

Krisenbewältigung aus Anlass des Virenbefalls

Vorgehensmodell und Empfehlungen

DI. Rudolf Köller, IT-Leiter des Landes Kärnten

<http://www.ktn.gv.at>



kundenorientiert
kompetent
innovativ
effizient

Themen

- Rahmenbedingungen
- Problemerkennung, Risikobewertung
- Bekämpfungsstrategie
- Informations- und Kommunikationsstrategie
- Absicherung und Prävention
- Erkenntnisse

Rahmenbedingungen

Eckdaten: 3000 PC, 200 Server (viele virtualisiert), 120 Standorte

Betriebsführungsbereiche:

- Server, Backbone, LAN: Landes EDV
- Betrieb dezentrale PC-Arbeitsplätze und Drucker: ausgelagert
- Helpdesk: ausgelagert (Remedy)
- Weitverkehrsstrecken: ausgelagert
- Alle Prozesse sind mit Service Level Agreements hinterlegt

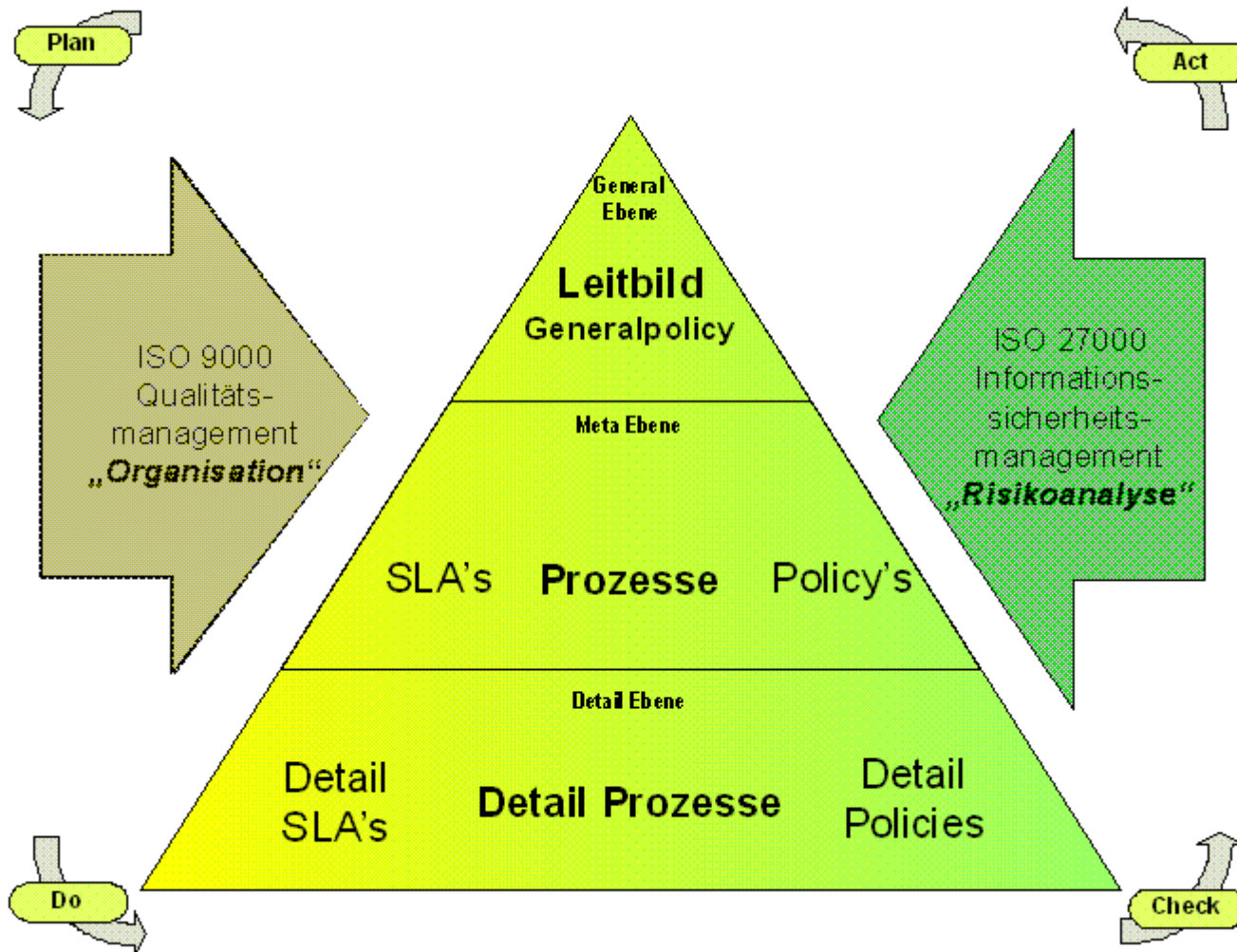
- Zertifiziertes System nach ISO 9001:2000 und ISO 27000

Management:

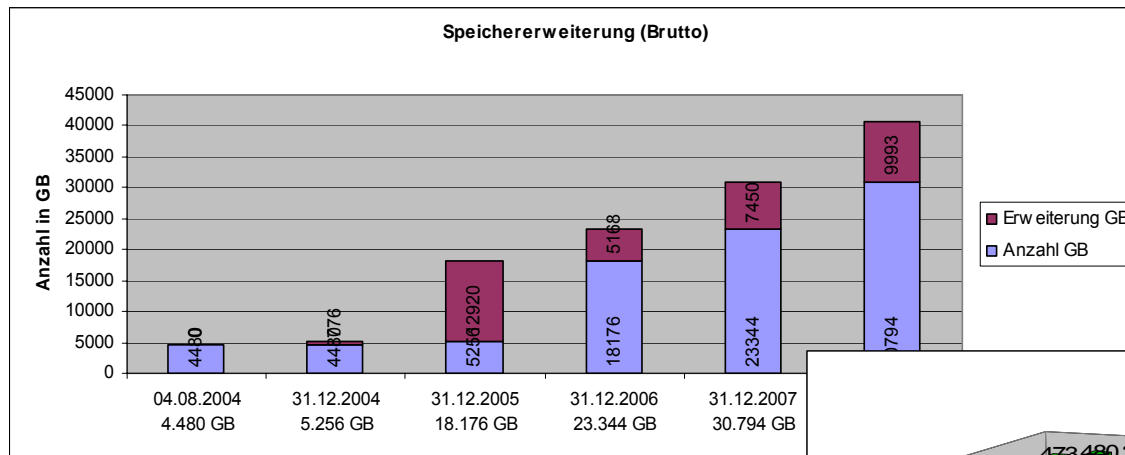
- Softwareverteilung: SMS 2003
- Sicherheitsupdates: SMS2003
- Virenschutz
- Zentrale Benutzerverwaltung für alle Systeme
- Vollständiges, exaktes Assetmanagement



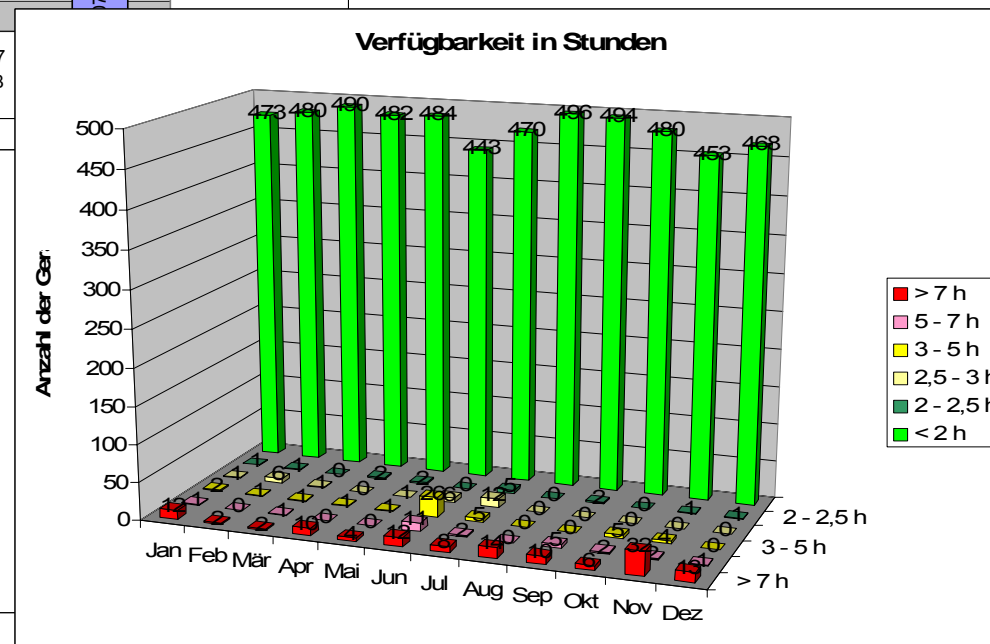
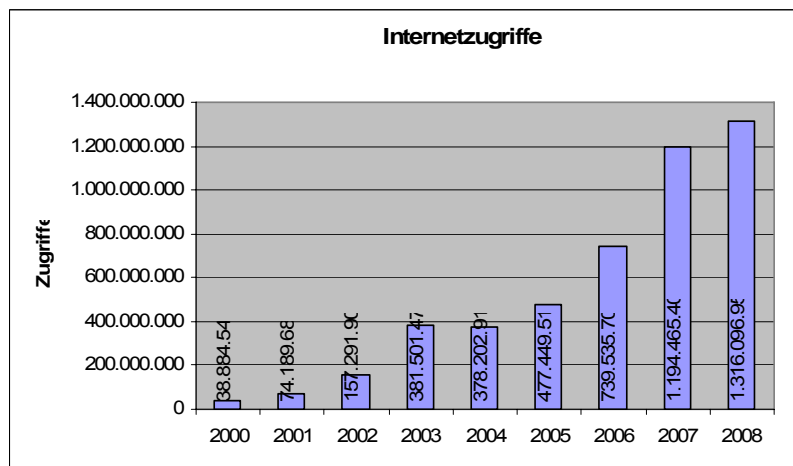
QISMS Pyramide



Datenvolumina und Verfügbarkeiten



Ausfallszeit (Stunden) pro Monat	Verfügbarkeit (%)
2	99,72
2,5	99,65
3	99,58
5	99,31
7	99,03



Bedrohungsszenarien und Maßnahmen für Risikominderung

Zerstörung von Teilsystemen des Rechnerraumes

Risiko	Maßnahmen zur Verringerung des Risikos
Brand	Löschanlage Rufbereitschaft Geordnetes Niederfahren nach Niederfahrplan
Wassereinbruch	Rufbereitschaft Sicherungsmaßnahmen erforderlich Geordnetes Niederfahren nach Niederfahrplan
Bombenalarm	Rufbereitschaft Geordnetes Niederfahren nach Niederfahrplan
Ausfall externer Datenanbindungen	Vertrag (Ausnahme Höhere Gewalt)
Ausfall externer Stromversorgung	Dieselaggregat für 10 Stunden
Teilsystemausfall	Wotan Verständigungssystem RZ Notfallplan

Zerstörung des Rechnerraums

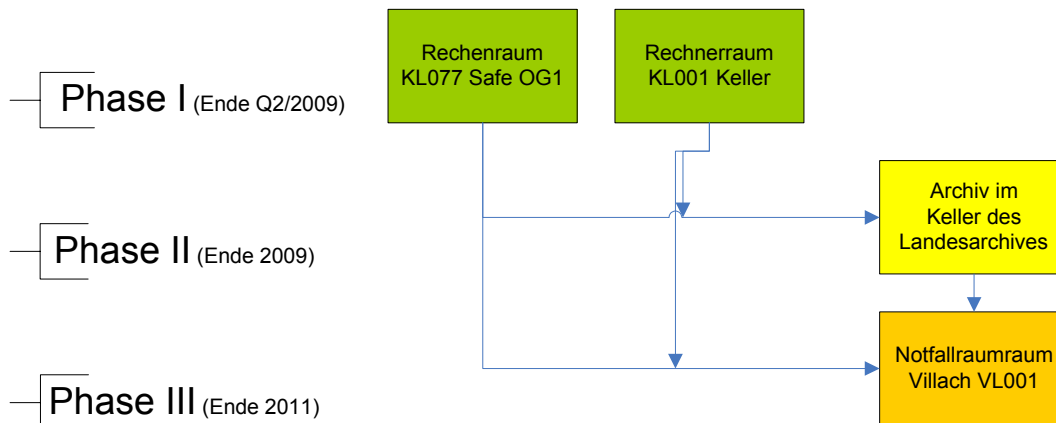
Risiko	Maßnahmen zur Verringerung des Risikos
Totalzerstörung	Ausfallrechnerraum
Totalzerstörung	Notfallplan bis zur Verfügbarkeit eines Ausfallrechnerraum

Zerstörung der Stadt Klagenfurt

Risiko	Maßnahmen zur Verringerung des Risikos
Totalzerstörung	Ausfallrechnerraum in anderer Stadt

Sicherheitsplan und Maßnahmen

Sicherheitsplanung Ausfallrechenzentrum



- **Ziel ist eine optimale Aufteilung, der bestehenden Systeme, zwischen den beiden Rechnerräumen in Klagenfurt zu realisieren. Dabei sollen vorhandene redundante Strukturen möglichst rasch getrennt werden.**
- **In Abhängigkeit der finanziellen Ressourcen, der Machbarkeit (Dark Fibre) und der Verhandlungsergebnisse werden die weiteren Phasen umgesetzt.**

Phase I

Aufteilung redundanter Systeme auf die zwei Rechnerräume; Aufstellung des Storage Systems im Safe; Aufstellung des Backup Roboters im Keller KL001; Aufbewahrung der Bänder außerhalb von Klagenfurt. Verhandlung mit dem Landesarchiv zur Bereitstellung eines Raumes für das Archivsystem; Verhandlung mit der BH Villach zur Bereitstellung eines Notfallraumes und Herstellung einer Basisinfrastruktur.

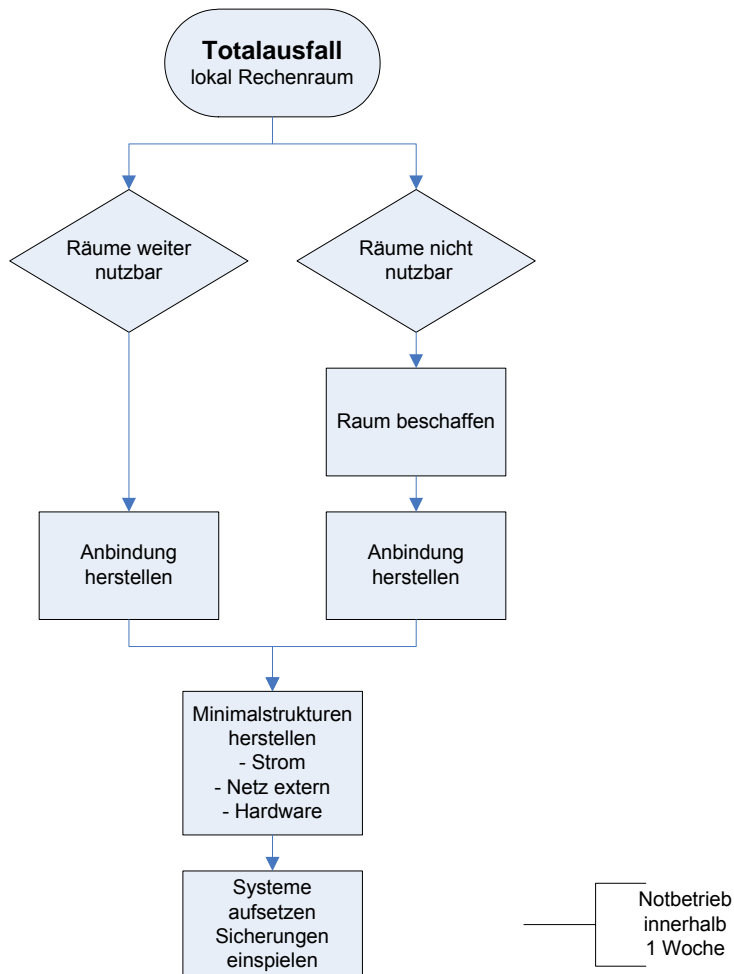
Phase II

Nach Ausschreibung und Anschaffung eines Backup- und Archivsystems wird die Hardware in den Räumen des Kärntner Landesarchives aufgestellt und mit Dark Fibre angebunden.

Phase III

Errichtung des Notfallraumes in den Räumen der BH Villach

Aufbauplan nach Zerstörung des Rechenzentrums



Hergestellt werden folgende Dienste mit verminderter Performance:

- Internetanbindung (Mail, Web)
- Oracle-Datenbanken
- Workflow
- Fileservices
- DPW Lohn

Das Storage System ist im Safe untergebracht – durch diesen Safe ist ein Ausfall dieses Systems so gut wie ausgeschlossen außer bei einem größeren Vorfall (Erdbeben, Terror). In der 3. Phase wird ein SAN mit geringerer Kapazität im Notfallraum aufgestellt.

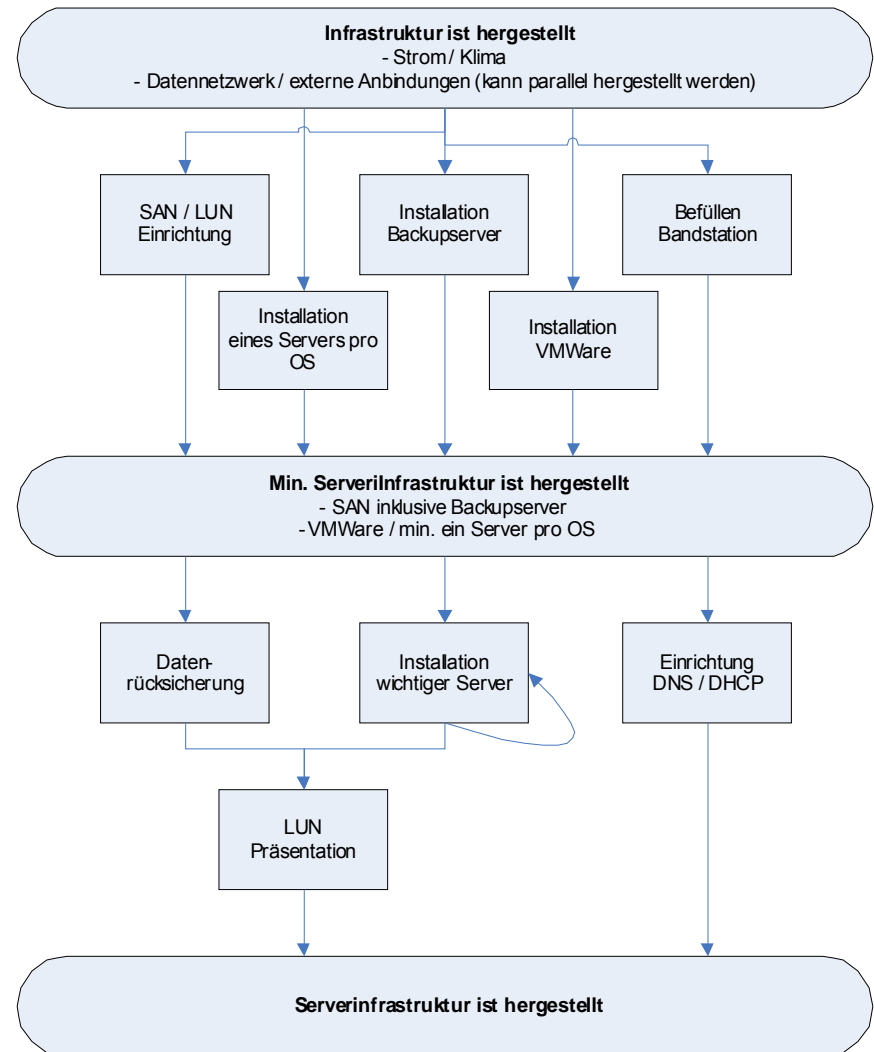
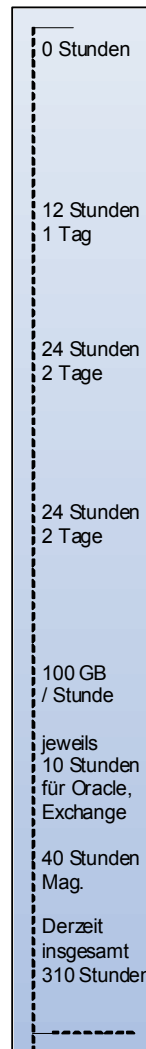
Sofortmaßnahmen zur Wiederherstellung von EDV Diensten

Risiko	Maßnahmen zur Verringerung des Risikos
Totalzerstörung der Rechnerräume	Feststellung des Schadens und noch verfügbarer Dienste
	Feststellung der notwendigen Ressourcen.
	Klärung Logistischer Fragen:
	Zusammenfassung externer Server der Außenstellen, Transportvorbereitungen, externe Netzanbindung, Hardwareanforderungen und Hersteller klären
Totalzerstörung der Rechenräume (Phase III)	Inbetriebnahme des Ausfallrechenraums mit den kritischen Anwendungen laut Detailrisikoanalyse.

Desaster Recovery Plan

Voraussetzungen:

- Die notwendige Infrastruktur wie Raum, Klima, Strom und externe Datennetzanbindung ist vorhanden.
- Die wichtigste Netzinfrastruktur, wie Backboneswitch und eine Firewall ist vorhanden
- SAN Infrastruktur inklusive Switches und Backupssystem ist vorhanden
- DB Server, VMWare, Server und Netzinfrastrukturserver, sind vorhanden!



Problemerkennung, Risikobewertung

Erste Vorzeichen (29.12.2009):

- Geringfügiger Anstieg der Passwortverletzungen (+15%)
- Kein Anschlagen des Virenschutzes
- Fehlannahme: technische Probleme beim AD

Ausbruch:

- Eskalation durch synchronisierte Bruteforce-Attacke um 3.1.2009, 21:00 Uhr
- Einberufung der erforderlichen Mitarbeiter in die Zentrale: **Krisenstab wird gebildet**
- Unverzögliche Sperre des Internetverkehrs

Erkennung:

- Installation mehrere Antivirenprodukte, um zu prüfen, ob, bzw. welcher Virus vorhanden ist
- Identifikation (11 von 39 Herstellern konnten den Befall diagnostizieren)
- Erstinformation an Landesamtsdirektor

Parallele Bearbeitung folgender Lösungsstrategien:

- Erkennung und Bekämpfung mit dem bestehenden System (4 Rollouts bis 5.1.2009, 16:00 Uhr)
- Erkennung und Bekämpfung mit einem Alternativsystem
- Bekämpfung des Verbreitungsmechanismus und Isolation mit Betriebssystemmitteln und diversen Systemkonfigurationen

Risikobewertung

Erstbeurteilung:

- Unbekannte Bedrohung
- Gezielter Angriff oder zufälliger Befall
- Hackerattacke im „Windschatten“
 - Datenkorruption
 - Datenspionage
 - Datenvernichtung
- Nachdem zuwenig valide Informationen vorlagen, Trennung aller PC vom Netz

Detailbewertung:

- Sicherstellung von Geräten und Studium in Laborumgebung
- Analyse von Wissen über Verbreitungswege und Mechanismen
- Bewertung der kritischen Strukturen (Mobile Equipment, Querverbreitung, Lokale Admins, ...)

Bekämpfungsstrategie

- Ressourcen: 4 Mann im Serversegment, 4 im Netzwerk – Einrichtung 24 Stundenbetrieb
- Automatische Deinstallation des alten Virenschutzes nicht möglich
- Softwareverteilung mit SMS 2003 nicht möglich
- Benutzereingriffe bei Bereinigung erforderlich - Mindestqualifikation erforderlich

Entscheidung:

- Nach 4 erfolglosen Bekämpfungsversuchen: Wechsel des Antivirenprogramms
- Manuelle Bereinigung mit kompakten Teams (insgesamt 40 Personen) (7.-10.1.2009)
- Erzeugen von Installationsmedien, Einsatzplänen und Checklisten

Harte Sicherheitsmaßnahmen:

- Sperre USB
- Sperre Mobile Internet
- Sperre jedes Gerätes mit der geringsten Anomalie

Informations- und Kommunikationsstrategie

Führungskräfte müssen über den Stand der Maßnahmen und Vorkommnisse informiert sein:

- Regierungskollegium
- Bezirkshauptleute
- Abteilungsvorstände

„IT-Kriegsrecht“:

- Alle erforderlichen Maßnahmen konnten von der IT ohne weitere Rücksprachen gesetzt werden
- Absolute Priorisierung
- Keine Ausnahmen

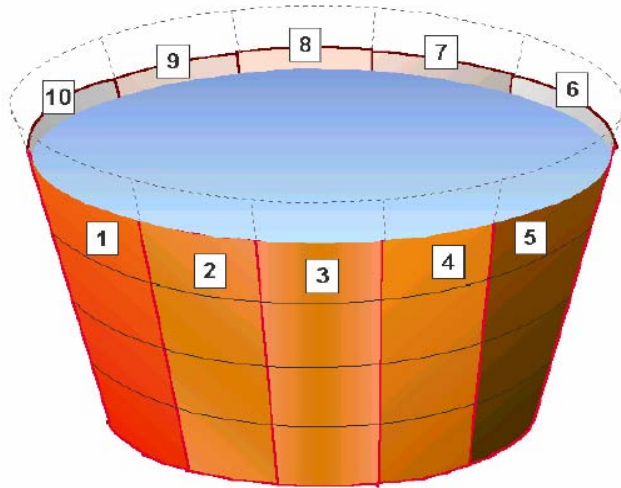
Kommunikation:

- Pressearbeit: Ausschließlich über LAD und IT-Leitung
- Informationsübermittlung an IT-Leiter der Bundesländer
- Informationsveranstaltung für IT-Leiter großer Kärntner Organisationen

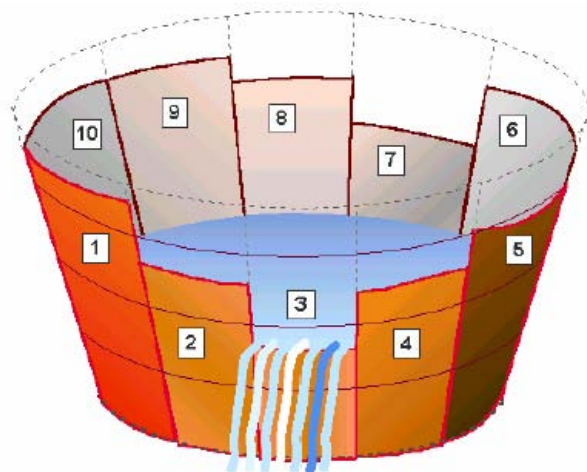
Absicherung und Prävention

- Einsatz einer lokalen Firewall auf allen PCs
- Unterschiedliche lokale Administratorpasswörter auf allen Rechnern
- Flächendeckende Einführung einer automatisierten Sicherheitsprüfung aller PCs (Trusted Network Computing)
- Noch feinere Unterteilung des Landesnetzes in Sicherheitszonen
- Kürzere Intervalle bei der Überwachung von Service Level Agreements
- Strengere Überprüfung der Einhaltung von IT-Sicherheitsbestimmungen
- Einführung eines Intrusion Prevention Systems

Komponenten des IT-Sicherheitssystems (nach ISO 27000)



- Sicherheitspolitik (Security Policy)
- Sicherheitsorganisation (Organizational Security)
- Klassifizierung von Vermögenswerten (Asset Classification and Control)
- Personalsicherheit (Personnel Security)
- Physische Sicherheit (Physical and Environmental Security)
- Sicherheit von Kommunikation und Betrieb (Communications and Operations Management)
- Zugriffskontrolle (Access Control)
- Sicherheit bei Systementwicklung und -wartung (Systems Development and Maintenance)
- Aufrechterhaltung der Betriebsbereitschaft (Business Continuity Management)
- Einhaltung von Sicherheitsvorschriften (Compliance)



Erkenntnisse

- Qualitäts- und Sicherheitsmanagement hat geholfen die Krise rasch zu bewältigen:
 - Ausgezeichnete Dokumentationen
 - Funktionierende Prozesse
 - Klare Vorgehensmodelle

- Restrisiko immer vorhanden – daher:
 - Entwicklung einer Notfallebene am lokalen PC-Arbeitsplatz
 - Prioritätenreihung bei der Instandsetzung des IT-Systems ausarbeiten
 - Analoge Ersatzverfahren für Geschäftsprozesse ausarbeiten
 - Verwaltungskooperation im Fall eines eingeschränkten IT-Betriebes
 - Risikobewusstsein der Mitarbeiter muss weiter gesteigert werden

- Endgerätesegment muss stärker in die Verfügbarkeitsbetrachtung einbezogen werden