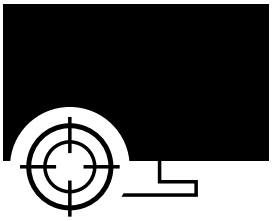
Cyberattacco



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

Definizione

Secondo la Cyberstrategia nazionale (CSN), i cyberattacchi sono atti deliberati e non autorizzati da parte di attori privati o statali attraverso mezzi informatici o di comunicazione (TIC) allo scopo di compromettere l'integrità, l'affidabilità o la disponibilità di informazioni e dati; a seconda del tipo di attacco, questo può avere anche conseguenze fisiche.

In base alla motivazione e ai mezzi dell'aggressore, i cyberattacchi si suddividono in:
- cybercriminalità: infrazione commessa nel cyberspazio o con mezzi informatici nell'intento di arricchirsi
- cyberspionaggio: ottenimento non autorizzato di informazioni economiche, politiche o militari (confidenziali)
- cybersabotaggio: causare danni mirati alle TIC e ai beni fisici per dimostrare il proprio potere e intimidire
- cybersovversione: minare il sistema politico di un altro Stato attraverso attori statali, parastatali o politici
- cyberattacco in conflitti armati: gestione ibrida e asimmetrica di un conflitto fino alla pura cyberguerra

Le forme di attacco si presentano spesso in combinazione tra di esse e i loro confini sono fluidi. Il presente dossier tratta in particolare la cybercriminalità, il cybersabotaggio e la cybersovversione.

Febbraio 2026

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Ufficio federale della protezione della popolazione UFPP

Indice

Esempi di eventi

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

Gennaio 2025
Svizzera

Attacco DDoS

Nel gennaio 2025 la Svizzera è stata vittima di diversi attacchi Distributed Denial of Service (DDoS), rivendicati da due diversi gruppi di hacker attivisti.

Il 6 gennaio 2025 i bancomat, il sito web e l'app per l'e-banking di una banca svizzera sono stati colpiti da un attacco DDoS, che è stato rivendicato dal gruppo di hacker attivisti pro-musulmani RooTDoS e motivato sostenendo che la Svizzera, con l'entrata in vigore del divieto di dissimulare il viso (LDDV), avesse introdotto una legge anti-musulmana. Alla fine della giornata la maggior parte dei servizi era nuovamente disponibile. In seguito, il 10 gennaio lo stesso collettivo ha sferrato ulteriori attacchi ai servizi web dell'Amministrazione federale: per circa 45 minuti sono stati compromessi servizi quali la telefonia, Outlook e diversi siti web e applicazioni specialistiche della Confederazione, ma grazie alle contromisure adottate è stato possibile stabilizzare la situazione.

Dal 20 al 26 gennaio 2025, il gruppo di hacker attivisti filorusso NoName057(16) ha condotto attacchi DDoS quotidiani contro diversi siti web svizzeri, tra cui quelli della regione di Davos, del settore dei media, di banche, Comuni e Cantoni svizzeri, nonché portali per l'accesso ai servizi statali. Gli attacchi, che sono stati rivendicati da NoName057(16), hanno coinciso con il Forum economico mondiale (WEF) di Davos, al quale era presente anche il presidente ucraino Volodymyr Zelensky. L'Ufficio federale della cybersicurezza (UFCS) aveva previsto la possibilità di attacchi di tale genere durante il WEF e aveva avvertito in anticipo gli operatori delle infrastrutture critiche.

Febbraio 2022
Ucraina

Cybersabotaggio

Il 24 febbraio 2022, in Europa si sono verificate diverse interruzioni delle connessioni con il satellite per le telecomunicazioni KA-SAT dell'azienda statunitense ViaSat, che è utilizzato da numerose aziende, autorità e utenti privati per accedere a Internet, in particolare nelle regioni discoste. ViaSat ha pubblicato un'analisi dell'accaduto, dalla quale emerge che si è trattato di un attacco informatico mirato e diretto esclusivamente alla parte della rete satellitare responsabile della copertura dell'Ucraina, ma con ripercussioni che non si sono limitate a quest'area. L'incidente ha causato disagi, per esempio, anche in Germania, dove non è stato più possibile accedere ai sistemi di sorveglianza e di controllo remoto degli impianti eolici. Dall'inizio della guerra in Ucraina sono comparsi anche numerosi wiper, ossia malware che hanno lo scopo di distruggere i dati, rendendoli illeggibili tramite crittografia o sovrascrittura e quindi cancellandoli in modo irreversibile. Sono stati usati per prendere di mira organizzazioni di diversi settori dell'amministrazione pubblica, dell'energia e della finanza.

Da marzo a dicembre 2020
Stati Uniti

Cyberspionaggio

Il 13 dicembre 2020 le autorità americane hanno segnalato che un gruppo di hacker era riuscito a penetrare nella loro rete tramite un aggiornamento compromesso del software Orion IT. Nel mese di marzo dello stesso anno era stata infatti inserita una backdoor nell'aggiornamento ufficiale del programma, che circa 18 000 utenti avevano scaricato. Gli attentatori hanno selezionato obiettivi interessanti per proseguire l'attacco e hanno chiuso la backdoor delle vittime colpite collateralmente. Secondo fonti americane, questa operazione ha fatto parte di una più ampia campagna di spionaggio che ha colpito altre aziende.

Fattori influenti

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

Fonte di pericolo	– Caratteristiche degli attentatori (ideologia e motivazione, predisposizione alla violenza, capacità e know-how, livello di organizzazione e professionalizzazione, accesso a mezzi finanziari nonché a risorse IT e a infrastrutture) – Comportamento degli aggressori (statali o no) – Vulnerabilità dei sistemi target (consapevolezza insufficiente dei rischi in relazione alle cyberminacce, software e hardware difettosi, compliance insufficiente, negligenza, assenza di misure di protezione organizzative, tecniche e architettoniche) – Dipendenze e complessità dei sistemi (p. es. servizi cloud, rischi della catena di approvvigionamento), grado di permeabilità di Stato, economia e società – Nuove possibilità di attacchi tecnici contro le quali non esistono ancora dispositivi di difesa adeguati (p. es. intelligenza artificiale, informatica quantistica)
Momento	– Dipende in genere da decisioni e sviluppi aziendali, politici o sociali – Orario e giorno della settimana: il cyberattacco viene spesso sferrato in un momento in cui la vittima ha poche risorse disponibili per rilevarlo e reagire (fine settimana/periodo di ferie) – I preparativi per mettere a segno il cyberattacco possono essere effettuati molto prima dell'attacco stesso, mentre i mezzi e le infrastrutture necessari possono essere predisposti anche in un altro momento
Luogo / Estensione	– Entità e caratteristiche rilevanti dell'oggetto o del sistema preso di mira (singola persona o singolo oggetto, organizzazione o azienda, ramo, settore o settori collegati in rete, tecnologia specifica, istituzioni statali, ecc.) – Identificazione dell'autore (attribuzione) e localizzazione (luogo in cui si trovano gli autori dell'attacco e i loro complici) – Risorse utilizzate (hardware/software, reti, interfaccia, tecnologie, protocolli, personale ecc.)
Decorso dell'evento	– Prevedibilità dell'insorgenza, dell'intensità e del tipo di evento (tempi di preallerta, momento delle raccomandazioni di comportamento) – Forma e caratteristiche dell'attacco (nota/sconosciuta) – Effetto delle misure di protezione preventive – Svolgimento dell'attacco vero e proprio (unico; a ondate; lento all'inizio poi in crescendo oppure con una rapida escalation; ibrido combinato con azioni fisiche) – Effetto delle contromisure adottate nel caso specifico – Comportamento/reazione delle persone coinvolte, delle organizzazioni, degli Stati – Comportamento/reazione delle forze d'intervento, delle autorità responsabili, degli esperti e dei fornitori di servizi di sicurezza coinvolti, come il Computer Security Incident Response Team (CSIRT), il Computer Emergency Response Team (CERT) e il Security Operation Center (SOC). – Reazione della popolazione e degli ambienti politici

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	– Forma d'attacco nota – Le contromisure sussistono o possono essere sviluppate rapidamente – L'attacco si verifica solo una volta – Attacchi a infrastrutture critiche nei settori industriali e dei servizi amministrativi – Furto di dati ufficiali ed economici rilevanti – L'opinione pubblica non è presa di mira dall'attacco – Attacco reso noto all'opinione pubblica solo una volta concluso
2 — forte	– Combinazione di forme d'attacco note oppure forma d'attacco relativamente sconosciuta – Le contromisure non sussistono, ma possono essere sviluppate in pochi giorni – L'attacco si verifica a ondate – Furto di dati ufficiali ed economici rilevanti – Attacchi a infrastrutture critiche nei settori finanziari e dei servizi amministrativi, manipolazioni mirate di informazioni alle pagine web statali e private nonché ai canali d'informazione, interruzione dei servizi elettronici presso gli istituti finanziari (ad esempio e-banking) – L'opinione pubblica viene informata sul fatto che sono in corso degli attacchi – L'opinione pubblica è coinvolta dagli attacchi, le conseguenze sono tangibili nella quotidianità (ad esempio non è più possibile prelevare contanti oppure effettuare transazioni)
3 — estremo	– Forma di attacco nuova o perfezionata – Assenza di contromisure, il cui sviluppo dura settimane o è impossibile in tempo utile – La forma dell'attacco evolve in crescendo – Attacchi a infrastrutture critiche nei settori dell'energia, della telecomunicazione e dei trasporti – Manipolazione e danneggiamento dei sistemi di monitoraggio del traffico e dell'energia, notevoli disagi ai servizi di telecomunicazione – L'opinione pubblica realizza immediatamente che sono in corso degli attacchi – L'opinione pubblica è direttamente coinvolta dagli attacchi, le conseguenze sono tangibili nella quotidianità

Scenario

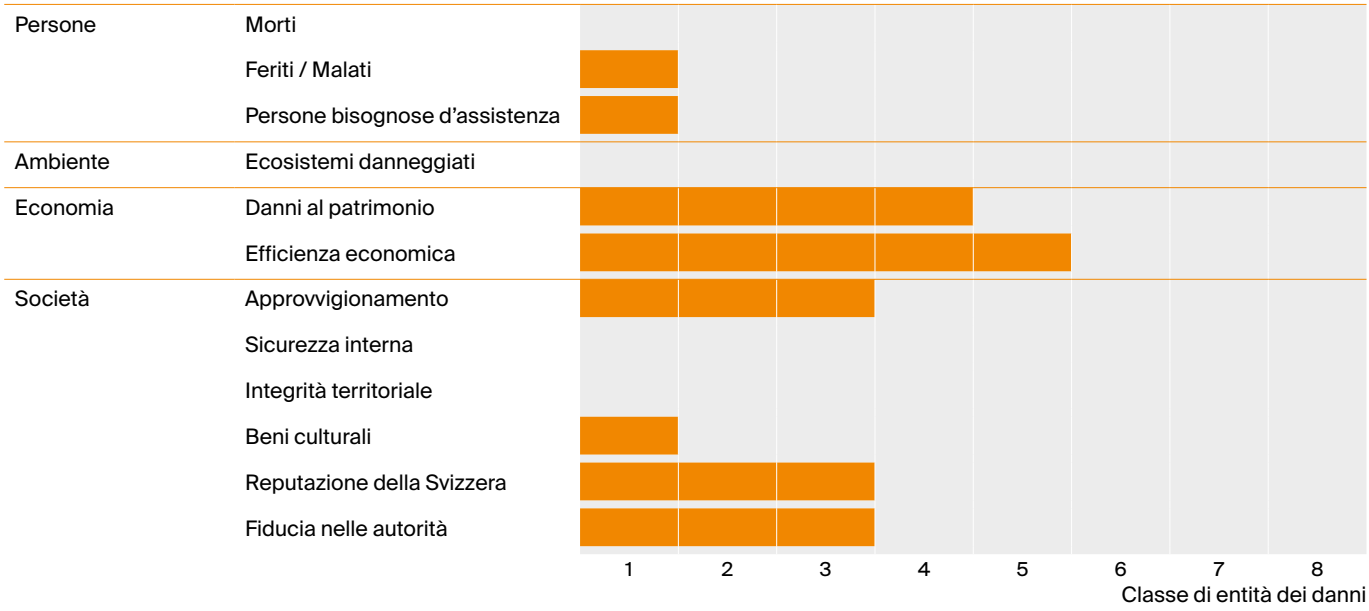
Il seguente scenario si basa sul livello d'intensità «forte».

Situazione iniziale / fase preliminare	Un evento politico (per es. l'esito di un voto popolare delicato) o un'attività tollerata in Svizzera di un'organizzazione, di un'impresa o di un settore vengono giudicati inaccettabili da un'organizzazione estera o da uno Stato terzo, che decide di reagire con un cyberattacco.
Fase dell'evento	Vari siti web di organizzazioni e portali d'informazione vengono hackerati. Questi siti compromessi e i social network vengono utilizzati in modo mirato per diffondere false informazioni. Gli attacchi, che si estendono su un periodo di due a tre mesi, colpiscono principalmente le imprese mediatiche. Inizialmente isolati e sporadici, diventano via via più frequenti. Alcune organizzazioni interessate segnalano gli attacchi all'organo di contatto nazionale dell'Ufficio federale della cybersicurezza (UFCS) o alle autorità locali preposte al perseguimento penale. L'UFCS valuta queste informazioni nel loro complesso e fornisce i risultati alle autorità competenti nonché alle imprese coinvolte. In una presa di posizione ufficiale, il Consiglio federale condanna gli attacchi ai siti web e difende la posizione della Svizzera. Da uno a tre giorni dopo la presa di posizione della Confederazione, hanno luogo attacchi DDoS concentrati sui siti web degli enti pubblici. Sono colpiti soprattutto i dipartimenti e gli uffici federali che hanno un legame con la controversia. Inizialmente si presume che il punto d'ingresso utilizzato dagli hacker siano dei server statali e cantonali piratati. Oltre ai siti web manipolati, vengono ora notevolmente perturbati anche i servizi online degli uffici federali coinvolti (E-Government). Numerosi collaboratori scelti casualmente ricevono e-mail con allegati contenenti dei ransomware. Rimuovere il virus e reimpostare i computer richiede molto tempo. Sporadicamente si registrano tentativi di violazione dei sistemi ITC della Confederazione, ma non viene accertato nessun furto di dati. Gli uffici interessati della Confederazione segnalano gli eventi all'UFCS. Tre settimane più tardi, gli attacchi vengono diretti al settore finanziario. Inizialmente colpiscono i siti web di vari fornitori di servizi finanziari. Di conseguenza, alcune funzioni importanti non sono disponibili o solo in modo limitato per una durata di due o tre settimane. In particolare, per diversi giorni le comunicazioni della Borsa svizzera sulle relative pagine web risultano difficoltose. Le operazioni interbancarie sono fortemente perturbate ma continuano a funzionare. Oltre ai servizi online degli istituti finanziari, sono colpiti anche i terminali di pagamento nel commercio al dettaglio in tutta la Svizzera, poiché per due giorni i server non sono più raggiungibili. Anche gran parte dei distributori automatici di contanti vengono sistematicamente bloccati.

	L'uso della posta elettronica è notevolmente compromesso a causa del massiccio invio di spam (fra cui molte e-mail di propaganda e di phishing). Sono prese di mira dagli attacchi anche le organizzazioni che offrono servizi agli istituti finanziari, in particolare quelle che forniscono le informazioni finanziarie e quelle che elaborano le transazioni. Si constatano inoltre dei tentativi di penetrare nei sistemi informatici di tali istituti. A tal fine vengono attaccati dapprima gli IT Managed Service Provider (MSP) e in seguito si tenta di accedere ai sistemi e ai dati tramite i loro diritti di accesso diretti. La Borsa di Zurigo subisce un attacco malware, apparentemente partito dalla Svizzera, proprio al momento dell'apertura delle contrattazioni. Gli attentatori sono infatti riusciti a introdurre dei malware in un sistema che è connesso a quelli della Borsa svizzera, la quale deve interrompere le negoziazioni e può riaprirle solo due giorni più tardi, dopo l'implementazione di meccanismi di protezione aggiuntivi. Gli organi federali svizzeri competenti collaborano da diverso tempo con i loro omologhi di altri Paesi. L'organizzazione criminale responsabile degli attacchi viene identificata e uno Stato terzo riesce a neutralizzarla, così come la sua infrastruttura. In seguito gli attacchi diminuiscono rapidamente.
Fase di ripristino	Poco alla volta i siti web delle autorità, degli istituti finanziari e delle imprese mediatiche vengono riattivati o stabilizzati. Una settimana dopo la fine degli attacchi, i siti web essenziali sono nuovamente disponibili. Tuttavia, il ripristino richiede più tempo o non è possibile per i provider non adeguatamente protetti. Circa un mese dopo la fine degli attacchi, tutti i siti web sono infine ripristinati. Non è possibile escludere che i pirati informatici siano riusciti ad appropriarsi illecitamente di dati presenti nei sistemi attaccati. Terminati gli attacchi, gli organi interessati sono impegnati ancora per settimane a valutare l'entità della fuga di dati. Per la popolazione, la situazione si normalizza un mese dopo la fine degli attentati.
Decorso temporale	La fase dell'evento dura circa cinque mesi e si svolge in tre ondate 1: compromissione dei siti web delle imprese mediatiche 2: attacchi all'infrastruttura IT della Confederazione 3: attacchi alle infrastrutture IT del settore finanziario) Gli effetti constatati si estendono complessivamente su un arco di circa sei mesi.
Estensione spaziale	Gli attacchi sono diretti contro i media online, gli enti pubblici e il settore finanziario della Svizzera. Si ripercuotono fondamentalmente su tutte le persone che hanno un rapporto con le organizzazioni interessate.

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

L'evento non causa vittime.

Gli alterchi che si verificano davanti ai bancomat possono causare feriti. Alcune persone necessitano di assistenza a causa dello stress psicologico. La difesa e la gestione immediata dell'attacco comportano un carico di lavoro elevato per il personale specializzato delle organizzazioni interessate e, di conseguenza, alcuni dipendenti del settore informatico sono portati all'esaurimento. Gli attacchi allo Stato e alla finanza, nonché la disinformazione, provocano inoltre in molte persone timori per il futuro. Si stima un centinaio di feriti, perlopiù in modo lieve.

L'interruzione dei servizi finanziari si ripercuote anche su circa 20 000 beneficiari di assistenza sociale, che non dispongono di riserve e necessitano quindi di un ulteriore supporto economico per una durata di 10 giorni.

Ambiente

L'evento non causa danni agli ecosistemi.

Economia

La Borsa rimane chiusa per due giorni.

Le operazioni interbancarie sono paralizzate, ma continuano a funzionare sul piano internazionale.

Il traffico dei pagamenti nel commercio al dettaglio è temporaneamente perturbato in tutta la Svizzera. Gran parte dei bancomat sono fuori uso, quelli ancora funzionanti sono presi d'assalto.

Dal momento che ci sono sempre meno sportelli dove è possibile prelevare, procurarsi contanti diventa molto difficile.

Dopo l'eliminazione dei disservizi si registra un forte aumento della domanda di generi alimentari, beni di prima necessità e contante, il che porta nuovamente a carenze a breve termine.

I servizi online degli istituti finanziari interessati sono fortemente limitati e, nel peggiore dei casi, compromessi o addirittura indisponibili. Poiché le relative transazioni, come ad esempio gli ordini di pagamento o di borsa, non possono essere effettuate nemmeno allo sportello, si verificano ritardi nei pagamenti. Alcuni clienti (in alcuni casi anche importanti) perdono fiducia negli istituti e sciolgono i loro rapporti d'affari. Altri chiedono il risarcimento dei danni o intentano cause.

Le organizzazioni colpite subiscono ulteriori danni finanziari a causa delle spese aggiuntive in termini di personale e tecnologia necessarie per contenere o respingere gli attacchi, valutare la portata della fuga di dati e identificare i responsabili. A questi vanno sommati gli investimenti in ulteriori misure di sicurezza.

Inoltre, a causa delle interruzioni, anche le dogane subiscono limitazioni.

I danni diretti e i costi di gestione ammontano a circa 870 milioni di franchi. I danni per la perdita di capacità economica si aggirano attorno a 1.7 miliardi di franchi.

Società

Si verificano le seguenti impasse e interruzioni dell'approvvigionamento.

- Finanze: in seguito all'evento si verificano interruzioni dei servizi finanziari (sia per quanto riguarda i contanti sia per le transazioni online) che interessano circa 4 milioni di persone per 3 giorni, ma che non comportano grandi impasse nell'approvvigionamento.
- Derrate alimentari: a causa delle restrizioni nel prelievo di contanti e nelle transazioni finanziarie, non tutte le persone possono fare la spesa come di consueto. Sono interessate circa 400 000 persone.
- Approvvigionamento di petrolio: a causa del malfunzionamento dei terminali di pagamento, in gran parte del territorio è possibile fare rifornimento di carburante solo in contanti. Sono interessate circa 100 000 persone.
- Media: l'attacco alle aziende di questo settore comporta una riduzione dell'offerta di servizi mediatici. Sono interessate circa 500 000 persone per 10 giorni.

Gli attacchi creano insicurezza, ma non si verificano reazioni di panico. Per contro, la fiducia della popolazione svizzera nelle autorità e nelle istituzioni finanziarie è compromessa. Gli istituti finanziari colpiti assumono più personale di sicurezza privato per far fronte al forte afflusso di persone agli sportelli. L'ordine e la sicurezza interna rimangono garantiti in ogni momento.

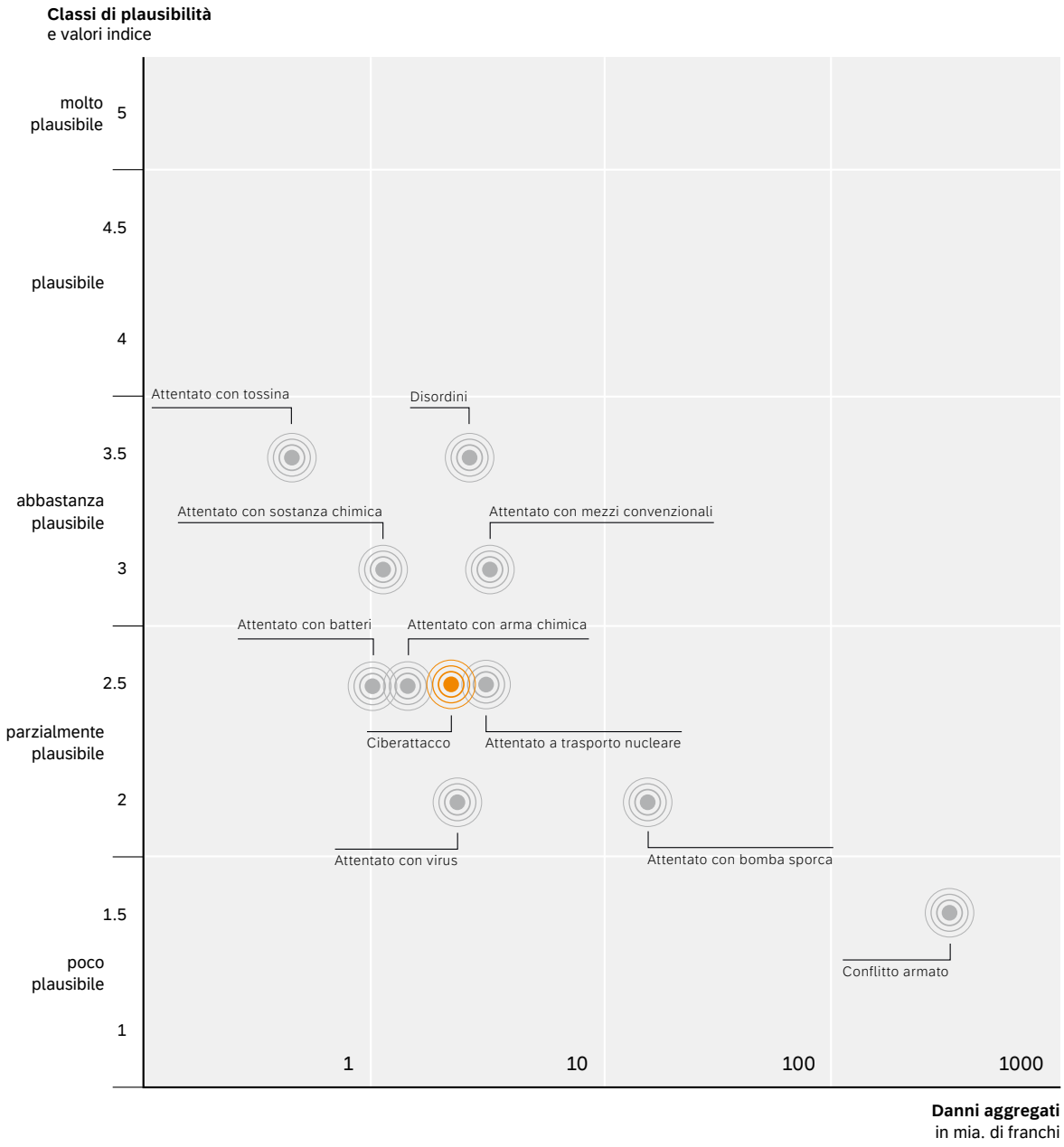
I beni culturali (digitali) sono poco esposti a rischi. Tuttavia, essendo gli archivi (in particolare quelli di grandi dimensioni) collegati ai sistemi TIC cantonali, gli attacchi informatici a questi ultimi possono comprometterne e ridurne la disponibilità. Informazioni sensibili contenute negli archivi possono inoltre subire distruzioni irreversibili, furti o diffusione non autorizzata.

I media internazionali riferiscono a più riprese del cyberattacco. All'estero fanno notizia soprattutto l'attacco agli istituti finanziari e l'interruzione di due giorni della borsa.

In seguito agli attacchi, per alcune settimane i media svizzeri riportano notizie molto critiche («La Svizzera così vulnerabile!»), che accendono polemiche e dibattiti e incidono sulla percezione che ha l'opinione pubblica dell'evento. Il legame tra cyberspazio, la possibile violazione dell'integrità territoriale e le misure che la Svizzera può adottare contro altri attacchi simili è oggetto di accese discussioni.

Rischio

La plausibilità dello scenario descritto e l'entità dei danni sono raffigurati insieme agli altri scenari di pericolo analizzati in una matrice del rischio. La plausibilità degli scenari provocati intenzionalmente viene rappresentata sull'asse y (in una scala con 5 gradi di plausibilità) e l'entità dei danni viene raggruppata e monetizzata in CHF sull'asse x (in scala logaritmica). Il rischio di uno scenario risulta dal prodotto tra plausibilità 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

Leggi	– Legge federale del 21 marzo 1997 sulle misure per la salvaguardia della sicurezza interna (LMSI); RS 120 – Legge federale del 18 dicembre 2020 sulla sicurezza delle informazioni (LSIn); RS 128 – Legge federale di complemento del Codice civile svizzero del 30 marzo 1911 (Libro quinto: Diritto delle obbligazioni); RS 220 – Legge federale del 25 settembre 2020 sulla protezione dei dati (LPD); RS 235.1 – Codice penale svizzero del 21 dicembre 1937 (CP); RS 311.0 – Legge federale del 17 giugno 2016 sull'approvvigionamento economico 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
Ordinanze	– Ordinanza dell'8 novembre 2023 sulla sicurezza delle informazioni in seno all'Amministrazione federale e all'esercito (Ordinanza sulla sicurezza delle informazioni, OSIn); RS 128.1 – Ordinanza del 7 marzo 2025 sulla cybersicurezza (OCS); RS 128.51 – Ordinanza del 20 dicembre 2024 sull'organizzazione di crisi dell'Amministrazione federale (OCAF); RS 172.010.8 – Ordinanza del 31 agosto 2022 sulla protezione dei dati (OPDa); RS 235.11
Altre basi legali	– Council of Europe (2001): European Convention on Cybercrime

Ulteriori informazioni

Sul pericolo

- Denning, D. E. (2007): A View of Cyberterrorism Five Years Later. In: Himma, K. (Ed.): Internet Security. Hacking, Counterhacking and Society. Jones and Bartlett, Boston.
- European Union Agency for Network and Information Security (ENISA) (2019): ENISA Threat Landscape Report 2018. 15 Top Cyberthreats and Trends. EU, Heraklion.
- Il Consiglio federale (2023): Strategia nazionale per la protezione delle infrastrutture critiche. UFPP, Berna.
- Il Consiglio federale (2023): Cyberstrategia nazionale (CSN). Ufficio federale della cybersicurezza (UFCS), Berna.
- Ministry of Economic Affairs and Communications: Department of State Information Systems (2008): Information Technology in Public Administration of Estonia. Yearbook 2007. Tallinn.
- Ufficio federale della cybersicurezza (UFCS) (vari anni): Sicurezza delle informazioni. La situazione in Svizzera e a livello internazionale. Rapporto semestrale. DFF e DDPS, Berna.

Sull'analisi nazionale dei rischi

- Ufficio federale della protezione della popolazione (UFPP) (2026): Raccolta dei dossier di pericolo. Catastrofi e situazioni d'emergenza in Svizzera 2025. UFPP, Berna.
- Ufficio federale della protezione della popolazione (UFPP) (2026): Metodo per l'analisi nazionale dei rischi. Catastrofi e situazioni d'emergenza in Svizzera 2025. Versione 3.0. UFPP, Berna.
- Ufficio federale della protezione della popolazione (UFPP) (2026): Quali rischi minacciano la Svizzera? Catastrofi e situazioni d'emergenza in Svizzera 2025. UFPP, Berna.
- Ufficio federale della protezione della popolazione (UFPP) (2026): Rapporto sull'analisi nazionale dei rischi. Catastrofi e situazioni d'emergenza in Svizzera 2025. UFPP, Berna.
- Ufficio federale della protezione della popolazione (UFPP) (2023): Catalogo dei pericoli. Catastrofi e situazioni d'emergenza in Svizzera 2025. 3a edizione. UFPP, Berna.

Impressum

Ufficio federale della protezione della popolazione UFPP
Guisanplatz 1B
CH-3003 Berna
risk-ch@babs.admin.ch
www.protpop.ch
www.risk-ch.ch

88.128.14.i