-Grundschutz-Baustein 4.4 zu finden. Organisatorische und planerische Maßnahmen zur Schlüsselverwaltung sind im IT-Grundschutz-Baustein 1.7 Kryptokonzept zu finden.

Einige Cloud-Lösungen erlauben es, auch temporär ohne eine Verbindung zum Anbieter weiter zu arbeiten, da der Client die zu bearbeitenden Daten lokal speichert und Änderungen mit dem Public-Cloud-Dienst abgleicht. Der Abgleich erfolgt, sobald die Verbindung wieder verfügbar ist. So ist es möglich, Netzausfälle zu kompensieren, hat aber letztendlich den Nachteil, dass man eventuell nicht immer Zugriff auf alle Daten oder deren letzten Versionsstand hat. Beispiele solcher Dienste sind z. B. Mail, Datensicherung und Replizierung sowie der oben beschriebene virtuelle Standort, sofern er nur ein IT-System in der Niederlassung ergänzt und nicht ersetzt. Auch sind diese Mechanismen nur für einen begrenzten Zeitraum in der Lage, den Ausfall auszugleichen und den Mitarbeitern die Arbeit zu ermöglichen.

Bei der Notfallvorsorge ist es daher erforderlich die interne Vernetzung im Büro, sowie die Anbindung an das Internet zu berücksichtigen und entsprechende Maßnahmen, welche die Verfügbarkeit der Anbindung an das Internet gewährleisten, zu definieren und etablieren. In vielen Fällen haben die Mitarbeiter bereits eine Mobile Anbindung, so wie im nächsten Kapitel beschrieben. Diese Mitarbeiter sind dann bei SaaS, IaaS und dem virtuellen Standort weiter arbeitsfähig. Um auch die anderen Büro-Arbeitsplätze mit einer redundanten Anbindung an das Internet zu versorgen, ist ein Router mit eingebauten UMTS-Modem als Backup ein oft gegangener Weg, der zumindest sicherstellt, dass die nur über das Internet erreichbaren Dienste weiter zur Verfügung stehen. Ein solcher Router kann auch im Falle des Verlustes eines Standortes

schnell an einem anderen Standort aufgestellt werden, so dass auch eine Vorsorge für Arbeitsplätze und ihre Versorgung mit Internet in den Notfallplan aufgenommen ist.

4.8 Mobile Anbindung an die Public Cloud

Durch die Möglichkeit der mobilen Anbindung an eine Public Cloud erweitert sich der Betrachtungsgegenstand bei der Notfallkonzeption erheblich. Stehen den Mitarbeitern mobile IT-Systeme zur Verfügung oder ist es ihnen erlaubt sich von ihren PCs zu Hause bei der Public Cloud einzuwählen, können Geschäftsprozesse für KMUs sogar kostengünstig gegen den Ausfall des Gebäudes abgesichert werden. Alle Geschäftsprozesse, die in einer Public Cloud ablaufen können so gegen Ausfall abgesichert bzw. in einer so kurzen Zeitdauer wieder anlaufen, wie dies ohne Cloud-Technik niemals möglich wäre.

Dies gilt nur für alle Dienste, die direkt aus der Public- oder Hybrid-Cloud bezogen werden. Bei selbst betriebenen IT-Systemen in den eigenen Räumen kann das Unternehmen diesen Vorteil nur dann ausschöpfen, wenn diese IT-Systeme auch im Rahmen der Notfallvorsorge in die Hybrid-Cloud gesichert sind. So kann ein IT-System im virtuellen Standort die Aufgaben eines Ausgefallenen IT-Systems an einem z. B. durch einen Brand vernichteten Standort fast reibungslos übernehmen und die Mitarbeiter dank mobiler Anbindung an Ausweicharbeitsplätzen umgehend mit den notwendigen Diensten versorgen.

4.9 Authentisierung

Alle Dienste, die über das Internet genutzt werden, haben den Vorteil, dass die Mitarbeiter von überall auf die Dienste zugreifen können. Daraus ergibt sich aber gleichzeitig ein Sicherheits-problem, weil damit die Gefahr eines unbefugten Zugriffs durch Dritte einhergeht. Daher kommt der Authentisierung der Mitarbeiter eine besondere Bedeutung zu. Es ist daher dringend erforderlich, hinreichend komplexe Passwörter zu nutzen und diese auch in regelmäßigen Intervallen zu ändern, wenn nicht sogar ein stärkeres Authentisierungsverfahren eingesetzt werden kann. Da auch ausgeschiedene Mitarbeiter ohne Zugang zum Firmengelände und zu den Büroräumen weiter ungehindert auf die Dienste in der Cloud zugreifen können, ist es besonders wichtig, mit dem Ende des Arbeitsverhältnisses auch die Zugänge zu den Diensten zu sperren.

4.9.1 Zwei Faktor Authentifizierung

Die Verarbeitung von Daten mit erhöhtem Schutzbedarf bedingt auch einen erhöhten Schutz. Beispiele solcher Daten sind Daten über natürliche Personen, die dem Datenschutz unterliegen, und vertrauliche Daten des Unternehmens, die für das Geschäft eine besondere Wichtigkeit haben. Das können z. B. Kalkulationen, Baupläne oder Kundendaten sein. Für die Verarbeitung solcher Daten empfiehlt es sich, nur Dienste mit zusätzlichen Methoden zur Authentisierung zu nutzen. Leider bieten nur wenige Anbieter Zwei-Faktor-Authentisierung an. Ein zweiter Faktor ist neben dem ersten Faktor, dem Passwort, z. B. etwas, das der Nutzer besitzt. Dies kann ein Token sein, das auf Knopfdruck Quasi-Zufallszahlen erzeugt und diese zur Authentisierung nutzt. Methoden, die auf dem Markt verbreitet und geeignet sind, umfassen:

- GridCards
- Zertifikate
- SMS-Token
- OTP-Token als Software oder Hardware

Sollte aufgrund des hohen Schutzbedarfs der Informationen eine Zwei Faktor Authentisierung angewendet werden, dann muss auch der Cloud-Dienstleister diesen Schutz bieten und es muss dafür gesorgt sein, dass die Token beim Dienstleister vorliegen und sich der Wiederanlauf dadurch nicht untragbar verzögert.

4.10 Auswahl des Cloud-Dienstleisters

Der eigentliche Fokus des Notfallmanagements nach einer Auslagerung von Komponenten und Diensten in die Cloud verändert sich. Während die Sicherstellung der Verfügbarkeit durch Kontinuitätsstrategien der eigenen Hardware die oberste Priorität der Notfallstrategie war, so steht nun die Auswahl des passenden Anbieters im Vordergrund, denn die Angebote sind standardisiert und können nur selten angepasst werden. Eine Vertragsgestaltung, die über die Auswahl eines Angebotes hinausgeht, ist in der Praxis zumindest mit größeren Anbietern nicht realistisch umzusetzen. Um einen Anbieter beurteilen zu können, sind auch Zertifizierungen wichtig, wie beispielsweise das Zertifikat „ISO 27001 auf der Basis von IT-Grundschutz“ und – wenn es besonders um die Verfügbarkeit des Dienstleisters geht – das Zertifikat des Notfallmanagements nach ISO 22301. Liegen solche Zertifikate vor, umfassen sie den Teil des Dienstleisters, in dem die gewünschten Dienstleistungen erbracht werden, und liegen entsprechend hohe Sicherheitsanforderungen beim KMU vor, sollten entsprechend zertifizierte Anbieter vorgezogen werden.

Zwar scheinen die Vorteile einer strategischen Entscheidung für Cloud-Computing zu überwiegen, aber es sind noch einige Faktoren zu berücksichtigen, bevor man wirklich den Schritt in die Cloud geht. So traumhaft sich auch die realisierbaren Verfügbarkeitszeiten und die geringe Wahrscheinlichkeit eines Ausfalls bei Cloud-Nutzung anhören, verbleiben zentrale Fragen, die sich jeder Geschäftsführer eines KMU stellen sollte:

- Wie verfahre ich bei einem Ausfall meines Cloud-Dienstleisters und wie stelle ich die Verfügbarkeit meines Geschäftsprozesses sicher?
- Was ist der Zeitraum, der für das Unternehmen tragbar ist, wenn Daten temporär nicht abgerufen werden können?

4.10.1 Berücksichtigung der Kritikalität

Eine Business Impact Analyse ist also erforderlich, um kritische Geschäftsprozesse identifizieren zu können. Die Ergebnisse der BIA sollten als Grundlage für die Auswahl des geeigneten Cloud-Anbieters und der vertraglichen Ausgestaltung genutzt werden. Dabei werden für sehr kritische Geschäftsprozesse nur Anbieter in Betracht kommen, die ein hinreichendes Maß an Automatisierung der Wiederanlaufprozesse anbieten. Dies muss im Einzelfall genau geprüft werden.

4.10.2 Schnittstelle zum Notfallmanagement

Der Public- und Hybrid-Cloud Anbieter übernimmt viele Aspekte der Notfallplanung für die Prozesse der KMU. Die Datensicherung der Images oder der einzelnen Daten ist vertraglich geregelt und muss daher nicht mehr von dem KMU selbst übernommen werden. Gleichzeitig ist aber immer auch nach den Vertragsstrafen oder sonstigen negativen Auswirkungen für den Anbieter zu fragen, wenn der Vertrag nicht eingehalten wird. So mögen Angebote, den Dienst für ein halbes Jahr kostenlos zu nutzen, attraktiv erscheinen, aber wenn wichtige Daten verloren gegangen sind, ist dies für das KMU trotzdem sehr schädlich. Daher sollten alle Daten auch zusätzlich durch das KMU auf eigene Systeme, z. B. einen Datenträger im eigenen Büro gesichert werden, da es sonst im schlimmsten Fall zu einem Totalverlust kommen kann.

Neben den technischen Anforderungen sind auch datenschutzrechtliche Aspekte beim Notfallmanagement mit Cloud-Techniken ein wichtiger Planungsaspekt. Details sind in dem Eckpunktepapier des BSI [BSI_2012a] und im Kapitel „Datenschutz und Cloud“ zu finden.

4.10.3 Verfügbarkeit des Anbieters

Um die Gefahr eines kompletten Stillstandes bei einem Dienstleister-Ausfall zu vermeiden, sollte man bei der Wahl der Dienstleister darauf achten, dass diese Dienstleister eine hohe Verfügbarkeit garantieren und

auch in der Vergangenheit dieses Versprechen eingehalten haben. Je länger ein Anbieter am Markt ist, desto eher kann auch das Risiko einer Insolvenz des Anbieters ausgeschlossen werden. Auch kann man auf einen gewissen Grad an Streuung setzten, also nicht alle Dienste durch einen einzelnen Dienstleister betreiben lassen. Somit wären dann nicht alle Geschäftsprozesse gleichermaßen bei einem Ausfall betroffen. Große Anbieter bieten teilweise, den Betrieb der Anwendungen in unterschiedlichen Verfügbarkeits-Zonen an, die voneinander unabhängig sind und so bereits eine Streuung der Ausfallrisiken beinhalten. Wichtig für die Bewertung der Verfügbarkeit des Anbieters sind neben der angegebenen Support-Zeit (z. B. 365x24x7) auch, welche RTOs und RPOs der Dienstleister anbietet. Auch kann es vorteilhaft sein, wenn bei dem Anbieter ein Self-Service-Portal angeboten wird, wo das KMU selbst notwendige Wiederanlaufschritte initiieren und überwachen kann.

Ein weiterer zu berücksichtigender Aspekt bei der Wahl eines Dienstleisters, ist die geografische Lokation. Dies ist zum einen wichtig bei der Betrachtung datenschutzrechtlicher Aspekte. Allerdings sollte ein KMU auch an die Abwehr von Wirtschaftsspionage durch ausländische Nachrichtendienste denken. Durch die Nutzung von Cloud-Diensten in anderen Ländern gilt auch der dortige rechtliche Rahmen. Bei Fragen zur Abwehr von Wirtschaftsspionage sollte sich das KMU an den Verfassungsschutz des jeweiligen Bundeslandes oder an das Bundesamt für Verfassungsschutz wenden.

Neben diesen Aspekten muss bei der Bewertung der geografischen Lokation auch darauf geachtet werden, dass die Support Zeiten des dortigen Help-Desks mit den Hauptgeschäftszeiten des Unternehmens kompatibel sind.

Auch die Authentisierung muss der Sicherheit der verarbeiteten Daten Rechnung tragen. So sollte, sofern besonders schutzwürdige Daten verarbeitet werden, der Anbieter eines Dienstes neben den üblichen Benutzernamen und Passwörtern auch zusätzliche Methoden wie z. B. Tokens unterstützen.

4.10.4 Mittelständische Partner für die KMU

Neben den großen Anbietern von Cloud-Dienstleistungen sind für KMU oft auch kleinere und mittelständische IT-Dienstleister wichtige Partner. Oft sind diese flexibler in den Dienstleistungen und stehen auch mit Personal vor Ort dem Unternehmen bei. So kann der IT-Dienstleister nicht nur den Betrieb eines virtuellen Standortes übernehmen, sondern es ist auch möglich, diesem Anbieter den Betrieb der IT-Systeme in den eigenen Niederlassungen zu übertragen und so Synergien erzeugen. Zudem werden durch einen lokalen Cloud-Dienstleister auch die datenschutzrechtlichen Probleme umgangen, die entstehen, wenn personenbeziehbare Daten außerhalb von Deutschland oder der EU verarbeitet werden. Ferner sollte ein KMU auch die Gefahr durch Wirtschaftsspionage bedenken, die außerhalb Deutschlands deutlich höher und schwerer zu verhindern ist, als innerhalb Deutschlands. Bei Fragen, wie ein KMU sich gegen Wirtschaftsspionage wehren kann, sollte Kontakt zu den Landesverfassungsschutzämtern oder dem Bundesamt für Verfassungsschutz aufgenommen werden.

5 Notfallplanung bei Nutzung der Public-Cloud

Das Unternehmen muss sich durch eine intensive Inanspruchnahme von Cloud-Diensten somit nur noch auf solche Notfälle vorbereiten, die das eigene Personal, die Client-Systeme, die interne IT-Vernetzung, das Weitverkehrsnetz (Internet Service Provider), der Liegenschaft oder den Cloud Service Provider selbst betreffen. Betrachtet man die Gefährdungen des BSI, welche dem Baustein 1.3 Notfallmanagement zugeordnet sind, so sollte die Betrachtung der folgenden Gefährdungen maßgeblich für das Notfallmanagement bei einer Auslagerung in die Cloud sein:

- G 1.1 Personalausfall
- G 1.2 Ausfall von IT-Systemen - nur Clients und noch vor Ort gehostete Komponenten
- G 1.10 Ausfall eines Weitverkehrsnetzes

Im Rahmen des Notfallmanagements müssen nun jedoch sämtliche Ausfallszenarien betrachtet werden, die auch wirklich das KMU betroffen. Die folgende Tabelle gibt eine Übersicht der möglichen Ausfallszenarien, die bei einer vollständigen Auslagerung von Anwendungen und Diensten eines KMUs in die Cloud, beim Notfallmanagementprozess zu berücksichtigen sind:

Kategorie des Ausfalls	Betrachtungsgegenstand für den Notfall-managementprozess	Nicht unmittelbarer Betrachtungsgegenstand	Kommentar
Ausfall Gebäude / Infrastruktur	• Datenanbindung / Internetanbindung • Interne Vernetzung (falls vorhanden)		Für die Nutzung von Cloud-Diensten ist eine leistungsfähige und redundante WAN Anbindung eine kritische Anforderung. Ausfallszenarien, die bei einem mobilen Einsatz auftreten können, sind im Notfallmanagementprozess ebenfalls zu berücksichtigen.
Ausfall Personal	• Krankheit • Pandemie • Unfall / Todesfall • Streik • Demonstration		Die Kontrolle des Personals liegt immer noch vollständig in der Hand des KMUs und muss im Notfallmanagementprozess weiterhin berücksichtigt werden.
Ausfall IT-Rechenzentrum	Es müssen nur noch jene kritischen Systeme und Infrastrukturkomponenten betrachtet werden, die noch direkt vor Ort beim KMU betrieben werden.	Systemstörungen oder Ausfälle von IT-Systemen, die bei einem Dienstleister betrieben werden, sind nicht mehr unmittelbarer Betrachtungsgegenstand. Allerdings muss betrachtet werden, wie zu verfahren ist, wenn es doch einmal zu einem unwahrscheinlichen Totalausfall des Dienstes kommen sollte.	
Ausfall Dienstleister	Ausfall des Cloud-Dienstleisters (sowohl kurzfristig durch Notfall beim Dienstleister als auch langfristig durch Insolvenz)	Wartungs- und Serviceverträge mit Hard- und Software Lieferanten müssen nicht mehr unbedingt Next-Business-Day Delivery garantieren. Gerade bei Hardwareverträgen müssen die Bereitstellungszeiten von	

Kategorie des Ausfalls	Betrachtungsgegenstand für den Notfall-managementprozess	Nicht unmittelbarer Be-trachtungsgegenstand	Kommentar
		Ersatzteilen bei Serversystemen nicht mehr allzu kritisch definiert werden. Im Fokus des Notfallmanagements sollten eher Client-Systeme stehen.	

Tabelle 5: Ausfallszenarien des Notfallmanagements und deren Behandlung für ein KMU

6 Datenschutz und Cloud

Datenschutz steht zwar nicht im Fokus des Notfallmanagements, dennoch muss man bei der Nutzung von Cloud-Diensten gezielt Aufmerksamkeit dem Datenschutz widmen. Während beim privaten Cloud-Computing die Kontrolle der Daten noch in der Hand des Unternehmens liegt, wird bei der Nutzung einer Public Cloud sämtliche Kontrolle der Daten aus der Hand gegeben. Die Registrierung für einen Public Cloud Dienst ist schnell durchgeführt, versucht man allerdings Informationen über die umgesetzten Vorkehrungen zur Sicherstellung der Datensicherheit beim Dienstleister in Erfahrung zu bringen, gestaltet sich dieses Unterfangen meist schwierig. Welche Datenschutzvorkehrungen der Dienstleister wirklich etabliert hat, kann häufig nur gemutmaßt werden. Gerade der Aspekt des Datenschutzes, wird hierdurch erschwert, da keine Möglichkeit besteht, auf den Umgang der beim Cloud-Anbieter hinterlegten Daten Einfluss zu nehmen.

Zunächst muss sich das Unternehmen im Klaren sein, ob die Daten, die er an den Cloud-Dienstleister übermittelt, dem Bundesdatenschutzgesetz (BDSG) unterliegen, wovon in den meisten Fällen auszugehen ist. Dies ist dann der Fall, wenn diese einen Personenbezug aufweisen, als sich mit ihnen Personen identifizieren oder Rückschlüsse auf bestimmte natürliche Personen zulassen. Informationen zu den Finanzen, der religiöse Überzeugung und der politischen Meinung einer Person unterliegen nach der Definition des BDSG einem besonderen Schutzbedarf. Dies können Daten von Kunden, Mitarbeitern oder Lieferanten sein. Die Nutzung von personenbezogenen Daten in der Cloud unterliegt den Anforderungen der Auftragsdatenverarbeitung und darf nur innerhalb des Europäischer Wirtschaftsraum (EWR) oder in einem US Amerikanischen Unternehmen mit gültiger SafeHarbor Zertifizierung [LDI_1] statt finden.

Im Eckpunktepapier des BSI [BSI_2012a], welches Sicherheitsempfehlungen für Cloud Computing Anbieter illustriert, wird auf die Auftragsdatenverarbeitung in der Cloud expliziter eingegangen:

“Bei der Auftragsdatenverarbeitung verbleibt die datenschutzrechtliche Verantwortlichkeit uneingeschränkt beim Cloud-Nutzer als Auftraggeber. Der Cloud-Nutzer behält datenschutzrechtlich die volle Kontrolle über die Daten. Die Auftragsdatenverarbeitung ist grundsätzlich an keine weiteren materiellen Voraussetzungen gebunden; es sind aber eine Reihe formaler Anforderungen umzusetzen. Die Auftragsdatenverarbeitung setzt eine schriftliche Vereinbarung voraus, die die in § 11 Abs. 2 BDSG aufgeführten Punkte mindestens enthalten muss. Der Cloud Computing Anbieter als Auftragnehmer unterliegt den Weisungen des Cloud-Nutzers und darf über die Verarbeitung und Nutzung der Daten nicht eigenverantwortlich entscheiden. Der Auftraggeber hat sich beim Auftragnehmer vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der technischen und organisatorischen Maßnahmen zu überzeugen. Dies muss nicht zwingend durch eine Vor-Ort-Kontrolle geschehen, sondern kann auch durch unabhängige Stellen testiert werden.”

Ein weiterer Aspekt, der bei der Ausgestaltung von Verträgen zur Auftragsdatenverarbeitung insbesondere betrachtet werden muss, ist der Ort der Speicherung. “Eine wichtige Voraussetzung ist, dass die Daten nur innerhalb des Europäischen Wirtschaftsraums (EWR) verarbeitet werden, also innerhalb der EU sowie Island, Liechtenstein und Norwegen. Nur dann erhält der Cloud-Anbieter eine Rechtsstellung, die mit einem internen Rechenzentrum des Unternehmens vergleichbar ist [IX_2012].

Die Übermittlung von nicht personenbezogenen Daten in die Cloud gestaltet sich wesentlich einfacher. Bei der Überlegung Daten in die Cloud zu verlagern, muss der Cloud-Nutzer dennoch überprüfen, ob dies wirklich im Interesse der Firma ist. Handelt es sich um besonders schutzbedürftige Daten, in denen z. B. sensible Firmeninformationen enthalten sind, sollte eventuell von der Nutzung eines Public-Cloud-Dienstes abgesehen werden oder zusätzliche Maßnahmen, wie z. B. Verschlüsselung, ergriffen werden.

7 Szenarien für eine Notfallplanung bei KMUs

In diesem Kapitel wird anhand dreier ausgewählter Szenarien illustriert, wie sich Cloud-Computing bzw. die intensive Nutzung von Virtualisierungstechniken auf den Prozess des Notfallmanagements auswirken. Die folgenden Szenarien wurden gewählt, da davon ausgegangen wird, dass deren Verbreitung in naher Zukunft weiterhin zunehmen wird. So zeigte eine repräsentative Umfrage im Auftrag der BITKOM und der Wirtschaftsprüfungsgesellschaft KPMG unter 436 Unternehmen, dass mehr als ein Drittel (37 Prozent) aller Unternehmen in Deutschland bereits im Jahr 2012 eine Form des Cloud-Computings, meist mit positiven Erfahrungen, eingesetzt haben (cloud monitor 2013).

Der Fokus bei den einzelnen beschriebenen Szenarien ist die Betrachtung der Vor- und Nachteile der Cloud-Dienste im praktischen Einsatz bei der Absicherung der kritischen Geschäftsprozesse.

7.1 Szenario 1: Alle Anwendungen in der Public Cloud

In diesem Szenario wird ein Ingenieurbüro mit primär mobilen Mitarbeitern betrachtet. Ein dediziertes Büro, in dem permanent alle Mitarbeiter untergebracht werden können, ist aufgrund der hohen Mobilität der Mitarbeiter nicht notwendig. Sie befinden sich meist beim Kunden vor Ort. Stattdessen werden nur eine begrenzte Zahl an Arbeitsplätzen und ein breitbandiger Zugang zum Internet in den Geschäftsräumen vorgehalten, welche die Mitarbeiter bei Bedarf für Besprechungen etc. in Anspruch nehmen können. Alle Geschäftsprozesse werden von Software-as-a-Service-Angeboten unterstützt.

Für die Durchführung produktiver Prozesse benötigt der einzelne Mitarbeiter nur noch seinen Laptop mit einer Internetverbindung, um die entsprechenden Cloud-Dienste zu nutzen.

Auf Grund der Vielzahl der am Markt angebotenen Cloud-Dienstleistungen wird in diesem Szenario nur eine Auswahl von Cloud-Dienstleistungen betrachtet, die elementar für jedes Unternehmen sind, und ohne die kein Unternehmen funktionieren kann. Solche Dienste sind z. B.

- Personal Information Management (PIM),
- Office Lösungen,
- zentrale Dateiablage und
- Virenschutz.

Beispielhaft soll im Folgenden der PIM-Dienst näher beleuchtet werden. Ein PIM-Dienst stellt die grundlegenden Funktionen für die Adressen-, Termin-, Aufgaben- und Notizverwaltung zur Verfügung. Normalerweise lässt dieser Begriff technisch eine komplexe Exchange-Infrastruktur vermuten, die in Form eines, auf den Mitarbeiter-Notebooks installierten Outlook-Clients, genutzt werden kann.

Will das Unternehmen hingegen seine eigene Exchange-Infrastruktur betreiben, so ist für die Realisierung die Anschaffung zusätzlicher Hard- und Softwarekomponenten sowie das entsprechende fachliche Know-how notwendig. Hinzu kommt noch, dass für den Aufbau von Exchange eine entsprechende Active-Directory-Infrastruktur vorausgesetzt wird. Der Einsatz von Spam-Filter- und Virenschutz-Gateways sollte ebenfalls berücksichtigt werden. Wie schon vorher erwähnt, wird für den Betrieb solcher Komponenten, deren Wartung und auch die entsprechende Fehlerbehebung, die Anforderung an entsprechend geschultes Personal gestellt. Zusätzlich kommt noch der zeitliche Aspekt hinzu, der für den Aufbau der Infrastruktur im eigenen Hause notwendig ist. Die sichere Unterbringung der Komponenten in einem geeigneten Serverraum stellt dann wiederum Anforderungen an die physische Beschaffenheit des Gebäudes und setzt ebenfalls eine entsprechende Stromversorgung sowie geeignete Klimatisierung voraus.

Auch die Umsetzung einer dem Schutzbedarf der Daten entsprechenden Datensicherung würde sich als aufwändig gestalten, da hier eine konkrete Abhängigkeit zu Hardware, Software und entsprechendem Personal besteht. Ein Ausfall des Gebäudes (z. B. Ausfall der Stromversorgung) würde sich sofort auf die

Mitarbeiter auswirken, da dort auch die PIM- und Speicherdienste laufen und diese im Notfall beeinträchtigt werden oder komplett ausfallen würden. Die Schaffung von Redundanzen (Stromversorgung, Hardware, Klimatisierung) für kritische Infrastruktursysteme kommt für das Ingenieurbüro auf Grund der anfallenden Kosten nicht in Frage.

Durch die Nutzung eines cloud-basierten PIM-Dienstes ist das Ingenieurbüro in der Lage, sich von den oben beschriebenen komplexen IT Infrastrukturen, wie sie z. B. von Exchange gefordert werden, loszulösen. Auch der zeitliche Rahmen, der bis zur produktiven Einführung eines entsprechenden Cloud-Dienstes verstreicht, ist kürzer als bei einer Eigenrealisierung.

Durch die Nutzung des cloud-basierten PIM-Dienstes enstehen dem Ingenieurbüro folgende Vorteile:

- Entlastung von IT-Personal,
- Sicherstellung von Ausfallsicherheit und adäquaten Backup-Strategien durch den Dienstleister (z. B. redundante Rechenzentren),
- bedarfsgerechte Bereitstellung von Ressourcen.

Selbst ein Ausfall des eigenen Gebäudes ist für die Mitarbeiter des Ingenieurbüros nicht kritisch, da sich dort nur die Buchhaltung befindet, deren kritische Ausfallzeit in der BIA auf drei Tage festgelegt wurde. Der Zugriff auf PIM-Dienste und den Cloud-Datenspeicher funktioniert auch noch beim Ausfall des Gebäudes und stellt sicher, dass die Mitarbeiter weiterhin arbeitsfähig sind.

Neben den PIM-Diensten können auch alle anderen Dienste in die Cloud verlagert werden. So sind mehrere Angebote für Office-Anwendungen auf dem Markt, bei denen auch die Datensicherung und die gemeinsame Arbeit mit enthalten sind. Eine Datensicherung der Laptops entfällt, da alle Nutzerdaten mit einem Speicherdienst synchronisiert werden. Eine Rücksicherung oder Wiederstellung von Daten kann der Mitarbeiter selbst durchführen, sobald sein neues Notebook verfügbar ist. Den Schutz der Notebooks übernehmen Virenscanner, die in der PIM-Lösung enthalten und auf dem Notebook wird ein Proxy eines Cloud-Anbieters, der den HTTP-Verkehr auf Malware überwacht.

Im Zuge der eigenen Notfallplanung wurde sichergestellt, dass die Mitarbeiter innerhalb eines festgelegten Zeitraums einen neuen Laptop vom IT-Support erhalten. Für die Sicherstellung der Verfügbarkeit und der Integrität der Daten, welche der Mitarbeiter in der Cloud abgelegt hat, ist der Cloud-Dienstleister verantwortlich.

Die Notfallstrategie des Ingenieurbüros sieht es vor, entsprechende SLAs mit dem Cloud-Dienstleister abzuschließen, in denen die Verfügbarkeiten der angebotenen Dienste vertraglich geregelt sind.

7.2 Szenario 2: Private Cloud und Backup in der Public Cloud

In diesem Szenario wird ein KMU betrachtet, welches über einen einzelnen Standort verfügt. Das Unternehmen betreibt bereits eine eigene IT-Infrastruktur und setzt verstärkt auf Server-Virtualisierung. Das Unternehmen betreibt insgesamt zwei Virtualisierungsserver in zwei voneinander getrennten IT-Räumen. Der Virtualisierungsserver hostet alle geschäftskritischen Serveranwendungen. Um die Backup-Anforderung zu erfüllen, hat sich das Unternehmen dafür entschieden, das Backup sämtlicher Unternehmensdaten in eine Public-Cloud auszulagern und nimmt somit die Dienstleistung eines darauf spezialisierten Cloud-Dienstleisters in Anspruch.

Im Rahmen des Notfallmanagements wird die Kontinuität der kritischen Prozesse (z. B. bei einem Ausfall eines Raumes) durch die Verteilung der virtualisierten Server auf die beiden Virtualisierungsserver gesichert. Die für die kritischen Geschäftsprozesse notwendigen virtuellen Server sind dabei auf beiden Servern gespeichert, wodurch entsprechende Redundanzen geschaffen werden. Ein Virtualisierungsserver fungiert somit als Master für die Hälfte der als virtuellen Maschinen, während der andere die Rolle des Slaves für diese virtuellen Maschinen übernimmt. Die andere Hälfte der virtuellen Maschinen betrachtet diesen Server als ihren Master und den anderen Server als den Slave. Im Normalbetrieb läuft die virtuelle Maschine auf dem Master. Kommt es zu einem Ausfall eines Virtualisierungsservers, oder ist der

entsprechende Gebäudeteil nicht mehr zugänglich, werden die wichtigen Serverdienste und virtuellen Maschinen auf dem noch betriebsbereiten Virtualisierungsserver gestartet.

. Ein Datenabgleich zwischen den virtuellen Maschinen auf den unterschiedlichen Virtualisierungsservern findet durch ein stündliches Kopieren der virtuellen Maschinen von Master zu Slave statt. Lediglich die Daten, welche seit dem letzten Kopiervorgang der virtuellen Maschinen erzeugt oder geändert worden sind, befinden sich noch nicht auf dem Slave-System. Diese sind bei einem Verlust des Masters verloren. Hier ist es wichtig eine ausreichend schnelle Synchronisation zu ermöglichen, damit der Zeitpunkt an dem alle die letzte Kopie erstellt wurde, nicht zu weit in der Vergangenheit liegt.

In diesem gedachten Unternehmen haben Notfalltests ergeben, dass der Umschaltvorgang von Master zu Slave in unter 5 Minuten erfolgt und dies wurde von der Geschäftsführung als ausreichend betrachtet. Diese kurze Zeit wird möglich, da sich das Unternehmen für den Kauf von entsprechenden Produkten entschieden hat, die die Umschaltung automatisch vornehmen. Dabei startet die Software die Maschinen automatisch und versieht sie mit den entsprechenden IP-Adressen, sobald ein Problem mit dem Master-System erkannt wird. Die Administratoren hinterlegten Anhand der Kritikalität der Systeme Prioritäten der einzelnen virtuellen Maschinen. Die Software startet im Notfall die kritischeren virtuellen Maschinen gezielt. Ein manuelles Umschalten ist ebenfalls möglich und wird für regelmäßige Notfalltests genutzt..

Die erforderlichen Prozeduren für das manuelle und automatische Umschalten hat das Unternehmen in einem Notfallhandbuch dokumentiert, um sicherzustellen, dass sie von dem im Notfall jeweils verfügbaren Personal ausgeführt werden können. Das Notfallhandbuch beschreibt ausführlich, wie sämtliche Systeme, inklusive der Virtualisierungsserver und der virtuellen Maschinen, auf dem Slave wieder in Betrieb genommen werden können. Es beschreibt auch Testverfahren, um zu verifizieren, dass die Dienste weiterhin wie gewünscht funktionieren.

Obwohl das Risiko eines Totalausfalls beider Virtualisierungsserver eher gering erscheint, hat sich das Unternehmen mit dieser Möglichkeit beschäftigt und im Rahmen des Notfallmanagements entsprechende Vorkehrungen getroffen.

So wurden bewusst auf die Einführung einer teuren Backup-Lösung im Unternehmen verzichtet und stattdessen das Backup sämtlicher virtueller Server-Images in eine Public-Cloud ausgelagert. Es wird ein Backup-Produkt genutzt, dass die Auslagerung gesamter virtueller Maschinen in die Cloud erlaubt. Das Hochladen der Images erfolgt automatisch zu definierten Zeiten. Durch die konfigurierbare Verschlüsselung wird sichergestellt, dass keine unberechtigten Parteien auf die Daten innerhalb des virtuellen Images zugreifen können. Durch intelligente Kompressionalgorithmen und dass nur veränderte Daten übertragen werden, wird die Zeit, die für das Hochladen des virtuellen Images benötigt wird, erheblich reduziert. Letztendlich wirkt sich die Kompression noch auf die Kosten für den Cloud-Speicher aus. Auch ein manuelles Kopieren der virtuellen Images oder Backups in die Cloud ist möglich, allerdings muss sich der IT-Administrator dann selbständig um die Verschlüsselung kümmern. Die folgende Abbildung illustriert die Ablage von Images von virtuellen Maschinen bei einem Anbieter von Cloud-Speicher.

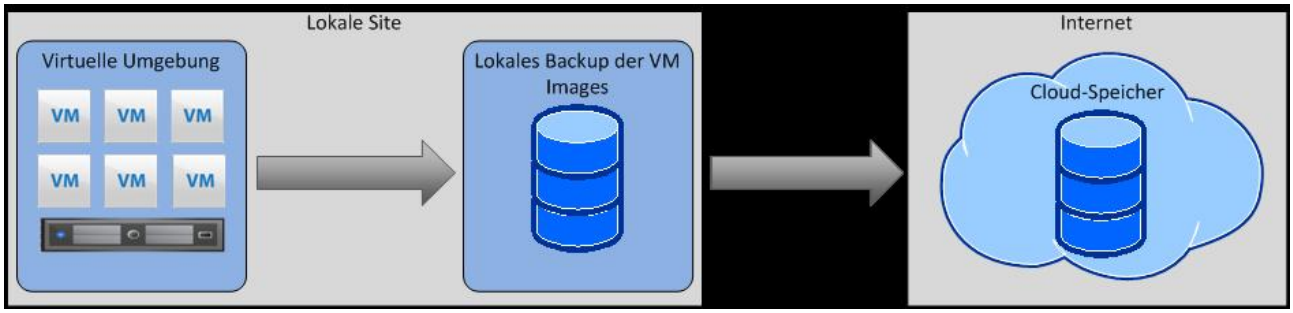

Abbildung 3: Veranschaulichung des Szenarios 2 "Private Cloud und Backup in der Public Cloud"

Bei Verlust beider Virtualisierungsserver bzw. des gesamten Gebäudes liegt beim Public-Cloud-Anbieter zumindest ein Backup aller Server-Images vor, die auf die neu beschafften Virtualisierungsserver bzw. an einem Not-Standort eingespielt und gestartet werden können.

Als Not-Standort bietet sich hier auch wieder eine Cloud an. Hierdurch kann die Zeit überbrückt werden kann, bis das Unternehmen wieder eine lauffähige Hardware für den Betrieb der virtuellen Maschinen beschafft hat. Dies hat das Unternehmen ebenfalls vorbereitet. Dauert ein Notfall länger als drei Tage und sind beide Server dauerhaft verloren, werden die Images nach der Schlüsselübergabe beim Anbieter entschlüsselt und in einer virtualisierten Umgebung gestartet.

Ohne die Nutzung der Virtualisierung würde der Wiederanlauf mehrere Stunden (bzw. bei Verlust beider Server und des Gebäudes mehrere Tage oder Wochen) benötigen, da ansonsten eine komplette Neuinstallation der Systeme zu erfolgen hätte, was mit einem erheblichen Mehraufwand verbunden wäre. Zusätzlich müssten die Geschäftsdaten noch aus dem entsprechenden Backup (sofern vorhanden) wiederhergestellt werden, was ebenfalls zu zeitlichen Beeinträchtigungen führt. Der manuelle Schwenk ist hier mit unter einer halben Stunde eine erhebliche Verbesserung. Bei Verlust aller Daten hätte das Unternehmen vor der Einführung des Off-Site Backups mit hoher Wahrscheinlichkeit die Geschäftstätigkeit einstellen müssen. Dieses Risiko konnte durch die Verwendung des Cloud-Dienstes zu sehr geringen Kosten stark reduziert werden.

7.3 Szenario 3: Zusätzlicher Standort in der Cloud

Dieses Szenario beschreibt ein KMU mit zwei Standorten, die wegen ihrer Lage in den Gewerbegebieten zweier Dörfer nur über eine langsame Internetanbindung verfügen. Die Benutzer beider Standorte sind in kritische Geschäftsprozesse eingebunden, weshalb die Mitarbeiter beider Standorte darauf angewiesen sind, auf die im anderen Standort bereitgestellten Anwendungen zuzugreifen. Hauptsächlich erfolgen die Zugriffe allerdings auf den Server in dem Standort auf dem sie Arbeiten. Eine schnelle Verlagerung oder gar Spiegelung der Daten oder der Anwendungen zwischen den Standorten ist wegen der limitierten Bandbreite nicht zu realisieren, denn die Leitungen wären dann zu sehr ausgelastet.

Um flüssigeres Arbeiten zu ermöglichen und die Notfallvorsorge zu verbessern, hat das KMU einen Server bei einem deutschen Cloud-Anbieter gemietet und spiegelt nun nachts, wenn keine Mitarbeiter arbeiten, die virtualisierten IT-Systeme an diesen Standort. Die Synchronisation ist schneller, denn nun müssen die Daten jeweils nur eine Leitung eines Standortes passieren und damit auch bei der geringen Geschwindigkeit der Datenleitungen in den Standorten möglich. Wenn einer oder beide Standorte ausfallen, kann der Administrator die Anwendungen an diesem zusätzlichen Standort in der Cloud in wenigen Minuten starten und die Daten sind nicht älter als einen Tag. Der Verlust der Daten eines Tages wurde vom Inhaber des KMU als tragbares Risiko bewertet.

Die folgende Abbildung illustriert die Architektur:

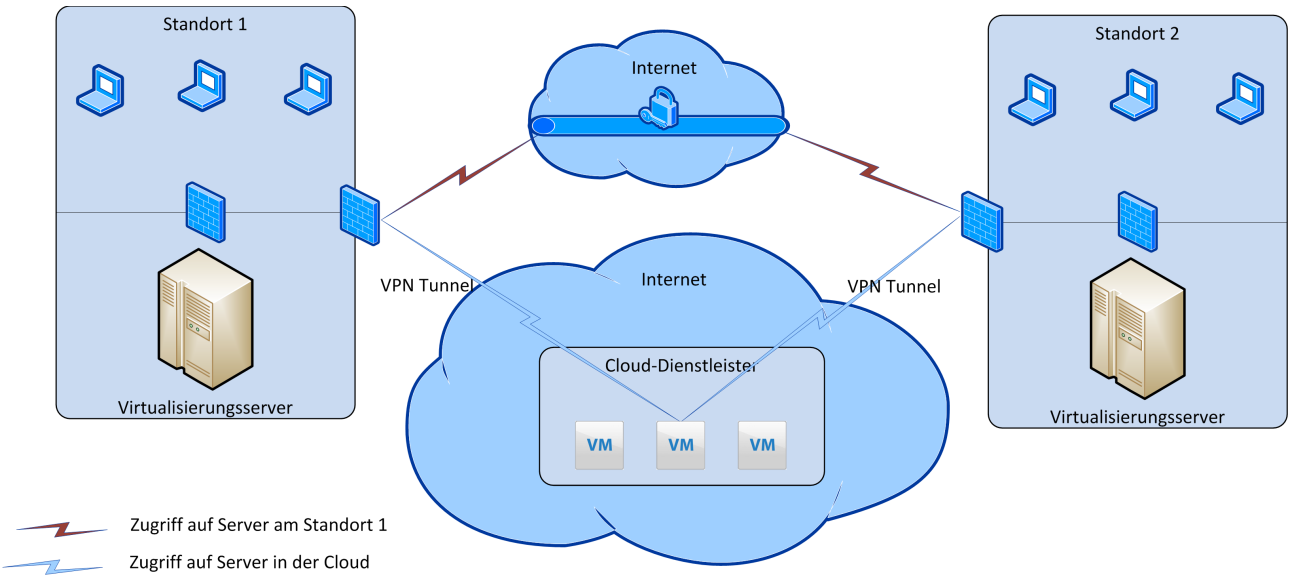

Abbildung 4: Veranschaulichung des Szenario 3 "Zusätzlicher Standort in der Cloud"

Durch diesen Aufbau ist es möglich, dass alle Mitarbeiter auch bei Verlust eines oder beider Standorte von ihren regulären oder anderen Arbeitsplätzen weiterarbeiten können. Sie sind durch diese Architektur nicht zwingend an einen bestimmten Standort gebunden, da für den Zugriff auf die Anwendung letztendlich nur eine entsprechend breitbandige Internetverbindung benötigt wird. So können sie bei einem Ausfall entweder von Not-Arbeitsplätzen in einem Standort oder auch vom Home-Office weiterarbeiten. Für das Home-Office wurde den Mitarbeitern ein VPN-Zugang auf den Notebooks installiert, den sie in einem solchen Falle nutzen.

Da mit dem Cloud-Anbieter vertraglich geregelt ist, auch die Backups der Anwendung durchzuführen, ist das KMU vor Datenverlusten geschützt und legt zur Sicherheit noch eine Kopie der Daten im Schließfach der Bankfiliale ab. Auch ein Ausfall von Hardware beim Anbieter ist für das KMU also in den meisten Fällen ohne Konsequenzen, da dieser die entsprechenden Notfallstrategien implementiert hat und unter anderem ausreichende Redundanzen geschaffen hat, welche ein Weiterarbeiten ermöglichen.

8 Fazit und Ausblick

Bisher wurden Virtualisierungs- und Cloud-Techniken häufig nur als Techniken mit großem Einsparpotenzial und immensen Herausforderungen für die Informationssicherheit betrachtet. Die großen Vorteile für die Absicherung von Geschäftsprozessen gegen Ausfall bzw. für den zügigen Anlauf mit einer verringerten Not-Kapazität, die aus diesen Techniken herrühren können, sind noch wenig beleuchtet.

Die Vorteile dieser Techniken liegen neben technischen Aspekten, wie der Möglichkeit zur sofortigen Übernahme bei Ausfall eines IT-Systems, vor allem in den geringeren Kosten im Vergleich zu Redundanzkonzepten ohne Virtualisierungs- oder Cloud-Techniken. Dieser Vorteil kann, wie in diesem Beitrag skizziert, gerade für KMUs bedeutsam sein, da diese Gruppe von Unternehmen nur sehr selten ein umfassendes Notfallmanagement betreibt. Wie hier gezeigt wurde, können diese Unternehmen dank Virtualisierungs- und Cloud-Techniken ein bisher unerreichtes und unfinanzierbares Niveau an Verfügbarkeit und Sicherheit vor Datenverlust erhalten. Mit den hier skizzierten Hilfsmitteln zur BIA kann zumindest ein rudimentäres Notfallmanagement in KMUs etabliert werden, was die Keimzelle für ein umfassenderes Notfallmanagement sein kann.

Allen Vorteilen über die leichter zu erreichende höhere Verfügbarkeit zum Trotz darf nicht vernachlässigt werden, dass Cloud-Computing zur Beantwortung vieler wichtiger Fragen der Informationssicherheit und des Datenschutzes nötigt. Insbesondere wenn sich der Cloud-Dienstleister im Ausland befindet, kommen noch Fragen zur Abwehr von möglicher Wirtschaftsspionage hinzu.

Das Vertrauen in die Verlässlichkeit und Vertraulichkeit in Cloud-Computing zu stärken ist eine wichtige Aufgabe für die Zukunft. Nur mit sicherem Cloud-Computing wird es möglich sein, dass volle Potenzial dieser Technik umfassend zu nutzen.

9 Anhang: Beispiel einer IT-BIA eines KMUs

Dieses Beispiel für eine Business Impact Analyse sollten die meisten KMU in dieser Form anwenden können.

9.1 Finanzbuchhaltung

Dieser Geschäftsbereich beinhaltet:

- Lohnbuchhaltung
- Faktura
- Steuern, insbesondere Umsatzsteuern

<table>
<tr><th>Nr.</th><th>Fragestellung</th></tr>
<tr><td>1</td><td>Welche Auswirkungen (1 - niedrig, 2 - mittel, 3 - hoch, 4 - sehr hoch) hat es auf das Unternehmen, wenn der Kernprozess ausfällt?
<table>
<tr><th>Ausfall <1d</th><th>Ausfall <3d</th><th>Ausfall >3d</th></tr>
<tr><td>Niedrig</td><td>Niedrig</td><td>Mittel</td></tr>
</table>
Welche Auswirkungen (1 - niedrig, 2 - mittel, 3 - hoch, 4 - sehr hoch) hat ein Datenverlust auf das Unternehmen?
<table>
<tr><th>Geringer Verlust</th><th>Teilweiser Verlust</th><th>Vollständiger Verlust</th></tr>
<tr><td>Mittel</td><td>Hoch</td><td>Sehr hoch</td></tr>
</table></td></tr>
<tr><td>2</td><td>Welche IT-Systeme sind für einen Notbetrieb des Prozesses zwingend erforderlich?

Arbeitsplatz-PC mit Textverarbeitung und Druckmöglichkeit</td></tr>
<tr><td>3</td><td>Welcher der IT-Systeme enthalten Daten, die bei einem Verlust nicht wiederbeschafft werden können?

Zentraler Buchhaltungsserver SXVRV013</td></tr>
<tr><td>4</td><td>Gibt es Alternativen oder alternative Arbeitsabläufe zu diesen IT-Systemen?

Rechnungsstellung zunächst aus der Textverarbeitung; Nacherfassung in der Buchhaltung</td></tr>
<tr><td>5</td><td>Welche IT-Dienstleister sind für einen Notbetrieb des Prozesses zwingend erforderlich?

Keine</td></tr>
<tr><td>6</td><td>Gibt es Alternativen oder alternative Arbeitsabläufe zu diesen IT-Dienstleistern?

Nein</td></tr>
</table>

9.2 Vertrieb

Dieser Geschäftsprozess beinhaltet:

- Verkauf
- Preisfindung
- Vertragsabwicklung
- Marketing

<table>
<tr><th>Nr.</th><th>Fragestellung</th></tr>
<tr><td>1</td><td>Welche Auswirkungen (1 - niedrig, 2 - mittel, 3 - hoch, 4 - sehr hoch) hat es auf das Unternehmen, wenn der Kernprozess ausfällt?
<table>
<tr><th>Ausfall <1d</th><th>Ausfall <3d</th><th>Ausfall >3d</th></tr>
<tr><td>Niedrig</td><td>Mittel</td><td>Hoch</td></tr>
</table>
Welche Auswirkungen (1 - niedrig, 2 - mittel, 3 - hoch, 4 - sehr hoch) hat ein Datenverlust auf das Unternehmen?
<table>
<tr><th>Geringer Verlust</th><th>Teilweiser Verlust</th><th>Vollständiger Verlust</th></tr>
<tr><td>Mittel</td><td>Hoch</td><td>Sehr hoch</td></tr>
</table></td></tr>
<tr><td>2</td><td>Welche IT-Systeme sind für einen Notbetrieb des Prozesses zwingend erforderlich?

Arbeitsplatz-PC mit Textverarbeitung und E-Mail-Kommunikation
E-Mail-Server mit Internetanbindung</td></tr>
<tr><td>3</td><td>Welcher der IT-Systeme enthalten Daten, die bei einem Verlust nicht wiederbeschafft werden können?

E-Mail-Server</td></tr>
<tr><td>4</td><td>Gibt es Alternativen oder alternative Arbeitsabläufe zu diesen IT-Systemen?

Web-Mail-Accounts zum Versand von Angeboten</td></tr>
<tr><td>5</td><td>Welche IT-Dienstleister sind für einen Notbetrieb des Prozesses zwingend erforderlich?

Web-Mail-Provider</td></tr>
<tr><td>6</td><td>Gibt es Alternativen oder alternative Arbeitsabläufe zu diesen IT-Dienstleistern?

Ein kurzfristiger Wechsel zu einem anderen Web-Mail-Provider ist grundsätzlich möglich.</td></tr>
</table>

9.3 Produktion

Dieser Geschäftsprozess beinhaltet:

- Projektmanagement
- Kundenkommunikation in Projekten und bei der Fertigung

<table>
<tr><th>Nr.</th><th>Fragestellung</th></tr>
<tr><td>1</td><td>Welche Auswirkungen (1 - niedrig, 2 - mittel, 3 - hoch, 4 - sehr hoch) hat es auf das Unternehmen, wenn der Kernprozess ausfällt?
<table>
<tr><th>Ausfall <1d</th><th>Ausfall <3d</th><th>Ausfall >3d</th></tr>
<tr><td>Niedrig</td><td>Mittel</td><td>Hoch</td></tr>
</table>
Welche Auswirkungen (1 - niedrig, 2 - mittel, 3 - hoch, 4 - sehr hoch) hat ein Datenverlust auf das Unternehmen?
<table>
<tr><th>Geringer Verlust</th><th>Teilweiser Verlust</th><th>Vollständiger Verlust</th></tr>
<tr><td>Mittel</td><td>Hoch</td><td>Sehr hoch</td></tr>
</table></td></tr>
<tr><td>2</td><td>Welche IT-Systeme sind für einen Notbetrieb des Prozesses zwingend erforderlich?

Keine (telefonische und persönliche Kommunikation ist ausreichend)</td></tr>
<tr><td>3</td><td>Welcher der IT-Systeme enthalten Daten, die bei einem Verlust nicht wiederbeschafft werden können?

Nicht zutreffend</td></tr>
<tr><td>4</td><td>Gibt es Alternativen oder alternative Arbeitsabläufe zu diesen IT-Systemen?

Nicht zutreffend</td></tr>
<tr><td>5</td><td>Welche IT-Dienstleister sind für einen Notbetrieb des Prozesses zwingend erforderlich?

Nicht zutreffend</td></tr>
<tr><td>6</td><td>Gibt es Alternativen oder alternative Arbeitsabläufe zu diesen IT-Dienstleistern?

Nicht zutreffend</td></tr>
</table>

9.4 Besonders schützenswerte IT-Systeme und Dienstleister

Es hat sich bewährt, eine Übersichtstabelle über die kritischen IT-Systeme und Dienstleister zu führen, die im Notfall schnell zu Schäden führen.

IT-System	MTA	Auswirkung in <1d	Auswirkung in <3d	Auswirkung in >3d	Alternative
Arbeitsplatz-PC	3 Tage	niedrig	mittel	hoch	
E-Mail-Server	3 Tage	niedrig	hoch	Sehr hoch	Web-Mail-Service

Literaturverzeichnis

BSI_2011a Bundesamt für Sicherheit in der Informationstechnik: Studie zur IT-Sicherheit in kleinen und mittleren Unternehmen; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/Studien/KMU/Studie_IT-Sicherheit_KMU.pdf?__blob=publicationFile

DI_2012 Dell: Der Umgang mit veränderten IT-Anforderungen; http://content.dell.com/at/de/unternehmen/d/business~smb~sb360~de/Documents~17595-Servers-Storage-Report-Feb-2012-PDF-V02-SM-LR-de.pdf.aspx

BSI_2012a Bundesamt für Sicherheit in der Informationstechnik: Eckpunktepapier - Sicherheitsempfehlungen für Cloud Computing Anbieter; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Mindestanforderungen/Eckpunktepapier-Sicherheitsempfehlungen-CloudComputing-Anbieter.pdf?__blob=publicationFile

BSI_2012b Bundesamt für Sicherheit in der Informationstechnik: Webkurs Notfallmanagement auf Basis von BSI-Standard 100-4; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Webkurs/Webkurs_Notfallmanagement.pdf?__blob=publicationFile

BSI_2008 Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-4: Notfallmanagement, Bundesanzeiger Verlag m.b.H., 2008, 978-3-89817-693-4, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1004_pdf.pdf?__blob=publicationFile

BSI_2012c Bundesamt für Sicherheit in der Informationstechnik: Überblickspapier Online-Speicher; https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/Ueberblickspapier_Online-Speicher_pdf.pdf?__blob=publicationFile

LDI_1 LDI: Wie wird der Schutz der Persönlichkeitsrechte bei der Übermittlung von Daten in das Ausland gewährleistet?; https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Datenschutzrecht/Inhalt/InternationalerDatenverkehr/Inhalt2/Schutz_der_Persoenlichkeitsrechte/Schutz_der_Persoenlichkeitsrechte.php

IX_2012 Böken, Arnd: Patriot Act und Cloud Computing: Zugriff auf Zuruf; IX Magazin für professionelle Informationstechnik, 2012, http://www.heise.de/ix/artikel/Zugriff-auf-Zuruf-1394430.html