



Verfügbarkeit von Information: ein Praxisbericht

Hannes Lubich

Chief Security Officer

Julius Bär Gruppe



Motivation

Confidentiality

Integrity

Availability
(Information und
deren Bearbeitung)

Authenticity

Obligation



Inhalt

- ◆ Bedrohungen der Verfügbarkeit
- ◆ Ein Katalog von Gegenmassnahmen
 - Technische Massnahmen
 - Organisatorische und rechtliche Massnahmen
 - Personelle und kulturelle Massnahmen
- ◆ Wirtschaftlichkeitsbetrachtungen
- ◆ Ausblick




Bedrohungen der Verfügbarkeit

- ◆ **Überlast** (durch Angriff, Fehlmanipulation oder unerwartete Attraktivität des Angebots)
 - ◆ **Verweigerung** des Zugangs (Bsp. Online-Banking mit Zugangssperre nach drei Fehlversuchen)
 - ◆ Physische oder logische Verfälschung oder **Zerstörung** (Virus, Brand, Manipulation etc.)
- Bedrohungen können intendiert oder nicht intendiert sein
- Bedrohungen haben interne und externe Quellen



Technische Massnahmen

- ◆ Redundanz **innerhalb** von Systemen (Bsp. RAID-Disks, Serverfarm, Netzverbund)
 - ◆ Redundanz **zwischen** Systemen (Bsp. Backup, Ersatz-Geräte)
 - ◆ Redundanz bezüglich **Standorten** (Bsp. mehrere Serverräume, mehrere Standorte)
- Es müssen physische (Elementarschaden) und logische Probleme (Manipulation, Y2K, etc.) bewältigt werden können.



Organisatorische und rechtliche Massnahmen

- ◆ Fähigkeit zu Prävention / Erkennung:
 - Systematische Risikoerkennung und –bewertung
 - Entscheid zum Umgang mit erkannten Risiken (z.B. Abwehren, Abschwächen, Abwälzen, Akzeptieren)
 - Prüfkriterien für Projekte, Beschaffungen, Betrieb
 - Verträge mit Lieferanten, Partnern, Kunden etc.
- ◆ Fähigkeit zur Bewältigung von Problemen:
 - Ausgebildeter Krisenstab und vorbereitetes Material
 - Tests, Übungen, Notfallpläne (inkl. Personal etc.)
 - Fähigkeit zu Agilität und Improvisation
- ◆ Nachweisbarkeit der Massnahmen gegenüber „stake holders“ und Dritten (z.B. Öffentlichkeit)

Beispiel: Risikoklassen



Risikoklasse	Risikogewicht	Personenschaden	Finanzieller Schaden	Image Schaden	Unterbrüche	BRP-Art
Katastrophe	4	Todesfälle	Grössenordnung Eigenmittel	Ruf der Bank zerstört, Bewilligung zu Geschäftstätigkeit entzogen	Gesamtunterbruch ganze Bank > 1 Woche	Gruppenweiter BRP
Grossrisiko	3	Schwerverletzte	Grössenordnung Dividende	Ruf der Bank nachhaltig angeschlagen	Gesamtunterbruch > 24 Stunden und < 1 Woche	Lokaler BRP
Mittleres Risiko	2	Leichtverletzte	< 1 Mio.	Kritik in den Medien	Gesamtunterbruch < 24 Stunden, Teilunterbrüche < 1 Woche	Kein BRP (normales Incident Vorgehen)
Normalrisiko	1	keine ernsthaften gesundheitlichen Schäden	< 100'000 CHF	Erwähnung in den Medien	Teilunterbrüche < 24 Stunden	Kein BRP (normales Incident Vorgehen)
Bagatellrisiko	0	keine Schäden mit Arbeitsausfall	im Rahmen des Selbst- behaltes von Ver- sicherungen	kein Medienkommentar	Teilunterbruch < 8 Stunden ohne Gefährdung Tagfertigkeit oder Abschluss von Geschäften	Kein BRP (normales Incident Vorgehen)



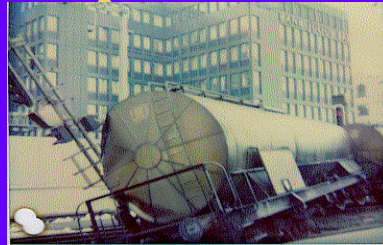
Personelle und kulturelle Massnahmen

- ◆ Bewusstseinsbildung bei potentiell Betroffenen (Mitarbeiter, Kunden, Lieferanten, etc.)
- ◆ Bewusstseinsbildung bei den Geldgebern, bes. für präventive Massnahmen

→ Zu beachten:

- Der „Risk Appetite“ ist kulturell sehr verschoben
- Ist lange Zeit „nichts passiert“, sinkt das Risikobewusstsein stark ab
- Der Nachweis verhinderter Schäden ist kaum führbar
- „Versicherungen“ bzw. Kosten für den Notfall geniessen kein hohes Wertschöpfungs-Ansehen

Beispiel: Krisenstabs-Übung



27.11.90 / 0940

im Krisenfall: Auftrag für den diensthabenden Mitarbeiter im Sicherheitsdienst

1. Übergeben Sie dem Krisenmanager die Karte 'Informationen und Auftrag für den Krisenmanager'.
2. Fragen Sie den Krisenmanager an welchem Standort er das Krisenlagezentrum einrichten wird.
3. Bitten Sie den Krisenmanager, dass er Ihnen seine Telefonnummer bei Ankunft am gewählten Standort mitteilt.
4. Übergeben Sie dem Krisenmanager ein Foto des Krisenlagezentrums.
5. Übergeben Sie jedem eintreffenden Krisenstabsmitglied ein Exemplar: 'Informationsblatt für Mitglieder des Krisenstabs'.
6. Geben Sie den Mitgliedern des Krisenstabs den vom Krisenmanager festgelegten Standort des Krisenlagezentrums bekannt.

Informationen und Auftrag für den Krisenmanager

Sie sind Krisenmanager! Bewahren Sie Ruhe und tätigen Sie der Reihe nach folgende Aktivitäten:

1. Lassen Sie sich vom Wächter in der Sicherheitszentrale oder vom Pikettendienst über den bisherigen Verlauf genau orientieren. Stellen Sie insbesondere fest, wer bereits alarmiert und welche Sofortmassnahmen in die Wege geleitet wurden.
2. Teilen Sie dem Sicherheitsdienst mit, welches Büro Sie als Krisenlagezentrum definiert haben und wie Sie erreichbar sind.
3. Beauftragen Sie den Sicherheitsdienst Ihre Entscheidung der Lage am Ge-

Informationsblatt für Mitglieder des Krisenstabs

Sie sind Krisenstabsmitglied! Bewahren Sie Ruhe und tätigen Sie der Reihe nach folgende Aktivitäten:

Erkundigen Sie sich beim Sicherheitsdienst, für welchen Standort sich der Krisenmanager entschieden hat.

- Begeben Sie sich unverzüglich zum Standort des Krisenmanagers und melden Sie sich persönlich bei ihm.
- Beginnen Sie mit der Arbeit gemäss Weisungen des Krisenmanagers.



Wirtschaftlichkeit I

- ◆ Methode 1: keine Massnahmen treffen, Rückstellungen für den Ernstfall
 - Geld bleibt blockiert, Umfang der Rückstellung unklar, ggf. regulatorisch nicht akzeptabel
- ◆ Methode 2: Abwälzen der Risiken (Versicherung, Geschäftsbedingungen, etc)
 - Versicherungen teilweise „Kunsth Handwerk“ oder Erfüllungsrisiko, ggf. für Kunden nicht akzeptabel



Wirtschaftlichkeit II

- ◆ Methode 3: technisch/organisatorische Prävention
 - Selektiv, Nutzung im Normalfall möglich (Load Balancing, Einsatz von Personal als Test-Team usw.)
- ◆ Methode 4: Volle (ggf. externe) Redundanz
 - Hohe Fixkosten, benötigt konsequente Umsetzung auch bei knapper Finanzlage



Ausblick

- ◆ **Regulatoren** und Rating Agencies werden aufmerksam (besonders nach dem 11. Sept. 01)
 - ◆ Die **Kunden** werden aufmerksam (ggf. Wettbewerbsvorteil für Dienstleister)
 - ◆ Der **Staat** wird aufmerksam (siehe Stiftung Infosurance im Umfeld des Bundesamtes für wirtschaftliche Landesversorgung)
-
- Generelle Vorgaben / Methoden fehlen
 - Spezifische Massnahmen pro Unternehmen