Zeitschrift: Bulletin des Schweizerischen Elektrotechnischen Vereins, des Verbandes Schweizerischer Elektrizitätsunternehmen = Bulletin de l'Association suisse des électriciens, de l'Association des entreprises électriques suisses

Herausgeber: Schweizerischer Elektrotechnischer Verein ; Verband Schweizerischer Elektrizitätsunternehmen

Band: 87 (1996)

Heft: 9

Artikel: Das Informatik-Notfallkonzept als Element der Notfallplanung : Teil 2 : wie sieht ein Informatik-Notfallplanungsprojekt aus?

Autor: Umiker, Bruno / Peer, Alfred / Truttmann, Paul A.

DOI: https://doi.org/10.5169/seals-902318

Im Teil 1 dieses Beitrags (Bulletin SEV/VSE 3/96) wurde aufgezeigt, welche Ausmasse die Abhängigkeit der Unternehmen von der Informatik angenommen hat und mit welch schwerwiegenden Folgen zu rechnen ist, wenn man keine Gegenmassnahmen trifft. Im vorliegenden zweiten Teil dieses Beitrags wird aufgezeigt, wie solche Gegenmassnahmen in Form eines Informatik-Notfallkonzepts aussehen können.

Das Informatik-Notfallkonzept als Element der Notfallplanung

Teil 2: Wie sieht ein Informatik-Notfallplanungsprojekt aus?

■ Bruno Umiker, Alfred Peer und Paul A. Truttmann

Welcher Zielsetzung soll die Informatik-Notfallplanung genügen?

Ein Informatik-Notfallplanungsprojekt besteht aus den in Bild 2 skizzierten, im Vergleich zu einem Informatikprojekt inhaltlich leicht angepassten Projektphasen, wobei es primär Aufgabe der Geschäftsleitung ist, die Zielsetzung an die Informatik-Notfallplanung in Abstimmung mit der gültigen Unternehmens- und Informatikstrategie festzulegen.

Dazu ist jedoch grundsätzlich eine hohe Sensibilität der Topmanager zu Risikofragen Voraussetzung. Darüber hinaus muss erkannt und anerkannt werden, dass besonders bei Ausfall der Informationsverarbeitung ein hohes, latent vorhandenes Risikopotential eintreten kann. Erfahrungsgemäss ist jedoch dieser Bewusstseinsprozess in vielen Chefetagen nicht nur ungenügend entwickelt, sondern stellt sogar eine der wunden Stellen dar. Nur allzuoft trifft man auf die Haltung, dass nicht sein kann, was nicht sein darf! Dieser äusserst wichtige Sensibilisierungs- und Zielfindungsprozess ist Bestandteil der hier vorgestellten Methoden und Werkzeuge einer Informatik-Notfallplanung. Sie bieten Gewähr für einen sinnvollen und machbaren Weg aus dem Dilemma der obersten Verantwortlichen, wie sie in dieser heiklen und ungeliebten Frage die Fäden des Handelns und Entscheidens in ihre Hände kriegen.

Wichtig bei der Festlegung der Zielsetzung ist eine Präzisierung des Dienstleistungsangebots der Informatik und der einzuhaltenden Rahmenbedingungen in einem Katastrophenfall. Notfallmassnahmen im Informatikbereich müssen auf Notfallkonzeptionen und Notfallmassnahmen anderer Unternehmensbereiche, zum Beispiel auf ein Produktions-Notfallkonzept, abgestimmt werden. Konkurrierende Zielsetzungen sind dabei möglichst zu vermeiden.

Welchen Zweck hat die Situations- und Risikoanalyse?

Es geht darum, das gesamte Risikopotential und dessen mögliche Auswirkungen in Erfahrung zu bringen. Dabei spielen Sachverhalte und Randbedingungen (z. B. bereits realisierte Brandschutzmassnahmen, Effizienz der Alarmorganisation, vorhandene Redundanzen im Informatikbereich, Art und Standort der Interventionskräfte) eine wesentliche Rolle zur Beantwortung der Frage, ob spezielle Notfallmassnahmen notwendig sind, um die generelle Zielsetzung erfüllen zu können.

Adresse der Autoren:
Bruno Umiker, dipl. El.-Ing. ETH, lic. phil., Alfred Peer, Wirtschaftsinformatiker, und *Paul A. Truttmann,* Dr. sc. nat. ETH, lic. phil., Walter Umiker+Co. AG, Consultants, Forchstrasse 301, 8029 Zürich.

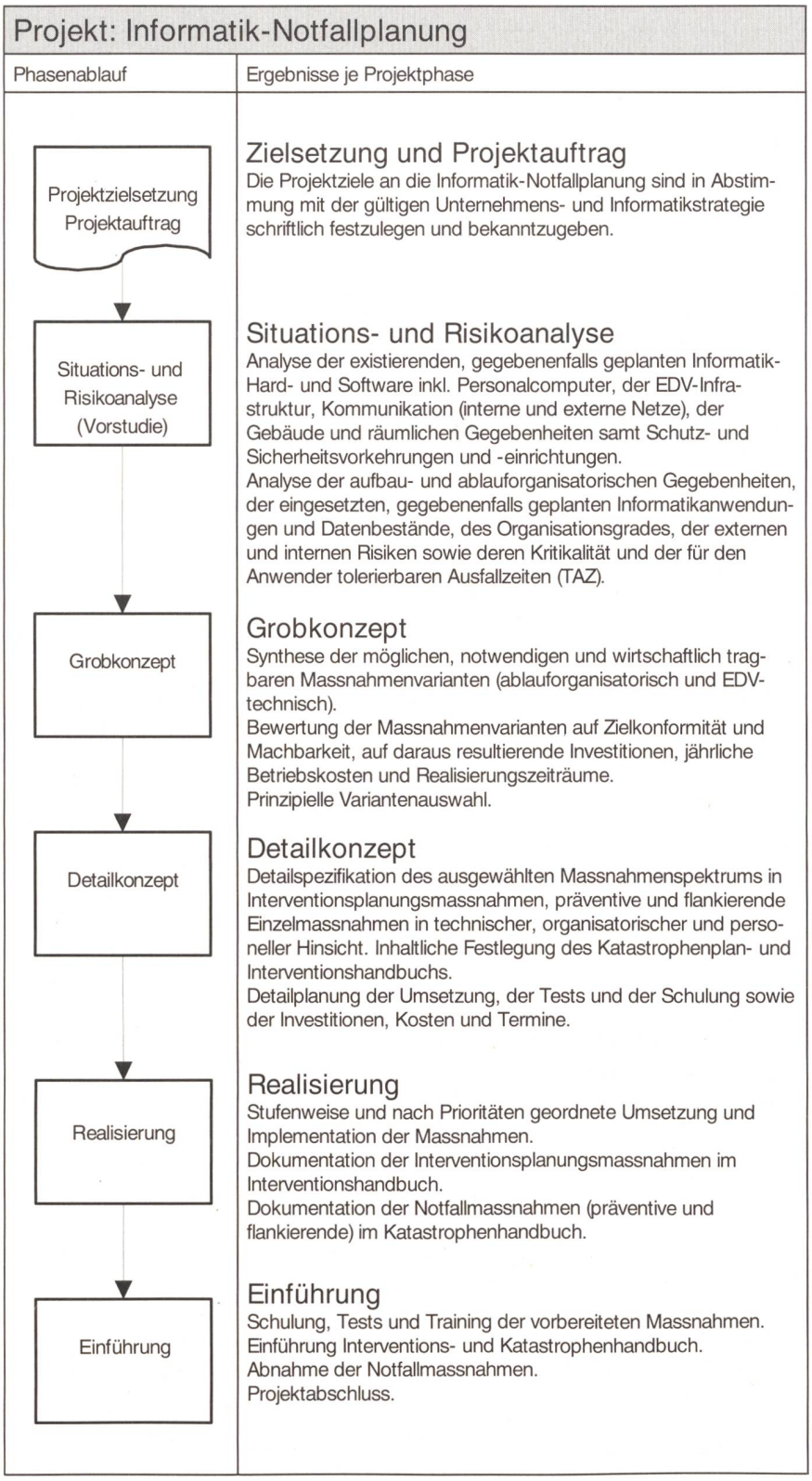

Bild 2 Projekt einer Informatik-Notfallplanung

Als weiteres wichtiges Kriterium gilt: Wie lange darf aus der Sicht des Anwenders die Informatikdienstleistung ausfallen, bevor an seinem Arbeitsplatz ernsthafte Probleme auftreten? Aufgrund der Tiefe der möglichen Störungen und Auswirkungen unterscheiden wir die vier verschiedenen Ausfallzeiten TAZ 1–4.

Für das Erheben der *notwendigen Informationen* in den Unternehmensbereichen und Fachabteilungen sowie in der Informatikabteilung selbst werden einerseits die bestehenden Abläufe analysiert und andererseits mittels Interviews die Führungskräfte aller Stufen befragt. Dazu empfiehlt sich ein Interviewleitfaden, welcher nicht nur die vorhandene Hard- und Software (inkl. Infrastruktur, Kommunikation, Schutz- und Sicherheitseinrichtungen), die Informatikanwendungen und Datenbestände erfasst, sondern auch ausführliche Fragen über die Rahmenbedingungen zur bestehenden Informatikumgebung sowie deren Anforderungen und Risiken aus der Sicht der Benutzer enthält.

Den Äusserungen und Ansichten der Befragten zur Risikosituation in ihrem Arbeitsbereich und im Gesamtunternehmen ist erfahrungsgemäss mit einiger berechtigter Skepsis zu begegnen. Einerseits hat jeder Mensch seine subjektive Sicht der Realität, andererseits spielen aber auch verschiedene tiefenpsychologische Abwehrmechanismen (wie Verdrängung, Projektion, Rationalisieren usw.) eine grosse Rolle, so dass die Aussagen kritisch hinterfragt und überprüft werden müssen. In diesem Zusammenhang ist auf das «Risky-shift»-Phänomen nach John A. F. Stoner hinzuweisen, wonach die Mitarbeiter Risiken, die sie eigentlich kennen müssten, verdrängen, weil sie nicht der Gruppenmeinung entsprechen, die im Betrieb vorherrscht.

Eine vollständige, ihren Namen verdienende Situations- und Risikoanalyse sollte sich allerdings auch eingehend mit ergonomischen und soziopsychologischen Risikofaktoren befassen. Hohe Frustrationsmomente am Arbeitsplatz (z. B. durch Mobbing) können ebenso Auslöser für eine Informatikkatastrophe sein wie etwa eine unachtsam weggeworfene Zigarette.

Dies erscheint uns jedenfalls wichtiger als eine hypothetische mathematische Analyse über die Frage, innerhalb welcher Zeitspanne ein bestimmtes Risiko eintreten könnte, denn einerseits fehlt abgesichertes und relevantes statistisches Material und andererseits spielt die Wahrscheinlichkeit im Einzelfall des Unternehmens keine Rolle mehr, wenn der Katastrophenfall tatsächlich eingetreten ist. (Der statistische Risikoausgleich ist schwergewichtig nur für versicherungsmathematische Überlegungen relevant.)

Welches sind Zweck und Ergebnisse des Grobkonzepts zur Informatik-Notfallplanung?

Zweck des Notfall-Grobkonzepts ist, das mögliche Massnahmenspektrum aufzuzeigen, indem die in der Situations- und Risikoanalyse bereits angedachten Lösungsansätze konkretisiert werden, sodann Entscheidungsgrundlagen zur Festlegung der notwendigen und wirtschaftlich tragbaren Massnahmenvariante(n) zu schaffen und schliesslich die prinzipiellen Abläufe

Tolerierbare Ausfallzeiten (TAZ) nach Kritikalitätsstufen	
TAZ 1 (Ausfallzeit 1)	Zeitspanne, während der trotz Totalausfall der Informatikdienstleistungen ohne wesentliche Behinderungen sämtliche permanenten Aufgaben noch ohne vorbereitete Notfallmassnahmen vollständig erledigt werden können.
TAZ 2	Zeitspanne, während der trotz Totalausfall der Informatikdienstleistungen unter Inkaufnahme eines kurzfristigen, persönlich gerade noch bewältigbaren Mehraufwandes sämtliche wesentlichen permanenten Aufgaben noch ohne vorbereitete Notfallmassnahmen erledigt werden können.
TAZ 3	Zeitspanne, während der trotz Totalausfall der Informatikdienstleistungen unter Inkaufnahme eines persönlich gerade noch bewältigbaren Mehraufwandes und unter Zuhilfenahme von vorbereiteten Notfallmassnahmen die wesentlichen permanenten Aufgaben erledigt werden können.
TAZ 4	Zeitspanne, während der trotz Totalausfall der Informatikdienstleistungen unter Zuhilfenahme von vorbereiteten organisatorischen und personellen Notfallmassnahmen die Aufgaben gerade noch erledigt werden können, bevor wesentliche Einbrüche in den Abläufen der Administration und/oder des Betriebs auftreten, welche eine Gewährleistung der Produktion, der Versorgung der Märkte oder der Liquidität des Unternehmens in Frage stellen.

Tabelle IV

vom Eintritt bis zur Bewältigung eines Katastrophenfalls, adaptiert auf die effektiven Verhältnisse des Unternehmens, transparent zu machen.

Voraussetzungen und Rahmenbedingungen zum Grobkonzept sind, dass die Resultate und Erkenntnisse aus der Situations- und Risikoanalyse sorgfältig überprüft und beurteilt worden sind, im besonderen die abteilungs- und anwendungsbezogen tolerierbaren Ausfallzeiten und deren Auswirkungen sowie die bestehende Informatik (Hardware, Software, Infrastruktur, Kommunikationseinrichtungen, PC-/IDV-Netzwerke, Ablauforganisation) und die bereits vorhandenen Sicherheitsvorkehrungen und -einrichtungen.

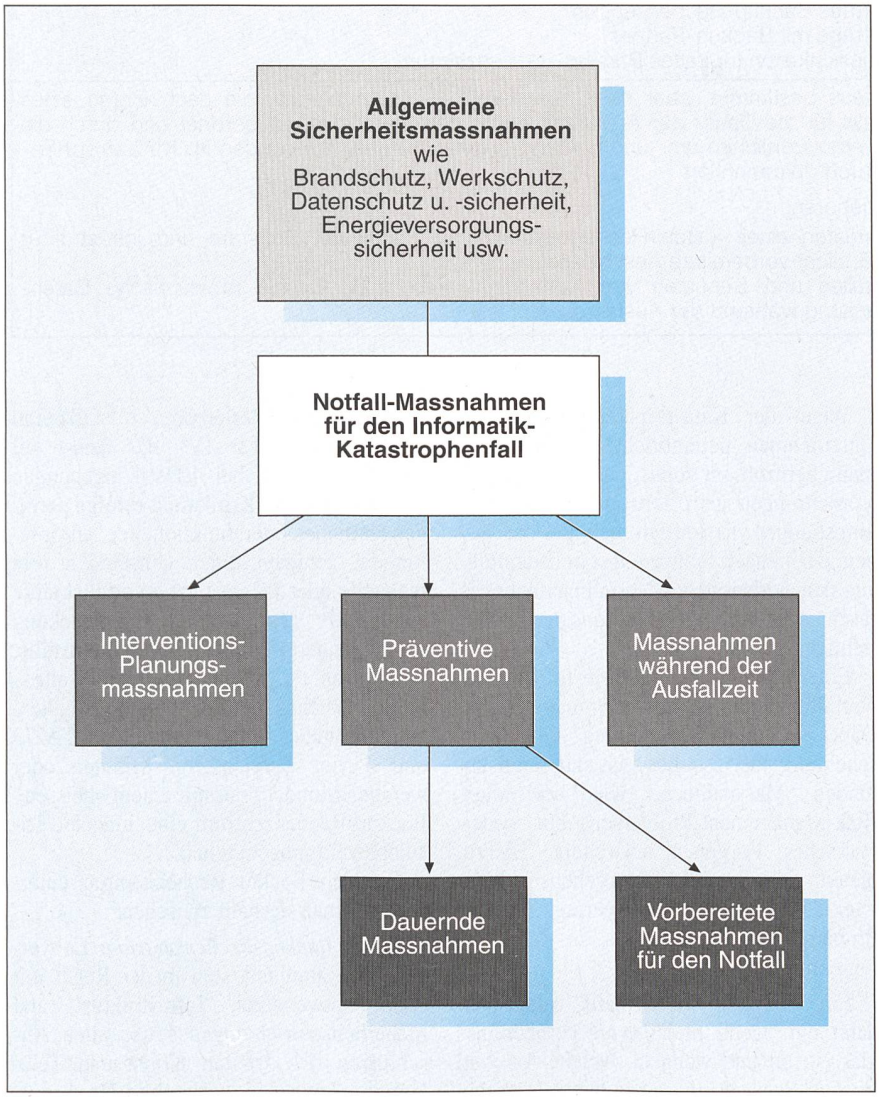

Bild 3 Notfallmassnahmen

Im Grobkonzept der Informatik-Notfallplanung sind darzustellen:

- die möglichen Massnahmenvarianten und deren Wirksamkeit
- die daraus resultierenden Investitionen, Kosten und internen Aufwendungen sowie die voraussichtlichen Realisierungszeiträume
- der Projektaufwand und der Terminplan für die Phasen Detailkonzept, Realisierung und Einführung

Welche Arten von Massnahmen für den Katastrophenfall gibt es?

Es ist grundsätzlich zwischen zwei Hauptgruppen von Massnahmen zu unterscheiden, nämlich zwischen primär den *allgemeinen vorbeugenden Sicherheitsmassnahmen* für den EDV-Bereich, die den Zweck verfolgen, den Eintritt von Schäden zu verhindern bzw. Schadenfälle nach Möglichkeit zu begrenzen, und sekundär den *Notfallmassnahmen für den Katastrophenfall,* die bei einem eingetretenen Katastrophenfall die Auswirkungen des Schadens so gering wie möglich halten sollen.

Es wird davon ausgegangen, dass die allgemeinen Sicherheitsmassnahmen in der heutigen Zeit zum Standard einer Informatik gehören und grösstenteils vorhanden sind. Sie werden in diesem Bericht nicht weiter behandelt. Sie sind jedoch im Rahmen der Informatik-Notfallplanung zu überprüfen. Festgestellte Schwachstellen müssen beseitigt werden.

Beurteilungskriterien für die Bewertung von Massnahmen (Alternativen)		
Kriterien	Gewicht	Erklärung, Bemerkungen
Zielerreichung	sehr hoch	Wird die Zielsetzung gemäss Auftrag zur Notfallplanung durch die Massnahmenvariante erfüllt?
• Produktion gewährleisten		
• Versorgung der Märkte		
• Liquidität sicherstellen		
Tolerierbare Ausfallzeiten	hoch	Deckt die Massnahme die tolerierbare Ausfallzeit ab?
• Ausfallzeit 4, bis Kollaps der Abläufe		
Risiko des Systemkollapses		
Machbarkeit der Massnahme	sehr hoch	Ist die Massnahmenvariante überhaupt realisierbar?
• Informatik-technisch		
• ablauforganisatorisch		
• personell (benutzerseitig)		
• personell (Informatikabteilung)		
Flankierende Massnahmen	mittel	Welchen Umfang an zusätzlichen flankierenden Massnahmen braucht die Massnahmenvariante?
• Umfang flankierender Massnahmen		
Wirksamkeit der Massnahme	hoch	Wie hoch ist der Wirkungsgrad einer Massnahme in einem Katastrophenfall und während der gesamten Ausfallzeit zu beurteilen?
• für das Gesamtunternehmen		
• für die einzelnen Ressorts/Abteilungen		
Realisierungszeitraum	hoch	In welchem Zeitabschnitt kann die Massnahmenvariante realistisch realisiert werden, d. h. ab wann ist die erwartete Sicherheit gewährleistet?
• frühester Beginn		
• spätestes Ende		
Realisierungskosten	hoch	Welche einmaligen und wiederkehrenden Investitionen und Kosten fallen für die Realisierung der Massnahmen im einzelnen und je Massnahmenvariante an?
• Investition Basismassnahmen		
• flankierende Massnahmen		
• Total Investitionen		
• jährliche Kosten der Basismassnahmen		
• jährliche Kosten flankierende Massnahmen		
• Total jährliche Kosten		
Betriebsinterner Aufwand	hoch	Welcher interne Aufwand muss durch die Mitarbeiter für die Realisierung der Massnahme aufgewendet werden (siehe dazu auch Machbarkeit)?
• einmalig		
• jährlich wiederkehrend		

Tabelle VI

eigene Rechenzentrum mit vollständiger Hardware, Software und Infrastruktur wieder aufgebaut und betriebsbereit ist. Falls dieser Wiederaufbau infolge einer sehr hohen Schadensintensität länger dauert als die vereinbarte maximale Nutzungsdauer im Backup-Rechenzentrum, muss als weitere Übergangslösung ein Ausweich-Rechenzentrum bezogen werden. In der Praxis muss davon ausgegangen werden, dass ein Backup-Rechenzentrum nicht länger als zwölf Wochen vertraglich reserviert werden kann.

3. Nachdem das eigene oder das Ausweich-Rechenzentrum betriebsbereit ist und sämtliche Hard- und Softwarefunktionen sowie alle Einrichtungen getestet und abgenommen sind, kann zum Normalbetrieb zurückgekehrt werden. Im einzelnen handelt es sich um die in der Tabelle VII vorgestellten Aktivitäten.

Worin liegt der Gewinn eines Informatik-Notfallkonzepts?

Der vor allem in mittelgrossen Unternehmen immer wieder gehörten Auffassung, wonach die meisten unternehmerischen Funktionsbereiche, selbst im Falle einer Grosskatastrophe, ablauforganisatorisch und EDV-mässig über längere Zeit hinweg mit manuellen und gar «ad hoc inszenierten» Notfallmassnahmen problemlos und ohne grosse Kostenfolgen weiter funktionieren würden, müssen wir aufgrund unserer Untersuchungen, unserer Erfahrungen und der Einschätzung der weiteren Entwicklung im Risikobereich entschieden entgegentreten. Generell kann festgestellt werden, dass mit zunehmender Beschleunigung und Optimierung von Geschäftsprozessen durch computergestützte und vernetzte Informationssysteme die Kritikalität für die einzelnen Abläufe und die Auswirkung von Katastrophenfällen für das Unternehmen stetig anwachsen. Mit einer vorausschauenden, auf präventiven Massnahmen zur möglichst geordneten und situationsgerechten Bewältigung einer eingetretenen Katastrophe und ihrer Auswirkungen ausgerichteten Notfallplanung für die Informatik kann das sonst unvermeidliche Chaos vermieden

Ablaufphasen der Katastrophenbewältigung	
Ingangsetzen und Durchführen der Notfallmassnahmen	Sobald der Informatik-Krisenstab beschlussfähig ist und die Lage beurteilt hat, leitet er die notwendigen Aktivitäten zur Krisenbewältigung ein:
Anordnen der Notfallmassnahmen (60)	Die anlässlich der Krisenstabsitzung beschlossenen Massnahmen müssen, wenn möglich schriftlich, angeordnet und unter Zuhilfenahme der entsprechenden Dokumentationen im Katastrophenhandbuch umgesetzt werden.
Initialisieren Backup-Betrieb (61/62)	Zur Initialisierung des Backup-Betriebes sind folgende Aktivitäten notwendig: • sofortiges Anmelden beim Backup-Vertragspartner • die im Katastrophenausweichplan (Notfallablauforganisation) festgelegten Arbeiten, wie Zusammenstellen der verfügbaren aktuellen Daten- und Programmsicherungen, Operatoranweisungen, Outputformulare usw.
Vorbereiten/Aufbau Backup-Betrieb (63)	• Organisieren der Transporte zum und vom Backup-Rechenzentrum • Aufbau der Kommunikation zwischen Backup-Rechenzentrum, Endbenutzern und gegebenenfalls Krisenstab • Einrichten der Informatik- und gegebenenfalls Benutzerarbeitsplätze im Backup-Rechenzentrum • Sicherstellen oder Wiederaufbau der Telekommunikationseinrichtungen • Installation und Hochfahren der Systemumgebung, der Kommunikations- und der Anwendungssoftware • Laden der Datensicherungen (Aufbau der Datenbank)
Flankierende Massnahmen zum Backup-Rechenzentrum	Folgende flankierende Notfallmassnahmen können notwendig sein: • Eigene manuelle oder PC-gestützte Notfallmassnahmen, welche dazu dienen, die Abläufe in der Informatikabteilung aufrechtzuerhalten • Manuelle und PC-gestützte Notfallabläufe bei den Benutzern, um bei sehr kurzen tolerierbaren Ausfallzeiten (TAZ 3 und 4) die Zeitspanne zwischen Katastrophenereignis und Aufnahme des Backup-Betriebs überbrücken zu können, gemäss Dokumentationen im Katastrophenhandbuch • Sofern notwendig, Wiederaufbau/Wiederinbetriebnahme der PC-Netzwerke, zerstörter Kommunikationseinrichtungen (Datenleitungen, DFÜ-Controller, Modems)
Aufnahme Backup-Betrieb (72)	Nachdem nun das Backup-Rechenzentrum betriebsbereit ist, müssen • zuerst die beim Eintritt des Katastrophenereignisses verlorengegangenen Daten und Arbeitsschritte nachgeholt (70), • anschliessend die während des RZ-Betriebsunterbruchs ausgefallene EDV-Produktion (71) aufgeholt werden. Danach kann der eigentliche Backup-Betrieb (72) aufgenommen werden
Wiederaufbau des eigenen oder eines Ausweich-Rechenzentrums	Sobald der Krisenstab Informatik von den Belastungen durch den Aufbau und die Inbetriebnahme des Backup-Betriebs entlastet ist, muss unverzüglich eine Situationsanalyse über die gesamte Informatik des Unternehmens durchgeführt und darüber entschieden werden, wie und wann der Normalbetrieb der Informatikaktivitäten wieder realisiert werden kann (80).
	Zu den prinzipiellen Schritten gehören: • Planung des Wiederaufbaus des Gebäudes oder der betroffenen Gebäudeteile, RZ-Räume und Infrastruktur (81) • Planung Ersatz der betroffenen Hardware, Software und Kommunikationseinrichtungen (81) • Realisierung (Bauen, Einrichten, Installation und Implementation HW/SW, Testen HW/SW/Infrastruktur und Anwendungen) (82/83) • Anpassen der Informatik-internen Ablauforganisation an die gegebenenfalls geänderten Bedingungen (84) • Restart des Rechenzentrumsbetriebs (85) (Überführen vom Backup-Rechenzentrumsbetrieb)

Tabelle VII

werden. Schliesslich darf ein weiterer wesentlicher Aspekt nicht übersehen werden: In einem Katastrophenfall werden das Management und die Mitarbeiter aller Stufen mit zusätzlichen, ungewohnten und ausserordentlichen Problemen und Belastungen konfrontiert. Das Unternehmen und seine Verantwortlichen sind deshalb in solchen Situationen besonders darauf angewiesen, dass wenigstens die Informationsverarbeitung (Informatik) möglichst reibungslos weiter funktioniert.

Le concept d'urgence informatique en tant qu'élément de la planification d'urgence

A la première partie de cet article (Bulletin ASE/UCS 3/96), on a pu voir dans quelle mesure les entreprises sont devenues tributaires de l'informatique et combien les conséquences peuvent être graves si l'on omet de prendre des mesures adéquates. Cette seconde partie montre comment ces mesures peuvent se présenter sous forme de concept d'urgence en informatique.