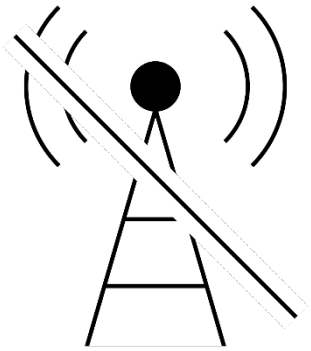
Panne dans un centre de calcul



Le présent dossier fait partie de l'analyse nationale des risques « Catastrophes et situations d'urgence en Suisse »

Définition

On parle de défaillance d'un centre de calcul lorsque ce dernier ne parvient plus à fournir ses services ou qu'il ne peut les fournir qu'en partie. C'est le cas lors d'une panne, d'un dysfonctionnement ou d'une défaillance affectant l'infrastructure ou les logiciels ou encore lors d'un sabotage ou d'une erreur humaine. Une telle défaillance peut avoir de graves conséquences dans la société eu égard à l'étroite interconnexion de tous les domaines d'activité. L'ampleur des dommages dépend de la durée de la défaillance, du type de technologie affecté, du volume et de l'importance des services concernés et de leurs utilisateurs et des dommages causés à des données. Les défaillances touchant des systèmes ou des prestations spécifiques peuvent causer de graves dommages si elles affectent des systèmes de contrôle d'infrastructures critiques (centrales électriques, réseaux de transport, etc.). Une défaillance touchant un centre de calcul peut ainsi entraîner différents dommages consécutifs.

Une telle défaillance peut avoir diverses origines, par exemple techniques comme une panne d'électricité ou un défaut affectant un composant, humaines comme une mauvaise manipulation, ou encore naturelles comme un tremblement de terre.

novembre 2020

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Office fédéral de la protection de la population OFPP

Exemples d’événements

Les exemples concrets aident à mieux comprendre la nature d’un type d’événement. Ils illustrent la manière dont il survient, son déroulement et ses conséquences.

28 mai 2019 Allemagne Différents services financiers	Une panne survenue auprès du prestataire de services Dataport affecte 141 services financiers dans les länder de Brême, Hambourg, Schleswig-Holstein, Saxe-Anhalt, Mecklembourg-Poméranie occidentale et Basse-Saxe. Près de 30 000 employés sont touchés. La panne est liée à un test de charge planifié ayant provoqué l’arrêt du système de refroidissement du centre de calcul, puis de tous les ordinateurs. La panne dure cinq jours ouvrables.
27 mai 2017 Grande-Bretagne British Airways	Suite à une erreur de manipulation d’un collaborateur du fournisseur de services informatiques CBRE Managed Services, qui a coupé le courant par inadvertance, les systèmes redondants d’un centre de calcul tombent subitement en panne et s’avèrent incapables de redémarrer. Le courant peut être rétabli au bout de quelques minutes. Le redémarrage incontrôlé cause cependant des dommages aux logiciels et aux serveurs. Le principal client du fournisseur, British Airways, subit de graves dommages, 75 000 passagers se retrouvant bloqués pour un week-end entier.
20 mars 2017 Zurich (Suisse) Centre de compétences informatiques municipal	Un composant central du système informatique de la Ville de Zurich tombe en panne au centre de calcul de Hagenholz. Cette panne se répercute sur les terminaux de l’administration communale et des hôpitaux. Tous les sites web de la Ville de Zurich sont hors service. La panne peut être réparée dans la nuit du 20 au 21 mars.

Facteurs d'influence

Les facteurs suivants peuvent influer sur la survenance, l'évolution et les conséquences d'un événement.

Source de danger	– Défaillance de l'approvisionnement électrique ou de vecteurs de données (p. ex. en raison d'un phénomène naturel ou d'un sabotage) – Défauts techniques (défaillance du matériel, bug logiciel, etc.) – Erreur de manipulation en cours d'exploitation ou de maintenance – Autres dysfonctionnements – Actions volontaires (vandalisme, sabotage, cyberattaque)
Moment	– Durant les heures de travail ou la nuit – Jour ouvrable, week-end, jour férié, vacances, moment de l'année
Localisation / étendue	– Degré de diffusion du système concerné – Degré d'interconnexion du système concerné (effet de cascade) – Nombre et importance des services touchés – Nombre et importance des secteurs, utilisateurs ou clients touchés – Ampleur de la perte de données – Solutions de rechange, systèmes propriétaires
Déroulement	– Délai de préalerte (temps de réaction) – Durée de la panne – Comportement des organisations concernées (gestion de l'événement) – Réaction des clients et des utilisateurs

Intensité des scénarios

Selon les facteurs d'influence, différents événements peuvent se dérouler avec des intensités différentes. Les scénarios ci-après représentent un choix parmi de nombreuses possibilités et ne constituent pas une prévision. Ils permettent d'anticiper les conséquences potentielles d'un événement afin de pouvoir s'y préparer.

---

1 — Considérable

- Répercussions limitées au secteur informatique
- Aucun service critique touché
- Événement et mesures connus
- Perte de données nulle ou limitée
- Durée limitée (moins d'un jour)

---

2 — Majeure

- Répercussions sur plusieurs secteurs critiques
- Services critiques touchés
- Événement inconnu, mais mesures dictées par l'expérience
- Données en partie altérées ou perdues
- Durée moyenne (deux à trois jours)

---

3 — Extrême

- Répercussions sur un grand nombre d'infrastructures critiques, notamment dans les secteurs de l'énergie, des télécommunications, des finances, des soins médicaux et des transports
- Grand nombre de services critiques touchés (p. ex. authentification altérée)
- Grand nombre de données altérées ou perdues
- Dommages aux systèmes de gestion de l'énergie et du trafic, perturbations majeures des services de télécommunication
- Absence de contre-mesures possibles (leur mise au point nécessiterait plusieurs semaines)
- Public touché indirectement mais sensiblement dans l'activité quotidienne
- Longue durée (plus d'une semaine)

Scénario

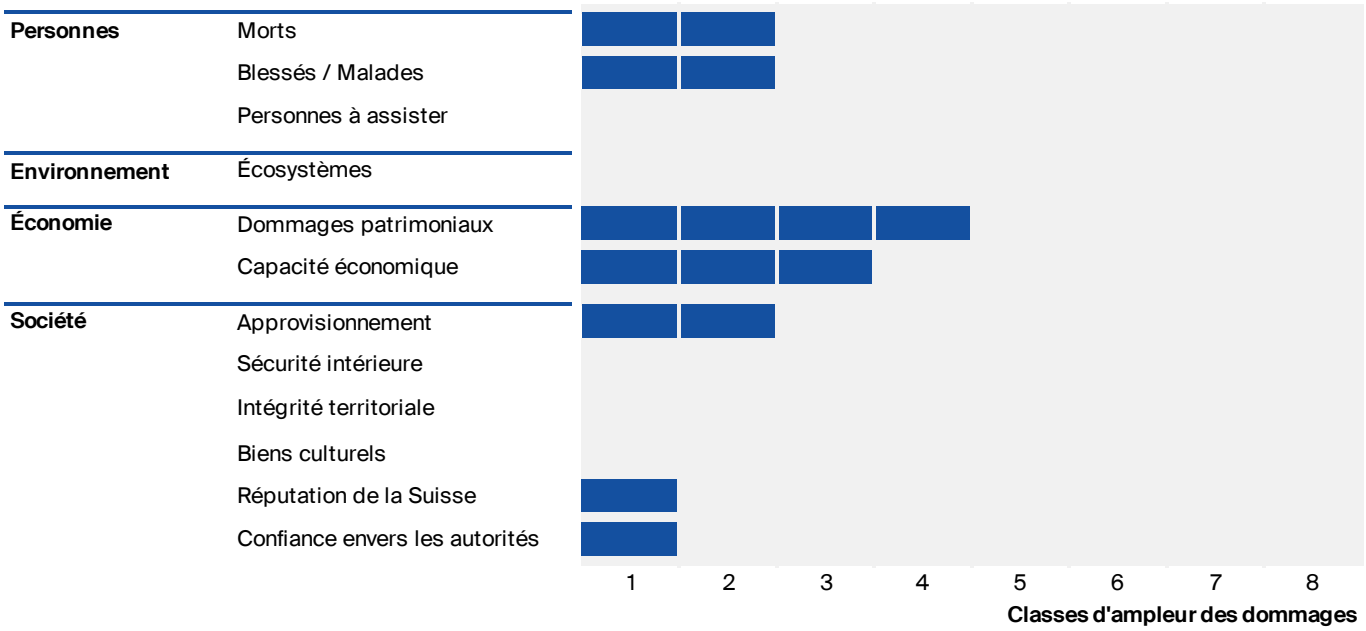
Le scénario suivant est fondé sur le degré d'intensité majeur.

Situation initiale / phase préliminaire	Un exploitant de centres de données dispose de serveurs de stockage fonctionnant de façon redondante en plusieurs lieux géographiques sur le cloud. Pour optimiser la circulation des données entre les centres de calcul, l'exploitant veut migrer vers un nouveau logiciel de gestion (load balancing software).
Phase de l'événement	En raison d'une erreur de configuration, la migration vers le nouveau logiciel provoque une surcharge d'un centre de calcul entraînant sa défaillance totale car le trafic des données n'est pas réparti de façon régulière. L'exploitant tente sans succès de corriger l'erreur par une configuration différente. Par la suite, il isole le centre de calcul du réseau et annule la migration. Étant donné que par redondance, les données du centre défaillant sont également conservées dans les autres lieux de stockage, ces derniers assurent momentanément l'échange des données avec les clients. À la remise en route du centre défaillant, les données des autres centres sont automatiquement partagées. Le cas se produisant pour la première fois, il apparaît rapidement que le transfert des données occupe énormément de bande passante, que le centre de calcul réactivé doit traiter une quantité extrême de données et que le processus de restauration dure par conséquent beaucoup plus longtemps que prévu. D'une part, des données corrompues sont générées durant la restauration (et devront être rectifiées par la suite), et d'autre part l'exploitant reste impuissant car le logiciel de gestion ne permet aucune interruption du processus de restauration. Il en résulte des heures durant un fort trafic sur le réseau, qui se répercute sensiblement sur les services travaillant avec l'exploitant. La plupart des services basés sur l'internet sont très perturbés ou ne fonctionnent plus du tout. Les premiers touchés sont les services tributaires d'une forte latence, notamment ceux qui dépendent de la synchronisation de grandes banques de données et de la diffusion en flux continu, par exemple les fournisseurs de contenus multimédias. Mais les accès web, le courrier électronique, les accès à distance, l'accès des appareils mobiles et une partie de la téléphonie sont également touchés. Les services d'urgence fonctionnent en revanche. Deux des dix plus grandes boutiques en ligne de Suisse, 20 000 PME, une grande entreprise de logistique, certains secteurs administratifs d'une ville et de nombreux petits hébergeurs sont directement frappés par l'événement en tant que clients de l'exploitant. Deux jours durant, ils n'ont qu'un accès limité à leur environnement virtuel et doivent faire face à des séries de données corrompues. En raison du processus erroné de restauration et de l'absence de copies de sauvegarde, nombre de clients perdent des données. Un hôpital de 500 lits et 2000 PME perdent une partie de leurs données, et 500 PME même la totalité. L'administration fiscale d'une ville de moyenne importance perd également une partie de ses données. Ne sont que peu ou pas touchés les utilisateurs bénéficiant de liaisons dédiées, de leurs propres réseaux ou de systèmes de rechange sous la forme par exemple de communication par ondes ou par satellite, et les fournisseurs disposant de leurs propres liaisons.

Phase de rétablissement	Après un peu plus de deux jours, la charge du réseau se normalise. Lorsque les clients ne sont pas suffisamment prêts à affronter ce type de panne (p. ex. absence d'une configuration adéquate ou de copies de sauvegarde des données), la remise en état dure bien plus longtemps, notamment en ce qui concerne le rétablissement de séries de données cohérentes, la saisie *a posteriori* de transactions et d'autres opérations semblables.
Déroulement dans le temps	L'événement se produit soudainement. Ses répercussions se font sentir au bout de quelques minutes. La charge du réseau se normalise après deux jours mais il faut quelques jours de plus pour réparer les dommages.
Extension dans l'espace	Aucune délimitation précise n'est possible. Les problèmes de surcharge se font sentir dans toute la Suisse, de même qu'en Europe.

Conséquences

Pour évaluer les conséquences d'un scénario, on l'examine à l'aune de douze indicateurs répartis dans quatre domaines. L'ampleur attendue du scénario décrit est représentée dans la diagramme et commentée dans le texte ci-après. Chaque classe d'ampleur supérieure correspond à une augmentation des dommages de facteur trois.



Personnes

En raison de la perte de données de patients dans l'hôpital touché et dans certains cabinets médicaux, des malades ne peuvent être soignés ou subissent des traitements erronés : il en résulte des dommages à la santé des patients, voire le décès de certains d'entre eux.

Les possibilités restreintes de communication peuvent provoquer des retards dans les prestations d'assistance aux personnes nécessitant des soins.

En fonction de la défaillance d'un service critique, jusqu'à 100 personnes au total souffrent d'atteintes à leur santé ou sont blessées. On ne peut pas exclure quelques décès, dix au maximum.

Environnement

L'événement n'a en principe aucune répercussion environnementale.

S'il devait avoir des conséquences sur la gestion d'installations et de systèmes présentant des risques pour l'environnement, ce dernier pourrait toutefois subir des dommages, par exemple en raison de la dissémination incontrôlée de substances dangereuses dans le sol, l'eau et l'air.

Économie

Les clients de l'exploitant du centre de données directement concernés de même que ceux des revendeurs doivent fournir un effort supplémentaire en ressources humaines et techniques pour préserver leurs services ou se voient contraints de cesser le travail dans les secteurs touchés : 20 000 PME sont déjà concernées.

Les chiffres d'affaires des deux boutiques en ligne directement touchées chutent fortement durant les deux jours de la perturbation. L'entreprise logistique encourt des charges supplémentaires considérables pour maintenir son offre. Les secteurs décentralisés de l'administration municipale ne sont que difficilement, voire pas du tout, atteignables en ligne ou par téléphone durant ces deux jours.

Lorsque des clients des revendeurs sont directement concernés, ou lorsque les prestations en ligne sont fortement réduites à cause de la saturation du réseau, l'activité commerciale ralentit durant deux jours.

L'administration fiscale et la police des habitants d'une ville de moyenne importance, de même que 2000 PME, perdent une partie de leurs données, y compris des données fiscales et personnelles importantes.

Par ailleurs, 500 PME perdent la totalité de leurs données stockées auprès de l'exploitant et doivent en supporter les conséquences.

Les dommages patrimoniaux et les coûts de gestion de l'événement s'élèvent à 1 milliard de francs environ et les capacités économiques se voient réduites de quelque 350 millions de francs.

Société

La panne provoque des difficultés et des ruptures d'approvisionnement en raison de la défaillance de la logistique de grands distributeurs.

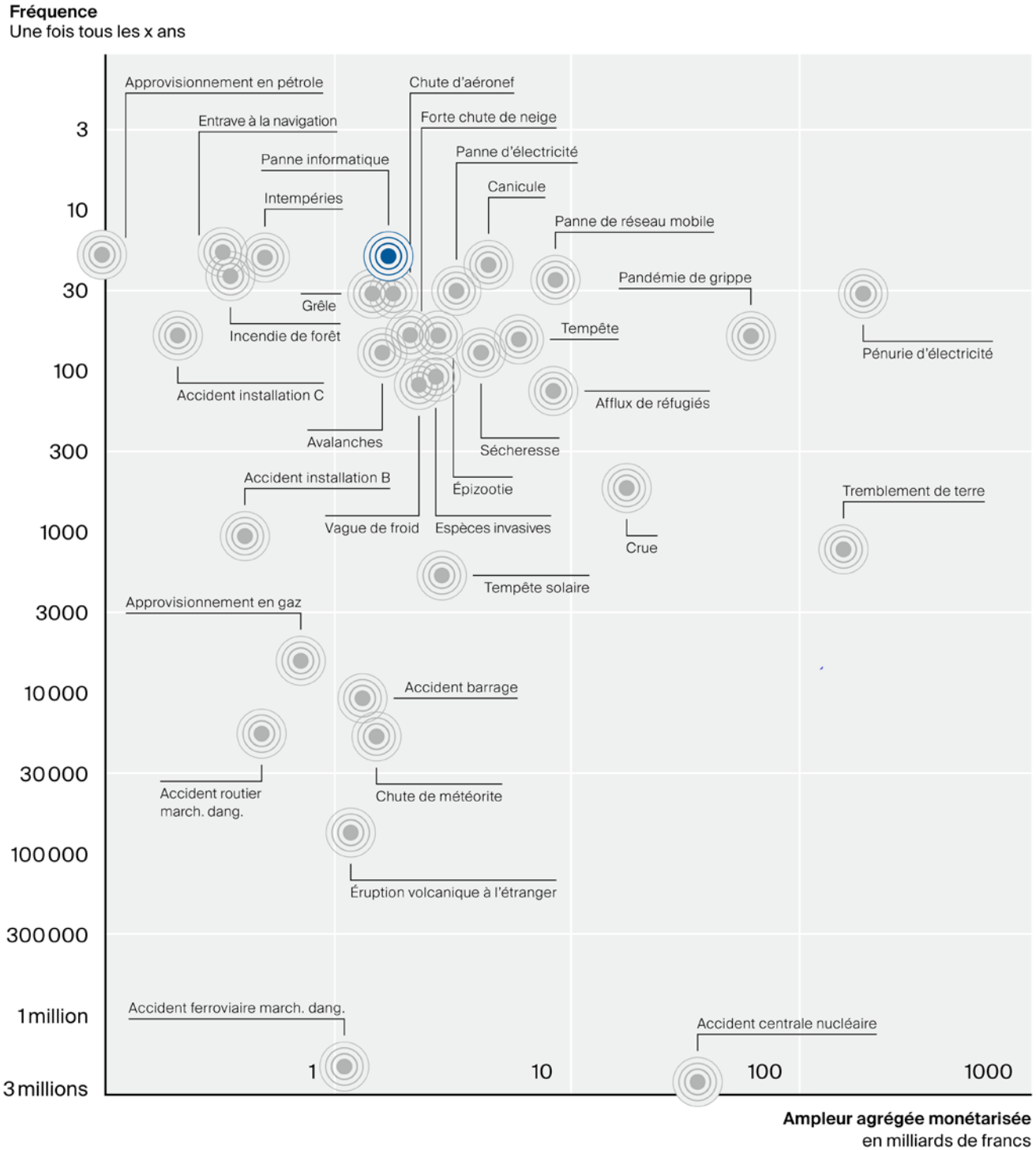
Les cercles d'utilisateurs concernés n'ont plus d'accès à l'internet (défaillance de services utilisant l'internet, p. ex. courrier électronique, réseaux sociaux, achats en ligne, diffusion en flux continu).

L'échange de données est limité entre, par exemple, les soins à domicile, les hôpitaux, la police des habitants, etc.

À la suite de la défaillance, les critiques pleuvent sur l'exploitant, accusé de ne pas être en mesure d'offrir un service fiable et de paralyser la moitié de la Suisse à cause de ses problèmes. Certains de ses clients se plaignent aussi publiquement de la forte dépendance par rapport à quelques centres de calcul et entreprises spécialisées ou du manque de prévoyance de l'exploitant.

Risque

Le risque lié au scénario décrit est comparé aux risques des autres scénarios analysés dans une matrice des risques (voir ci-dessous). La probabilité d'occurrence y est saisie comme une fréquence (une fois tous les x ans) sur l'axe des y (échelle logarithmique) et l'ampleur des dommages est agrégée et monétarisée en CHF sur l'axe des x (échelle logarithmique également). Le produit de la probabilité d'occurrence et de l'ampleur des dommages représente le risque lié à un scénario. Plus un scénario se situe en haut à droite de la matrice, plus le risque est élevé.



Bases juridiques

Constitution	— Art. 13 (Protection de la sphère privée), 92 (Services postaux et télécommunications) et 173 (Autres tâches et compétences) de la Constitution fédérale de la Confédération suisse du 18 avril 1999 ; RS 101.
Lois	— Loi fédérale du 21 mars 1997 instituant des mesures visant au maintien de la sûreté intérieure (LMSI) ; RS 120. — Loi fédérale du 19 juin 1992 sur la protection des données (LPD) ; RS 235.1. — Loi fédérale du du 17 juin 2016 sur l'approvisionnement du pays (LAP) ; RS 531. — Loi fédérale du 18 mars 2016 sur la surveillance de la correspondance par poste et télécommunication (LSCPT) ; RS 780.1. — Projet de loi fédérale sur la sécurité de l'information, encore en examen au Parlement.
Ordonnances	— Ordonnance du 17 février 2010 sur l'organisation du Département fédéral des finances (Org DFF) ; RS 172.215.1. — Ordonnance du 14 juin 1993 relative à la loi fédérale sur la protection des données (OLPD) ; RS 235.11. — Ordonnance du 2 mars 2018 sur l'État-major fédéral Protection de la population (OEMFP) ; RS 520.17. — Ordonnance de la Banque nationale suisse (OBN) du 18 mars 2004 ; RS 951.131.

Informations complémentaires

Au sujet du danger de défaillance d'un centre de calcul

- Autorité fédérale de surveillance des marchés financiers (FINMA) (2018) : Circulaire 2018/3. Outsourcing – banques et assureurs. Externalisations dans le secteur des banques et des entreprises d'assurance. FINMA, Berne.
- Centrale d'enregistrement et d'analyse pour la sûreté de l'information (MELANI) (différentes années) : Sûreté de l'information. Situation en Suisse et à l'étranger. Rapports semestriels. DFF et DDPS, Berne.
- Le Conseil fédéral (2018) : Stratégie nationale de protection de la Suisse contre les cyberrisques (SNC) 2018–2022. UPIC, Berne.
- Le Conseil fédéral (2017) : Stratégie nationale de protection des infrastructures critiques 2018–2022. Berne.
- Office fédéral de la protection de la population (OFPP) (2015) : Guide pour la protection des infrastructures critiques. OFPP; Berne.
- ISO/IEC 27001 (2013): Informationstechnik – IT-Sicherheitsverfahren – Informationssicherheits-Managementsysteme – Anforderungen. ISO.
- ISO/IEC 27018 (2019): Information technology — Security techniques — Code of practice for protection of personally identifiable information (PII) in public clouds acting as PII processors. ISO.
- ISO 50001 (2011): Energiemanagement – Energiemanagementsysteme – Anforderungen mit Anleitung zur Anwendung. ISO.
- National Institute of Standards and Technology (NIST) (2018): Framework for Improving Critical Infrastructure Cybersecurity. Version 1.1. NIST.

Au sujet de l'analyse nationale des risques

- Office fédéral de la protection de la population (OFPP) (2020) : À quels risques la Suisse est-elle exposée ? Catastrophes et situations d'urgence en Suisse 2020. OFPP, Berne.
- Office fédéral de la protection de la population (OFPP) (2020) : Méthode d'analyse nationale des risques. Catastrophes et situations d'urgence en Suisse 2020. Version 2.0. OFPP, Berne.
- Office fédéral de la protection de la population (OFPP) (2020) : Rapport sur l'analyse nationale des risques. Catastrophes et situations d'urgence en Suisse 2020. OFPP, Berne.
- Office fédéral de la protection de la population (OFPP) (2019) : Liste des dangers. Catastrophes et situations d'urgence en Suisse. 2e édition. OFPP, Berne.

Office fédéral de la protection de la population OFPP

Guisanplatz 1B
CH-3003 Berne
risk-ch@babs.admin.ch
www.protpop.ch
www.risk-ch.ch