ETAT DE FRIBOURG
STAAT FREIBURG

Organe cantonal de conduite OCC
Kantonales Führungsorgan KFO

Protection de la population
Bevölkerungsschutz

Zeughausstrasse 16, Postfach 185, 1705 Freiburg

T +41 26 305 30 30, F +41 26 305 30 04

Kantonaler Einsatzplan

—

Ausfall der Informationsnetze

—

Direction de la sécurité et de la justice **DSJ**
Sicherheits- und Justizdirektion **SJD**

ETAT DE FRIBOURG
STAAT FREIBURG

Organe cantonal de conduite OCC
Kantonales Führungsorgan KFO

Protection de la population
Bevölkerungsschutz

Zeughausstrasse 16, Postfach 185, 1705 Freiburg
T +41 26 305 30 30, F +41 26 305 30 04
www.fr.ch/absm

Freiburg, den 25. April 2017

Ausfall der Informationsnetze
—
Einsatzplan

Inhaltsverzeichnis

1. Einführung 4
1.1. Grundlagen 4
1.2. Ziele des Plans 4
1.3. Abgrenzungen 4
1.4. Beziehung mit andern Einsatzplänen 5
1.5. Definitionen 6
1.5.1. Ausfall der Informationsnetze 6
1.5.2. Ausser Betrieb 6
1.5.3. Teilweise funktionstüchtig 7
1.5.4. Identifikation 7
1.5.5. Falschinformation 7
1.5.6. Vektor 7
1.5.7. Information 7
1.5.8. Produktionssysteme 7
1.5.9. Transportmittel 7
1.5.10. Sender/Empfänger 7
1.5.11. Gefahrenstufe 7
1.6. Beschreibung 8
1.6.1. Thema 8
1.6.2. Hauptelemente 8
1.7. Akteure 9
1.8. Struktur des Einsatzplans 10
2. Führungsprinzipien 10
2.1. Achsen 10
2.1.1. Überwachung, Erkennung und Analyse 10
2.1.2. Unmöglichkeit zu kommunizieren 11
2.2. Verbindungen zwischen Akteuren 11
2.3. Zeitliche Aspekte 11
2.3.1. Zulässige Dauer der Nichtverfügbarkeit 11
2.3.2. Notwendige Dauer der Inbetriebsetzung 12
2.4. Auslöser 12
3. Aufträge 13
3.1. Lösungen 13
3.2. Matrix der Verantwortlichkeiten 13
3.3. Allgemeine Aufgaben 13
3.3.1. Staatsrat 13
3.3.2. KFO 13
3.3.3. GFO 14
3.3.4. Polizei 14

3.3.5. Feuerwehr 14
3.3.6. SFO 14
3.3.7. ZS 14
3.3.8. Infozelle 14
3.3.9. ITA 15
3.3.10. Medien 15
3.3.11. Bereitsteller des Zugangs / Telefonbetreiber 15
3.3.12. KI-Betreiber 15
3.3.13. Bund 16
3.4. Ereignisführungsplanung 16
4. Besondere Bestimmungen 17
4.1. Zusammenarbeit 17
4.1.1. Intern im Kanton 17
4.1.2. Ausserhalb des Kantons 17
4.2. Informationsbeschaffung 17
4.3. Information 18
4.3.1. Ausserhalb des Ereignisses 18
4.3.2. Im Ereignis 18
4.4. Kommunikation 18
4.5. Vertraulichkeit 19
4.6. Verhaltensempfehlungen 19
4.7. Zwingende Massnahmen 19
4.8. Tests 19
4.9. Finanzierung 19
4.9.1. Tests und Vorbereitungsmassnahmen 19
4.9.2. Beim Einsatz 19
5. Schlussbestimmungen 19

Abbildungsverzeichnis

Abbildung 1: Darstellung der Beziehung mit andern Einsatzplänen 6
Abbildung 2: Transversalität des Einsatzplans 6
Abbildung 3: Vektortypen 9
Abbildung 4: Kommunikationsfluss zwischen den Akteuren 11
Abbildung 5: Zufflov-Pyramide 12
Abbildung 6: Planungsebenen 16

Abkürzungsverzeichnis

BCM/BCP	Business Continuity Management / Business Continuity Plan[1]
CASU144	Sanitätsnotrufzentrale (SNZ) 144
EAZ	Einsatz- und Alarmzentrale (112-117-118)
Info-Zelle	Informationszelle
Lage-Zelle	Nachrichtenzelle, Info zur Lage
FinD	Finanzdirektion
KFS	Kantonaler Führungsstab

[1] Management / Continuity Plan

BST ABCN	Bundesführungsstab ABCN (atomar-biologisch-chemisch-natürlich)
KI	Kritische Infrastruktur
MELANI	Melde- und Analysestelle Informationssicherung
KFO	Kantonales Führungsorgan
SFO	Sanitätsdienstliches Führungsorgan
ORCAF	Katastrophen-Organisation Freiburg
GFO	Kommunales Führungsorgan
ZS	Zivilschutz
ITA	Amt für Informatik und Telekommunikation
Spez.	Spezialist(en)
IKT	Informations- und Kommunikationstechnologie

1. Einführung[2]

Unsere moderne Gesellschaft stützt sich in grossem Umfang auf IKT-Systeme (Informations- und Kommunikationstechnologie) – im vorliegenden Einsatzplan «Informationsnetze» genannt (siehe auch Unterkapitel 1.5.1). Sozusagen alle Produktions- und Kommunikationssysteme basieren auf Informatiksystemen oder benutzen Informatiksysteme; es ist selten, noch ein System zu finden, das nur mechanisch funktioniert. Überdies können die Medien ohne Informatik die Bevölkerung nicht mehr informieren und die Bevölkerung kann ohne Informatiksysteme nicht mehr kommunizieren.

Bei einem Ausfall dieser Informationsnetze ist notwendig, Massnahmen zum Schutz der Bevölkerung und deren Existenzgrundlagen zu treffen. Bei einem Ereignis sind konkrete Führungsmassnahmen zu treffen, um das Aufrechterhalten der Informationsnetze sicherzustellen.

Es ist daher die Aufgabe des vorliegenden Einsatzplans, die notwendigen Massnahmen vor und während eines solchen Ereignisses zu definieren.

1.1. Grundlagen

> Radio- und Fernsehverordnung (RTVV, SR 784.401) vom 9. März 2007
> Gesetz vom 13. Dezember 2007 über den Bevölkerungsschutz (BevSG, BDLF 52.2)
> Gesetz vom 9. September 2009 über die Information und den Zugang zu Dokumenten (InfoG, RSD 17.5)
> Verordnung vom 14. März über die Kommunikation bei ausserordentlichen Ereignissen (RS 52.24)
> Plan ROUGE

1.2. Ziele des Plans

Dieser Einsatzplan dient dazu:
> Das gleiche Informationsniveau unter allen Akteuren beizubehalten
> Eine solche Situation zu erkennen und zu bezeichnen
> Sich vorzubereiten, um für ein solches Ereignis gewappnet zu sein
> Dem Staatsrat und den Führungsorganen die für die Ereignisführung erforderlichen Elemente bereitzustellen
> Die Aufgaben der Partner zu definieren
> Die Auswirkungen einzudämmen
> Die für die Bewältigung eines Ausfalls der Informationsnetze notwendigen Massnahmen und Mittel zu definieren
> Die Zusammenarbeit mit den Unternehmen und vor allem mit den kritischen Infrastrukturen zu definieren

1.3. Abgrenzungen

> Der vorliegende Einsatzplan behandelt keine Präventionsmassnahmen.

> Der vorliegende Einsatzplan deckt lediglich den kantonalen Teil der Ereignisbehandlung ab, stellt aber den Link zum Bund her.

[2] Bei Abweichungen zwischen der deutschen und der französischen Fassung ist die Französische massgebend.

- Der Ausfall der Informatiksysteme muss durch die Betreiber/Besitzer, d. h. die Unternehmen geregelt werden. Sie sind nicht Gegenstand dieses Einsatzplanes.
- Die Suche nach der Ursache eines Ausfalls wird für den Schutz der Bevölkerung und ihrer Existenzgrundlagen als nicht wichtig erachtet. Sie ist eng mit der Lösung der Ausfälle der Informatiksysteme verbunden, die Sache der Unternehmen ist; die Suche nach der Ursache ist daher nicht Teil dieses Einsatzplans.
- Die indirekten Auswirkungen eines Ausfalls der Informationsnetze (Ausfall der Elektrizität, Unterbrechung der Lebensmittelversorgung ...) sind nicht Gegenstand dieses Einsatzplanes. Sie werden entsprechend der dazu vorgesehenen Einsatzpläne (Bsp. Einsatzplan Stromversorgungsunterbruch) behandelt.
- Die staatlichen Krisenstäbe, die einen solchen Ausfall innerhalb des «Unternehmens Staat» behandeln müssen, werden wie jedes andere Unternehmen angesehen und behandelt.
  - Ein Ausfall der Informationsnetze innerhalb des Staates wird durch SITel und daher durch den Krisenstab der FinD behandelt. Dagegen wird SITel als IKT-Lieferant betrachtet, insbesondere zugunsten des KFO.
- Ein Ausfall der Kommunikation zwischen den Führungsstufen des Bundes und der Kantone (KFO/KFS) ist dank dem Projekt «Sicheres Datenverbundnetz» (SDVN) mit 99-prozentiger Sicherheit nicht mehr möglich. Wenn indessen doch ein Ausfall auftreten sollte, werden die Massnahmen der redundanten oder alternativen Kommunikation, wie in diesem Plan definiert, angewendet.

1.4. Beziehung mit andern Einsatzplänen

Dieser Einsatzplan wird offensichtlich in einer Situation aktiviert, in der die Informationssysteme ausgefallen sind.

Aber er kann auch bei anderen Ereignissen (z. B. Stromversorgungsunterbruch) verwendet werden, wenn daraus ein Ausfall der Informationsnetze resultiert. Er stellt seitdem eine gewisse Transversalität dar und seine Verwendung hängt dadurch von der Situation ab.

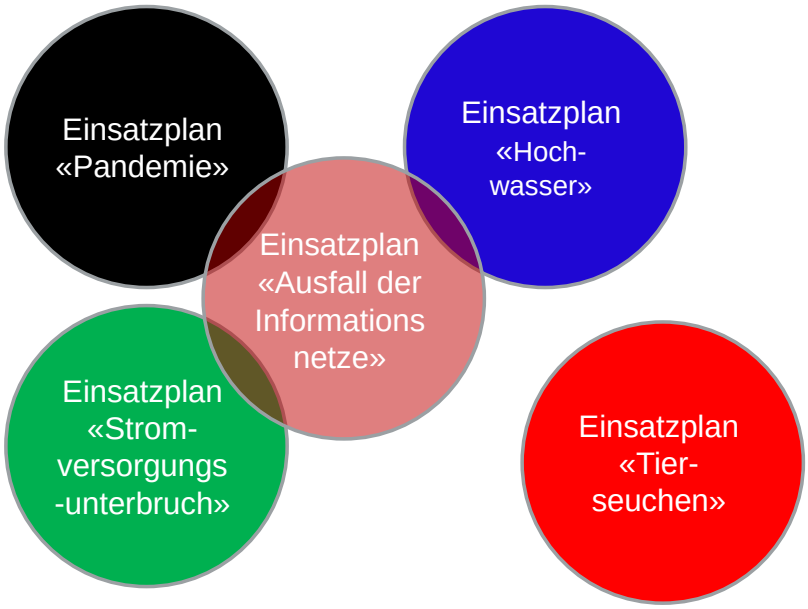

Abbildung 1: Darstellung der Beziehung mit andern Einsatzplänen

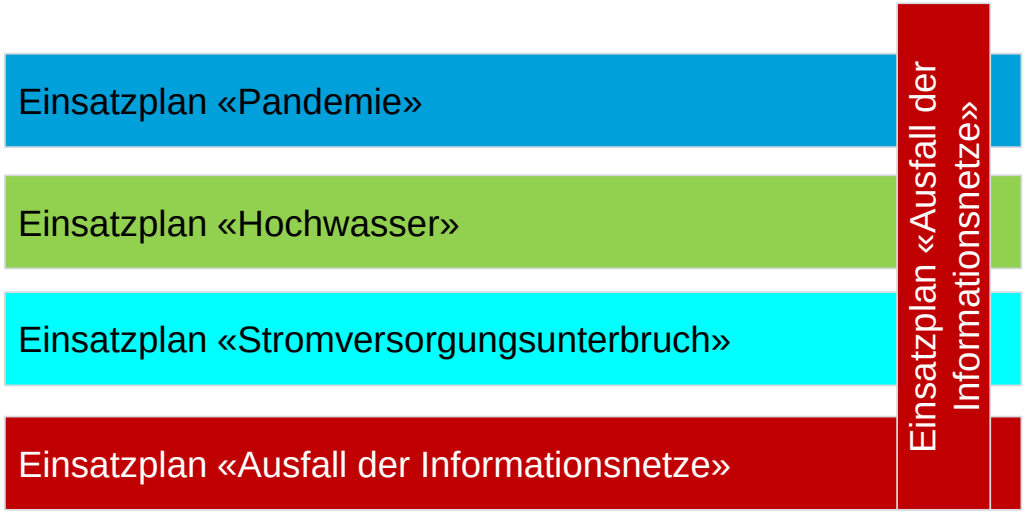

Abbildung 2: Transversalität des Einsatzplans

1.5. Definitionen

1.5.1. Ausfall der Informationsnetze

Unter Ausfall der Informationsnetze wird verstanden:
> Der Ausfall der Systeme (Produzenten, Transporteure und Sender) der **Informationsnetze**
> Der Ausfall der **Informatik**-Netze und -Systeme

1.5.2. Ausser Betrieb

Vollständige Nichtverfügbarkeit einer Maschine, eines Gerätes oder eines Systems oder eines Dienstes.

1.5.3. Teilweise funktionstüchtig

Nichtverfügbarkeit gewisser Teile einer Maschine, eines Gerätes, eines Systems oder eines Dienstes.

1.5.4. Identifikation

Operation, durch die das System ein anderes System bzw. seinen Ursprung identifiziert und nachweislich bestätigt.

1.5.5. Falschinformation

Fehlerhafte, lückenhafte, bruchstückhafte oder nicht integre Information, die durch ein System gesendet oder empfangen wird.

1.5.6. Vektor

Was als Träger für die Übertragung von Informationen dient. Unter den Vektoren werden Produktionssysteme, Transportmittel und die Sender/Empfänger verstanden.

1.5.7. Information

Die Information bezeichnet gleichzeitig die zu übermittelnde Meldung, ihr Format und ihren Inhalt.

1.5.8. Produktionssysteme

Ein Produktionssystem umfasst die Gesamtheit der untereinander verbundenen Elemente oder Untersysteme, materielle und immaterielle Güter und die Prozesse, die für die Produktion von Informationen notwendig sind.

1.5.9. Transportmittel

Die Transportmittel umfassen alle Mittel, die zur Übertragung von beliebiger Information von einem Ort zu einem andern durch Technologien wie zum Beispiel Kupferdraht, Glasfaser, Laser, Funk oder Infrarotlicht dienen.

1.5.10. Sender/Empfänger

Umfasst alle technischen, elektronischen und menschlichen Mittel, die das Senden und Empfangen von Informationen ermöglichen.

1.5.11. Gefahrenstufe

Für seine Informations- und Warnmeldungen hat MELANIE die untenstehenden Gefahrenstufen definiert:

- **Latent**: Die Bedrohung ist in der Schweiz nicht vorhanden. Sie wird jedoch dauernd beobachtet und neue Elemente können zu einer Neubewertung führen.
- **Contained**: Kritische Informationsinfrastrukturen in der Schweiz werden angegriffen. Aufgrund der getroffenen Massnahmen sind indessen keine Schäden aufgetreten.
- **Low**: Die Bedrohung betrifft die Schweiz und die Benutzer. Diese Bedrohung ist für die kritischen Infrastrukturen nur mässig.
- **Medium**: Die Bedrohung betrifft die Schweiz und hat eine starke Auswirkung auf die Benutzer und die kritischen Infrastrukturen.

> **Imminent**: Die kritischen Infrastrukturen werden gezielt so angegriffen, dass kritische Funktionen bedroht sein können.

1.6. Beschreibung

1.6.1. Thema

Aus dem Blickwinkel des Bevölkerungsschutzes hat ein Ausfall von Informatik- und IKT-Systemen – im vorliegenden Einsatzplan Informationsnetze genannt – direkt wesentliche Auswirkungen auf die interne Kommunikation der Führungsorgane und der Einsatzkräfte und auch auf die Information der Bevölkerung. Die indirekten Auswirkungen ihrerseits sind vielfältig, denn jeder Ausfall eines Systems, das für die Existenzgrundlage der Bevölkerung lebenswichtig ist, kann sich dramatisch auswirken.

Ein Ausfall dieser Informatik- und IKT-Systeme kann sich auch beträchtlich zum Beispiel auf die Nahrungsmittel- und Energieproduktion auswirken und die Bevölkerung verunsichern. Wie bei der Elektrizität ist es heute undenkbar, dass die Informationsnetze nicht verfügbar sind.

Die Verwundbarkeit dieser Informationssysteme ist nicht nur sehr gross, sondern kann auch ohne Vorwarnung plötzlich auftreten und schnell grosse Auswirkungen verursachen. Ein solcher Ausfall mit relativ schwachen Auswirkungen ist sehr wahrscheinlich, während die Wahrscheinlichkeit des Auftretens eines Ausfalls mit Auswirkungen, die den Einsatz der KFO erfordern, relativ klein ist.

Schliesslich sind diese Systeme so vernetzt, dass ein lokaler, unbedeutender Ausfall anderswo grosse Auswirkungen haben kann (Domino- oder sogar Schmetterlingseffekt[3]).

1.6.2. Hauptelemente[4]

1.6.2.1. Vektoren

Um die verschiedenen Aspekte der Informationsnetze oder der Informations- und Kommunikationstechnologie (IKT) zu behandeln, erschien es notwendig, die verschiedenen Vektoren dieser Information zu unterscheiden. So gehören zu den Vektoren der Informationsthemen:
> die **Produktionssysteme**,
> die **Transportmittel**
> und die **Sender und Empfänger**
dieser Information.

[3] Schmetterlingseffekt: Der Flügelschlag eines Schmetterlings in Brasilien kann einen Tornado in Texas auslösen
[4] Siehe auch die Definitionen unter 1.5

Abbildung 3: Vektortypen

1.6.2.2. Ausfallkategorien

Bei einem Ausfall der Informationsnetze ist es wichtig, zwischen den verschiedenen, untenstehenden Ausfallkategorien zu unterscheiden:

> **Ausser Betrieb**
> **Teilweise funktionstüchtig**
> **Falschinformationen**
> **Identifikation**

Diese Kategorien, vor allem im Rahmen der Auslöseelemente (siehe unter 2.4), erlauben, die Bedeutung des Ausfalls abzuschätzen und die geeigneten Massnahmen festzulegen.

1.7. Akteure[5]

Um einem Ausfall der Informationsnetze zu begegnen wurden verschiedene Bereiche als Akteure bezeichnet, nämlich:

> **Staatsrat**: ist für die politische Führung des Ereignisses zuständig; er trifft politische Entscheide, gibt zuhanden des KFO Weisungen aus und bewertet seine Massnahmenvorschläge.

> **KFO**: sichert durch die Koordination der Operationen auf kantonaler Ebene die kantonale operative Führung. Zu diesem Zweck wird es je nach Lage durch Spezialisten unterstützt.

> **GFO**: ist zuständig für die operative Führung auf lokaler Ebene indem es die Operationen auf Gemeindeebene koordiniert. Es erhält vom KFO die notwendigen Anweisungen.

> **Blaulichtorganisation**: umfasst die Kantonspolizei, den Feuerwehrkorps und die Einheiten des Gesundheitsbereichs[6]. Sie führt die durch das KFO getroffenen Massnahmen vor Ort aus.

---

[5]Es werden nur die Hauptakteure aufgeführt; sämtliche Akteure, die eine Aufgabe im Rahmen dieses Einsatzplans haben, sind in der Matrix der Verantwortlichkeiten aufgeführt.

- **ZS:** unterstützt einerseits die Blaulichtorganisationen bei der Gewährleistung der Nachhaltigkeit eines Einsatzes, andererseits ist er ein wichtiges Element für die Wiederherstellung des ursprünglichen Zustandes.
- **Infozelle**: stellt die Informationsverwaltung zugunsten des KFO sicher.
- **SITel**: stellt den Betrieb der Informatik- und Telefonnetze und jene der Endgeräte des Staates sicher.
- **Medien**: sie stellen sicher, dass die Bevölkerung informiert wird.[7]
- **Betreiber der IKT-Netze**: sind Teil der Betreiber der IKT-Netze, der Lieferanten des Internetzugangs und der Telefonbetreiber. Sie stellen den Betrieb der Kommunikationsnetze sicher
- **Bund**: über seine spezialisierten Instanzen stellt er die Überwachung der Informatiksituation sicher und trifft bei Bedarf Massnahmen auf Landesebene.

1.8. Struktur des Einsatzplans

Der vorliegende Hauptteil des Einsatzplans enthält die allgemeinen Elemente, um einem Ausfall der Informationsnetze zu begegnen. Er gibt insbesondere allen Akteuren Leitlinien für die Behandlung des Ereignisses sowie besondere Bestimmungen.

Die konkreten Führungselemente, insbesondere die Lösungen, die für die Bewältigung des Ereignisses anzuwenden sind, befinden sich in den Führungsdokumenten «Matrix der Verantwortlichkeiten» (siehe Anhang 1) und «Ereignisführungsplanung» (siehe Anhang 2).

2. Führungsprinzipien

2.1. Achsen

Der Einsatzplan definiert zwei Aspekte des Ausfalls der Informationsnetze, die behandelt werden müssen:

1. **Die Überwachung, die Erkennung und die Analyse**
2. **Die Unmöglichkeit zu kommunizieren** (intern und extern)

Die anderen Konsequenzen eines Ausfalls der Informationsnetze werden mithilfe der ad-hoc-Pläne behandelt (siehe Anmerkungen im Kapitel 1.3 «Abgrenzungen»).

2.1.1. Überwachung, Erkennung und Analyse

Die Überwachung, die Erkennung und die Analyse der Situation der Informationsnetze wird idealerweise mithilfe des Monitorings durchgeführt (siehe unter Kap. 2.4). Sie bilden die Grundlage, um abschätzen zu können, ob es notwendig ist, den vorliegenden Einsatzplan einzusetzen.

---

[6] Führungen durch das SFO.

[7] Diese Verpflichtung hängt von den rechtlichen Grundlagen ab, denen sie unterliegen; Bsp. Die audiovisuellen Medien unterliegen der RTVV.

2.1.2. Unmöglichkeit zu kommunizieren

Um einer Unmöglichkeit zu begegnen, innerhalb der Katastrophenorganisation des Kantons Freiburg (ORCAF), d. h. mit/zwischen den Führungsorganen und den Einsatzkräften, kommunizieren zu können, gehören zu den wichtigsten Massnahmen die Verwendung alternativer Medien, darunter zum Beispiel das Ausweichen auf andere Kommunikationsnetze oder die Verwendung alternativer Systeme.

Zur Information der Bevölkerung werden alternative Mittel wie Informationsstellen/-stände eingesetzt.

2.2. Verbindungen zwischen Akteuren

Die verschiedenen Akteure, wie sie unter 1.7 erwähnt sind, interagieren untereinander auf der Ebene des Informationsaustauschs. Jeder hat auf diese Weise eine Rolle zu spielen, damit das KFO über ein fundiertes Bild der Situation verfügt.

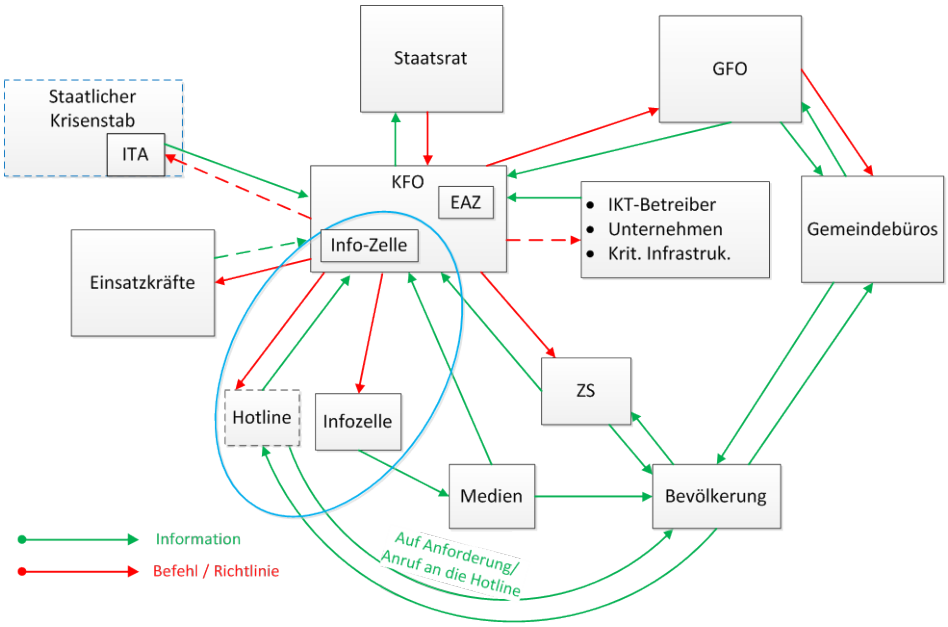

Abbildung 4: Kommunikationsfluss zwischen den Akteuren

2.3. Zeitliche Aspekte

Bei einem Ausfall der Informationsnetze ist es für die Führungsorgane wichtig,

> im Voraus die akzeptable Dauer eines Systemausfalls definiert zu haben (**zulässige Dauer der Nichtverfügbarkeit**)
> die **notwendige Dauer für die Inbetriebsetzung** einer alternativen Lösung zu kennen.

2.3.1. Zulässige Dauer der Nichtverfügbarkeit

Diese Zeiten, die im Wesentlichen kritische Systeme und Leistungen, insbesondere jene der kritischen Infrastrukturen betreffen, können nicht präzise definiert werden. Daher ist es vorzuziehen, die kritischen Infrastrukturen abhängig von ihrer Bedeutung für das Überleben und die Existenzgrundlage der Bevölkerung zu priorisieren. Zu diesem Zweck wird die Priorisierung nach der Zufflov-Pyramide (siehe unten) zugrunde gelegt. Unter Berücksichtigung der kritischen

Infrastrukturen und ihrer Priorität nach Zufflov ergibt die frühe Kritikalität (C') einen guten Indikator zur Priorisierung der Infrastrukturen.

Im Einsatz wird es trotzdem notwendig sein, eine Beurteilung der Situation für jede kritische Infrastruktur vorzunehmen.

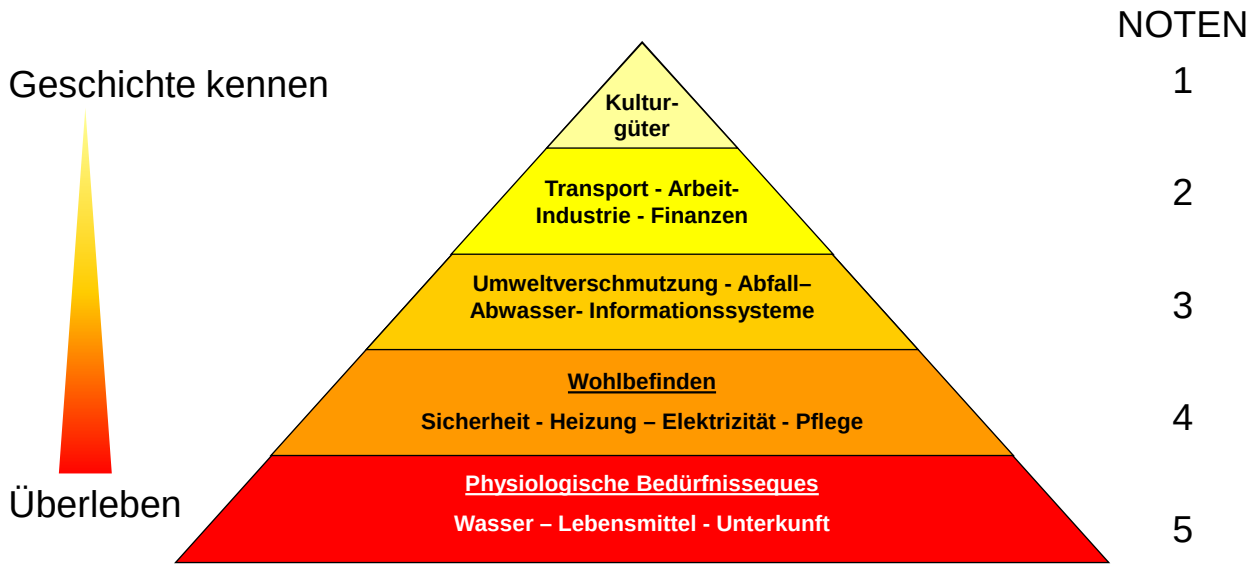

Abbildung 5: Zufflov-Pyramide

2.3.2. Notwendige Dauer der Inbetriebsetzung

Abhängig von der Situation, insbesondere der Dringlichkeit der zu treffenden Massnahmen, ist es zwingend notwendig, dass die Führungsorgane die Zeit kennen, die für das Einsetzen einer Massnahme notwendig ist. Zu diesem Zweck wurden die Massnahmen, die beim Einsatz getroffen werden, mit einer Abschätzung der Umsetzungszeit ergänzt (siehe Anhang 2 Ereignisführungsplanung). Diese Abschätzung ist subjektiv, sie liefert nur einen Anhaltspunkt für die notwendige Umsetzungszeit und es wird notwendig sein, sie beim Einsatz neu zu beurteilen.

2.4. Auslöser

Obwohl die endgültige Entscheidung zur Auslösung des vorliegenden Einsatzplans und der darin enthaltenen resp. zu treffenden Massnahmen beim KFO und in den Händen des Leiters des KFO liegt, stützt sich Letzterer auf die von SITel oder der Kantonspolizei (sie stellt das Monitoring sicher [8]) erhaltenen Informationen.

Dieses Monitoring umfasst eine globale und subjektive Überwachung der Situation, indem die empfangenen Informationen extrapoliert werden. SITel und die Kantonspolizei sind gewissermassen die Indikatoren einer kantonalen Situation resp. dass der Kanton sich in der Situation mit einem Ausfall der Informationsnetze befindet.

[8] Andere Lösungen für das Monitoring sind denkbar wie z. B. ein Monitoring mit den Unternehmen.

Auf diese Weise:

> Überwacht **SITel** das Netz des Staates und analysiert die Situation. Auf dieser Basis und unter Berücksichtigung der von MELANIE empfangenen Informationen, extrapoliert es die Situation für den ganzen Kanton und berichtet dem KFO[9].

> Die **Kantonspolizei**, insbesondere basierend auf den Informationen der EAZ und der Finanzpolizei, beurteilt die Situation und berichtet dem KFO[9].

3. Aufträge

Eine Matrix der Verantwortlichkeiten (siehe unter 3.2) und eine Ereignisführungsplanung (siehe unter 3.4) wurden auf der Grundlage der Beurteilung der Probleme erstellt[10], die ein Ausfall der Informationsnetze stellen kann. Ziel dieses Plans ist die Festlegung der Tätigkeiten und Massnahmen, die jeder Akteur abhängig von der jeweiligen Phase treffen muss.

3.1. Lösungen

Um den bei der Beurteilung des Problems festgestellten Schwierigkeiten zu begegnen, wurden Lösungen ausgearbeitet (sieh Anhang 3). Diese Tabelle listet für jeden Vektor und abhängig von jeder Ausfallkategorie die möglichen Lösungen auf[10]. Diese müssen durch das Führungsorgan oder die zuständigen Einsatzkräfte (siehe untenstehende Matrix der Verantwortlichkeiten) bezüglich ihrer Zweckmässigkeit beurteilt werden.

3.2. Matrix der Verantwortlichkeiten

Die Matrix der Verantwortlichkeiten teilt die Verantwortlichkeiten der Vorbereitungsmassnahmen, der Planung und der Aktion (siehe Anhang 1) an die verschiedenen Akteure gemäss der ihnen zugeteilten Rolle zu.

3.3. Allgemeine Aufgaben

Als Ergänzung der Aufgaben im Plan ROT erfüllen die Akteure die untenstehenden allgemeinen Aufgaben. Die speziellen Aufgaben sind in der Ereignisführungsplanung im Detail aufgeführt (siehe unter 3.4).

3.3.1. Staatsrat

> Bestätigt die vom KFO vorgeschlagenen Massnahmen.
> Auf die Anforderungen des KFO bezüglich der Abweichungen von den gewöhnlich geltenden Regeln antworten, insbesondere bezogen auf den Datenschutz und die berufliche Geheimhaltung.

3.3.2. KFO

> In der Lage sein, sich auch ohne Kommunikationsmittel auf den Weg zu machen
> In der Lage sein, intern und mit seinen Partnern mithilfe alternativer oder gesicherter Mittel zu kommunizieren.
> Die Information führen
> Die Verbindung zum Bund sicherstellen

---

[9] Ausserhalb des Ereignisses an den Bevölkerungsschutz.
[10] Unvollständige Liste

3.3.3. GFO

> In der Lage sein, sich auch ohne Kommunikationsmittel auf den Weg zu machen
> In der Lage sein, intern und mit seinen Partnern mithilfe alternativer oder gesicherter Mittel zu kommunizieren
> Die KFO-Richtlinien anwenden

3.3.4. Polizei

> Die Koordination der Information der Blaulichtorganisationen sicherstellen
> Den Bedrohungsgrad für die Informatik des Kantons analysieren und spontan der KFO melden[11]
> In der Lage sein, sich auch ohne Kommunikationsmittel auf den Weg zu machen
> In der Lage sein, intern und mit ihren Partnern mithilfe alternativer oder gesicherter Mittel zu kommunizieren
> Jederzeit die sicherheitsbedingten Leistungen, des Einsatzes und seiner Alarmzentrale garantieren
> Die Aktivitäten priorisieren

3.3.5. Feuerwehr

> In der Lage sein, sich auch ohne Kommunikationsmittel auf den Weg zu machen
> In der Lage sein, intern und mit ihren Partnern mithilfe alternativer oder gesicherter Mittel zu kommunizieren
> Jederzeit die sicherheitsbedingten Leistungen und den Einsatz garantieren
> Die Aktivitäten priorisieren

3.3.6. SFO

> In der Lage sein, sich auch ohne Kommunikationsmittel auf den Weg zu machen
> In der Lage sein, intern und mit seinen Partnern mithilfe alternativer oder gesicherter Mittel zu kommunizieren
> Jederzeit die sicherheitsbedingten Leistungen, des Eingriffs und seiner Alarmzentrale garantieren
> Die Aktivitäten priorisieren

3.3.7. ZS

> In der Lage sein, sich auch ohne Kommunikationsmittel auf den Weg zu machen
> In der Lage sein, intern und mit ihren Partnern mithilfe alternativer oder gesicherter Mittel zu kommunizieren
> Die Auslösung der Sirenen garantieren
> Für die Partner alternative Kommunikations- und Informationsmittel einsetzen und den Betrieb aufrechterhalten.
> Partner, insbesondere Blaulichtorganisationen in ihren Aufgaben unterstützen

3.3.8. Infozelle

> In der Lage sein, sich auch ohne Kommunikationsmittel auf den Weg zu machen
> In der Lage sein, intern und mit ihren Partnern mithilfe alternativer oder gesicherter Mittel zu kommunizieren

---

[11] Ausserhalb des Ereignisses an den Bevölkerungsschutz

> Die Kommunikation mit der Bevölkerung sicherstellen

3.3.9. ITA

> Den Bedrohungsgrad für die Informatik des Kantons analysieren und spontan der KFO melden[12]
> In der Lage sein, intern und mit ihren Partnern mithilfe alternativer oder gesicherter Mittel zu kommunizieren
> Die für ORCAF notwendigen technischen Leistungen zur Verfügung stellen

3.3.10. Medien

> In der Lage sein, intern und mit ihren Partnern mithilfe alternativer oder gesicherter Mittel zu kommunizieren
> Alle notwendigen Massnahmen treffen, um ihre Leistungen zu garantieren

3.3.11. Bereitsteller des Zugangs / Telefonbetreiber[13]

> In der Lage sein, intern und mit ihren Partnern mithilfe alternativer oder gesicherter Mittel zu kommunizieren.
> Alle notwendigen Massnahmen treffen, um die Widerstandsfähigkeit ihrer Systeme zu erhöhen und ihre lebenswichtigen Leistungen zu garantieren
> Redundanzen für die Systeme bereitstellen
> Darüber wachen, dass ihre Systeme dauernd:
  > verfügbar sind
  > zuverlässig sind
  > Sicher sind
> Ihre BCM/BCP einrichten, um für ein Ereignis «Ausfall der Informationsnetze» bereit zu sein
> Die für ORCAF notwendigen technischen Leistungen zur Verfügung stellen
> Das KFO über die Lösung des Ausfalls informieren

3.3.12. KI-Betreiber

> Die notwendigen Präventionsmassnahmen treffen, um die Widerstandsfähigkeit ihrer Systeme zu erhöhen und ihre lebenswichtigen Leistungen zu garantieren
> Redundanzen für die lebenswichtigen Systeme bereitstellen
> Ihre BCM/BCP einrichten, um für ein Ereignis «Ausfall der Informationsnetze» bereit zu sein
> Das KFO über die Lösung des Ausfalls informieren

[12] Ausserhalb des Ereignisses an den Bevölkerungsschutz
[13] Yc. Netzbetreiber IKT

3.3.13. Bund

> In der Lage sein, intern und mit seinen Partnern mithilfe alternativer oder gesicherter Mittel zu kommunizieren.
> Die für ORCAF notwendigen technischen Leistungen zur Verfügung stellen

3.4. Ereignisführungsplanung

Die Ereignisführungsplanung (siehe Anhang 2) setzt sich aus drei Ebenen zusammen:

> Die erste Ebene, Aktionen genannt, enthält gewissermassen die Hauptaufgabe jedes Akteurs. Aus ihr geht grosso modo der Handlungsspielraum hervor. Sie sind im Anhang 4 «Tätigkeiten – Beschreibung» beschrieben.

> Die zweite Ebene stellt die spezifische Aufgabe jedes einzelnen Akteurs dar, sodass dieser das Vorhaben / die Aufgabe der ersten Ebene umzusetzen kann.

> Die dritte Ebene umfasst die konkreten Planungsmassnahmen. Die verschiedenen Akteure beurteilen die Notwendigkeit und die Gelegenheit für ihren Dienst, diese Massnahmen zu realisieren.

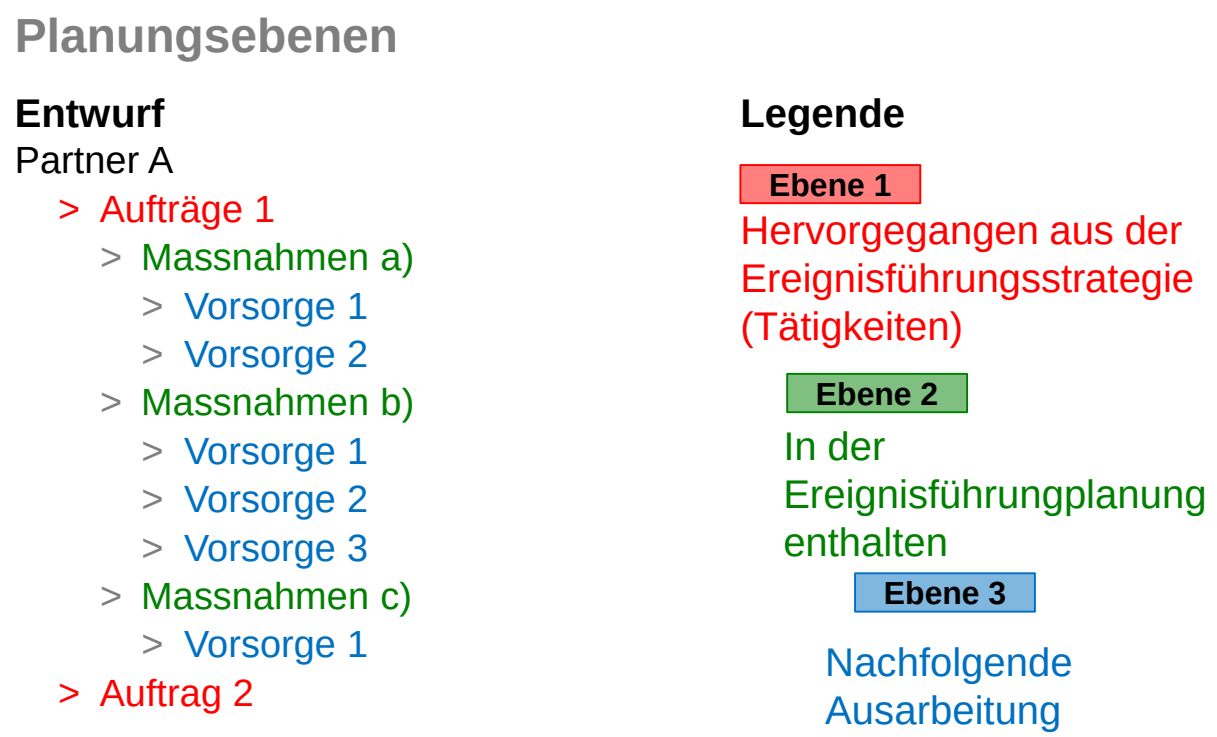

Abbildung 6: Planungsebenen

Diese Planung umfasst auf diese Weise die möglichen Lösungen, um für eine solche Situation gewappnet zu sein, sowie die detaillierten Aufgaben jedes Akteurs. Diese Akteure sind verantwortlich für die Massnahmen, die sie vorbereiten beziehungsweise zur Verfügung stellen wollen.

Für das Verständnis der Planungstabelle notwendigen Erklärungen sind in Anhang 5 aufgeführt.

4. Besondere Bestimmungen

4.1. Zusammenarbeit

4.1.1. Intern im Kanton

Es ist wünschenswert, dass die Unternehmen auch spontan ihre Situation melden, um das Bild der kantonalen Situation zu konsolidieren. Sie spielen tatsächlich eine wichtige Rolle als «Auslöser der Warnung».

4.1.2. Ausserhalb des Kantons

4.1.2.1. Swiss Cyber Experts

Die Swiss Cyber Experts bestehen aus einer Gruppe hochqualifizierter Experten der IKT-Industrie, aus Kreisen der Wirtschaft, der Administration und der Hochschulen. MELANI ist beauftragt, ihre Analyseaktivitäten zu koordinieren; alles in der Anonymität des Auftraggebers.

Die Swiss Cyber Experts erlauben den privaten Unternehmen und der Administration bei schweren Cyber-Zwischenfällen auf hochspezialisierte Experten zurückzugreifen. Die Partnerschaft zwischen Öffentlichkeit und Privatwirtschaft bezweckt, alles unter Wahrung der Vertraulichkeit, bei Cyber-Angriffen deren Tragweite die Ressourcen der Opfer übersteigen, eine schnelle Diagnose zu stellen und so die Voraussetzungen für eine effiziente Lösung zu schaffen. Dagegen trägt sie nichts zur Behebung des Ausfalls bei, die Sache des Unternehmens ist.

Alle Unternehmen des Kantons können die Hilfe dieser Spezialisten anfordern, indem sie sich an den Bevölkerungsschutz wenden, der die Verbindung zu dieser Gruppe sicherstellt.

4.1.2.2. Cyber-NDB

Der Cyber-NDB[14], der ein Teil von MELANI ist, stellt den Cyber-Teil des Auskunftsdienstes des Bundes dar. Er überwacht und analysiert die Informatik-Bedrohung und übermittelt die Situationsberichte und andere Information an die Partner.

Der Bevölkerungsschutz stellt die Verbindung mit der Cyber-NDB sicher.

Jedes Unternehmen, das nicht Mitglied von MELANIE ist, kann mithilfe des Bevölkerungsschutzes jeden Ausfall, Angriff oder Störungsfall MELANIE melden.

4.2. Informationsbeschaffung

Es ist Sache jedes Einzelnen, sich zu informieren. Jedes Amt organisiert den Auskunftsdienst innerhalb seiner Dienstleistung.

Die Partner des KFO leiten weiter
> ausserhalb des Ereignisses an den Bevölkerungsschutz
> im Ereignis an die Info-Zelle des KFO
spontan oder auf Anforderung alle Auskünfte, insbesondere bezüglich des Zustands der Situation und ihres Einsatzes.

Ausserdem kann jeder insbesondere mithilfe der EAZ ein Ereignis melden.

---

[14] Nachrichtendienst des Bundes (Service de renseignement de la Confédération)

4.3. Information

4.3.1. Ausserhalb des Ereignisses

Ausserhalb eines Ereignisses stellt der Bevölkerungsschutz die Information seiner Partner, Führungsorgane, Betreiber kritischer Infrastrukturen und der Bevölkerung über die Situation, die Bedrohungen und die Verhaltensempfehlungen sicher. Zu diesem Zweck stützt er sich auf die vom Bund, seinen Partnern und seinem Netz von Unternehmen und IKT-Spezialisten erhaltenen Informationen.

4.3.2. Im Ereignis

Die Informationsleitung wird gemäss den geltenden Richtlinien des KFO von der Informationszelle sichergestellt.

Die Kommunikationsmassnahmen werden im Rahmen des Möglichen mit den Nachbarkantonen und dem Bund koordiniert.

4.4. Kommunikation

Bei einem Ausfall des Informations- und Kommunikationssystems, können alternative Kommunikationsmittel wie sie in der Ereignisführungsplanung aufgeführt sind (siehe Anhang 2), abhängig von ihrer Zweckmässigkeit, Relevanz, Verfügbarkeit, Dauer der Inbetriebnahme verwendet/aktiviert werden. Diese, verwendbar entweder für die interne oder externe Kommunikation, können sein[15]:

> Anzeige an öffentlichen Anschlagsäulen
> Mobile Antennen (Natel)
> Kirchenglocken
> POLYCOM IDR Sender
> Private Post/Transportunternehmen
> Meldeläufer
> Gruppe von Kurzwellenamateuren[16]
> Mobile Lautsprecher
> Verbindungspersonen
> Hotline, für die Einsatzkräfte
> Abwurf von Flugblättern aus dem Flugzeug
> Brieftauben
> Informationsstellen
> Radio IPCC (IBBK-Radio)
> Automatischer Beantworter (für die Einsatzkräfte und die Bevölkerung)
> Mobile oder manuelle Sirenen
> Mitteilungen an alle

[15] Unvollständige Liste ohne Prioritätsreihenfolge
[16] Vertraulichkeit der Daten beachten

4.5. Vertraulichkeit

Alle ausserhalb des Ereignisses oder im Ereignis erhaltene Information ist streng vertraulich und darf nur an Personen weitergegeben werden, die diese Information zur Erledigung ihrer Aufgaben im Unternehmen benötigen.

4.6. Verhaltensempfehlungen

Siehe unter 4.3.1 «Ausserhalb des Ereignisses» und unter www.fr.ch/catastrophe.

4.7. Zwingende Massnahmen[17]

Der KFO kann dem Staatsrat vorschlagen insbesondere die untenstehenden Einschränkungsmassnahmen:

- Die Unternehmen verpflichten, den Situationszustand ihrer IKT-Systeme zu melden
- Die IKT-Lieferanten verpflichten:
  - Massnahmen zu treffen, um den Umfang des Ausfalls zu begrenzen
  - Zwingende Massnahmen gegenüber der Bevölkerung zu treffen
- Alle Medien einer Meldepflicht unterstellen[18]

Aufgrund des Artikels 8 des Gesetzes über den Bevölkerungsschutz *«Tritt ein Ereignis ein, so treffen der Staat und die Gemeinden die Massnahmen, die nötig sind, um die Katastrophe oder die Notlage zu bewältigen»* kann das KFO mithilfe des Staatsrates bei einem Ereignis alle andern einschränkenden Massnahmen anordnen.

Für die Bevölkerung ordnet das KFO nur Verhaltensempfehlungen an.

4.8. Tests

Jeder Akteur und jeder Besitzer von Informationssystemen ist angehalten, seine Systeme sowie die redundanten, alternativen und Notfallsysteme regelmässig zu testen.

4.9. Finanzierung

4.9.1. Tests und Vorbereitungsmassnahmen

Die mit den Vorbereitungsmassnahmen verbundenen Kosten gehen zu Lasten jedes Einzelnen.

4.9.2. Beim Einsatz

Die Finanzierung der Einsätze wird durch den Staat Freiburg sichergestellt.

Der Staatsrat kann auf eine Entschädigung der Betreiber von kritischen Infrastrukturen und der Betreiber der IKT-Netze für mögliche Verluste aufgrund der auferlegten Massnahmen eintreten.

5. Schlussbestimmungen

Der vorliegende Einsatzplan wurde am Donnerstag, 16. Februar 2017 anlässlich einer ordentlichen Sitzung des KFO, basierend auf dem Gesetz vom 13. Dezember 2007 über den Bevölkerungsschutz (BevSG), genehmigt. Der Staatsrat nahm am 25. April 2017 davon Kenntnis.

---

[17] Unvollständige Liste

[18] Gemäss ICARO, die nur eine Verpflichtung für Radio- und Fernsehstationen ist, die der RTVV unterstellt sind

Das Amt für Bevölkerungsschutz und Militär (ABSM) hat den Auftrag, den Plan zu aktualisieren, grundsätzlich einmal pro Legislaturperiode, es sei denn, der Lauf der Dinge habe die Aktualisierung schon vorher gefordert.

Anhänge

—

1. Matrix der Verantwortlichkeiten
2. Ereignisführungsplanung
3. Lösungen - Bestandesaufnahme
4. Massnahmen - Beschreibungen
5. Nutzung der Ereignisführungsplanung

Verteiler

—

Staatsrat
Oberamtmänner
KFO
Spez KFO Gefahren "Versorgung"
SFO
GFO
EAZ
CASU144
ITA
EMF ABCN
MELANI
Kritische Infrastrukturen (Kritikalität ≥3)

Impressum

Projektleitung
—
Kantonales Führungsorgan KFO
Bevölkerungsschutz

Zeughausstrasse 16, Postfach 185, 1705 Freiburg

T +41 26 305 30 00, F +41 26 305 30 04
www.fr.ch/absm

Auskünfte
—
Amt für Bevölkerungsschutz und Militär ABSM
Bevölkerungsschutz

Zeughausstrasse 16, Postfach 185, 1705 Freiburg

T +41 26 305 30 30, F +41 26 305 30 04
sppam_protpop@fr.ch, www.fr.ch/absm

Die elektronische Version des vorliegenden Plans kann heruntergeladen werden:
www.fr.ch/katastrophe

Titelblattabbildung
—
Foto: istockphoto.com

Übersetzung
—
Jensen Fachübersetzen GmbH

25. April 2017