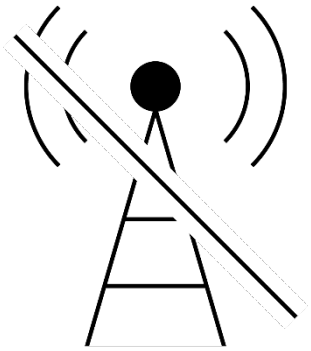
Interruzione di un centro elaborazione dati



Questo dossier di pericolo è parte integrante dell'analisi nazionale dei rischi «Catastrofi e situazioni d'emergenza in Svizzera»

Definizione

Si parla di interruzione di un centro elaborazione dati quando quest'ultimo non può più fornire servizi o solo in parte. Ciò si verifica in caso di guasto, malfunzionamento o interruzione dell'infrastruttura o del software oppure in caso di una manipolazione involontaria o intenzionale. Considerata la forte interdipendenza dei vari settori della società, una simile interruzione può avere gravi conseguenze. L'entità dei danni dipende dalla durata dell'interruzione, dal tipo di tecnologie colpite, dal volume e dall'importanza dei servizi e degli utenti colpiti e dai danni causati ai dati. Interruzioni di sistemi o servizi specifici possono causare gravi danni se colpiscono i sistemi di gestione delle infrastrutture critiche (centrali elettriche, reti di trasporto, ecc.). Un'interruzione di un centro elaborazione dati può quindi portare a vari danni conseguenti.

Le cause dell'interruzione di un centro elaborazione dati possono essere diverse: ad esempio interruzioni di corrente, guasti ai componenti, errori umani, sabotaggi o eventi naturali (sisma, ecc.).

novembre 2020

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Ufficio federale della protezione della popolazione UFPP

Esempi di eventi

Eventi reali del passato contribuiscono a una migliore comprensione di un pericolo. Illustrano l'origine, il decorso e le conseguenze del pericolo preso in esame.

---

28 maggio 2019
Germania

Vari uffici fiscali

Una perturbazione presso il provider «Dataport» ha colpito tutti i 141 uffici fiscali negli stati tedeschi di Brema, Amburgo, Schleswig-Holstein, Sassonia-Anhalt, Meclemburgo-Pomerania Anteriore e Bassa Sassonia. Il guasto ha toccato quasi 30 000 dipendenti. È riconducibile a un test di carico pianificato, che ha causato l'arresto del sistema di raffreddamento. Di conseguenza, tutti i sistemi del centro elaborazione dati si sono spenti. La perturbazione è durata cinque giorni lavorativi.

---

27 maggio 2017
Inghilterra

British Airways

Un dipendente del provider «CBRE Managed Services» ha provocato un cortocircuito accidentale nel centro elaborazione dati, in seguito al quale il sistema principale (power supply) e i sistemi ausiliari (uninterruptable power supply) si sono spenti. La situazione si è rapidamente aggravata poiché anche i sistemi di backup e di disaster recovery non si avviavano più. L'alimentazione di corrente è stata ripristinata nel giro di alcuni minuti, ma il riavvio incontrollato ha danneggiato hardware e software. Il principale cliente, British Airways, ha subìto ingenti perdite poiché 75 000 passeggeri sono rimasti bloccati a terra per l'intero fine settimana.

---

20 marzo 2017
Zurigo (Svizzera)

Centro di competenza informatica della città di Zurigo

Un componente centrale del sistema informatico della città di Zurigo (OIZ) ha subìto un guasto che ha causato gravi problemi informatici negli uffici amministrativi e negli ospedali cittadini. Tutti i siti web della città di Zurigo non erano più accessibili. Il guasto è stato riparato durante la notte.

Fattori influenti

I seguenti fattori possono influenzare l'origine, lo sviluppo e le conseguenze del pericolo.

Fonte di pericolo	– Interruzione dell'alimentazione di corrente o delle linee dati (per es. a causa di eventi naturali, sabotaggio) – Difetti tecnici (materiale o software difettoso, ecc.) – Errori di manipolazione durante l'esercizio o la manutenzione – Altri malfunzionamenti – Atti intenzionali (vandalismo, sabotaggio, ciberattacco)
Momento	– Nell'orario d'ufficio o di notte – Giorno lavorativo, weekend, giorno festivo, periodo di vacanze, stagione
Luogo / Estensione	– Grado di diffusione ai sistemi colpiti – Grado di interconnessione dei sistemi colpiti (effetto domino) – Numero e importanza dei servizi colpiti – Numero e importanza dei settori / utenti / clienti colpiti – Entità della perdita di dati – Soluzioni alternative; sistemi proprietari
Decorso dell'evento	– Tempo di preallerta – Durata dell'interruzione – Comportamento delle organizzazioni colpite (gestione dell'evento) – Reazione dei clienti e degli utenti

Intensità degli scenari

A seconda dei fattori influenti, possono svilupparsi diversi eventi di varia intensità. Gli scenari elencati di seguito costituiscono solo una scelta di possibili decorsi e non sono previsioni. Servono per anticipare le possibili conseguenze al fine di prepararsi ai pericoli.

1 – marcato	– Conseguenze limitate al settore ICT – Nessun servizio critico colpito – Evento noto e contromisure note – Perdita di dati nulla o limitata – Durata limitata (meno di 1 giorno)
2 – forte	– Conseguenze per alcuni settori critici – Servizi critici colpiti – Evento noto e contromisure dedotte dall'esperienza – Alcune corruzioni o perdite di dati – Durata media (due o tre giorni)
3 – estremo	– Conseguenze per numerose infrastrutture critiche, incluse quelle dei settori energia, telecomunicazioni, finanze, cure mediche e trasporti – Numerosi servizi critici colpiti (per es. autentificazione corrotta) – Numerose corruzioni o perdite di dati – Danni ai sistemi di gestione del traffico e dell'energia, forte perturbazione dei servizi di telecomunicazione – Le contromisure non sono disponibili e la loro preparazione richiede settimane. – La popolazione è indirettamente, ma sensibilmente colpita nella vita quotidiana. – Lunga durata (più di 1 settimana)

Scenario

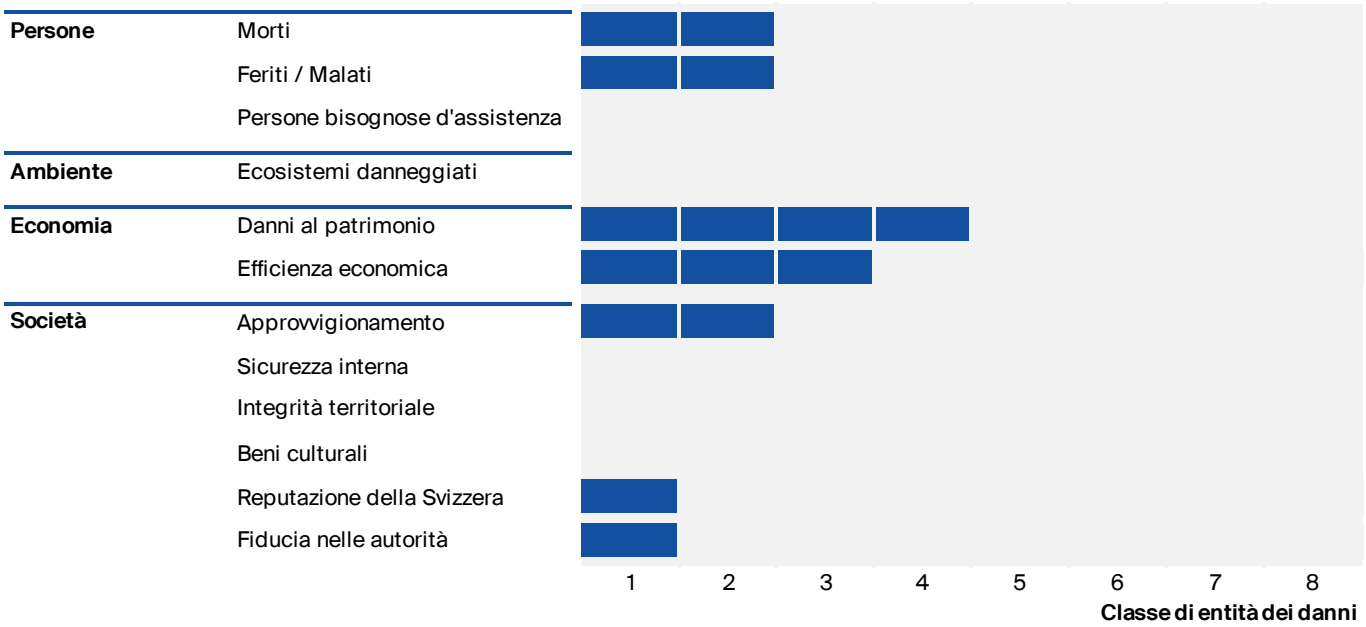
Il seguente scenario si basa sul livello d'intensità «forte».

Situazione iniziale / fase preliminare	Un operatore di centri elaborazione dati (CED) dispone di diversi server cloud geograficamente separati e gestiti in modo ridondante. Per regolare meglio il carico del traffico dei dati tra i CED, intende migrare l'esercizio su un nuovo software di gestione (Load Balancing Software).
Fase dell'evento	A causa di un errore di configurazione, la migrazione sul nuovo software sovraccarica e manda in tilt uno dei CED poiché il traffico dei dati non viene ripartito in modo uniforme. L'operatore cerca senza successo di correggere l'errore cambiando la configurazione. In seguito, disconnette il centro elaborazione dati dalla rete e annulla la migrazione. Dato che i dati di questo CED sono memorizzati anche su altri server per ridondanza, lo scambio dei dati con i clienti avviene tramite questi server. Non appena il CED interrotto viene riattivato, i dati degli altri CED vi vengono automaticamente ritrasferiti. Essendo la prima volta che si verifica una situazione del genere, non si era previsto il trasferimento di una tale quantità di dati. Il processo di recupero richiede quindi molto più tempo del previsto. Da un lato, durante il recupero si creano dei file corrotti, che devono poi essere ripristinati singolarmente, e dall'altro, l'operatore non può intervenire poiché il software di gestione non permette di interrompere il processo di recupero. Per diverse ore, si crea un intenso traffico di rete che penalizza i servizi che collaborano con l'operatore. Le loro prestazioni basate su Internet subiscono forti limitazioni o addirittura interruzioni. I primi ad essere colpiti sono i servizi che si basano sulla bassa latenza, come quelli che dipendono dalla sincronizzazione di grandi banche dati, così come i servizi di streaming come ad esempio i provider multimediali. Ma anche l'accesso al web, la posta elettronica, l'accesso remoto e l'accesso da dispositivi mobili così come parti della telefonia sono toccati dal sovraccarico. I servizi d'emergenza invece continuano a funzionare senza problemi. 20 000 piccole e medie imprese (PMI), due dei dieci più grandi negozi online della Svizzera, una grande azienda di logistica, parti di un'amministrazione cittadina e numerosi piccoli fornitori di hosting che sono clienti dell'operatore, riescono ad accedere solo con difficoltà al loro ambiente virtuale per due giorni e devono far fronte a dati corrotti. A causa del processo di recupero difettoso e dei backup mancanti, un ospedale con 500 posti letto, 2000 PMI e l'amministrazione fiscale di una città di media grandezza perdono una parte dei loro dati, 500 PMI perdono addirittura tutti dati. Gli utenti con connessioni dedicate, reti proprie o sistemi alternativi come la radiocomunicazione, la comunicazione satellitare e i provider con connessioni proprie non sono toccati o solo leggermente dall'evento.
Fase di ripristino	Dopo due giorni, il carico della rete torna alla normalità. Ai clienti che non erano adeguatamente preparati per un tale evento (per es. non avevano eseguito i backup dei dati e delle configurazioni), serve molto più tempo per recuperare i dati. Tra le misure rientrano il ripristino di record di dati coerenti, il reinserimento a posteriori di transazioni perse e altre operazioni simili.

Decorso temporale	L'evento si verifica repentinamente. Le sue conseguenze si fanno sentire nel giro di pochi minuti. Il carico normale della rete viene ripristinato dopo due giorni, ma il ripristino completo dei dati richiede ancora qualche giorno.
Estensione spaziale	Una delimitazione precisa dell'evento non è possibile. Le conseguenze si fanno sentire in tutta la Svizzera e anche in Europa.

Conseguenze

Per valutare le conseguenze di uno scenario, sono stati esaminati dodici indicatori di danno per i quattro settori soggetti a danni. L'entità prevista dei danni per lo scenario descritto sopra è riassunta nella seguente figura e spiegata nel testo sottostante. Il danno aumenta di un fattore 3 per ogni classe d'entità.



Persone

La perdita dei dati dei pazienti in un ospedale e in singoli studi medici comporta mancati trattamenti o trattamenti errati, che causano danni alla salute o addirittura la morte di alcuni pazienti.

A causa delle limitate possibilità di comunicazione, le prestazioni assistenziali a diverse persone bisognose di cure subiscono ritardi.

A seconda del servizio critico colpito, fino a 100 persone possono subire danni alla salute o ferite. Non si può escludere qualche decesso, una decina al massimo.

Ambiente

Di principio, l'evento non causa danni agli ecosistemi.

Se l'evento mette fuori uso i comandi di impianti e sistemi potenzialmente pericolosi per l'ambiente, possono verificarsi danni ambientali, ad esempio un'emissione incontrollata di sostanze nocive nel suolo, nell'acqua o nell'aria.

Economia

I clienti del centro elaborazione dati e i rivenditori direttamente colpiti (circa 20 000 PMI) devono far fronte a costi supplementari nel campo dell'informatica e del personale per mantenere i loro servizi o sono costretti a cessare la loro attività.

I due negozi online colpiti subiscono un forte calo delle vendite nei due giorni dell'interruzione. L'azienda logistica colpita deve far fronte a elevati costi supplementari per mantenere i suoi servizi. Le sedi esterne dell'amministrazione cittadina sono difficili da raggiungere online o per telefono per due giorni.

I clienti dei rivenditori direttamente colpiti e i servizi online penalizzati dal sovraccarico della rete subiscono un rallentamento della loro attività commerciale per due giorni.

2000 PMI, gli enti fiscali e l'ufficio anagrafe della città colpita subiscono una perdita parziale di dati aziendali, fiscali e anagrafici.

500 PMI subiscono addirittura una perdita completa dei dati memorizzati sui server dell'operatore, con gravi conseguenze.

Le perdite finanziarie e i costi di gestione ammontano a circa 1 miliardo di franchi. L'evento riduce la prestazione economica della Svizzera di circa 350 milioni di franchi.

Società

L'interruzione del centro elaborazione dati blocca la logistica di varie aziende (per es. grandi distributori) causando serie difficoltà d'approvvigionamento.

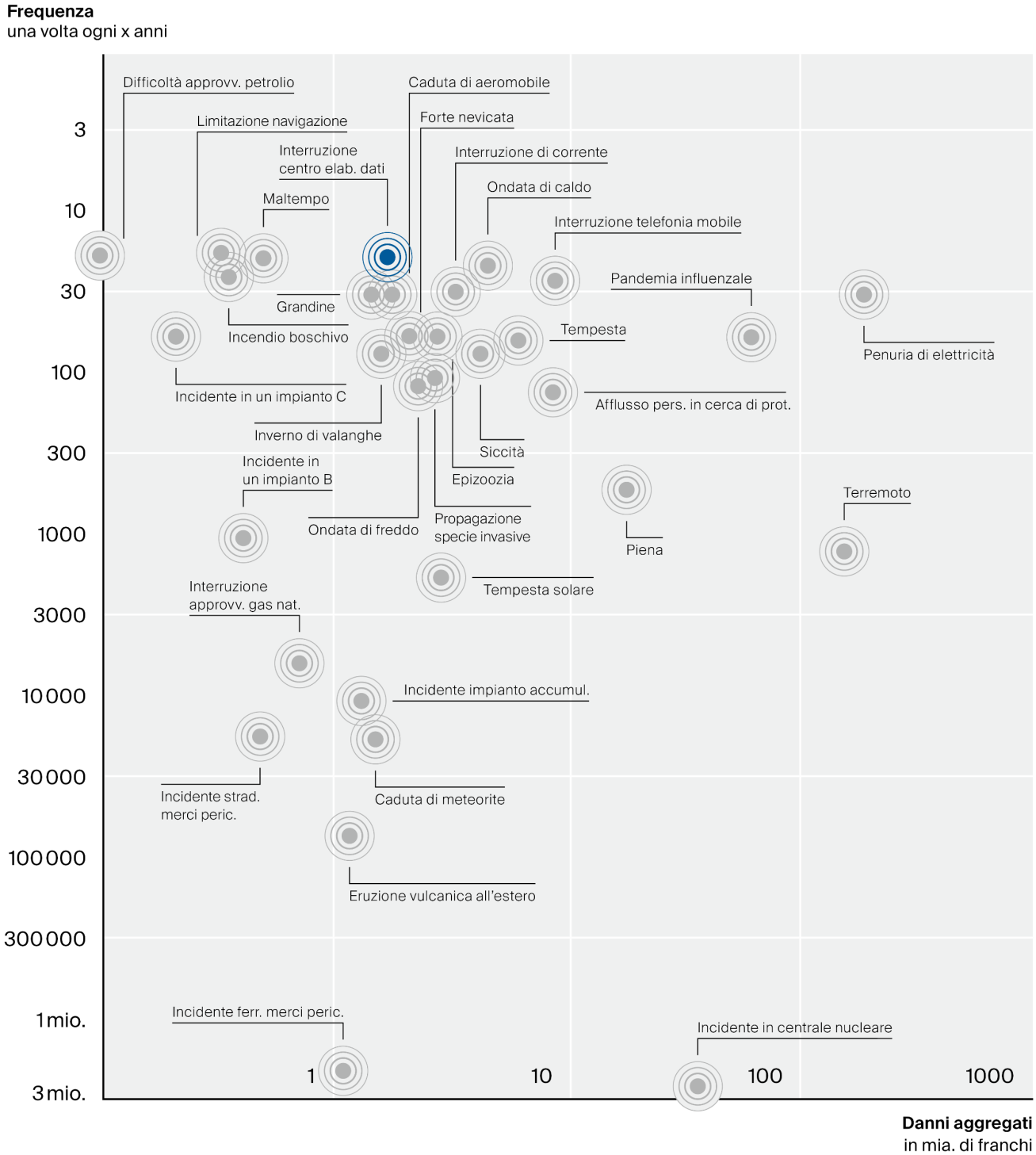
Gli utenti colpiti non hanno accesso al web (interruzione dei servizi basati su internet come e-mail, social media, shopping online, servizi di streaming, ecc.).

Lo scambio di dati tra Spitex, ospedali, uffici dell'anagrafe ecc. è limitato.

Dopo l'evento, i mass media criticano l'operatore del centro elaborazione dati giudicandolo «incapace di fornire un servizio affidabile e responsabile di aver paralizzato metà Svizzera». Anche i clienti del provider finiscono nel mirino della stampa per la loro forte dipendenza da pochi CED o aziende specializzate o per la mancanza di precauzioni proprie.

Rischio

Il rischio dello scenario descritto viene presentato insieme agli altri scenari di pericolo analizzati in una matrice del rischio in cui la probabilità d'occorrenza viene rappresentata come frequenza (1 volta ogni x anni) sull'asse y (in scala logaritmica) e l'entità dei danni viene raggruppata e monetizzata in CHF sull'asse x (pure in scala logaritmica). Il rischio di uno scenario risulta dal prodotto tra probabilità d'occorrenza ed entità dei danni. Quanto più a destra e in alto nella matrice si trova uno scenario, tanto più elevato è il rischio che comporta.



Basi legali

Costituzione	— Costituzione federale della Confederazione Svizzera del 18 aprile 1999; RS 101: art. 13 (Protezione della sfera privata), art. 92 (Poste e telecomunicazioni) e art. 173 (Altri compiti e attribuzioni)
Leggi	— Legge federale del 21 marzo 1997 sulle misure per la salvaguardia della sicurezza interna (LMSI); RS 120 — Legge federale del 19 giugno 1992 sulla protezione dei dati (LPD); RS 235.1 — Legge federale del 17 giugno 2016 sull'approvvigionamento economico del Paese (Legge sull'approvvigionamento del Paese, LAP); RS 531 — Legge federale del 18 marzo 2016 sulla sorveglianza della corrispondenza postale e del traffico delle telecomunicazioni (LSCPT); RS 780.1 — Disegno di legge federale sulla sicurezza delle informazioni nella Confederazione (legge sulla sicurezza delle informazioni, LSI); ancora in esame in Parlamento.
Ordinanze	— Ordinanza del 17 febbraio 2010 sull'organizzazione del Dipartimento federale delle finanze (Org-DFF); RS 172.215.1 — Ordinanza del 14 giugno 1993 relativa alla legge federale sulla protezione dei dati (OLPD); RS 235.11 — Ordinanza del 2 marzo 2018 sullo Stato maggiore federale Protezione della popolazione (OSMFP); RS 520.17 — Ordinanza del 18 marzo 2004 relativa alla legge federale sulla Banca nazionale svizzera (Ordinanza sulla Banca nazionale, OBN); RS 951.131

Ulteriori informazioni

Sul pericolo

- Autorità federale di vigilanza sui mercati finanziari (FINMA) (2018): Circolare 2018/3. Outsourcing - banche e assicurazioni. Esternalizzazioni presso banche e imprese di assicurazione. FINMA, Berna
- Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) (diverse annate): Sicurezza dell'informazione. Situazione in Svizzera e a livello internazionale. Rapporto semestrale. DFF e DDPS, Berna
- Consiglio federale (2018): Strategia nazionale per la protezione della Svizzera contro i cyber-rischi informatici (SNPC) 2018-2022. ISB, Berna
- Consiglio federale (2017): Strategia nazionale per la protezione delle infrastrutture critiche 2018-2022. Berna
- ISO/IEC 27018 (2019): Tecnologia dell'informazione - Tecniche di sicurezza - Codice in materia di protezione dei dati personali (PII) nei cloud pubblici in qualità di processori PII. ISO
- ISO/IEC 27001 (2013): Tecnologia dell'informazione - Tecniche di sicurezza - Sistemi di gestione della sicurezza delle informazioni - Requisiti. ISO
- ISO 50001 (2011): Gestione dell'energia - Sistemi di gestione dell'energia - Requisiti e linee guida all'uso. ISO
- National Institute of Standards and Technology (NIST) (2018): Framework for Improving Critical Infrastructure Cybersecurity. Versione 1.1. NIST
- Ufficio federale della protezione della popolazione (UFPP) (2015): Guida alla protezione delle infrastrutture critiche. UFPP, Berna

Sull'analisi dei rischi a livello nazionale

- Ufficio federale della protezione della popolazione (UFPP) (2020): Metodo per l'analisi nazionale dei rischi. Catastrofi e situazioni d'emergenza in Svizzera 2020 (in tedesco). Versione 2.0. UFPP, Berna
- Ufficio federale della protezione della popolazione (UFPP) (2020): Quali rischi minacciano la Svizzera? Catastrofi e situazioni d'emergenza in Svizzera 2020. UFPP, Berna
- Ufficio federale della protezione della popolazione (UFPP) (2020): Rapporto sull'analisi nazionale dei rischi. Catastrofi e situazioni d'emergenza in Svizzera 2020. UFPP, Berna
- Ufficio federale della protezione della popolazione (UFPP) (2019): Catalogo dei pericoli. Catastrofi e situazioni d'emergenza in Svizzera. 2ª edizione. UFPP, Berna

Ufficio federale della protezione della popolazione UFPP

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