HOCHSCHULE
MITTWEIDA
UNIVERSITY OF
APPLIED SCIENCES

DIPLOMARBEIT

Herr Ing.
Christian Kern

IT-Notfallplanung

Mittweida, 2015

Fakultät Elektro- und Informationstechnik

DIPLOMARBEIT

IT-Notfallplanung

Autor:
Herr Ing. Christian Kern

Studiengang:
Informationstechnik

Seminargruppe:
KI09sWA

Erstprüfer:
Prof. Dr.-Ing. habil. Lutz Winkler

Zweitprüfer:
Dipl.-Ing. Johann Joham

Einreichung:
Mittweida, 09.03.2015

Verteidigung/Bewertung:
Mittweida, 2015

Bibliografische Beschreibung:

Kern, Christian:
IT-Notfallplanung – Einführung des IT-Grundschutz in einem Klein- und Mittelbetrieb. Bestimmung des Schutzbedarfs mit Hilfe des IT-Grundschutz Kataloges. 2015. – 63 S.
Mittweida, Hochschule Mittweida, Fakultät Elektro- und Informationstechnik, Diplomarbeit, 2015

Referat:

Ziel ist es, in einem Klein- und Mittelbetrieb nach dem IT-Grundschutz und der IT-Grundschutzkataloge eine IT-Notfallplanung zu erstellen.
Für dessen Umsetzung wird die IT-Infrastruktur eines Klein- und Mittelbetriebes ermittelt und in Abhängigkeiten gesetzt. Die notwendigen IT-Schutzmaßnahmen werden mit Hilfe der IT-Grundschutzkataloge ermittelt. Abschließend wird die prototypische Umsetzung einer Notfallplanung dargestellt.

Inhalt

Abbildungsverzeichnis

Tabellenverzeichnis

Abkürzungsverzeichnis

BSI	Bundesamt für Sicherheit in der Informationstechnik
IT	Informationstechnik
ISMS	Information Security Management System
CISO	Chief Information Officer
ASP	Application Service Provider
SAN	Storage Area Networks
VPN	Virtual Private Network
RAID	Redundant Array of Independent Disks
USV	unterbrechungsfreie Stromversorgung
LAN	Local Area Network
HW	Hardware
PC	Personal Computer
OS	Operation System
VM	Virtual Machine

Danksagung

Mein Dank gilt in erster Linie meiner Familie - sie alle haben mir das Studium durch ihre Unterstützung erst möglich gemacht.

Seitens der Firma bedanke ich mich bei allen meinen Mitarbeitern, mit denen ich eine äußerst konstruktive und nette Zusammenarbeit geführt habe.

Ein besonderer Dank gilt auch meinem persönlichen Betreuer Herrn DI Johann Joham, er hat durch seine konstruktiven Anmerkungen und Unterstützung einen wertvollen Beitrag zum Erfolg dieser Arbeit geleistet.

Nicht vergessen möchte ich auch meinen Betreuer von der Fachhochschule Mittweida, Herrn Prof. Dr.-Ing. habil. Lutz Winkler. Ich danke ihm herzlich für die außerordentlich gute Betreuung und Unterstützung.

1 Einleitung

In diesem Kapitel wird vor allem auf die Zielsetzung und Motivation dieser Diplomarbeit eingegangen. Im letzten Punkt wird die Gliederung der Arbeit erläutert.

1.1 Zielsetzung

Das Thema dieser Diplomarbeit ist die Erstellung einer IT-Notfallplanung in einem Klein- und Mittelbetrieb. Als Grundlage hierfür wird auf den IT-Grundschutz - insbesondere auf die IT-Grundschutz-Kataloge - eingegangen. [GS-KATALOGE] Die Darstellung und Ermittlung der IT-Infrastruktur in den einzelnen Abhängigkeiten wird mit Hilfe der IT-Grundschutz-Kataloge erstellt. Abschließend wird mit deren Hilfe eine prototypische Umsetzung erarbeitet und implementiert.

1.2 Motivation

Da der Verfasser dieser Arbeit in der IT-Abteilung eines internationalen Konzerns tätig und ständig mit der IT-Sicherheit konfrontiert ist, hat er sich der Aufgabe gestellt, für dieses Unternehmen eine IT-Notfallplanung nach dem IT-Grundschutz zu erstellen.

Eine sehr hilfreiche Unterstützung bietet die Plattform des Bundesamts für Sicherheit in der Informationstechnik (BSI). [GS-KATALOGE] Diese stellt wichtige Informationen und Werkzeuge im Bereich IT-Grundschutz zur Verfügung.

1.3 Gliederung der Diplomarbeit

Diese Diplomarbeit besteht aus sechs Kapiteln.

Das **erste Kapitel** beinhaltet eine kurze Einleitung der Arbeit, zeigt die Ziele auf und beschreibt die Motivation.

Im **zweiten Kapitel** gibt es einen kurzen Überblick zum Thema IT-Grundschutz.

In **Kapitel 3** werden die einzelnen IT-Grundschutz-Kataloge erklärt und es wird verstärkt auf den Bereich IT-Notfallplanung eingegangen.

Im **vierten Kapitel** werden die Aufgabenstellung und Ziele der Diplomarbeit festgelegt.

In **Kapitel 5** wird die prototypische Umsetzung einer IT-Notfallplanung dargestellt.

Das letzte **Kapitel 6** enthält Ergebnisse und gibt einen Ausblick auf offene Punkte.

2 IT-Grundschutz

In [GS-KATALOGE] ist erklärt, dass nahezu alle Geschäftsprozesse elektronisch gesteuert sind und es daher umso wichtiger ist, diese Daten zu schützen. Auf Grund der Tatsache, dass die Geschäftsprozesse immer komplexer werden, bilden sich natürlich auch Gefährdungspotentiale in der Informationstechnologie. Wie in [GS-Kataloge] beschrieben, bietet der IT-Grundschutz eine simple Methodik, auf dem Stand der Technik angebrachte Sicherheitsmaßnahmen zu erkennen und umzusetzen. Das Bundesamt für Sicherheit in der Informationstechnik (BSI) bietet auf deren Webseite zahlreiche Werkezeuge und Informationen an, um ein notwendiges Sicherheitsniveau zu erzielen. Beispiele hierfür sind die BSI-Standards zum Informationssicherheitsmanagement und die IT-Grundschutzkataloge, die in Kapitel 3 bearbeitet werden. Abschließend gehört auch die ISO 27001-Zertifizierung, die auf Basis des IT-Grundschutzes basiert, dazu.

2.1 Informationssicherheit

In den letzten Jahren und Jahrzehnten hat sich der Bedarf an Informationssicherheit deutlich erhöht.
Der Grund hierfür ist die starke Vernetzung von mobilen Geräten, wodurch stetig an einem höheren Maß an Sicherheit gearbeitet werden muss. [GS-KATALOGE]

2.1.1 Informationssicherheit–ein Muss für jedes Unternehmen

Ein Unternehmen muss sich systematisch den Risiken und den entsprechenden Gegenmaßnahmen stellen. Die Maßnahmen schützen die Unternehmen vor Bedrohungen wie zum Beispiel einer Zerstörung, Manipulation oder einer nicht autorisierten Benutzung. Die Ziele hierbei sind, dass der laufende Unternehmensbetrieb und die Erreichung der vordefinierten Ziele nicht gefährdet werden. [GS-KATALOGE]

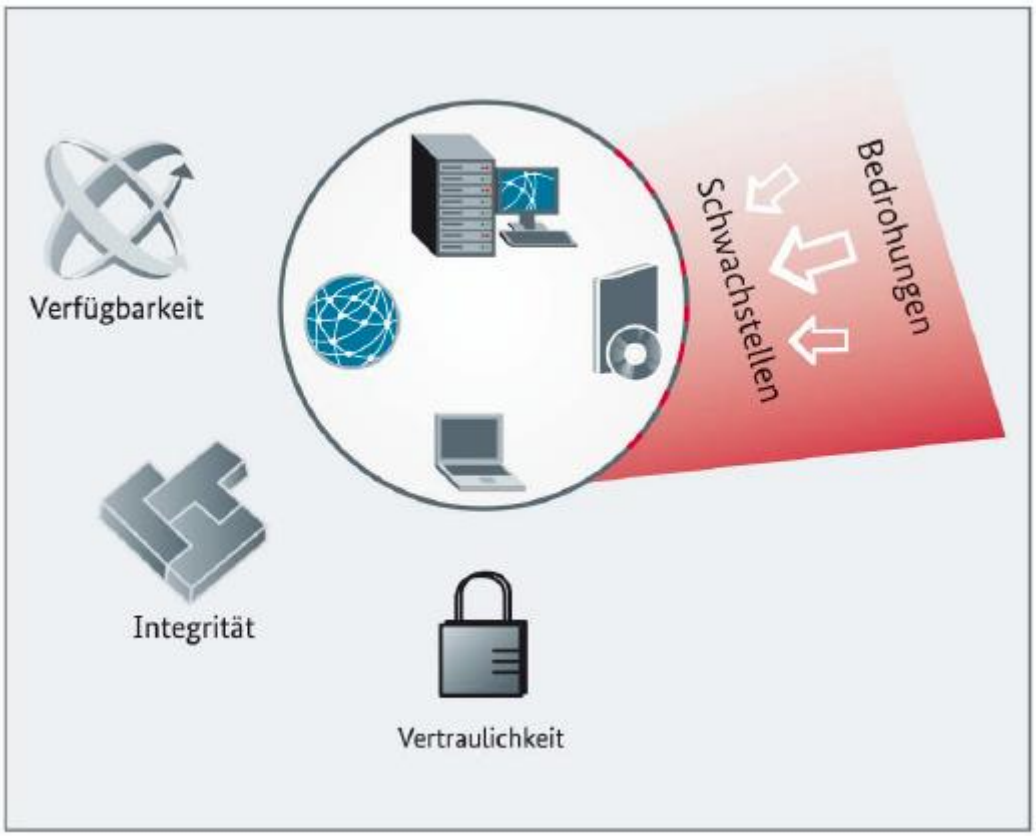

Abbildung 1: Hauptziele der Informationssicherheit [BSI-GS-BROSCH]

Wie in Abbildung 1 zu sehen ist, sind die positiven Hauptziele der Informationssicherheit die Vertraulichkeit, Verfügbarkeit und Integrität. Es gibt auch noch andere Vorteile die aus der Informationssicherheit gewonnen werden. Hierzu zählen die betriebswirtschaftliche Wertschöpfung und der organisatorische Nutzen. [BSI-GS-BROSCH]

2.1.2 Informationssicherheit–Betriebswirtschaftlicher Nutzen

Durch die Informationssicherheit kann die Wettbewerbsfähigkeit gesteigert werden. Es erhöht bei Kunden, Partner und Mitarbeitern das Vertrauen. Interne Abläufe können optimiert werden und somit kann kosteneffizienter gearbeitet werden. [BSI-GS-BROSCH]

2.1.3 Informationssicherheit–Organisatorischer Nutzen

Transparente Informationssicherheit fördert die Vorgehensweise von Unternehmen. Beispielsweise können bei Erfolgskontrollen durch interne Sicherheitsaudits auch Verbesserungspotentiale aufgezeigt werden. Das Sicherheitsmanagement überprüft laufend die Änderungen und somit ist gewährleistet, dass es ein sehr hohes Sicherheitsniveau gibt. [BSI-GS-BROSCH]

2.2 Organisation und Informationssicherheit

Das Management für Informationssicherheit (ISMS) hat Schnittstellen in vielen Bereichen eines Unternehmens. Diese betreffen alle wichtigen Geschäftsprozesse und Aufgaben.
Für den Erfolg der Integration eines Managementsystems für Informationssicherheit ist in einem Unternehmen das Management verantwortlich.
Dieses sogenannte Sicherheitsmanagement muss die entsprechende finanzielle und personelle Kompetenz besitzen um so ein System aufbauen zu können.

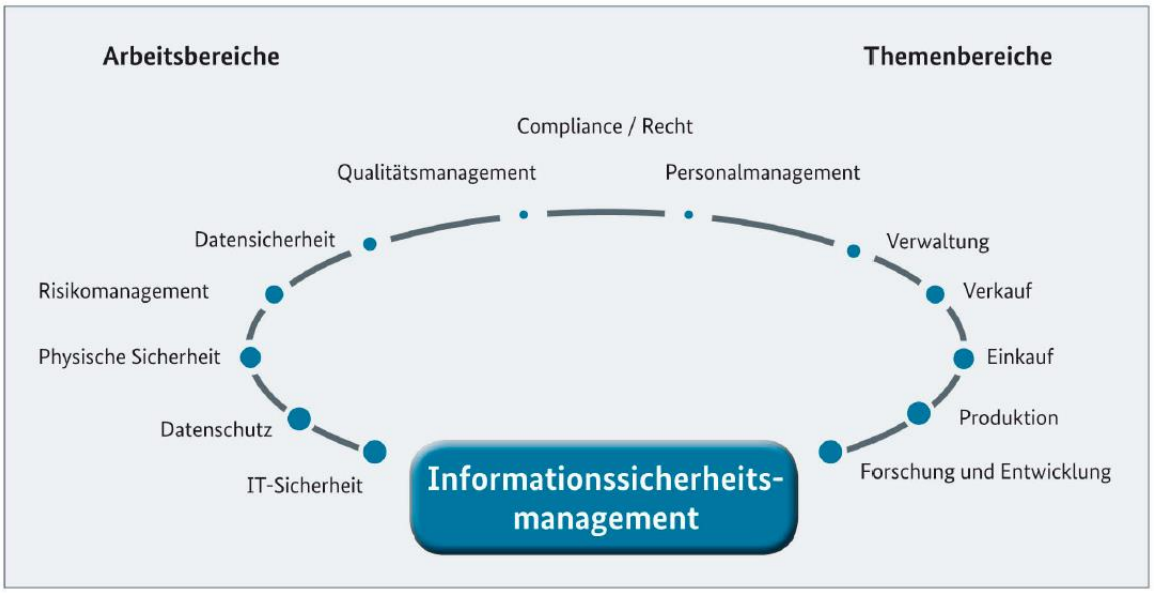

Abbildung 2: Bereiche des Informationssicherheitsmanagement [BSI-GS-BROSCH]

In Abbildung 2 werden die Schnittstellen mit den einzelnen Arbeitsbereichen dargestellt. Der grundlegende Aspekt hierbei ist, dass keiner der Bereiche wichtiger als der andere ist. [BSI-GS-BROSCH]

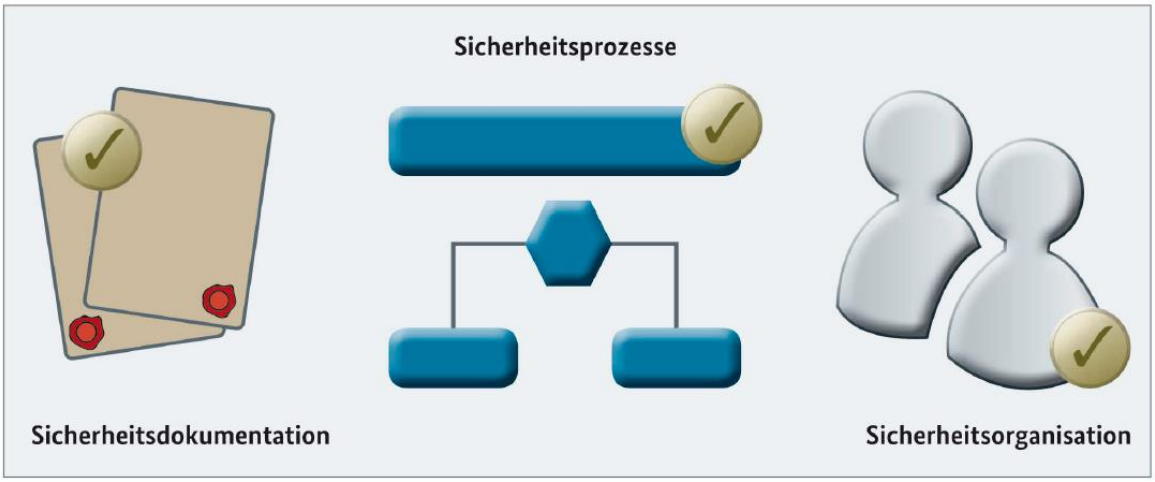

Abbildung 3: Aufbau des Informationssicherheitsmanagement [BSI-GS-BROSCH]

Abbildung 3 zeigt eine Darstellung der Hauptbereiche, welche für eine erfolgreiche Implementierung eines Informationssicherheitsmanagement bedacht werden sollen. [BSI-GS-BROSCH]

In einem Unternehmen sollte es für dieses komplexe Projekt einen Ansprechpartner geben. Zumeist wird dieser IT-Sicherheitsbeauftragte Chief Information Security Officer (CISO) genannt. Er koordiniert innerhalb der Organisation die Aufgaben und ist für den Projektverlauf verantwortlich.

2.3 Praktische Unterstützung durch das BSI: Der IT-Grundschutz

Die Informationssicherheit beinhaltet nicht nur die Absicherung von IT-Systemen und den Schutz von Informationen, sondern auch den Aufbau eines Managementsystems für Informationssicherheit. Das Managementsystem gewährleistet die Nachhaltigkeit und stellt sicher, dass Gefahren erkannt und entsprechend behandelt werden. Zu diesem Punkt gehören auch die organisatorischen, personellen sowie etwaige baulichen Aspekte. Somit kann für den Normalbedarf sehr rasch ein entsprechendes Sicherheitsniveau erreicht werden.

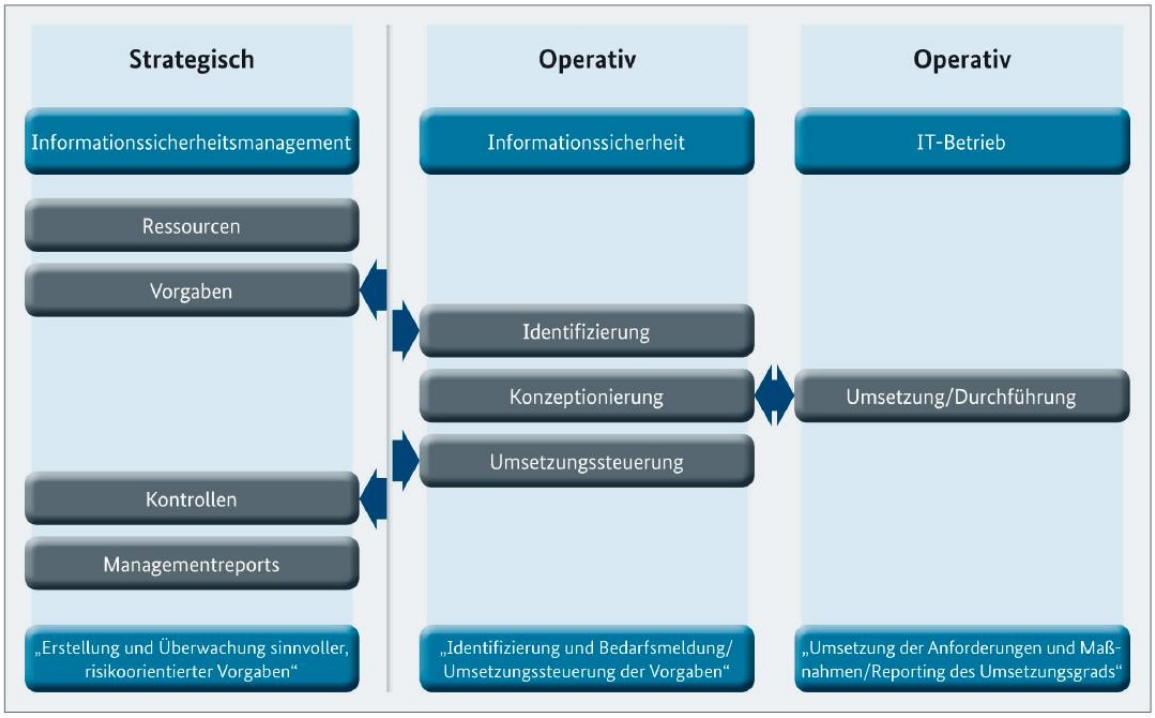

Abbildung 4: Verantwortung für Informationssicherheit [BSI-GS-BROSCH]

In Abbildung 4 wird dargestellt, wie sich die Verantwortung für Informationssicherheit zusammensetzt.
Der IT-Grundschutz deckt durch einer Kombination von Methodik und Maßnahmen nicht nur die technischen Empfehlungen ab, sondern ermöglicht auch eine schnelle Soll-Ist-Analyse. [BSI-GS-BROSCH]

Abbildung 5: Leitfaden Informationssicherheit [BSI-GS-BROSCH]

Der IT-Grundschutz wird in zwei Teile unterteilt.
Auf der einen Seite sind das die BSI-Standards und auf der anderen Seite die IT-Grundschutz-Kataloge, welche im Kapitel 3 behandelt werden. [BSI-GS-BROSCH]

2.3.1 BSI-Standards

Aktuell gibt es vier BSI-Standards zur Informationssicherheit.

2.3.1.1 BSI-Standard 100-1 „Managementsysteme für Informationssicherheit“

In diesem Standard werden die allgemeinen Anforderungen an das Management für Informationssicherheit (ISMS) definiert. Die Vorgaben sind inhaltlich kompatibel zum internationalen Standard ISO 27001. Somit ist auch ein internationaler Austausch möglich. [GS-STANDARD]

2.3.1.2 BSI-Standard 100-2 „IT-Grundschutz-Vorgehensweise“

Hier wird Schritt für Schritt beschrieben, wie man ein Managementsystem für Informationssicherheit aufbaut und in weiterer Folge auch betreibt. Wichtige Themen wie, Sicherheitsmanagement und Aufbau von Organisationsstrukturen werden in diesem Standard vorrangig behandelt. [GS-STANDARD]

2.3.1.3 BSI-Standard 100-3 „Risikoanalyse auf der Basis von IT-Grundschutz“

Im BSI-Standard 100-3 wird eine Methodik für eine Risikoanalyse vorgestellt, die angewendet werden kann, wenn ein Unternehmen nach IT-Grundschutz arbeitet. [GS-STANDARD]

2.3.1.4 BSI-Standard 100-4 „Notfallmanagement“

In diesem Standard wird beschrieben wie ein Notfallmanagementsystem aufgebaut wird. Desweiteren wird erklärt, wie die dahinterstehenden Schnittstellen gestaltet sind und zusammenhängend betrieben werden können. [GS-STANDARD]

3 IT-Grundschutz Kataloge

Die IT-Grundschutz-Kataloge [GS-KATALOGE] können in unterschiedliche Bereiche unterteilt werden, welche hier kurz zum besseren Verständnis dargestellt sind. Zur Einleitung wird die Vorgehensweise und Handhabung bei der Erstellung eines Sicherheitskonzeptes nach IT-Grundschutz erklärt.
Die Planung oder Erstellung, welche notwendig ist um einen Informationssicherheitsprozess aufzubauen, wird als Informationssicherheitsmanagement bezeichnet.
Die Praxis zeigt uns, dass es ohne ein funktionierendes Informationssicherheitsmanagement nicht möglich ist, ein entsprechendes Sicherheitsniveau zu erreichen.
Die IT-Grundschutzkataloge gemäß [GS-KATALOGE] umfassen die Bausteinkataloge, Gefährdungskataloge und abschließend die Maßnahmenkataloge. Eine große Sammlung von Information ist auf der Internetplattform des Bundesamts für Sicherheit in der Informationstechnik (BSI) zu finden. Zusätzlich findet man dort noch eine große Anzahl von Hilfsmittel zur Implementierung des IT-Grundschutzes.

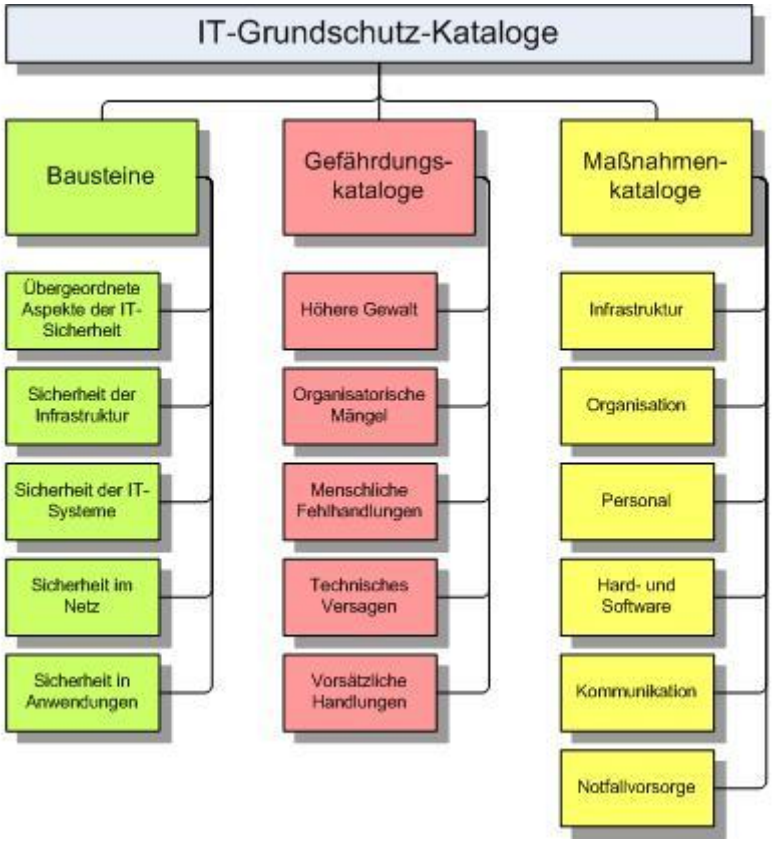

Abbildung 6: Aufbau BSI Grundschutzkataloge [GS-WIKI2015]

3.1 Bausteinkatalog

Der Bausteinkatalog nach [GS-KATALOGE] ist ein zentrales Element und folgt, wie auch die anderen Kataloge, einem Schichtenmodell. Der Bausteinkatalog wird wie in [GS-WIKI2015] dargestellt, in fünf Schichten unterteilt. Diese fünf Schichten beschreiben die übergreifenden Aspekte, Infrastruktur, IT-Systeme, Netze und IT-Anwendungen.

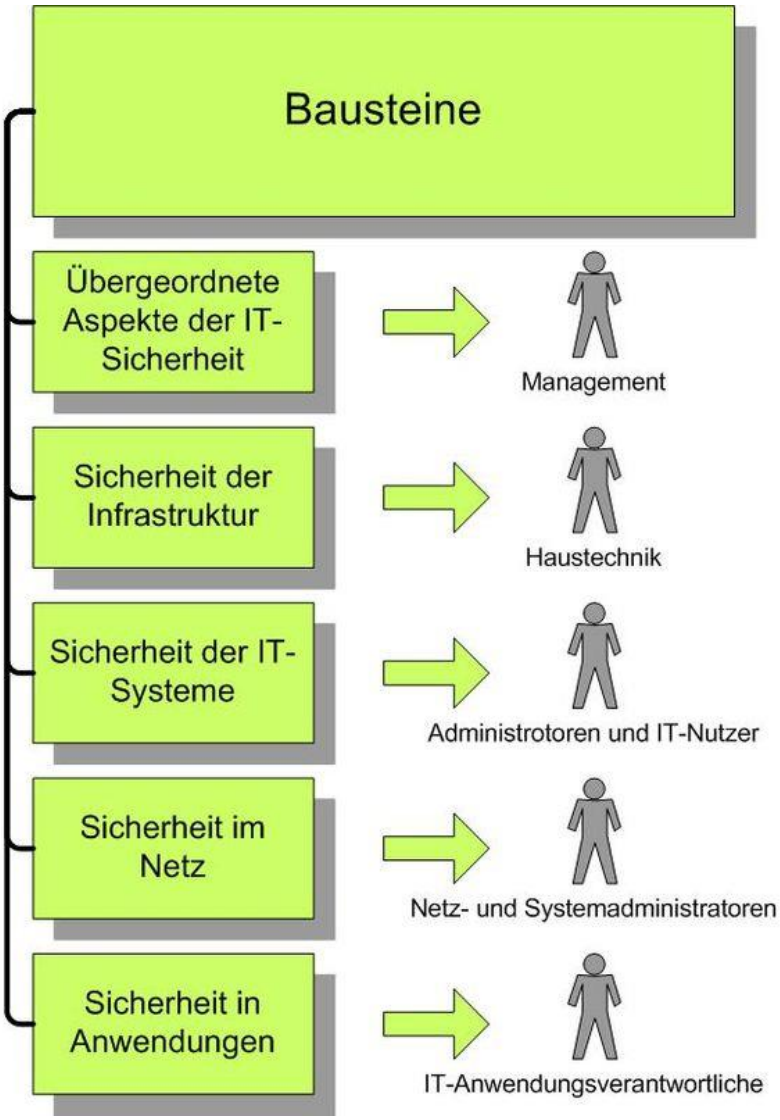

Abbildung 7: Bausteinzuordnung BSI Grundschutzkataloge [GS-WIKI2015]

Die schichtübergeordnete Aspekte beschäftigen sich mit organisatorischen Fragen betreffend Management, Personal und Outsourcing. In der zweiten Schicht wird der Schwerpunkt auf die baulichen Aspekte gelegt. In der Schicht der IT-Systeme werden Themen wie beispielsweise Clients, Server sowie Telefonanlagen behandelt. In der vierten Schicht werden Netzwerke genauer unter die Lupe genommen. In der letzten Schicht der Anwendungen befasst

man sich mit den Fragen der Sicherheit im Bereich der Software, wie zum Beispiel der einer E-Mail oder eines Webservers.
Durch die klare Aufteilung der einzelnen Schichten lassen sich die dazugehörigen Personengruppen einfach eingrenzen.

3.1.1 Übergeordnete Aspekte

Zu den übergeordneten Aspekten gehört in erster Linie das Sicherheitsmanagement. Eine sichere Verarbeitung von Informationen ist nahezu für alle Unternehmen von sehr hoher Bedeutung. Informationen können nicht nur in Köpfen, auf Computern und auf Papier gespeichert sein, sondern es muss auch durch gut organisiertes und geplantes Vorgehen aller Beteiligten ein angemessenes Sicherheitsniveau garantiert sein. Für das Erreichen einer erfolgreichen Sicherheitsmaßnahme ist es wichtig, dass die Umsetzung systematisch erfolgt. In der Literatur wird der Begriff IT-Sicherheit noch sehr oft gebraucht, wobei der Begriff Informationssicherheit viel aussagekräftiger wäre. In Publikationen sowie auch in den [GS-KATALOGE] wird ebenfalls noch vermehrt der Begriff IT-Sicherheit verwendet. Ein funktionierendes Sicherheitsmanagement muss in jeder einzelnen Firma auf deren Struktur angepasst werden.

In der Organisation werden die übergreifenden Maßnahmen dargestellt. Wichtig hierbei ist es, durch organisatorische Maßnahmen ein entsprechendes Sicherheitsniveau zu erreichen.
Der Bereich Personalwesen umfasst IT-Grundschutzmaßnahmen in Bereichen wie beispielsweise der Einstellung von Mitarbeitern, oder deren Weiterbildungen in internen und externen Schulungen. Ein besonderes Augenmerk wird hierbei auch auf den Umgang mit Besuchern oder Wartungstechnikern gelegt.

In Unternehmen ist es unerlässlich ein funktionierendes Datensicherungskonzept zu haben. Durch ein versehentliches oder bewusst herbeigeführtes Löschen können gespeicherte Daten schnell unbrauchbar gemacht werden oder sogar gänzlich verloren gehen. Eine Datensicherung soll gewährleisten, dass durch einen redundanten Datenbestand der Datenbetrieb wiederaufgenommen werden kann.

Die Aufgabe des Datenschutzes ist es, dass mit der Preisgabe jedes einzelnen mit seinen personenbezogenen Daten keiner in seinem Recht beeinträchtigt wird. In [GS-KATALOGE] gibt es eine sehr enge Verflechtung zwischen Datenschutz und Informationssicherheit. Daher werden in diesem Katalog nur die Rahmenbedingungen für den Datenschutz aufbereitet. Im Katalog für IT-Grundschutz hingegen wird die Informationssicherheit bearbeitet.

Jedes Unternehmen sollte vorbeugende Maßnahmen gegen Schadprogramme erstellen. Unter dem Begriff Schadprogramme, versteht man im Allgemeinen die klassischen Computer-Viren oder auch trojanische Pferde und Computer-Würmer. Um das Eindringen von Schadprogrammen zu verhindern sollte man ein geeignetes Sicherheitskonzept entwickeln. Auch nachdem so ein Sicherheitskonzept erstellt wurde, kann man leider nicht über einen hundertprozentigen Schutz verfügen. Ein wichtiger Grundsatz ist die konsequente Anwendung von Maßnahmen zur ständigen Aktualisierung der eingesetzten technischen Aspekte. Durch die ständige Weiterentwicklung von Betriebssystemen und Anwenderprogrammen entstehen regemäßig neue Angriffspunkte für Schadprogramme, wodurch auch rechtzeitig geeignete Gegenmaßnahmen gesetzt werden müssen.

Um den notwendigen Sicherheitsgrad in der IT-Organisation zu gewährleisten genügt es nicht nur die IT-Komponenten zu sichern, sondern ist es auch erforderlich, alle Abläufe und Vorgänge zu eruieren, zu pflegen, abzuschließen und zu befolgen. In diesem Baustein wird hauptsächlich auf das Hard- und Software-Management geachtet, um einen ordnungsgemäßen IT-Betrieb sicher zu stellen.

Unter Standardsoftware versteht man im Allgemeinen eine Software die über den Fachhandel gekauft werden kann. Diese Software zeichnet sich dadurch aus, dass sie einfach von jedem einzelnen Anwender selbst installiert werden kann.

Das Thema Outsourcing ist ein bekanntes und beliebtes Thema um Arbeits- und Geschäftsprozesse an externen Dienstleistern auszulagern. Das Outsourcing kann sowohl Hard- als auch Software betreffen. Typische Beispiele hierzu sind der Betrieb eines Rechenzentrums, einer Applikation oder einer Webseite. Im Applikationsbereich spricht man oft von Application Service Provider (ASP), das ist ein Dienstleister, der auf seinen eigenen Systemen einzelne Anwendungen für seine Kunden betreibt. Ein Beispiel hierfür sind E-Mail, Webshops, Archivierung oder SAP-Anwendungen. Bei diesem Betrieb sind Auftraggeber und Dienstleister über das Internet mit einem VPN miteinander verbunden.
Die Gründe für Outsourcing sind sehr vielfältig. Ein Unternehmen kann sich mit Hilfe von Outsourcing auf sein eigentliches Kerngeschäft konzentrieren und somit seine Kernkompetenzen stärker aufbauen.
Ein Risiko entsteht hierbei bei der engen Verbindung zwischen Auftraggeber und Dienstleister, da für den Auftraggeber das Sicherheitsrisiko entsteht, dass Daten gewollt oder ungewollt nach außen preisgegeben werden. Der Schwerpunkt in diesem Katalog ist, dass es Maßnahmen und Kontrollen gibt, welche die vereinbarten Ziele, Leistungen und Sicherheitsmaßnahmen sicherstellen.

Ein essentieller Part ist die Archivierung. Als Archivierung bezeichnet man die dauerhafte und unveränderbare Speicherung von Daten. Die Archivierung ist auch ein Teil des Dokumentenmanagement-Prozesses. Es wird erwartet, dass die Dokumente bis zum Ablauf einer vorgegeben Frist verfügbar sein müssen. Es kann in gewissen Fällen auch vorkommen, dass Dokumente auch zeitlich unbegrenzt verfügbar sein sollen.
Die technische Darstellung eines solchen Prozesses erfolgt über ein Dokumentenmanagement- und Archivierungssystem. [GS-KATALOGE]

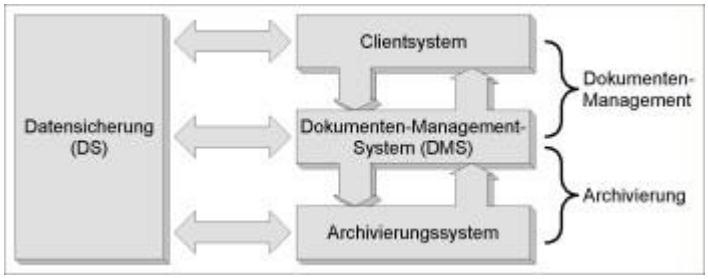

Abbildung 8: Technische Ausgestaltung über Dokumentenmanagement und Archivierungssysteme [GS-KATALOGE]

Die Reichweite eines Archivierungssystems reicht von einem kleinen Archivsystem mit einer Festplatte bis hin zu komplexen Archivsystemen mit RAID-Systemen oder der Anbindung an ein Storage Area Networks (SAN) für das zentrale Speichern von Daten.
Es ist wichtig die Abgrenzung zwischen Archive und Datensicherung zu finden. Die Datensicherung beinhalten nur die Kopien von System und Nutzdaten. Die Daten werden vom IT-System physikalisch getrennt und gefahrengeschützt gelagert. Archive hingegen sind ständig in den IT-Systembetrieb eingebunden damit die Daten jederzeit abgerufen werden können.
In diesem Baustein soll gezeigt werden, wie ein Unternehmen ein Konzept für die elektronische Archivierung erstellen kann. Ein Unternehmen sollte diese Art der langfristigen Aufbewahrung nur dann wählen, wenn diese Daten wirklich relevant sind, da der Aufbau eines elektronischen Archivierungssystems sehr kosten- und ressourcenintensiv ist.

3.1.2 Infrastruktur

Die Infrastruktur beginnt mit einem Gebäudekomplex. In diesem Gebäude befinden sich die einzelnen Arbeitsplätze. Bei einem Gebäude muss eine optimale Umgebung für Menschen sichergestellt sein, die in diesem arbeiten. Unberechtigte sollen dort keinen Zutritt haben, wo diese die Sicherheit beeinträchtigen können, damit auch die Technik effizient und sicher betrieben werden kann.

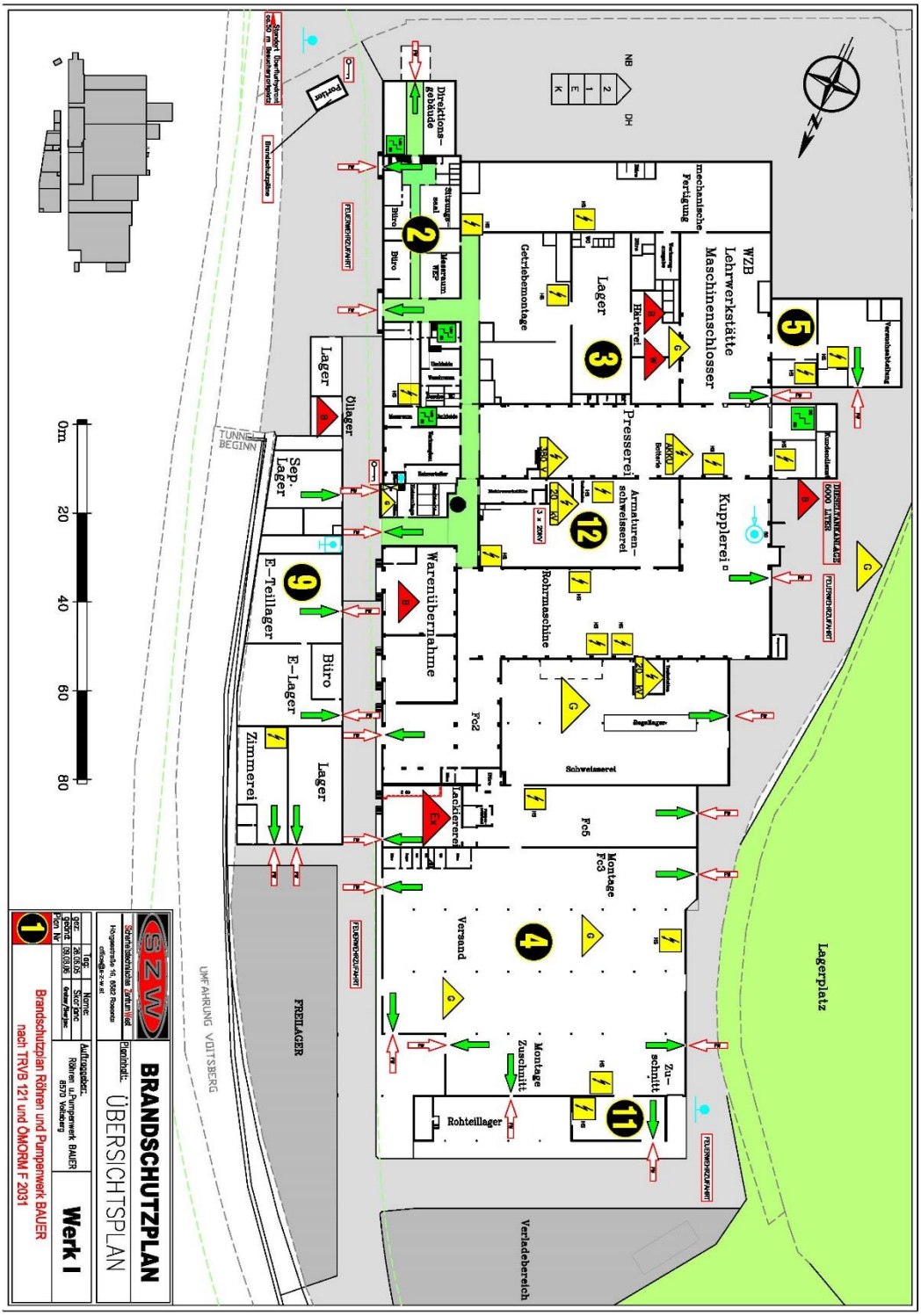

Abbildung 9: Gebäudeplan der Firma Bauer GmbH aus dem Jahr 2009

Die Verkabelung von IT-Systemen beginnt beim Einspeisepunkt des Verteilernetzes und geht bis hin zum Verbraucher wie Computer oder Monitor. Hierbei ist nicht zu vergessen, dass die Verkabelung im Gebäude und Verteilerpunkte im Haus miteingeschlossen werden. Die ordnungsgemäße und normgerechte Ausführung der Verkabelung ist die Grundlage für einen sicheren IT-Betrieb.

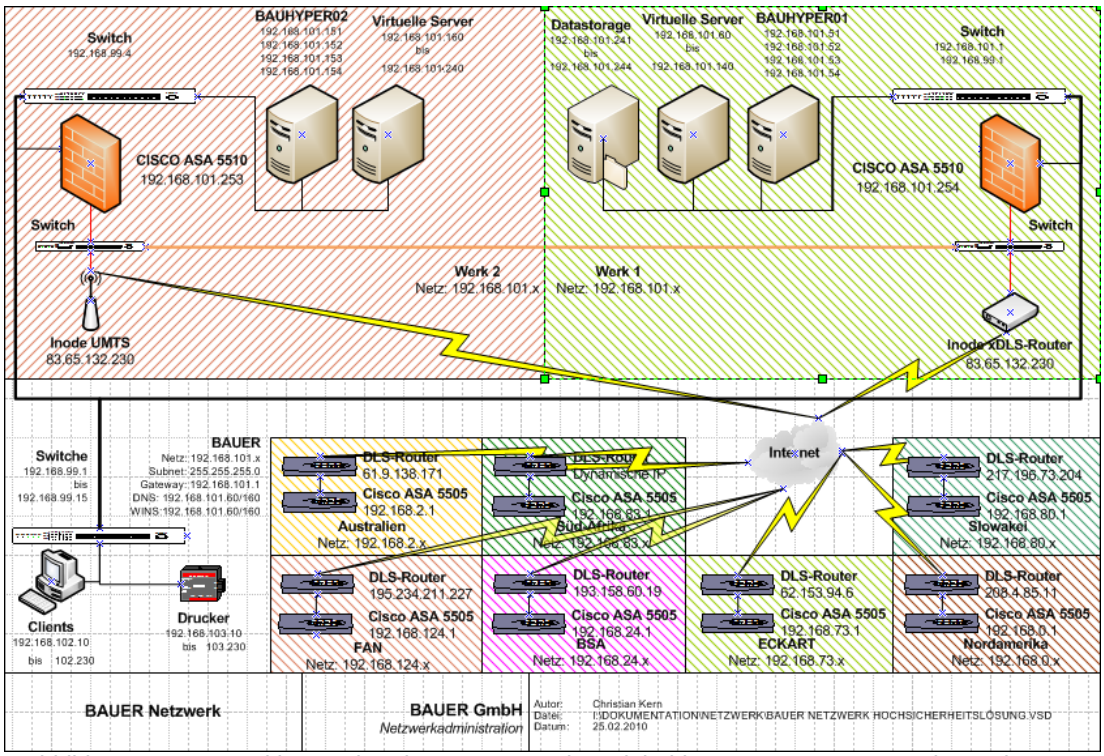

Abbildung 10: Netzwerklayout der Firma Bauer GmbH mit beiden Serverräumen aus dem Jahr 2010

Ein Arbeitsplatz oder Büroraum ist in einem Unternehmen ein Bereich, wo sich mehrere Mitarbeiter aufhalten können um ihre Arbeit zu erledigen. Die Tätigkeiten der Mitarbeiter in einem Unternehmen können sich auf ganze IT- oder nur teilweise IT-unterstützte Tätigkeiten beziehen. In einem Unternehmen kann es aus sicherheitstechnischen Gründen sein, dass Zugangs- oder Brandschutzkontrollen vorausgesetzt sind. [GS-KATALOGE]

Der Serverraum beherbergt in erster Instanz vor allem Server, Netzwerkkomponenten oder Datenspeicher. In einem Serverraum sind auch klimatechnische Hardwarekomponenten eingebunden. Ein Serverraum ist kein Raum in dem sich ständig Mitarbeiter aufhalten, sondern dieser Platz ist nur für Geräte bzw. dient Mitarbeitern als vorübergehender Arbeitsplatz bei Wartungsarbeiten. [GS-KATALOGE]

In den Bereich Infrastruktur fällt auch das Thema eines Datenträgerarchivs. Ein Datenträgerarchiv dient zur Lagerung von Datenträgern jeder Art. Der Bezug zum IT-Grundschutz wird in diesem Bereich nur die Auflagen des Brandschutzes gelegt. Dieser Baustein eignet sich nicht nur für die IT sondern auch für Papier-, Film-, oder sonstige Akten.

In Räumen für die technische Infrastruktur sind in der Regel Geräte untergebracht, die nur selten von Personal bedient werden müssen. Hierbei handelt es sich meistens um Verteilerpunkte oder Verteilerschränke. Denkbar ist auch, dass diese Punkte mittels unterbrechungsfreier Stromversorgung kurz USV angebunden sind.

Als nächstes in diesem Zusammenhang werden die Schutzschränke genannt. Diese Schutzschränke dienen zur Aufbewahrung von Datenträgern oder zur Unterbringung von informationstechnischen Geräten („Serverschrank“). In größeren Rechenzentren sollten Server die von mehreren Administratoren zugänglich sind, getrennt aufgestellt werden, damit die Schutzwirkung erhöht wird.
Bei einem Homeoffice-Arbeitsplatz, bei freien oder selbstständigen Mitarbeitern, wird ein Arbeitsplatz außerhalb des Unternehmens genutzt. Hierbei muss eine Trennung zwischen beruflicher und privater Sphäre ermöglicht werden. Die Sicherheit an einem häuslichen Arbeitsplatz ist nicht so ausgeprägt wie in einem Unternehmen, da in privaten Räumlichkeiten auch Besucher und Familienangehörige Zutritt haben. In dem Baustein werden die typischen Gefährdungen und Maßnahmen für einen häuslichen Arbeitsplatz dargestellt.

Die IT-Anwender werden immer mobiler und können auf Grund der immer stärker werdenden Geräte, immer mehr von unterwegs arbeiten. In diesem Fall ist es notwendig, dass die Sicherheitssituation einem Büroarbeitsplatz angepasst wird.

Das Hauptaugenmerk liegt bei der Infrastruktur natürlich im Bereich Rechenzentrum. In den meisten Unternehmen werden die strategischen und operativen Aufgaben von der Informationstechnik (IT) unterstützt oder sind ohne IT gar nicht auszuführen. Die IT-Systeme eines Unternehmens und deren Anbindung an das externe Netzwerk müssen in einer entsprechenden Umgebung betrieben werden.
Als Rechenzentrum bezeichnet man die komplexen IT-Infrastrukturen (Server- und Speichersysteme, Datensicherungssysteme, aktive Netzwerkkomponenten, Drucksysteme usw.). Zusätzlich kommen hier noch die erforderlichen Einrichtungen hinzu (Klimatechnik und Stromversorgung). Ein Rechenzentrum sollte in zwei physisch getrennte Bereiche ausweisen. Der erste Bereich ist der organisatorische Bereich und den zweiten Teil bildet die Infrastruktur selbst. Ein Rechenzentrum sollte entweder ständig personell besetzt sein (Schichtdienst) oder über eine Rufbereitschaft (mit einer Fernadministrationsmöglichkeit) abgesichert sein. In dem Baustein des Rechenzentrums beschränken sich die Sicherheitsanforderungen zumeist auf zwei Serverräume. Der Aufbau richtet sich an Anwender, die ein Rechenzentrum betreiben oder im Zuge einer Revision überprüfen möchten. Das Ergebnis sollte den Anwendern zeigen, ob die Sicherheitsmaßnahmen ordnungsgemäß umgesetzt wurden. Im Bereich Outsourcing, kann diese Überprüfung auch dahingehend genutzt werden um festzustellen, ob die angebotenen Leistungen im Hinblick auf deren Sicherheitsniveau gegeben sind. [GS-KATALOGE]

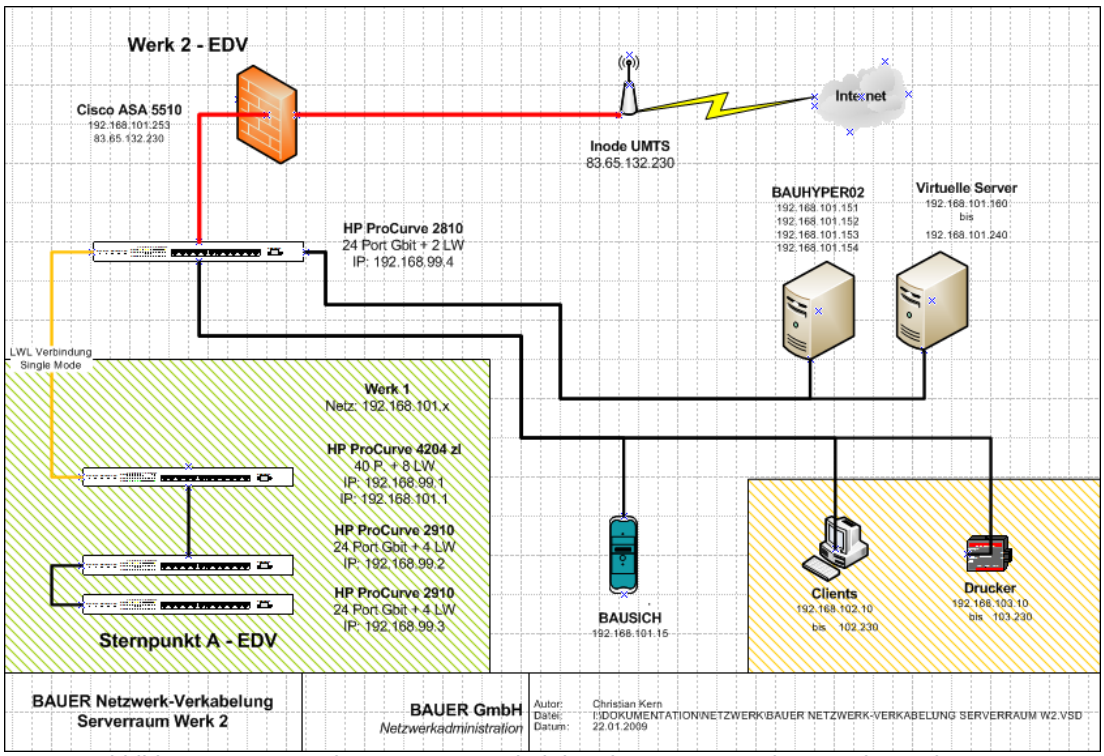

Abbildung 11: Layout des Serverraums bei der Firma Bauer GmbH aus dem Jahr 2009

Abschließend wird das Thema IT-Verkabelung behandelt. Die IT-Verkabelung nach [GS-KATALOGE] umfasst alle Kommunikationskabel und passiven Komponenten (Patchpanel oder Spleißverteiler). Die IT-Verkabelung beginnt beim Übergabepunkt aus einem Fremdnetz und endet im Unternehmen bei der LAN-Dose, an der ein PC angeschlossen wird. Die IT-Verkabelung ist auch ein Teil der technischen Infrastruktur in Gebäuden und zählt daher zur strukturierten Verkabelung. Diese wird unterteilt in Primär-, Sekundär- und Tertiärbereich.

Zum Primärbereich gehören die Kabelführungen, die Gebäude oder auch größerer Entfernungen mit wenigen Anschlusspunkten miteinander verbinden. Als Sekundärbereich bezeichnet man den Bereich der Verkabelung zwischen dem Gebäudeverteiler und Verteilern von Etagen oder einzelnen Gebäudebereichen.

Die Tertiärverkabelung ist die Anbindung der Endgeräte zu den zentralen Verteilerpunkten in den Etagen oder Gebäudebereichen. [GS-KATALOGE]

3.1.3 IT-Systeme

In dem Bereich der IT-Systeme fallen vor allem die Server eines Unternehmens mit ihren Diensten (Services). Diese werden wie schon im Punkt 3.1.2. Infrastruktur beschrieben, in den entsprechenden Räumen untergebracht. Nach [GS-KATALOGE] betrachtet man im Baustein Katalog unabhängig vom eingesetzten Betriebssystem die Sicherheitsaspekte nach dem IT-Grundschutz.

Bei der Erstellung von Hardwaredokumentationen müssen die Serversysteme in einem Unternehmen genau untersucht werden. In einem einfachen Beispiel wird gezeigt, wie so eine Liste aussehen könnte.

	Hardwareinformation								
Server	CPU	Arbeitsspeicher	Festplattenpartitionen	Festplattengesamtgröße	IP-Adresse	Subnetzmaske	Gateway	DNS Server 1	DNS Server 2
BAUSRV01	1	2048 MB	3 - C, D, V	500 GB	192.168.101.11	255.255.255.0	192.168.101.1	192.168.101.5	192.168.101.3
BAUSRV02	1	4096 MB	5 - C, D, S, T, V	500 GB	192.168.101.12	255.255.255.0	192.168.101.1	192.168.101.5	192.168.101.3
BAUAD01	1	1024 MB	3 - C, D, V	80 GB	192.168.101.5	255.255.255.0	192.168.101.1	192.168.101.5	192.168.101.3
BAUMAIL01	2	8192 MB	3 - C, D, V	400 GB	192.168.101.3	255.255.255.0	192.168.101.1	192.168.101.5	192.168.101.3
BAUMRSFAX	1	1024 MB	1 - C	80 GB	192.168.101.21	255.255.255.0	192.168.101.1	192.168.101.5	192.168.101.3
BAUSICH	1	1024 MB	2 - C, D	160 GB	192.168.101.15	255.255.255.0	192.168.101.1	192.168.101.5	192.168.101.3
BAUBACKUP	1	8192 MB	2 - C, D	1,5 TB	192.168.101.25	255.255.255.0	192.168.101.1	192.168.101.5	192.168.101.3
BAUBATCH	1	1536 MB	5 - C, D, S, T, V	320 GB	192.168.101.8	255.255.255.0	192.168.101.1	192.168.101.5	192.168.101.3
BAUWEB01	1	2048 MB	2 - C, D	80 GB	192.168.101.7	255.255.255.0	192.168.101.1	192.168.101.5	192.168.101.3
W2-Codekey	1	512 MB	2 - C, D	80 GB	192.168.101.20	255.255.255.0	192.168.101.1	192.168.101.5	192.168.101.3
ECKAD002	1	512 MB	2 - C, D	40 GB	192.168.101.28	255.255.255.0	192.168.101.1	192.168.101.5	192.168.101.3
AUSAD002	1	512 MB	2 - C, D	40 GB	192.168.101.29	255.255.255.0	192.168.101.1	192.168.101.5	192.168.101.3
DEMSAD002	1	512 MB	2 - C, D	40 GB	192.168.101.26	255.255.255.0	192.168.101.1	192.168.101.5	192.168.101.3
FANAD002	1	512 MB	2 - C, D	40 GB	192.168.101.27	255.255.255.0	192.168.101.1	192.168.101.5	192.168.101.3
BAUDIGSIG	1	1024 MB	3 - C, D, V	100 GB	192.168.101.13	255.255.255.0	192.168.101.1	192.168.101.5	192.168.101.3
SERVER1 (Zuschnitt)	1	2048 MB	1 - C	160 GB	192.168.101.30	255.255.255.0	192.168.101.1	192.168.101.5	192.168.101.3

Abbildung 12: Hardwareaufstellung der bestehen Server der Firma Bauer GmbH aus dem Jahr 2009

In dem nachfolgenden Beispiel wird aufgezeigt, wie eine einfache Serverliste mit deren Diensten aufgebaut werden kann.

	Server														
Dienste	BAUSRV01	BAUSRV02	BAUSRV03	BAUJAD01	BAUMAIL01	BAUMRSFAX	BAUSICH	BAUBACKUP	BAUBATCH	BAUWEB01	W2-Codekey	ECKAD002	DEMSAD002	FANAD002	AUSAD001
Activ Directory (Dom. Contoller)				x	x							x	x	x	x
Adobe Reader 6						x									
Adobe Reader 8			x						x						
Allways Sync Version 8.3.10		x													
Apache Tomcat 6.0										x					
ARCserve							x								
ARCserve Backup Agent for MS Exchange					x										
CVSNT										x					
cyberJack Base Components			x												
Logon Scripts				x	x							x	x	x	x
DHCP				x											
Dimension 4 v5.0	x	x		x	x	x				x	x				
DNS				x	x							x	x	x	x
GFI MailEssentials					x										
WINS				x								x	x	x	x
Mail (Exchange 2003)					x										
Datenserver	x										x				
Printserver	x														
Movex Server	x										x				
Streamserve 4.1.2	x														
Streamserve Tools 4.1.2	x														
Statistik		x													
Cognos		x							x						
DBASE		x							x						
Codekey Equalizer		x													
Codekey - Stempelkarte											x				
Trend Micro Client/Server Security Agent	x		x		x		x		x	x					
Trend Micro Console		x													
e-Quest		x													
Intranet										x					
Intrexx										x					
IPCheck Server Monitor				x											
IBM iSeries	x	x							x						
iOpus BEEE		x							x						
USV-Manager (LanSafe)	x	x		x	x	x	x								
Lizenzmanager SolidEdge (FlexIm)		x													
Personal 4.6.1			x												
Signaturserver f. digitale Signatur			x												
MS Data Access Components		x													
MS Exchange Administrator						x									
MS Exchange ActiveSync Administrator Tool					x										
MS Gruppenrichtlinien-Verwaltungskonsole					x										
MS Office Outlook 2003					x										
MS Office Professional 2003		x							x						
MS Report Viewer Redistributable 2005				x											
MS SQL Server 2000		x													
MS SQL Server Desktop Engine		x								x					
MS Windows Server Update Services 3.0				x											
MRSFAX						x									
VM-Ware								x							
Visual Basic		x													
WinCvs 2.0										x					

Abbildung 13: Serviceliste der bestehenden Server bei der Firma Bauer GmbH aus dem Jahr 2009

3.1.4 Netzwerk

Nach [GS-KATALOGE] dient ein Managementsystem für ein lokales Rechnernetz dazu jede Hard- und Softwarekomponente zentral zu verwalten. Dieses System unterstützt den Administrator in seiner täglichen Arbeit und hilft im Allgemeinen auch die Hardware zu überwachen.
Ein Managementsystem kann in zwei Kategorien unterteilt werden. Zum einen gibt es ein Systemmanagement welches sich in erster Linie mit dem Management der IT-Systeme befasst. Dieses System befasst sich auch mit der Softwareverwaltung, Verwaltung der Benutzer und dem Management der Anwendungen. Der andere Teil wird als Netzmanagement bezeichnet. Das Netzmanagement umfasst alle Aktivitäten zur Sicherstellung eines funktionierenden Netzwerkes.

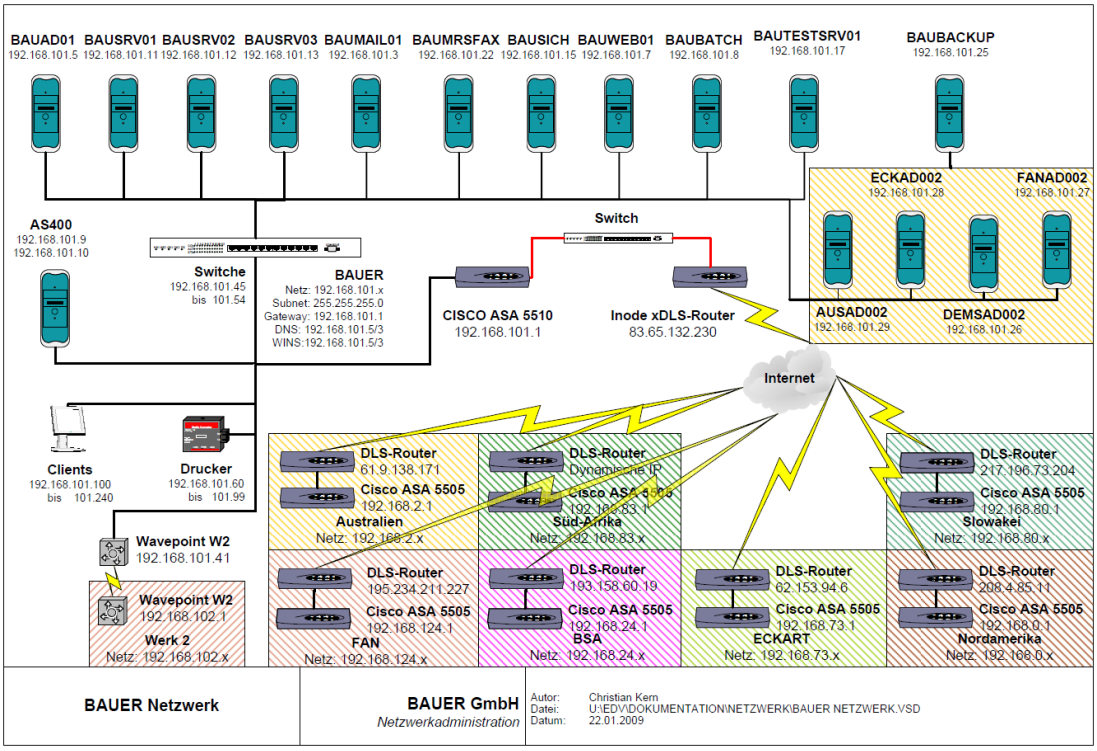

Abbildung 14: Netzwerklayout der Firma Bauer GmbH aus dem Jahr 2009

3.1.5 Anwendungen

Laut [APPL-WIKI2015] versteht man unter Anwendungssoftware alle Computerprogramme, die genutzt werden um systemtechnische Funktionalitäten zu bearbeiten. Diese Anwendungen beinhalten Textverarbeitungen, Tabellenkalkulationen, Bild- und Videobearbeitungen. In Unternehmen werden diese auch in bestimmten Bereichen wie Finanzbuchhaltung und Warenwirtschaftssystemen eingesetzt. Anwendungssoftware beinhaltet keine Betriebssysteme - diese werden als Systemsoftware bezeichnet. Eine Anwendungssoftware wird auf einem lokalen Arbeitsplatzrechner nach der Installation des Betriebssystems installiert.

BAUER FOR A GREEN WORLD — **Bauer-Softwareliste** — Bereich: EDV

Software	BH	IT	EK	E-Lager	KUB	E-Werk	GL	KALK	KONST	PM	PRD	PRDL	QM	QMNB	SEK	VK	VS	VW	WB	VK-NB
Adobe Acrobat Reader 9	X	X	X	X		X		X	X		X	X	X		X	X	X	X	X	
Adobe Flashplayer	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Adobe Photoshop										X									X	
Adobe Acrobat Pro 9					X		X			X				X						X
ACDsee Pro 2	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Auto CAD									X										X	X
Access	X	X					X													
Business Planner	X	X																		
CAexpress	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Cognos	X	X					X								X	X				X
Coral Draw										X									X	X
Dbase	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Easy Cleaner		X																		
E-Quest	X	X																		
Excel	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Fernwartung					X		X					X		X						X
FaxMapi	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Hardcopy	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Inode		X			X															X
iPass					X															X
Java Runtime	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Media Player 11	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Movex	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X			X
Lawson M3	X	X	X	X	X	X	X	X	X	X	X	X	X	X		X	X			X
Nero 9		X			X		X			X									X	X
Outlook	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
PDFCreator	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
pptViewer	X		X	X	X	X		X	X		X	X	X	X	X		X	X		
Powerpoint		X					X			X						X			X	X
Symphonie								X												
QM-Soft													X							
Windows Defender	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Solid Edge									X											
Stempelkarte	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Trend Micro	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
UltraVNC Viewer		X																		
UltraVNC Server	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
VPN Client		X			X		X			X										X
Word	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
Linestar					X		X			X										X
Centerstar					X		X			X										X
Rainstar					X		X			X										X
VLC Player	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X	X
CRM Outlook							X			X						X				X
CRM Offline client							X			X										X

Abbildung 15: Softwareliste der Firma Bauer GmbH aus dem Jahr 2010

3.2 Gefährdungskataloge

3.2.1 Höhere Gewalt

Im Kapitel Höhere Gewalt werden die Themen Personenausfall, Ausfall von IT-Systemen, Feuer und Ausfall eines Gebäudes behandelt.
Zum Thema Personalausfall ist zu sagen, dass auf Grund eines Ausfalls von Schlüsselfiguren für ein Unternehmen erheblich negative Folgen entstehen können. Personal kann auch durch längere Krankheit, Unfall oder Tod unvorhergesehen ausfallen. Planbare Ausfälle hingegen sind Urlaub, Fortbildung oder die reguläre Beendigung eines Dienstverhältnisses.
Obwohl nach diesen planbaren Ausfällen die Projekte koordiniert werden, kann es trotzdem vorkommen, dass Aufgaben auf Grund eines Ausfalles nicht mehr erledigt werden können. Dadurch können abhängige Prozesse zum Teil gestört oder sogar gar nicht erledigt werden.

Im Falle eines Ausfalls einer Komponente in einem IT-System kann es im Anschluss zu einem Ausfall des kompletten IT-Betriebs kommen und folglich zur Einschränkung wichtiger Unternehmensprozesse. Zu den Komponenten gehörten nicht nur IT-Komponenten, sondern es können auch Infrastrukturelemente wie beispielsweise eine defekte Klima- oder Stromversorgung sein. Für den Ausfall ist nicht nur immer technisches Versagen verantwortlich zu machen, sondern es kann auch menschliches Fehlverhalten dazu beitragen. Zum menschlichen Fehlverhalten gehört u.a. die fahrlässige Zerstörung eines Geräts oder von Daten, Diebstahl sowie Sabotage oder Manipulation.

Zur höheren Gewalt gehören auch Feuer oder Brände in einem Unternehmen. Ein Feuer kann nicht nur direkten Schaden an einem Gebäude oder an einer Infrastruktur anrichten, sondern es können auch Folgeschäden auftreten. Vor allem in der Informationstechnik können diese Folgeschäden ein katastrophales Ausmaß annehmen.
Brände entstehen nicht nur durch die fahrlässige Handhabung mit dem Feuer, sondern auch durch den unsachgemäßen Umgang mit elektrischen Geräten. Als klassisches Beispiel kann hier der unbeaufsichtigte Betrieb einer Kaffeemaschine oder die Überlastung einer Verteilersteckdose angegeben werden.

Ein Gebäude kann durch ein Feuer oder einen Großbrand teilweise oder vollständig unbenutzbar werden. Andere Gründe für den Ausfall eines Gebäudes können sein, dass ein Gebäude aufgrund eines Bombenfund gesperrt wird, oder einen Tunnelbau wodurch die unmittelbare Umgebung gesperrt wird.

3.2.2 Organisatorische Mängel

Die organisatorischen Mängel beschäftigen sich laut [GS-KATALOGE] mit Regelungen, Richtlinien und Dokumentationen.
Unzureichende oder auch fehlende Regelungen können durch ihre Defizite zu Schäden in Unternehmen führen. Durch eine mangelhafte Betriebsmittelverwaltung kann in einem Unternehmen der termingerechte Arbeitsablauf stark beeinträchtigt werden. Ein Beispiel hierfür kann sein, dass durch eine fehlende oder zu späte Druckpapierbestellung, Aufträge nicht oder verspätet fertiggestellt werden können.
Fehlende oder unzureichende Dokumentation der eingesetzten IT-Komponenten nach [GS-KATALOGE] kann für die Produktion eines Produktes eine erhebliche negative Auswirkung haben.
Diese negativen Auswirkungen können sich auch bei Bauarbeiten in und rund um ein Gebäude auswirken, wenn die Verkabelung fehlerhaft oder nicht dokumentiert ist. Es kann dabei sogar zu längeren Ausfallszeiten und unter Umständen sogar zu lebensbedrohlichen Gefahren wie einem Stromschlag kommen.

3.2.3 Technisches Versagen

Im Gefährdungskatalog G 4 nach [GS-KATALOG] gibt es mit Stand März 2015 89 Unterkategorien, die sich mit dem Thema Technisches Versagen beschäftigen.
Den Hauptgrund für technisches Versagen stellt eine mangelhafte Stromversorgung dar. Die E-Control Austria konnte im Berichtsjahr 2013 für Österreich eine leistungsbezogene Nichtverfügbarkeit von 50,18 min ermitteln. In dieser Berechnung nicht einbezogen sind die Ausfälle durch regional außergewöhnlichen Ereignisse. Werden diese Ausfälle und Werte auch berücksichtigt, kommt man auf einen Wert von 57,08 min. [ECONTROL-2014]

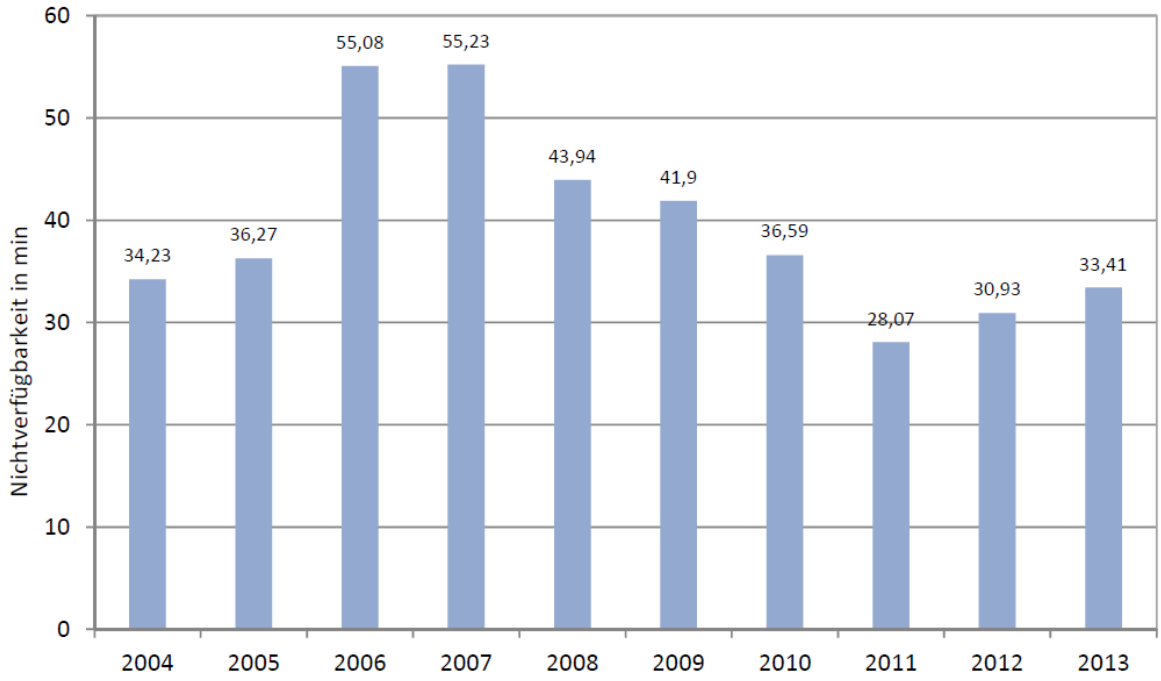

Abbildung 16: Jährliche ungeplante kundenbezogene Nichtverfügbarkeit der Stromversorgung in Österreich der letzten zehn Jahre [ECONTROL-201] Stand August 2014

3.2.4 Vorsätzliche Handlungen

Was sind vorsätzliche Handlungen ? Es sind nach [GS-KATALOGE] Handlungen wie Manipulation von Geräten, oder Manipulation an Informationen, Diebstahl, Vandalismus und der Zugriff von Viren, um nur einige zu nennen.
Manipulationen an Software oder Informationen können von Mitarbeitern eines Unternehmens sehr schnell und einfach durchgeführt werden. So kann ein Mitarbeiter die Kundendaten verfälschen oder auch kopieren und sie gegebenenfalls an ein Konkurrenzunternehmen verkaufen. Bei [GS-KATALOGE] können viele andere Beispiele nachgelesen werden.

3.3 Maßnahmenkataloge

Laut [GS-KATALOGE] gibt es sechs Maßnahmenkataloge. Nach Informationen von [MM-INET2015] enthalten die Maßnahmenkataloge eine umfangreiche Sammlung von Gefahren.

- M1 Maßnahmenkatalog Infrastruktur
- M2 Maßnahmenkatalog Organisation
- M3 Maßnahmenkatalog Personal
- M4 Maßnahmenkatalog Hardware und Software
- M5 Maßnahmenkatalog Kommunikation
- M6 Maßnahmenkatalog Notallvorsorge

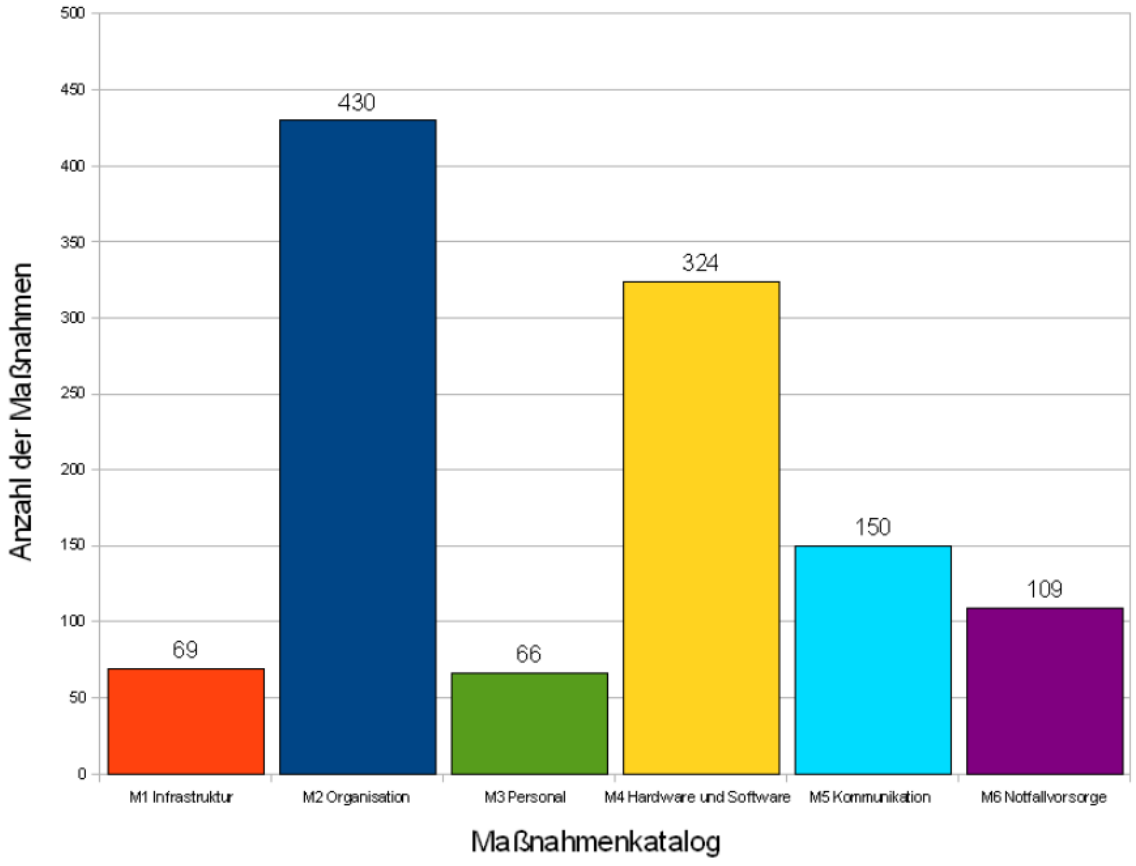

Abbildung 17: Zeigt den Maßnahmenkatalog von [MM-INET2015] aus dem Jahr 2008

Der Fassung der Maßnahmenkataloge von [MM-INET2015] aus dem Jahr 2008 wird entnommen, dass der Maßnahmenkatlog M 1 wichtige Hinweise beinhaltet wie die Infrastruktur in einem Unternehmen aussehen sollte. M 2 behandelt die Organisation worin die Zuständigkeiten in der IT-Abteilung und deren Umfeld besprochen wird. Dieser Katalog umfasst die meisten Unterpunkte und wird daher als einer der wichtigsten Maßnahmenkataloge geführt. Der Katalog M 3 erörtert wie mit dem Personal verfahren wird. Vertreterregelungen, Schulungen und die Einweisung der Mitarbeiter in die IT wird hier behandelt. Im Maßnahmenkatalog M 4, welches der zweitgrößte Katalog ist, werden die Hard- und Software Maßnahmen dargestellt. M 5 befasst sich mit der Kommunikation und umfasst nicht nur die Verbindungen zwischen den Computern und Servern, sondern auch die Kommunikation von Fax, E-Mail und Daten über das Internet. Im letzten Maßnahmenkatalog M 6 wird die Notfallvorsorge näher dargestellt, auf die im Kapitel 3.3.6 Notfallvorsorge näher eingegangen wird.

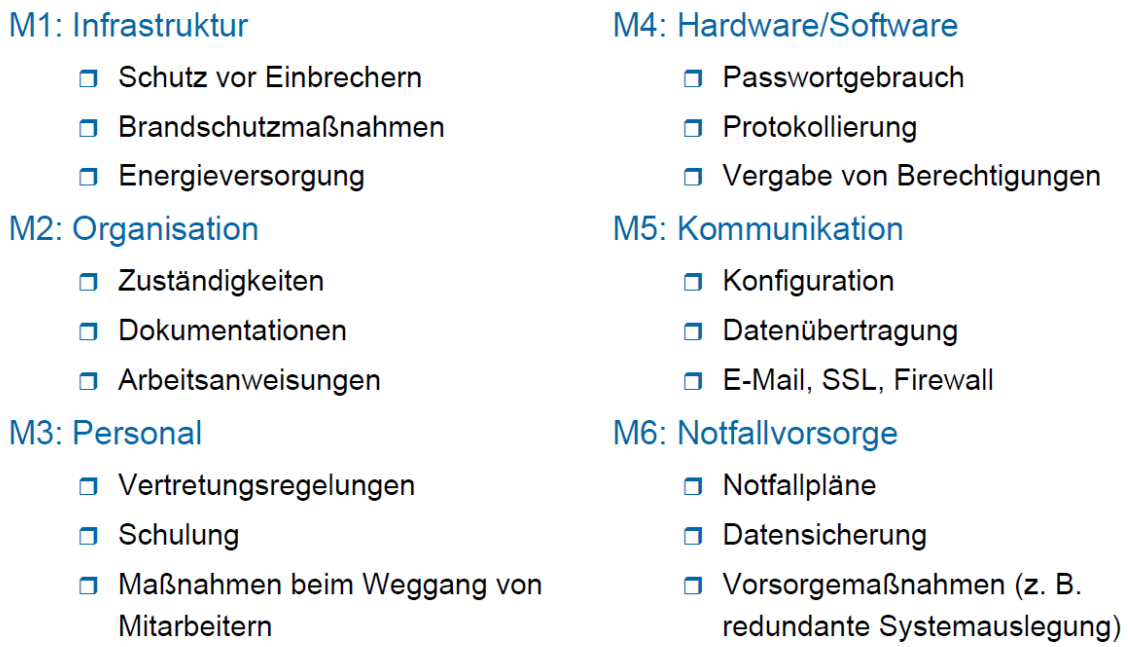

Abbildung 18: Typische Maßnahmen [IM-INET2015] von Seite 32

3.3.1 Infrastruktur

Im Maßnahmenkatalog für den Bereich der Infrastruktur gibt es laut [GS-KATALOGE] mit Stand März 2015, 80 Unterkategorien. Diese Unterkategorien beziehen sich nicht alle auf den Bereich der Informationstechnologie. Ein Teil der relevanten IT-Themen wird hier nun erörtert.
Um ein Rechenzentrum oder einen Serverraum betreiben zu können sind die beteiligten Personen angewiesen dieses mit den entsprechende Kabeltypen zu versorgen. Themen wie Überspannungsschutz, Not-Aus-Schalter bis hin zur Inbetriebnahme einer unterbrechungsfreien Stromversorgung müssen in Betracht gezogen werden. Ein Überspannungsschutz dient zur Absicherung und zum Schutz von IT-Geräten. Hierzu gibt es auch eine Norm DIN EN 62305 „Blitzschutz“, die seit Oktober 2006 gültig ist. Eine USV hat die Aufgabe, das IT-System oder einzelne IT-Geräte gegen kurzfristige Ausfälle zu schützen. Spannungsschwankungen können von einer entsprechenden USV ebenfalls abgefangen werden und somit den IT-Betrieb nicht stören. In Rechenzentren bietet sich auch an, dafür Sorge zu tragen, dass die Stromversorgung von zwei verschiedenen Energieversorgern oder zumindest von zwei verschiedenen Einspeisepunkten versorgt wird.
Bei der Wahl zur Aufstellung eines IT-Systems müssen verschiedene Voraussetzungen beachtet werden. IT-Systeme sollten so aufgestellt werden, dass nur befugtes Personal die Informationen einsehen kann und diese vor Manipulation und Diebstahl geschützt sind. Ein wesentlicher Punkt ist auch, dass das IT-System vor Umwelteinflüssen geschützt ist.
Um die Haltbarkeit der Server und Komponenten zu schützen und diese langfristig zuverlässig zu betreiben, ist die Klimatisierung der IT-Technik sicherzustellen. Wichtig hierbei ist, dass die Klimageräte in einem entsprechenden Intervall gewartet werden und bei einer Änderung der IT-Geräte die Kühlleistung angepasst wird.
Die IT-Geräte die eine seltene Bedienung durch IT-Personal benötigen, werden in den Serverräumen untergebracht. Um eine schleichende Gefahr einzudämmen ist es notwendig, dass es eine Fernanzeige von Störungen gibt. Hier kann über ein Überwachungsprogramm der Serverraum, die Hardware oder auch die Software überwacht werden. In Fehlersituationen können zuständige Personen alarmiert werden um Teil- oder Komplettausfälle zu vermeiden oder ihnen vorzubeugen.
Um die IT-Infrastruktur schützen zu können ist es natürlich notwendig, dass es in einem Unternehmen Brandschutzvorschriften gibt und diese auch eingehalten werden. In einem Unternehmen gibt es in der Regel einen Brandschutzbeauftragten, der für die Einhaltung der Vorschriften verantwortlich ist. Diese Person ist auch für die Absprache mit der Feuerwehr verantwortlich und sorgt für einen reibungslosen Gedankenaustausch. [GS-KATALOGE]

3.3.2 Organisation

Der Maßnahmenkatalog Organisation nach [GS-KATALOGE] beinhaltet mit dem Stand März 2015 515 Unterkategorien. Für die wesentlichen Aufgaben in einem Unternehmen müssen die Verantwortlichkeiten nachvollziehbar geregelt sein. Die sicherheitsrelevanten Aufgaben müssen zwischen den Mitarbeitern im Unternehmen und den Dienstleistern nachvollziehbar festgelegt sein. Die Bereiche die geregelt werden müssen sind:

- Zuweisung der Verantwortlichkeiten an Rollen und Organisationseinheiten
- Vertraulichkeit, Integrität und Verfügbarkeit müssen geschützt werden
- Einbeziehung des Sicherheitsbeauftragten bei Projekten
- Sicherheitsunterweisung der Firmendaten
- Festlegen der Verhaltensregeln und Informationspflichten

Für die Regelungen der Informationssicherheit in einem Unternehmen, müssen Datenschutzes und Geheimhaltung in geeigneter Weise zusammengeführt werden. Wichtig hierbei ist, dass die Regelungen einfach verstanden werden und widerspruchsfrei formuliert sind.

Andere organisatorische Themen sind laut [GS-KATALOGE] wie folgt:

- Datensicherung
- Datenarchivierung
- Datenträgertransport
- Datenübertragung
- Datenträgervernichtung
- Dokumentation von IT-Verfahren, Software und IT-Konfigurationen
- Zutritts-, Zugangs- und Zugriffsberechtigungen
- Wartungs- und Reparaturarbeiten
- Datenschutz
- Schutz gegen Schadsoftware
- Revision
- Notfallvorsorge
- Vorgehensweise bei der Verletzung von Sicherheitsrichtlinien

Die Regelungen müssen den Mitarbeitern in einem Unternehmen in einer geeigneten Weise kommuniziert und bekannt gegeben werden.
Diese Regelungen bedürfen einer regelmäßigen Überprüfungen und Aktualisierung, wobei der Vermerk eines Datums mit Versionsnummer zwingenderweise erforderlich ist.

3.3.3 Personal

Für den Maßnahmenkatalog Personal nach [GS-KATALOGE] gibt es mit Stand März 2015 90 Unterkategorien. Um Fehler in der IT vorzubeugen, sollte das IT-Personal entsprechend eingeschult werden. Weiterbildungen wie Kurse und Schulungen helfen die Sicherheitsrisiken zu reduzieren. Auf der Anwenderseite muss das IT-Personal die IT-Benutzer trainieren und diesen sollte eine entsprechende Richtlinie zur Verfügung gestellt werden, damit diese wissen wie sie mit dem Thema IT umgehen müssen. Diese Richtlinien sollten verbindlich, verständlich und vor allem aktuell sein.

3.3.4 Hardware und Software

Der Katalog M4 nach [GS-KATALOGE] Hardware und Software ist der zweit Größte Maßnahmenkatalog. Dieser Katalog umfasst mit Stand März 2015 435 Unterkategorien. Auf Grund der Tatsache, dass die Bearbeitung des Maßnahmenkataloges nicht für alle Unternehmen gleich angewendet werden kann, wird hier im ähnlichen Schema wie aus [MM-NET2015] verfahren.

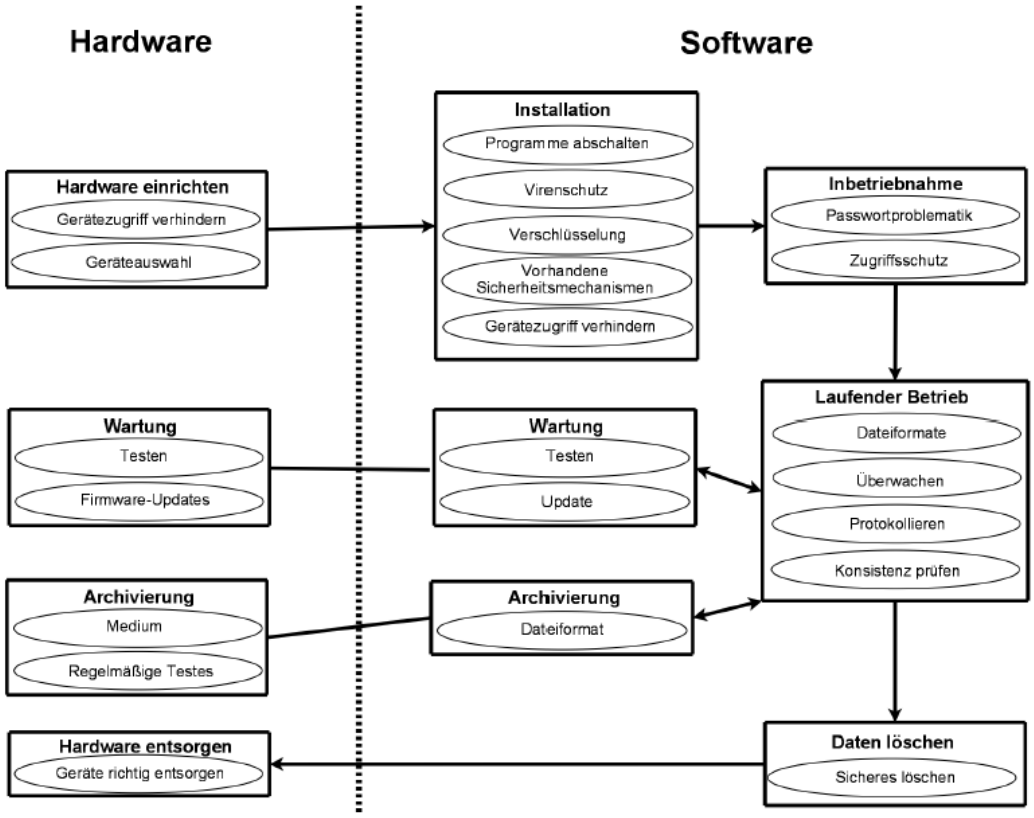

Abbildung 19: Einteilung von Hardware und Software nach [MM-INET2015] aus dem Jahr 2008

Die Abbildung 19 zeigt wie in Klein- und Mittelbetrieben der Maßnahmenkatalog Hard- und Software angewendet werden kann. In größeren Unternehmen sollte ein IT-Sicherheitsexperte die Planung der Maßnahmenvorsorge übernehmen, da die Gefahren komplizierter und weitreichender sind.

3.3.5 Kommunikation

Der Maßnahmenkatalog M 5 nach [GS-KATALOGE] umfasst laut Stand März 2015 173 Unterkategorien und behandelt alle Aufgaben und Anwendungen einer Kommunikation.
In der Informationstechnik ist es wichtig, dass Netzwerkpläne ordnungsgemäß dokumentiert werden und mit Datum und Versionsnummer gekennzeichnet sind.
In der Abbildung 20 ist ein Beispiel einer Netzwerk-Verkabelung ersichtlich, inklusive Datum und Versionsnummer. Diese Informationen können von Administrator zu Administrator oder zu anderen Personen weiter kommuniziert werden.

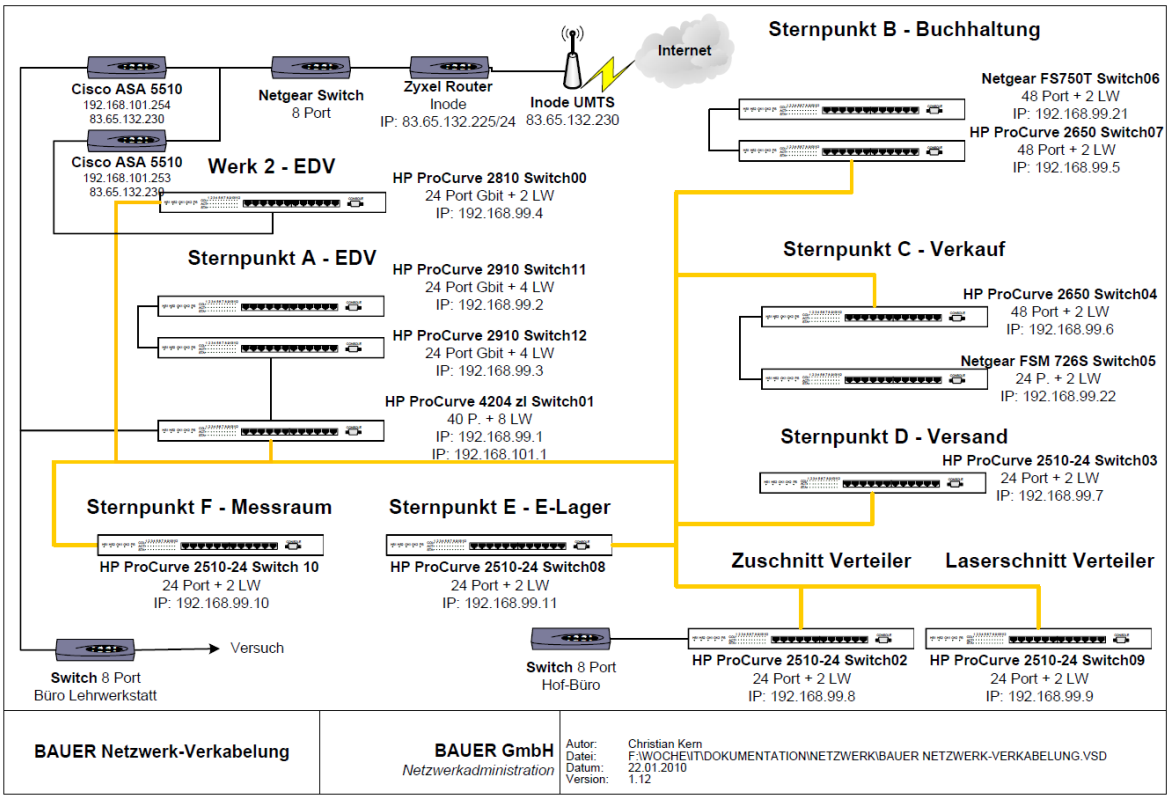

Abbildung 20: Netzwerkverkabelungsplan der Firma Bauer aus dem Jahr 2010

3.3.6 Notfallvorsorge

In den letzten Jahren hat sich die Rolle von IT-Systemen zunehmend von reinen arbeitsunterstützenden Werkzeugen zu Systemen gewandelt, die für die Generierung des Unternehmenserfolges entscheidend sind. Vielfach sind Unternehmen heutzutage nicht mehr in Lage die Produktion, Logistik und auch begleitende administrative Abteilungen auch nur kurzzeitig ohne Vorhandensein von IT-Systemen aufrechtzuerhalten.

Die Sicherstellung der Verfügbarkeit, und die Gewährleistung eines schnellen Anlaufes nach Systemfehlern oder externen Einflüssen (Katastrophen) zählen immer mehr zu den Hauptaufgaben der IT-Abteilungen.
Das vorliegende Dokument soll die unternehmenseigene IT-Abteilung bei der Umsetzung dieses Zieles unterstützen.
Im Detail sind die Zielsetzungen dieses Dokumentes die folgenden:

- Klare Definition der vorhandenen IT-Services.
- Gruppierung der Services nach Relevanz im Unternehmen.
- Finden und Erkennen von realistischen Katastrophenszenarien, die das Unternehmen treffen können.
- Allen im Katastrophenfall eingebundenen IT-Mitarbeitern klare Rollen und Aufgaben zuteilen.
- Erstellen von Aktionsplänen, die einen Wiederanlauf entsprechend der eingetretenen Katastrophe und der notwendigen Wiederherstellungszeiten ermöglichen.
- Eine Handlungsvorschrift für die involvierten Personen während der Krise und unmittelbar nach der Katastrophe zum Einsatz kommt.
- Alle notwendigen Wiederanlaufinformationen an einer Stelle griffbereit vorliegen zu haben.
- Alle benötigten externen Lieferanten und Partner einzubinden und von den von Ihnen erwarteten Leistungen zu unterrichten.
- Ein nach Außen sichtbares Dokument vorliegen zu haben, welches die unternehmerischen Bemühungen zur Vermeidung / Reduktion von Folgeschäden nach der Katastrophe transparent darstellt.

3.3.6.1 Allgemeines

Da es von der Natur eines Desasters aus schwer ist alle möglichen Gefahren zu erfassen und zu planen, ist es Intention dieser IT-Notfallplanung ein möglichst offenes und an die jeweilige Katastrophe adaptierbares Dokument zu erstellen.
Basis der Überlegungen ist ein IT-Service. Ein IT-Service ist eine für die IT, als zusammenhängende Funktion, begreifbare Applikation, die unabhängig von anderen Services wieder in Gang gebracht werden kann. Üblicherweise versteht man darunter ein (oder mehrere) Hardwaresysteme, eine Software, dazugehörige Konfigurationen und Daten der Benutzer.
Beispiele für Services sind:

- Personalsystem: Server + Applikation + Daten
- LAN: die aktiven Elemente des LANs sowie die Verbindung zu anderen Elementen (Services)
- Authentifizierung: ein oder mehrere Domaincontroller (HW + Basis OS + Konfiguration)

Aus der Sicht des Benutzers / der Unternehmung können einzelne Services in Prioritätsstufen zum Wiederanlauf eingeteilt werden. Diese sind:

- ROT: Unternehmenskritische Services – müssen unmittelbar nach der Katastrophe behandelt werden, für ausgefallene HW muss ein Work-Arround gefunden werden
- GELB: Wichtige Services – müssen unmittelbar nach Wiederinstandsetzung der ROT Services behandelt werden, es gibt aber einen innerbetrieblichen Work-Arround für die Initialphase des Wiederanlaufes. Ausgefallene HW kann über normale Vertriebswege angeschafft werden.
- GRÜN: alle anderen IT-Services

Zu beachten ist, dass auch Services in sich eine unterschiedliche Gewichtung erfahren können. Beispiel: Das ERP System der Unternehmung wurde als ROT identifiziert. Allerdings bearbeiten von den 30 Benutzern dieses Services nur 5 unmittelbar unternehmenskritische Funktionen im ERP. Dies bedeutet, dass neben dem Server des ERPs nur 5 Arbeitsplätze im ROT Bereich unmittelbar wiederhergestellt werden müssen.
Dies führt in unserer Betrachtung zur Einbindung der einzelnen Hardwarekomponenten. Über diese Matrix ist eine direkte Zuordnung zwischen Service und Hardware möglich. In den meisten Fällen (bei serverseitigen Services) ist eine eins zu eins Abbildung möglich.
Einzelne Services müssen allerdings untergliedert werden. Dies trifft Hauptsächlich den PC und LAN Bereich. So gibt es ein Service „PC-ROT“ und „LAN-ROT“ welches die Anzahl der unmittelbar benötigten Workstations und LAN Zugangspunkte beschreibt. „PC-GELB“, „PC-GRÜN“, „LAN-GELB“ und „LAN-GRÜN“ sind dementsprechend die Abbildungen für die weniger wichtigen Services.
Intention der IT-Notfallplanung ist es nun, nach einer Aufnahme des Zustandes der Unternehmung (welche Raumbereiche, Hardwarekomponenten und Services sind ausgefallen), dem Wiederanlaufteam eine Unterlage in die Hand zu geben, möglichst schnell gezielte Aktionen durchführen zu können. Dies setzt aber einen kreativen gesteuerten Prozess nach Eintritt des Desasters voraus.

3.3.6.2 Wie verwendet man die IT-Notfallplanung im Katastrophenfall

Nach der Erstalarmierung eines Wiederanlaufkoordinators durch eine im IT-Notfallplanung-Verteiler aufgenommene Person, erfolgt zuerst eine Bewertung der Katastrophe. Wird die Katastrophe als ernst genug eingestuft um die IT-Notfallplanung in Kraft zu setzen, erfolgt die Alarmierung des restlichen IT-Personals.
Nächster Schritt ist die Identifizierung der Schäden nach:

- noch vorhandenen Raumbereichen
- noch vorhandener HW
- noch vorhandenen Services

Dies erfolgt in der Hauptverfahrensanweisung Kapitel 5.10 Hauptverfahrensanweisung. In einer gemeinsamen Sitzung aller vorhandenen IT-Ressourcen erfolgt dann die Zuordnung der Wiederanlaufaktivitäten (ebenfalls in der Hauptverfahrensanweisung beschrieben). Zu diesem Zweck werden aus dem Dokument für alle nicht mehr funktionsfähigen Services die entsprechenden Serviceblätter entnommen und zugeordnet. Diese Blätter bilden auch die Dokumentation über den Wiederanlauf und werden vom Wiederanlaufkoordinator zur Statusabklärung benötigt.

Als Nebenprozess erfolgt die Hardwarebeschaffung – basierend auf der Definition für ROT Services für alle ausgefallenen ROT-Services. Im Anschluss daran die Kontaktaufnahme zu Lieferanten und Beschaffungseinleitung für alle ausgefallenen GELB und GRÜN-Services.
Nachdem jede Person (ihrer Rolle entsprechend) eine gereihte Folge an Services zugeteilt bekommen hat erfolgt die Wiederherstellung (Installation) des Services. Hat ein Mitarbeiter eine Aufgabe abgehandelt, so vermerkt er dies am entsprechenden Blatt und gibt das Blatt an die nächstgereihte Funktion weiter. Jeder Mitarbeiter hat so eine Folge von Serviceblättern, die gegenwärtig Aktionen von seiner Seite benötigen und kann entsprechend vorhandener HW und der in der Hauptverfahrensanweisung erfolgten Reihung selbständig Aktionen setzen.
Nach vollständiger Wiederherstellung eines Services wird das Serviceblatt dem Wiederanlaufkoordinator übergeben, der so einen vollständigen Überblick über den Zustand des Wiederanlaufes hat.

4 Übersicht des Projektes bei BAUER GmbH

4.1 Aufgabenstellung

Die Firma Bauer GmbH verfügt über eine Infrastruktur in Voitsberg ohne Notfallplanung. Das Unternehmen besitzt in der Firmenzentrale einen Serverraum, wo alle Dienste und Services des Konzerns weltweit verwaltet werden. Die Firma Bauer besitzt zwei, voneinander örtlich getrennte, Produktionsgebäude. Diese beiden Produktionswerke sind mit zwei ca. 800 m langen Rohren verbunden. Diese Rohre wurden in den 90er Jahren unterirdisch verlegt und dienten bis zum Jahr 2000 zur Wasserkühlung in den beiden Produktionswerken. Seit dem Abschalten der Wasserkühlung sind diese beiden Rohre frei und können für eine Verkabelung der beiden Gebäuden genutzt werden. Im Hauptproduktionswerk (Werk 1) befindet sich die Hauptzentrale der komplette IT Infrastruktur der BAUER Group. Im zweiten Produktionswerk (Werk 2) existiert derzeit keine intakte IT Infrastruktur. Die Verbindung zwischen beiden Werken wird derzeit mit zwei WLAN Accesspoints hergestellt. Aufgabe der Diplomarbeit ist es, eine neue Verbindung der beiden Werke zu schaffen, sowie eine intakte Infrastruktur für einen Backupserverraum um in weiterer Folge einen zweiten IT Standort aufzubauen.

4.2 Zielsetzung

Das Ziel der DA ist es unter Zuhilfenahme der der BSI Standards und des IT-Grundschutzes einen IT-Notfallplan für die Firma Bauer zu erarbeiten. Dieser Plan hilft dem Unternehmen, im Falle eines Desasters unternehmenskritische Services in einem möglichst kurzen Zeitraum wieder zur Verfügung zu stellen. Um dies zu erreichen wird auch ein neuer Backupserverraum geschaffen und in die Infrastruktur integriert. In diesem Backupserverraum soll zukünftig die komplette Sicherung durchgeführt werden. Weiters soll auch ein vollwertiger Server installiert werden, worauf alle wichtigen Dienste für die Aufrechterhaltung des Betriebes installiert werden sollen.
Um die Internetverbindung ständig aufrecht zu erhalten soll ein UMTS Modem mit Failover Schaltung des derzeitigen Internetproviders installiert werden. Für die VPN Verbindungen zu den weltweiten Töchterfirmen soll eine zweite Firewall mit Failover Schaltung installiert werden. Diese Maßnahmen werden alle nach den Vorgaben des IT-Grundschutzes erarbeitet.

4.3 Vorgehensweise

Um an das Projekt strukturiert heran zu gehen, wurde der Notfallmanagement-Prozess nach [BSI-STD100-4] herangezogen.

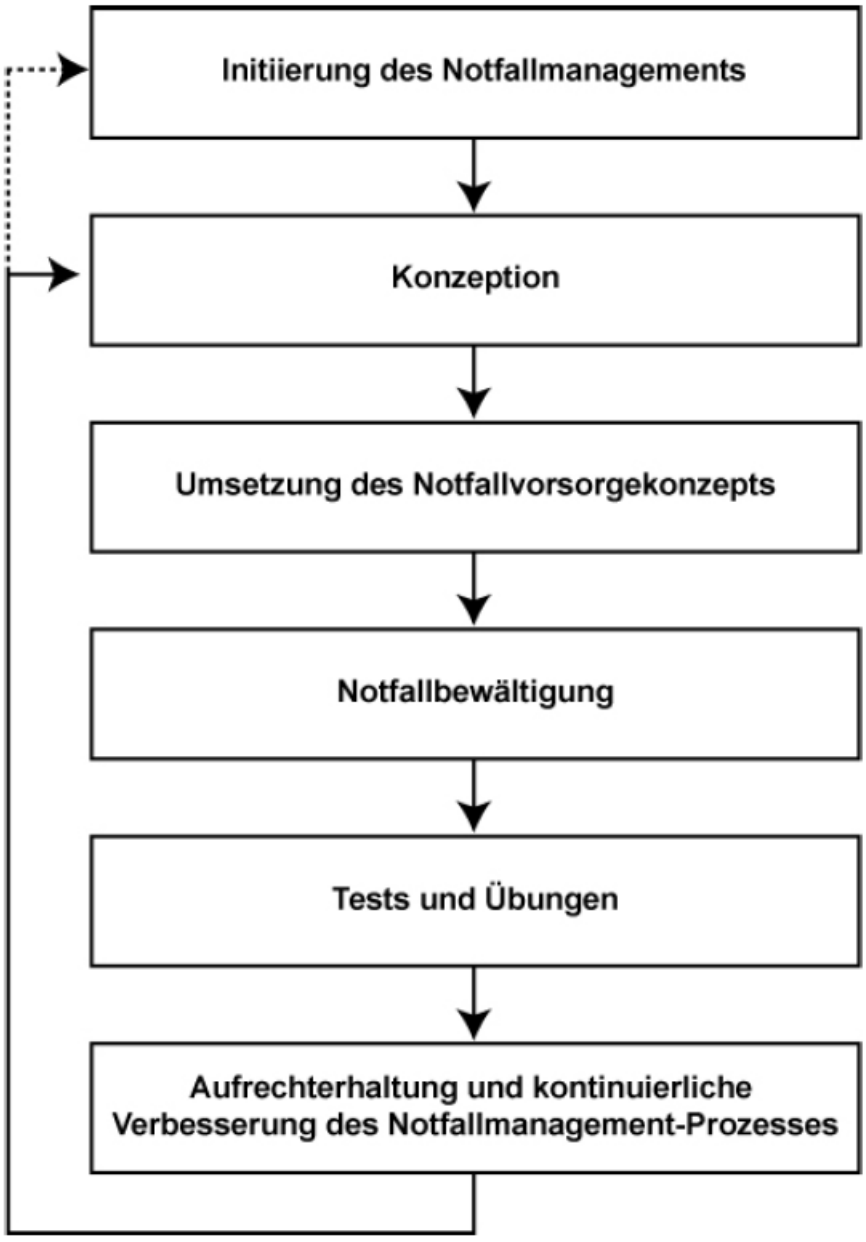

Abbildung 21: Notfallmanagementprozess nach [BSI-STD100-4]

4.3.1 *Initiierung des Notfallmanagements*

Das Ziel des Notfallmanagements ist es, dass Ausfallzeiten möglichst kurz gehalten werden. Ein nützlicher Nebeneffekt ist die Dokumentation und das bessere Verständnis der vorhandenen Prozesse. Hierzu mussten bei der Firma Bauer alle Services aufgenommen und in Abhängigkeiten gestellt werden.

4.3.2 *Konzeption*

Um einen Notfallplan erstellen zu können, muss zuerst eine Bestandsaufnahme der vorhandenen Services und Businessprozesse durchgeführt werden. Erst durch die Analyse dieser ist es möglich, Handlungsanweisungen für den Ernstfall zu definieren. Weiters müssen die Ziele des Notfallplans genau eingegrenzt und mit der Abteilungsleitung besprochen werden. Auch die Vergabe der Prioritäten der Services wird gemeinsam mit der Firmenleitung erarbeitet.

4.3.3 *Umsetzung des Notfallvorsorgekonzeptes*

Das Notfallvorsorgekonzept bildet die Grundlage, um in einem Unternehmen anhand einer einfachen Anleitung, organisiert ans Werk gehen zu können. Bei der Firma Bauer ist die IT-Notfallplanung ein Handbuch, in dem ein klar definierter Ablauf vorgegeben ist, wie in einem Ernstfall vorgegangen werden muss. Das Notfallmanagement muss regelmäßig das Konzept überprüfen und aktualisieren.

4.3.4 *Notfallbewältigung*

Für die Notfallbewältigung muss es eine Ablauforganisation geben, die darauf achtet, dass der Notfallplan eingehalten wird. Diese Organisation bestimmt die Maßnahmen welche ausgeführt werden müssen und verantwortet auch die Koordination von internen und externen Ansprechpersonen.

4.3.5 *Test und Übungen*

Für die Umsetzungen von Verbesserungsvorschläge werden in bestimmten Abständen bei der Firma Bauer Tests und Übungen mit den verantwortlichen Personen durchgeführt. Hierbei soll sichergestellt werden, ob Maßnahmen umgesetzt wurden oder noch umgesetzt werden müssen.

4.3.6 *Aufrechterhaltung und Verbesserung des Notfallmanagement-Prozesses*

Der Notfallkoordinator ist verantwortlich, dass der IT-Notfallplan ständig aktualisiert wird. Zusätzlich muss darauf geachtet werden, dass der Notfallmanagement-Prozess regelmäßig kontrolliert wird. Die Ergebnisse müssen zwecks Nachvollziehbarkeit vollständig dokumentiert werden.

4.4 Untersuchungsbereich

Der Untersuchungsbereich dieser Arbeit liegt darin, in einem Klein- und Mittelbetrieb eine Ist-Aufnahme aller Services zu machen. Die Betrachtung der finanziellen, administrativen und organisatorischen Abwicklung welche sich durch eine IT-Notfallplanung ergeben, soll Aufschluss geben, welcher Schaden entstehen kann, wenn kein Notfallmanagement vorhanden ist.

5 Prototypische Umsetzung einer Notfallplanung

5.1 Verankerung der IT-Notfallplanung im Unternehmen

Das Bewusstsein über die Notwendigkeit einer Vorsorge im Katastrophenfall ist im Management des Unternehmens verankert. Zu diesem Zweck wurde auch die IT beauftragt entsprechende Aktivitäten (im Speziellen die Erstellung dieses Planes) durchzuführen.
Innerhalb des Unternehmens sind einzelne IT-Bereiche noch nicht vollständig in diesem Plan eingebunden. Dazu gehörten spezielle Clientprogramme und einzelne prozessnahe Maschinen in der Fertigung. Im Zuge der Katastrophenvorsorge ist es aber geplant hier eine saubere Abgrenzung der Verantwortungen und gegebenenfalls die Übernahme der Services durchzuführen.

5.2 Definition einer Katastrophe und Festlegung der maximal zu erwartenden Katastrophe (aus IT-Sicht)

Als Katastrophe im Sinne dieser IT-Notfallplanung wird definiert:
Jeder durch einen „unvorhersehbaren“ äußeren Umstand (wie etwa Brand, Überflutung, Feuer, Stromausfall, oder Betriebsunfälle etc...) hervorgerufene Ausfall der primären Server und Kommunikationskomponenten.
Jeder gleichzeitige Ausfall mehrerer Server und Kommunikationskomponenten, der ein über das „normale“ Ausfallsbackup hinausgehendes Handeln erforderlich macht. (Ein Ausfall betrifft üblicherweise stets eine Komponente.)
Als maximale für den Standort zu erwartende Katastrophe wird durch die räumliche Verteilung der Totalausfall des gesamten Gebäudes angenommen.
Bei kleinräumigen Ausfällen (Brand im Serverraum) wird abhängig vom Vorhandensein der Kommunikationsanbindung und dem Vorhandensein von Strom der Wiederanlauf im Serverraum durchgeführt.
Auf großräumige Katastrophen (Erdbeben) bei denen auch der Ausfallsraum in Mitleidenschaft gezogen wird, wird in der IT-Notfallplanung nicht explizit eingegangen – der Wiederanlauf erfolgt jedoch nach denselben Schemata je nach Verfügbarkeit der Services
Als realistische Szenarios für den Katastrophen-Fall gelten: Feuer, Wassereinbruch in einzelnen Kellerräumen, Betriebsunfällen (Explosionen) die einen Teil des Gebäudes oder das ganze Gebäude unbetretbar machen.

5.3 Organisation der IT-Bereiche

Die im Unternehmen verwendeten IT-Gerätschaften werden von der zentralen IT administriert. Diese ist auch für IT-Aktivitäten in den Standorten zuständig. Die zentralen Services des Unternehmens der Firma Bauer GmbH werden auch weltweit in Voitsberg gehostet.
Dazu gehören:

- Movex als zentrales ERP
- Mail
- Authentifizierung (Root Domäne)
- Einzelne Datenbankapplikationen und Spezialapplikationen

Durch eine immer weiter fortschreitende Einbindung der IT in Produktionsprozesse (Stichwort Prozesstechnik) ist in Zukunft auch ein strukturierter Aufbau dieses Supports notwendig. Ebenfalls wird eine vollständige Einbettung einzelner, noch von den Fachabteilungen betreuten, Clientapplikationen geplant.

5.4 Generelle Backupstrategie, Lagerung der Software und Passwörter

5.4.1 *Backupstrategie*

Die Hauptsicherung im Datenbereich erfolgt über einen Backupserver (Arcserve) und daran angeschlossenen USB – Festplatten. Die AS-400 sichert über ein integriertes Bandlaufwerk auf eigene Bänder.
Im Datenbereich erfolgt die Sicherung innerhalb einer Woche als Zuwachssicherung immer auf die gleiche Festplatte. Am Ende der Woche wird eine Wochensicherung erstellt und im Safe abgelegt. Es werden 3 Generationen gesichert.
Im Bereich der AS400 wird das tägliche Band im Safe abgelegt und eine Woche gelagert. Am Ende der Woche wird eine Wochensicherung und am Ende des Monats eine Monatssicherung erstellt. Es gibt 4 Generationen der Wochensicherung und 12 Generationen der Monatssicherungen.
Der Backupserver und die dazugehörigen Platten befinden sich im Werk 2. Die jeweils letzte Wochensicherung wird im Safe in Werk 1 gelagert. Im AS400 Bereich wird die jeweils letzte Wochen- und Monatssicherung im Werk 2 gelagert. Sowohl Bänder als auch Platten werden wechselweise im Safe und im Werk 2 gelagert.
Durch diese physische Aufteilung der Bänder und Platten ist ein vollständiger Verlust aller Backup-Datenträger im Falle einer Katstrophe in einem der beiden Werke ausgeschlossen. Es steht weiterhin auch jede zweite Sicherung zur Verfügung.
Die Beschriftung der Bänder erfolgt über eine Dokumentation, die auch im Werk 2 in Voitsberg abgelegt wurden.
Die Beschriftung über Bänder der AS400 ist mit dem Wochentag beschriftet.

5.4.2 *Lagerung der Software*

Die Microsoft-Software wird über DVD-Sätze geliefert und gelagert. Es existiert ein Prozess zur zentralen Ablage aller benötigten Softwareprodukte in einem Schrank in der IT. Diese Produkte werden regelmäßig abgeglichen und es existiert ein Satz an Software im Werk 2.
Passwörter sind auf einer Excel-Liste gespeichert, welche im ausgedruckten Format auch im Werk 2 abgelegt sind.

5.5 Stromversorgung

Der IT-Bereich ist mit einer USV ausgestattet, die den Strom für ca. 15 Minuten hält. Es ist keine weitere Notstromversorgung vorhanden. Die Server fahren bei Stromausfall automatisch nieder.
Die Versorgung des Werkes erfolgt über einen zentralen Transformator im Werk. Bei Ausfall dieser Einheit (oder anderer zentraler Stromkomponenten) erfolgt ein Wiederanlauf in Werk 2.

5.6 Genereller Ansatz zur Wiederherstellung

5.6.1 *Allgemeiner Ansatz*

Durch die räumliche Struktur des Gebäudes ist ein Totalausfall des gesamten Gebäudes möglich. Als Ausfallsraum (und alternatives Anlaufszenario) wird der Aufbau eines zweiten kleinen Serverraums im Werk 2 gesehen.
Die Anbindung zwischen Werk 1 und Werk 2 erfolgt über ein eigenes Lichtwellenkabel in dessen Besitz die Firma Bauer GmbH ist.
Im Office-Bereich sind alle ROT-Services über eine VM-Ware Struktur und einem im Werk 2 stehenden VM-Ersatzserver abgesichert. Ein Anlauf dieser Services kann daher ohne großen Aufwand erfolgen. Die Sicherungsdaten (Backupserver) ist generell im Werk 2 aufgestellt.
Die AS400 als zentraler Movex-Datenbankserver ist über einen Wartungsvertrag auch gegen Totalausfall abgesichert.

5.6.2 *Wiederanlauf Basissysteme*

- Datensicherung: Die Daten als zentrales Element des Wiederanlaufes sollte durch eine räumliche Trennung vom Serverraum vor einem gleichzeitigen Verlust geschützt werden. Es kann daher von einem Vorhandensein entweder der Platten oder der Server ausgegangen werden.
- VM-Ware: Es steht im Werk 2 ein Ersatz VM-Server zur Verfügung. Alle ROT-Services laufen bereits unter VM-Ware und müssen im Ausfallsfall nur über die letzte Plattensicherung auf den Ersatzhost zurückgespielt und manuell gestartet werden.
- Die AS400 ist mit einem Wartungsvertrag mit 8 Stunden Lieferzeit auch bei Totalverlust abgesichert.

5.6.3 *Wiederanlauf der Peripherie*

- PCs und Notebooks: Es kann mit großer Wahrscheinlichkeit von dem Vorhandensein von genügend GELB-PCs als Ersatz für die ROT-PCs ausgegangen werden. Diese werden als Ersatz für ausgefallenen ROT-PCs nach Entscheidung durch den Wiederanlaufkoordinator herangezogen. Die Nachbeschaffung erfolgt im Rahmen eines geregelten Einkaufsprozesses.
- Drucker: Es sind keine Spezialdrucker im Einsatz. Die Drucker können durch vorhandene Strukturen ersetzt werden.
- LAN: Der Wiederaufbau des ROT-Not-Lans erfolgt über einen Ersatzswitch im Werk 2. Die Anbindungen an die aktiven Knoten über ein auf Lager liegendes Ersatzkabel.

5.7 Erreichung des Normalbetriebes

Die Beendigung des K-Falles (und die Wiederaufnahme des Normalbetriebes) erfolgt auf Basis der Übergabe eines Services an den Business-Owner durch den Wiederanlaufkoordinators und richtet sich nach folgender Definition des Normalbetriebes:
Der Normalbetrieb pro Service ist erreicht, wenn:

- Die vor dem K-Fall zur Verfügung gestellte Computerperformance wieder zur Verfügung steht
- Die vor dem K-Fall etablierten Ausfallsgeräte wieder nachgekauft und installiert wurden (Bereitstellung der Redundanzen)

Ein Normalbetrieb richtet sich nicht nach einer vollständigen Wiederherstellung des Gebäudes.

5.8 Abhängigkeitsmatrix

Die Abhängigkeiten der Services sind in Tabelle 1 dargestellt.

Tabelle 1: Abbildungsmatrix der Services der Firma Bauer GmbH aus dem Jahr 2010

Service	Priorität	Abhängigkeiten	Internes Zuliefersystem	Wird in Standorten benötigt
PC - Rot	a			
PC - Gelb	b			
LAN - Rot	a			
LAN - Gelb	b			
Drucker - Rot	a			
Drucker - Gelb	b			
Bausich (Plattenlibrary)	a			
Backupserver (Arcserve)	a			
VM-Ware	c		Zuliefersystem	Auch für Standorte
Internet WAN - VPNs Standorte	a		Zuliefersystem	Auch für Standorte
Anbindung ans Werk 2	c		Zuliefersystem	
Mail (Exchange 2003)	a	Internet, VM-Ware, SPAM, AD		Auch für Standorte
AD - DNS / DHCP / WINS	a		Zuliefersystem	Auch für Standorte
File	a	AD		Auch für Standorte
Print	a	AD		Auch für Standorte
Antivirussoftware	b			Auch für Standorte
SPAM	b			
WSUS	c	AD		Auch für Standorte
IP-Check - Überwachungstool	c			
USV-Manager	c			
Telefonie	a			
Fax	c	Mail, AD		Auch für Standorte
Movex-Datenbankserver (AS-400)	a		Zuliefersystem	Auch für Standorte
Movex-Applikationsserver	a	AS-400		Auch für Standorte
Streamserver (Druck - Movex)	a	AS-400, Signaturserver		Auch für Standorte
Zentrale DBASE Instanz	b			Auch für Standorte
Solid-Edge - Clients	b	Lizenzmanager		
Zentralrechner Fertigungszentrum	b			
Zentralrechner Zuschnitt	b			
Cognos	c			Auch für Standorte
Code-Key - Stempelprogramm	c			
Synchronizer	c	File		Auch für Standorte
e-Quest	c	SQL		
Intranet	c	AS-400		Auch für Standorte
Intrexx	c	SQL, AD		
Lizenzmanager Solid-Edge	c		Zuliefersystem	
Signaturserver f. digitale Signatur	c		Zuliefersystem	
SQL-Server	c		Zuliefersystem	
Banksoftware	c			
QM-Soft	c	File		
Elda-GKK	c			
Symphonie	c			
LGA	c			
TNT	c	SQL		
DHL	c	SQL		
DPD	c	SQL		
Business Planner	c			
Visual-Basic (Server)	c			

5.9 Externe Supportorganisationen oder Techniker

In Tabelle 2 ersichtlich ist, welche Services von externen Organisationen gewartet werden.

Tabelle 2: Externe Supportorganisationen aus dem Jahr 2010

Service	*Organisation*	*Adressinfos*
Hardwarelieferant	Ulbel&Freidorfer Gmbh & Co KG	Andritzer Reichsstraße 66, 8045 Graz Hr. Ing. Josef Stockreiter
AS400	ALJA GesmbH & Co KG	Telepark 1, 8572 Bärnbach Hr. Alfred Jarema
Firewall	ACP IT Solution GmbH	Herrgottwiesgasse 203, 8055 Graz Hr. Heinz Novosel
Internetprovider	UPC Austria GmbH	St. Peter Gürtel 10b, 8042 Graz Hr. Stefan Wipfler +43 59 999 4000 office@inode.at
Internetleitung	Telekom	Exerzierplatz 34, 8051 Graz Hr. Gerhard Mayer
WSUS	Active-IT	Parkring 6, 8403 Lebring Hr. Ing. Michael Wretschko
IP-Überwachungstool	Active-IT	Parkring 6, 8403 Lebring Hr. Ing. Marko Klein
Telephonanlage und Fax-Server	Kapsch BusinessCom AG	Triesterstraße 40, 8020 Graz Hr. Ing. Andreas Zöhrer
Zentralrechner Fertigungszentrum Softwarelösung	Fa. Maurer Alexander	Föhrenstraße 43, 8580 Köflach Hr. Alexander Maurer
Zentralrechner Zuschnitt	Kasto Maschinenbau GmbH & Co KG	Industriestr. 14, 77855 Achern-Gamshurst Hr. Patrick Petrat
Zeiterfassung	Wolfgang Schrack IT Solutions & Consulting	Schillerstraße 3, 4623 Gunskirchen Hr. Wolfgang Schrack
Solid Edge - Lizenzen	PDU-Cad Solid Edge	Franzosenhausweg 53, 4030 Linz Technik Hotline
Signaturserver	Xicrypt GmbH	Hub 109, 8046 Graz Hr. Gerald Scherr

QM-Software	Negotia Kalibrierlabor	Werk-VI-Straße 55, 8605 Kapfenberg Hr. Thomas Fladl
LGA	Softwaretechnik GmbH	Rubensstrae 40, 4050 Traun Fr. Monika Klug
TNT	TNT Express (Austria) GmbH	Cargo Nord Obj. 3, 1300 Wien Hr. Christopher Kral
DHL	DHL Express	Am Terminal 4b, 8402 Werndorf Hr. Christian Zinggl
DPD	Gebrüder Weiss Paketdienst GmbH	Arbeitergasse 50, 2333 Leopoldsdorf b. Wien Hr. Jürgen Frank

Die Telefonnummern und E-Mailadressen wurden aus Datenschutzgründen aus der Tabelle 2 entfernt.

5.10 Hauptverfahrensanweisung

5.10.1 *Verfahrensanweisung im Katastrophenfall*

5.10.1.1 Erste Einschätzung der Katastrophe

Tabelle 3: Erste Einschätzung der Katastrophe aus dem Jahr 2010

Erste Einschätzung der Katastrophe		
Verantwortliche Rolle:	Wiederanlaufkoordinator	
Ziel: Erkennen ob der Start des Katastrophenwiederanlaufplanes notwendig ist, oder es sich um einen normalen Systemausfall handelt		
Notwendige Verfahrensschritte:		
- Einholen eines ersten optischen Eindruckes (was war Ursache der Alarmierung) - Kontaktaufnahme mit dem Brandschutzbeauftragten - Bei Anwesenheit der Feuerwehr – Kontaktaufnahme zu Einsatzverantwortlichem und Abklärung der Situation Entscheidung: - Katastrophe JA: Gehe zum nächsten Schritt - Katastrophe NEIN: Alle weiteren Entscheidungen außerhalb dieses Planes		
Erledigt:	*Datum, Uhrzeit*	*Name:*

5.10.1.2 Aktiviere Personen

Tabelle 4: Aktiviere Personen aus dem Jahr 2010

Aktiviere Personen		
Verantwortliche Rolle:	Wiederanlaufkoordinator	
Ziel: Aktiviere alle notwendigen IT-Ressourcen, Überblick über vorhandene Ressourcen		
Notwendige Verfahrensschritte:		
- INPUT: Kontaktadressliste - Kontaktaufnahme (Telephon, SMS,...) zu allen internen IT-Kontakten - Vermerken der Response im entsprechenden		
Erledigt:	*Datum, Uhrzeit*	*Name:*

5.10.1.3 Einschätzung der Sonderverfahrensanweisung

Tabelle 5: Einschätzung der Sonderverfahrensanweisung aus dem Jahr 2010

Einschätzung Sonderverfahrensanweisung		
Verantwortliche Rolle:	Wiederanlaufkoordinator	
Ziel: Erkennen und Einschätzung, ob ein Wiederanlauf am Werksgelände in der vorhandenen Struktur möglich ist, oder ob das alternative Wiederanlaufszenario gewählt werden muss		
Notwendige Verfahrensschritte:		
- Beantwortung aller Fragen zum Start der Sonderverfahrensanweisung wie lt. Kapitel Sonderverfahrensanweisung - Wurden alle Fragen mit „NEIN“ beantwortet – oder kommt es aus anderen Gründen nicht zum Start der Sonderverfahrensschritte – weiter im nächsten Schritt - Wurde eine Frage mit „JA“ beantwortet – oder kommt es aus anderen Gründen zum Start der Sonderverfahrensschritte – weiter mit Punkt: Abklärung Services unter Einbeziehung der Verfahrensanweisungen unter: Verfahrensvorschriften - Eintragen etwaiger zusätzlich gefundenen Gründe in die entsprechende Rubrik in Kapitel Hauptaktion – Start des Sonderverfahrens		
Erledigt:	*Datum, Uhrzeit*	*Name:*

5.10.1.4 Aktiviere Krisenraum

Tabelle 6: Aktiviere Krisenraum aus dem Jahr 2010

Aktiviere Krisenraum		
Verantwortliche Rolle:	Wiederanlaufkoordinator	
Ziel: Aktivierung des Krisenraumes als zentraler Planungspunkt des Teams		
Notwendige Verfahrensschritte:		
- Nach Abklärung des Anlaufszenarios Entscheidung, ob der Krisenraum im Werk 2 bezogen wird. - Information an alle IT-Mitarbeiter und des Managements bezüglich des neuen zentralen Koordinationsraumes		
Erledigt:	*Datum, Uhrzeit*	*Name:*

5.10.1.5 Einteilung vorhandener Räume

Tabelle 7: Einteilung vorhandener Räume aus dem Jahr 2010

<table>
<tr><td colspan="3">Einteilung vorhandener Räume</td></tr>
<tr><td>Verantwortliche Rolle:</td><td colspan="2">Wiederanlaufkoordinator</td></tr>
<tr><td colspan="3">Ziel: Abklärung, welche Gebäudeteile sind noch intakt und können für den Wiederanlauf verwendet werden</td></tr>
<tr><td colspan="3">Notwendige Verfahrensschritte:</td></tr>
<tr><td colspan="3">- Informationsbeschaffung über Kontaktaufnahme zu Feuerwehr, Housing, oder anderen in der Schadensbegrenzung beschäftigen Verantwortlichen
- Begehung des Geländes
- Einteilung eines jeden in Kapitel Aufteilung der Räume definieren Bereiches in:
▪ GRÜN: Dieser Bereich ist zur Gänze benutzbar
▪ ROT: Dieser Bereich ist zur Gänze unbenutzbar
▪ Gelb: die einzelnen Services müssen auf Funktionsfähigkeit überprüft werden
- Fragen pro Bereich:
▪ Ist der Raum benutzbar – wie viele Personen können hier untergebracht werden
• Eintrag in Spalte: Anzahl Personen
▪ Sind die LAN Anschlüsse in diesem Bereich mit einem benutzbaren aktiven LAN-Segment verbunden (sind die Kabel zum Patchkasten noch vorhanden und ist der Patchkasten noch verwendbar)
• Eintrag in Spalte: LAN
▪ Kann dieser Raumbereich leicht mit Strom versorgt werden (abzuklären mit Housing oder Stromverantwortlichem)
• Eintrag in Spalte: Strom</td></tr>
<tr><td>Erledigt:</td><td>Datum, Uhrzeit</td><td>Name:</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

5.10.1.6 Abklärung vorhandener Räume und Hardware

Tabelle 8: Abklärung vorhandener Räume und Hardware aus dem Jahr 2010

<table>
<tr><td colspan="3">Abklärung vorhandener Räume / HW</td></tr>
<tr><td>Verantwortliche Rolle:</td><td colspan="2">Wiederanlaufkoordinator</td></tr>
<tr><td colspan="3">Ziel: Abklärung der in den gelben Raumbereichen noch vorhandenen und nutzbaren HW</td></tr>
<tr><td colspan="3">Notwendige Verfahrensschritte:</td></tr>
<tr><td colspan="3">- Zuordnung der Gelbbereiche auf vorhandene IT-Ressourcen
- Begehung der Gelb-Bereiche
- Einschätzung der vorhandenen HW auf Verfügbarkeit:
▪ Optisch
▪ Wenn Strom vorhanden – Startversuch
▪ Wenn kein Strom vorhanden – Transport der HW in einen mit Strom versorgten Bereich und Startversuch
▪ Markierung der HW als Vorhanden in der Hardwareliste</td></tr>
<tr><td>Erledigt:</td><td>Datum, Uhrzeit</td><td>Name:</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

5.10.1.7 Abklärung Services

Tabelle 9: Abklärung Services aus dem Jahr 2010

<table>
<tr><td colspan="3">Abklärung Services</td></tr>
<tr><td>Verantwortliche Rolle:</td><td colspan="2">Wiederanlaufkoordinator</td></tr>
<tr><td colspan="3">Ziel: Abklärung welche Services sind nicht mehr vorhanden und müssen wiederhergestellt werden</td></tr>
<tr><td colspan="3">Notwendige Verfahrensschritte:</td></tr>
<tr><td colspan="3">- Vermerk des HW-Status in der Service-Liste
▪ Rote Raumbereiche: alle Services in diesem Raumbereich werden als ausgefallen markiert
▪ Grüne Raumbereiche: alle Services in diesem Raumbereich werden als verfügbar markiert
▪ Gelbe Raumbereiche: Verteilung wurde in Punkt Abklärung vorhandener Räume und Hardware durchgeführt
- Zuordnung LAN und PCs
▪ Abzählung verfügbarer PCs und verfügbarer LAN-Verbindungen (nur PC bis nächstes aktives Element)
- Herausnahme der Blätter aller nicht mehr vorhandenen Services aus Kapitel: Verfahrensvorschriften</td></tr>
<tr><td>Erledigt:</td><td>Datum, Uhrzeit</td><td>Name:</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

5.10.1.8 Einordnen der Services

Tabelle 10: Einordnen der Services aus dem Jahr 2010

Einordnung der Services		
Verantwortliche Rolle:	Wiederanlaufkoordinator	
Ziel: Zuordnung ausgefallener Services zu verantwortlichem Techniker und Reihung der Services		
Notwendige Verfahrensschritte:		
Gruppensitzung aller vorhandenen IT-Mitarbeiter - Sortierung aller herausgelösten (ausgefallenen) ROT-Services nach dem Gesichtspunkt: Welcher vorhandene Techniker ist in der Lage, die in der Serviceverfahrensanweisung definierte erste Aufgabe zu lösen? - Eintrag des verantwortlichen Technikers in der Serviceverfahrensanweisung - Gemeinsame Reihung der ROT-Services pro Techniker nach Priorität der Wiederherstellung – Eintrag im Feld „Nummer der Abarbeitungsreihenfolge“ im Format „Techniker/Nummer“		
Erledigt:	*Datum, Uhrzeit*	*Name:*

5.10.1.9 Information über das Ausmaß der Katastrophe an die Geschäftsführung

Tabelle 11: Information an die Geschäftsführung aus dem Jahr 2010

Information über das Ausmaß der Katastrophe an Geschäftsführung		
Verantwortliche Rolle:	Wiederanlaufkoordinator	
Ziel: Information des Vorstandes und Einbindung der TO-K		
Notwendige Verfahrensschritte:		
- Information der Geschäftsführung anhand der Liste Verständigungsplan über das Ausmaß der Katastrophe und erste Einschätzungen über den Wiederanlauf. - Information der Standorte - Abklärung mit Geschäftsführung, welche Informationen an externe weitergegeben werden dürfen - Kommunikation der abgestimmten Informationen an externe von der IT zu informierenden Kunden und Lieferanten laut Liste: Externe Supportorganisationen oder Techniker		
Erledigt:	*Datum, Uhrzeit*	*Name:*

5.10.1.10 Personalabschätzung

Tabelle 12: Personalabschätzung aus dem Jahr 2010

<table>
<tr><td colspan="3">Personalabschätzung</td></tr>
<tr><td>Verantwortliche Rolle:</td><td colspan="2">Wiederanlaufkoordinator</td></tr>
<tr><td colspan="3">Ziel: Abklärung, ob mit dem vorhandenem IT-Personal der Wiederanlauf entsprechend durchgeführt werden kann, oder ob externes Personal mit eingebunden werden muss</td></tr>
<tr><td colspan="3">Notwendige Verfahrensschritte:</td></tr>
<tr><td colspan="3">Gemeinsame Gruppensitzung:
- Diskussion, ob der Wiederanlauf mit dem vorhandenem Personal durchgeführt werden kann oder externes Personal eingebunden werden muss
▪ Fragestellungen: zerstörte Services (Anzahl, Welche)
▪ Abschätzung über andere zerstörte Unternehmensbereiche (welche Abteilungen benötigen welche Services wie schnell)
- Entscheidung: wird externes Personal alarmiert oder nicht
▪ Bei NEIN: Start des Wiederanlaufes
▪ Bei JA:
• Alarmierung des entsprechenden Personals laut Kontaktliste in Kapitel: Externe Supportorganisationen oder Techniker durch Wiederanlaufkoordinator
• Start des Wiederanlaufes</td></tr>
<tr><td>Erledigt:</td><td>Datum, Uhrzeit</td><td>Name:</td></tr>
<tr><td></td><td></td><td></td></tr>
</table>

5.11 Sonderverfahrensanweisung

5.11.1 *Fragen zum Start der Sonderverfahrensanweisung*

Tabelle 13: Start der Sonderverfahrensanweisung aus dem Jahr 2010

Frage:	Eingetreten Ja	Eingetreten Nein
Stromversorgung im Werk 1 längerfristig nicht möglich		
Ganzes Gebäude nicht mehr benutzbar		
Einschätzung des Schadens nicht kurzfristig möglich		
WAN-Verbindung längerfristig nicht aufbaubar		

5.11.2 *Sondergründe*

Tabelle 14: Sondergründe aus dem Jahr 2010

Eintragender – Name	Unterschrift:	Datum / Uhrzeit:
Sondergrund:		

5.12 Aufteilung der Räume

Tabelle 15: Aufteilung der Räume aus dem Jahr 2010

Bereich:	Kurze Beschreibung:	Status:	Anz. Pers.	LAN:	Strom:
VW- KG - Vorne					
VW-EG - Vorne					
VW-EG - Hinten					
VW-1.Stock - Vorne	Telephonie, LAN				
VW-1.Stock - Hinten	LAN				
VW-2.Stock - Vorne					
FC4 - Mech Fertigung					
FC4 - 1.Stock IT-Serverraum	Serverraum, LAN, Safe				
Versuch					
FC1 - Rohrfertigung					
FC2 - Stahlbau					
Warenübernahme					
Versand und Fertigwarenlager	LAN				
Zuschnitt					
Ersatzteillager	LAN				
Portier					

5.13 Verständigungsplan

Es sind die Mitglieder des Führungskreises vom Eintritt der Katastrophe zu verständigen.

Tabelle 16: Verständigungsplan aus dem Jahr 2010

Name	*Position*	*Verständigt am/um:*
Hr. DI Otto Rois	Geschäftsführer	
Hr. Mag. Andreas Schitter	Geschäftsführer/Kaufm. Leiter	
Hr. Johann Langmann	Produktionsleiter	

5.14 Verfahrensvorschriften

5.14.1 *Sonderverfahrensvorschriften*

5.14.1.1 Hauptaktion – Start des Sonderverfahrens

Tabelle 17: Sonderverfahrensvorschriften aus dem Jahr 2010

Verfahrensanweisung	
Hauptaktionen – Start des Sonderverfahrens	

Ziel / kurze Beschreibung	
Abhandlung aller speziell benötigten Aktionen im Zuge eines vollständigen Wiederanlaufes im Ausweichzentrum	
Beteiligte Rollen	*Zugewiesene Personen*
WK-Wiederanlaufkoordinator	
Kurze Beschreibung	
Es sind keine speziellen Wiederanlaufaktionen notwendig.	

5.14.2 *Verfahrensvorschriften – Services*

5.14.2.1 Service ROT

Tabelle 18: Verfahrensanweisung Service - ROT aus dem Jahr 2010

Verfahrensanweisung	
PCs und Notebooks – ROT	

Priorität:	*Abarbeitungs Nr:*
ROT	

Ziel / kurze Beschreibung	
Wiederherstellung der als „ROT“ definierten PCs mit den entsprechenden Services	
Beteiligte Rollen	*Zugewiesene Personen*
WK – Wiederanlaufkoordinator	
HW-Hardware-Beschaffer	
FA – First Line (Desktop) Administrator	

Informationen zum Service:	
Während der Erstellung des DRPs wurden 9 PCs als „ROT“ identifiziert. Die Zur Verfügung Stellung der PCs erfolgt prinzipiell über noch vorhandene Gelb-PCs. Sollten aufgrund der Größe der Katastrophe nicht mehr genügend GELB-PCs zur Verfügung stehen müssen die Geräte ehestmöglich nachbeschafft werden. Die Installation erfolgt durch vollständige manuelle Nachinstallation. SW ist am Installationsverzeichnis und Produktkeys sind im Wiederanlaufkoffer.	
Standort:	Siehe Liste

Aktionen – HW-Beschaffung / Standortdefinition	*Rolle*	*Name*	*Beg.*	*Ende*	*Unterschr.*
Abklärung wie viele ROT-PCs sind nicht mehr vorhanden	WK				
Abklärung sind noch genügend GELB-PCs funktionsfähig – wenn ja – Verwendung dieser nach freier Auswahl durch den Koordinator	WK				
Sind nicht mehr genügend GELB-PCs vorhanden, sofortige Aktivierung des Lieferanten und Bestellung der Fehlmenge	HW				
Aufstellung in den in den als PC-Aufstellungsorten definierten Bereichen nach Entscheidung durch den Koordinator	WK				
Aktionen	*Rolle*	*Name*	*Beg.*	*Ende*	*Unterschr.*
Beschaffung der HW	HW				
Basisinstallation des Clients	FA				

5.14.2.2 Service GELB

Tabelle 19: Verfahrensanweisung Service - GELB aus dem Jahr 2010

Verfahrensanweisung	
PCs – GELB	

Priorität:	*Abarbeitungs Nr:*
GELB	

Ziel / kurze Beschreibung	
Wiederherstellung der restlichen im Betrieb eingesetzten Desktop-Geräte	
Beteiligte Rollen	*Zugewiesene Personen*
WK – Wiederanlaufkoordinator	
HW-Hardware-Beschaffer	
FA – First Line (Desktop) Administrator	

Informationen zum Service:	
Eine Liste der Desktops und Notebooks befindet sich in der Hardwareliste.	
Standort:	Siehe Liste
Wiederanlaufinformationen:	
Wiederbeschaffung der verlorenen Geräte und manuelle Installation der Geräte. Die benötigte Software befindet sich am Installationsverzeichnis, Produktkeys sind im Wiederanlaufkoffer.	

Aktionen	*Rolle*	*Name*	*Beg.*	*Ende*	*Unterschr.*
Abklären des Fehlbestandes	WK				
Bestellung des Fehlbestandes beim Lieferanten	HW				
Installation der Geräte nach Eintreffen	FA				

5.14.2.3 Service GRÜN

Tabelle 20: Verfahrensanweisung Service - GRÜN aus dem Jahr 2010

Verfahrensanweisung	
Intranet - GRÜN	

Priorität:	*Abarbeitungs Nr:*
GRÜN	

Ziel / kurze Beschreibung	
Wiederherstellung des Services	
Beteiligte Rollen	*Zugewiesene Personen*
HW-Hardware-Beschaffer	
SA-Server Administrator	

Informationen zum Service:	
Bei diesem Service handelt es sich das zentrale Internet des Unternehmens. Das Service läuft auf einem physischen Server (BauWEB01)	
Standort:	Serverraum
Wiederanlaufinformationen:	
Die Wiederherstellung erfolgt durch Nachbeschaffung der Hardware und Installation der Applikation	

Aktionen	*Rolle*	*Name*	*Beg.*	*Ende*	*Unterschr.*
Beschaffung der Hardware	HW				
Installation des Servers	SA				
Rückspielen der Intranetdaten	SA				

6 Ergebnis und Ausblick

6.1 Ergebnis

Im Rahmen der Diplomarbeit wurde ein IT-Notfallplan für die Firma Bauer erstellt und in den laufenden Betrieb übernommen. Durch die strukturierte Vorgehensweise haben sich einige Maßnahmen im Hinblick auf den IT-Grundschutz ergeben. Bereits bei der Einarbeitung in das Thema wurde deutlich, dass für die Erstellung eines Notfallplanes ein sehr umfangreiches Wissen über die vorhandenen Prozesse und den damit verbundenen IT-Komponenten aufgebaut werden musste. Als Ausgangspunkt wurde gemeinsam mit allen Abteilungen ein Servicekatalog erstellt und eine Wertung der Services in Abhängigkeit Signifikanz für das Unternehmen durchgeführt. Die für die Erstellung des Servicekataloges notwendige Dokumentation aller Infrastruktur- und Serverkomponenten bildet eine wertvolle Grundlage für die IT-Abteilung und kann in weiterer Folge als Basis für ein serverweites Monitoring der IT-Services betrachtet werden. Im Zuge der Diplomarbeit und des Projektes wurde auch ein neuer zweiter Serverraum geschaffen. In dieser Umstrukturierung und Planung wurde ein Ersatzserver installiert und in die Infrastruktur implementiert. Die bestehende Datensicherung konnte nach erfolgreicher Inbetriebnahme des Serverraums, wie nach dem IT-Grundschutz definiert, in den neuen Serverraum übernommen werden. Das Hauptziel der Diplomarbeit wurde durch die Formulierung von Hauptverfahrensanweisungen erreicht.

6.2 Ausblick

Diese Diplomarbeit zeigt, dass die Erstellung eines IT-Notfallplans nach der Umsetzung von Maßnahmen des IT-Grundschutzes mit viel Aufwand, Zeit und Kosten verbunden ist. Es wurde festgestellt, dass einige Services effektiver und kosteneffizienter in einem externen Rechenzentrum betrieben werden könnten. Vor allem Abhängigkeiten von bestimmten Services der Hauptzentrale würden durch Outsourcing minimiert und effektiver (sicherer) gestaltet werden. Als Kernaspekt muss festgehalten werden, dass sich hinter einem IT-Notfallplan ein dynamischer Prozess verbirgt, der einer ständigen Überprüfung und Wartung/Ergänzung unterliegt. Dieser Prozess muss bei der Anschaffung neuer Services bzw. neuer Software immer berücksichtigt werden. Auch ein Desaster Recovery Test in definierten Zeitabständen ist für die Überprüfung eines Notfallplanes und dessen Qualitätssicherung unumgänglich. Abschließend muss man sagen, dass die Einführung einer IT-Notfallplanung für das Unternehmen Bauer ein voller Erfolg und für mich eine berufliche und persönliche Weiterentwicklung war.

Literatur

[GS-KATALOGE]	Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Kataloge, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzKataloge/itgrundschutzkataloge_node.html, verfügbar am 17.01.2015
[GS-WIKI2015]	IT-Grundschutz-Kataloge: Wikipedia, http://de.wikipedia.org/wiki/IT-Grundschutz-Kataloge, verfügbar am 02.02.2015
[BSI-GS-BROSCH]	Bundesamt für Sicherheit in der Informationstechnik: Broschüre „Überblick IT-Grundschutz“, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/Download/UberblickGrundschutz.pdf?__blob=publicationFile, verfügbar am 22.02.2015
[GS-STANDARD]	Bundesamt für Sicherheit in der Informationstechnik: IT-Grundschutz-Standard, https://www.bsi.bund.de/DE/Themen/ITGrundschutz/ITGrundschutzStandards/ITGrundschutzStandards_node.html, verfügbar am 10.02.2015
[BSI-STD100-1]	Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-1, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1001_pdf.pdf?__blob=publicationFile, verfügbar am 02.03.2015
[BSI-STD100-2]	Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-2, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1002_pdf.pdf?__blob=publicationFile, verfügbar am 02.03.2015
[BSI-STD100-3]	Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-3, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1003_pdf.pdf?__blob=publicationFile, verfügbar am 02.03.2015

[BSI-STD100-4] Bundesamt für Sicherheit in der Informationstechnik: BSI-Standard 100-4, https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Publikationen/ITGrundschutzstandards/standard_1004_pdf.pdf?__blob=publicationFile, verfügbar am 02.03.2015

[APPL-WIKI2015] Anwendungssoftware: Wikipedia, http://de.wikipedia.org/wiki/Anwendungssoftware, verfügbar am 03.03.2015

[MM-INET2015] Einsatz des BSI Maßnahmenkatalogs: Internet, http://marco-muench.de/dokumente/Seminararbeit%20-%20Einsatz%20des%20BSI%20Massnahmenkataloges.pdf, verfügbar am 02.03.2015

[IM-INET2015] Bundesamt für Sicherheit in der Informationstechnik: Compliance und IT-Sicherheit, http://www.dsri.de/downloads/itc2007/folien/07-Muench.pdf, verfügbar am 26.02.2015

[ECONTROL-2014] Ausfall- und Störungsstatistik für Österreich: E-Control, http://www.e-control.at/portal/page/portal/medienbibliothek/statistik/dokumente/pdfs/AuSD_Ver%C3%B6ffentlichung2014_v1.0.pdf, verfügbar am 21.02.2015

Selbstständigkeitserklärung

Hiermit erkläre ich, dass ich die vorliegende Arbeit selbstständig und nur unter Verwendung der angegebenen Literatur und Hilfsmittel angefertigt habe.

Stellen, die wörtlich oder sinngemäß aus Quellen entnommen wurden, sind als solche kenntlich gemacht.

Diese Arbeit wurde in gleicher oder ähnlicher Form noch keiner anderen Prüfungsbehörde vorgelegt.

Köflach, den 07.März.2015

Christian Kern