



Sind Ihnen mögliche Risiken und Konsequenzen bei einem Ausfall Ihrer Informatik bekannt? Wie lange können Sie auf einzelne Anwendungen verzichten? Wann schalten Sie auf ein Notkonzept um? Wissen Ihre Mitarbeiter damit umzugehen? Wir gehen mit Ihnen Schritt für Schritt jedes „Was-Wenn“ durch und zeigen Ihnen, wo Massnahmen nötig sind. Sicher!

LEVEL 6	PROZESSE	Abhängigkeiten, Drehbücher für Katastrophenfall Ansprechpartner, Notfallnummern
LEVEL 5	APPLIKATION DATEN	Applikations-Software wie CRM, ERP, Collaboration, etc.
LEVEL 4	BETRIEBS- SYSTEM	Betriebssystem Software Images der Server Treiber-Software
LEVEL 3	HARDWARE	Serverhardware Storage Backupgeräte USV
LEVEL 2	NETZWERK	Intern: Networkservices (ADS, DHCP, DNS, Switch) Extern: Firewall, Internetan- bindung
LEVEL 1	GEBÄUDE	Serverraum Räumlichkeiten weitere Lokalitäten

REVIEW & KONZEPT DISASTER RECOVERY & BUSINESS CONTINUITY

Die Verantwortung wahrnehmen

Gesetzliche Anforderungen wie Sarbanes-Oxley oder Basel II sowie die Zunahme von hinterhältigen Attacken aus dem Web steigern den Bedarf nach krisensicheren Geschäftskonzepten. Systemausfälle und möglicher Datenverlust bedeuten für viele Unternehmen ein bedrohliches Geschäftsszenario. Disaster Recovery und Business Continuity setzen sich zur Standard-Prozedur durch. Deren Beurteilung gehört zusehends in die Aufgabenliste der Geschäftsführung. Das gekoppelte Konzept untersucht und bestimmt, wie Geschäftsprozesse und der gesicherte unternehmensweite Zugriff auf relevante Informationen im Falle von ungeplanten Vorkommen aufrecht erhalten werden können.

Ein Konzept für den Notfall

Zusammen untersuchen wir alle möglichen Gefahren und Ursachen für einen Ausfall. Anschliessend bestimmen wir die für Ihr Geschäft verkraftbaren Ausfallzeiten in Stunden oder gar Tagen. In einem speziellen Schichten-Modell werden danach für jedes System die Wiederherstellungs-Prozeduren definiert. Eventuell vorhandene Lücken, welche den Geschäftsbetrieb massgeblich gefährden, werden dabei aufgedeckt und in einem Massnahmen-Katalog erfasst. Der Abschluss bilden ein revisionsgerechtes Konzept und das Schulen des IT-Verantwortlichen.

Vorgehensschritte

Methodisches Interview / Risiko-Analyse / Ermittlung Toleranz Ausfälle / GAP-Analyse / Massnahmenkatalog / Schulung / Testen

Konzept-Inhalt

Disaster-Recovery Verfahren / Gebäude und Arbeitsplätze / Netzwerk / Hardware / Betriebssystem / Applikationen / Daten / Prozesse / Personal / Management-Verantwortung / Notfall-Listen

Der Dienstleistungsaufwand für den Review und die Konzepterstellung richtet sich nach Branche/Grösse, ab drei Arbeitstagen