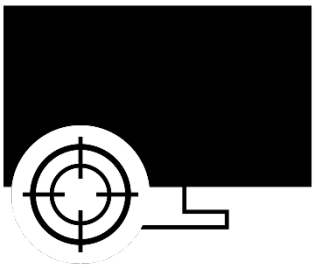
Ciberattacco



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

Definizione

Secondo la Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC), i ciberattacchi sono atti deliberati e non autorizzati da parte di attori privati o statali nel ciberspazio, 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 ciberattacchi si suddividono in:

- cibercriminalità: infrazione commessa nel ciberspazio o con mezzi informatici nell’intento di arricchirsi
- ciberestorsione: riscatto con ransomware
- cibersabotaggio e ciberterrorismo: danni alle infrastrutture informatiche e a beni fisici come dimostrazione di potere o intimidazione
- ciberspionaggio: ottenimento non autorizzato di informazioni economiche, politiche e militari (confidenziali)
- disinformazione/propaganda: diffusione mirata di false informazioni allo scopo di generare insicurezza
- ciberattacco in conflitti: gestione ibrida e asimmetrica di un conflitto fino alla pura ciberguerra

I confini tra le varie forme di ciberattacco sono fluidi.

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.

---

27 giugno 2017
Ucraina

Attacco con «Cryptolocker»

Nel giugno 2017, il *cryptolocker* «NotPetya» ha infettato dei computer in tutto il mondo, ma in particolare in Ucraina. I dati sul disco rigido venivano crittografati e la vittima invitata a pagare un riscatto per decrittografarli. Oltre a organizzazioni ucraine, sono finite nel mirino degli attentatori anche grandi aziende, quali ad es. la compagnia di navigazione danese Maersk Line, la compagnia petrolifera russa Rosneft, la società farmaceutica americana Merck Sharp & Dohme o la multinazionale Mondelez International, attiva nel settore agroalimentare. La Maersk Line stima i danni subìti a 300 milioni di dollari; altre imprese dichiarano danni per cifre analoghe.

Dicembre 2010
Svizzera

Attacco DDoS «Operazione Payback»

Dopo il congelamento, da parte di PostFinance Svizzera, e la chiusura, da parte di MasterCard e Visa, dei conti del fondatore di WikiLeaks Julian Assange, i siti web dei fornitori di servizi finanziari sono stati presi di mira da massicci attacchi Denial of Service (DoS). Si ritiene che questa operazione di resa dei conti (operation Payback) possa essere collegata al gruppo di hacker Anonymous. I siti web sono rimasti inaccessibili per diverse ore ed era impossibile effettuare transazioni online. Non è possibile quantificare l'ammontare esatto dei danni.

Aprile/maggio 2007
Estonia

Importante attacco DDoS

Dopo la decisione del governo estone di spostare la statua del Milite ignoto dal centro della capitale Tallinn a un cimitero militare in periferia, a cavallo tra aprile e maggio 2007 persone non identificate hanno messo in ginocchio con un attacco Distributed Denial of Service (DDoS) varie organizzazioni estoni, fra cui il Parlamento (incl. il server di posta elettronica), banche, ministeri e portali di notizie. Vari siti web sono stati piratati e modificati. Gli attacchi ai router nel backbone internet e ai server DNS hanno provocato brevi interruzioni (inferiori ai cinque minuti) nel traffico di dati attraverso i backbone. Gli attacchi alle due maggiori banche estoni hanno interrotto per quasi due ore il sistema di e-banking di una delle due banche. Una delle banche colpite stima i danni finanziari dovuti al ciberattacco a circa 1 milione di dollari. Non sono disponibili informazioni sui danni a infrastrutture e sistemi IT statali. L'integrità dei sistemi principali non è stata compromessa, tuttavia la rete dei sistemi era fortemente sovraccarica e inaccessibile, o solo difficilmente accessibile, per la popolazione.

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, infrastruttura controllata/già disponibile) — Comportamento di uno Stato o di organizzazioni con sede nel Paese (di natura criminale o parastatale) — Vulnerabilità dei sistemi target (manutenzione carente o impossibile dei sistemi target, consapevolezza insufficiente dei rischi soprattutto tra i quadri dirigenti, governance e processi insufficienti in merito alla sicurezza delle informazioni, collegamento tra i sistemi nonché dipendenze e complessità, grado di permeabilità di Stato, economia e società, monocultura informatica, software e hardware difettosi, compliance insufficiente, negligenza, misure di protezione organizzative, tecniche e architettoniche adottate)
Momento	— Dipende in genere da decisioni e sviluppi aziendali, politici o sociali — Giorno feriale o festivo/fine settimana. Di norma in un momento inaspettato per la vittima — I preparativi per mettere a segno l'attacco possono essere effettuati molto prima del ciberattacco stesso. I mezzi necessari e le infrastrutture possono essere realizzati anche in un altro contesto
Luogo / Estensione	— Entità e caratteristiche rilevanti dell'oggetto attaccato (singola persona o singolo oggetto, organizzazione o azienda, ramo, settore o settori collegati in rete, tecnologia specifica, istituzioni statali, ecc.) — Fonte dell'attacco (luogo in cui si trovano gli autori dell'attacco e i loro complici) — Infrastrutture utilizzate (hardware/software, reti, interfaccia, tecnologie, protocolli, ecc.)
Decorso dell'evento	— Effetto delle misure di protezione preventive, prassi giuridica compresa — Preparazione dell'attacco — Svolgimento dell'attacco vero e proprio (unico; a ondate; lento all'inizio poi in crescendo; 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 e degli esperti coinvolti — 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 non sorprende; 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

- Forma d'attacco relativamente sconosciuta risp. combinazione di forme note
- Le contromisure non sussistono, ma possono essere sviluppate in pochi giorni
- L'attacco non sorprende del tutto; 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 (e-banking)
- L'opinione pubblica viene informata sul fatto che sono in corso degli attacchi
- L'opinione pubblica non è direttamente coinvolta dagli attacchi, le conseguenze sono tangibili nella quotidianità

---

3 — estremo

- Forma di attacco nuova o perfezionata (per es. attacchi ransomware con backup crittografati)
- Assenza di contromisure, il cui sviluppo dura settimane o è impossibile in tempo utile
- L'attacco coglie di sorpresa e la sua forma evolve in crescendo
- Attacchi a infrastrutture critiche nei settori del traffico, dell'energia e della telecomunicazione
- 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 ciberattacco.

Fase dell'evento	Vari siti web di organizzazioni e portali d'informazione vengono hackerati e vengono diffuse in modo mirato 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 al centro d'annuncio nazionale (Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI / Centro nazionale per la cibersicurezza NCSC) o alle autorità inquirenti locali. MELANI/NCSC 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 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 cantonali piratati. Oltre ai siti web modificati, 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 troiani (*CryptoLocker*). Rimuovere il virus e reimpostare i computer richiede molto tempo. Sporadicamente si registrano tentativi di violazione delle banche dati della Confederazione. Tuttavia non è rilevabile un furto di darti. Gli uffici interessati della Confederazione segnalano gli eventi a MELANI. Tre settimane più tardi, gli attacchi si spostano al settore finanziario. Inizialmente gli attacchi colpiscono i siti web di vari fornitori di servizi finanziari. In seguito, per due o tre settimane importanti funzioni sono temporaneamente non disponibili. In particolare, per diversi giorni le comunicazioni della Borsa svizzera su Internet risultano difficoltose. Le operazioni interbancarie sono fortemente perturbate ma continuano a funzionare. Oltre ai servizi online degli istituti finanziari, sono localmente e temporaneamente colpiti anche i terminali di pagamento nel commercio al dettaglio, poiché per due giorni i server non sono più raggiungibili. Anche i distributori automatici di contanti vengono sistematicamente bloccati. Il traffico di e-mail 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 forniscono servizi agli istituti finanziari, in particolare quelle che forniscono le informazioni finanziarie o che elaborano le transazioni. Si constatano inoltre dei tentativi di penetrare nei sistemi informatici di questi 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.

Una mattina in cui le borse asiatiche aprono in calo, proprio al momento dell'apertura delle negoziazioni la Borsa di Zurigo subisce un attacco DDoS, apparentemente partito dalla Svizzera. Gli attentatori sono infatti riusciti ad attivare dei malvare preventivamente introdotti in un'applicazione per smartphone molto diffusa. La Borsa 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 neutralizzare sia l'organizzazione che 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. 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 ripristinati.

Una settimana dopo la fine degli attacchi, tutti i siti web della Confederazione e degli istituti finanziari coinvolti sono nuovamente disponibili. 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

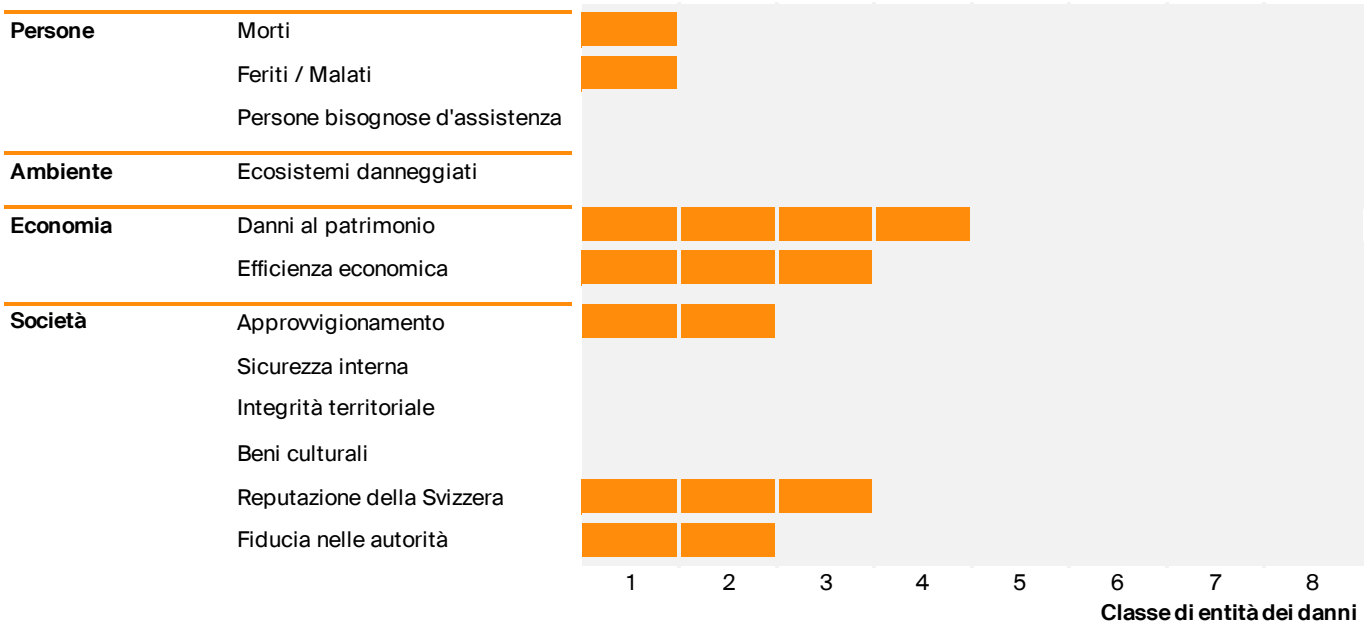
La fase dell'evento dura circa cinque mesi e si svolge in tre ondate (1: siti web di media hackerati, 2: attacchi all'infrastruttura IT della Confederazione, 3: attacchi alle infrastrutture IT del settore finanziario). Gli effetti constati si estendono complessivamente su un arco di circa sei mesi.

Estensione spaziale

Gli attacchi sono diretti contro i media online, gli enti pubblici e il settore finanziario della Svizzera. Gli attacchi 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 può causare delle vittime (per es. suicidi) e/o feriti. Alcune persone potrebbero necessitare di assistenza.
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. Gli enti direttamente interessati devono investire in misure tecniche e risorse di personale supplementari per contenere gli attacchi e difendersi da questi ultimi nonché per identificare gli autori. Inoltre sono obbligate a rafforzare le misure di sicurezza. Il traffico dei pagamenti nel commercio al dettaglio è localmente e temporaneamente interrotto. In parte si registrano guasti ai bancomat, tuttavia è possibile prelevare contanti da altri distributori automatici o ritirandoli allo sportello. Poiché i servizi online non sono disponibili o solo in parte, sempre più operazioni vengono sbrigate allo sportello. I disagi subìti dagli istituti finanziari interessati comportano ritardi nei pagamenti. Una parte dei clienti effettua i pagamenti allo sportello; ne consegue un sovraccarico di lavoro per il personale dell'istituto finanziario e lunghi tempi d'attesa per i clienti. Alcuni clienti, persa la

fiducia sciolgono i loro rapporti d'affari. Altri chiedono il risarcimento dei danni o intentano cause per l'impossibilità di effettuare i pagamenti.

Gli istituti interessati subiscono inoltre un danno finanziario, da un lato per gli investimenti volti a contenere gli attacchi e difendersi dagli stessi e per stimare la fuga di dati, dall'altro per gli affari persi a causa dell'impossibilità di offrire i propri servizi.

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 ai 150 milioni di franchi.

Società

In singoli giorni, le interruzioni nella fornitura di servizi finanziari dovute ai ciberattacchi toccano fino a diverse migliaia di persone. Nel complesso, il disagio non provoca tuttavia maggiori problemi di fornitura agli istituti finanziari interessati.

Non sono toccati processi essenziali o molto importanti. Alcuni provider sono esortati a rimuovere dalla rete i server che sono stati utilizzati come stazioni intermedie per gli attacchi informatici.

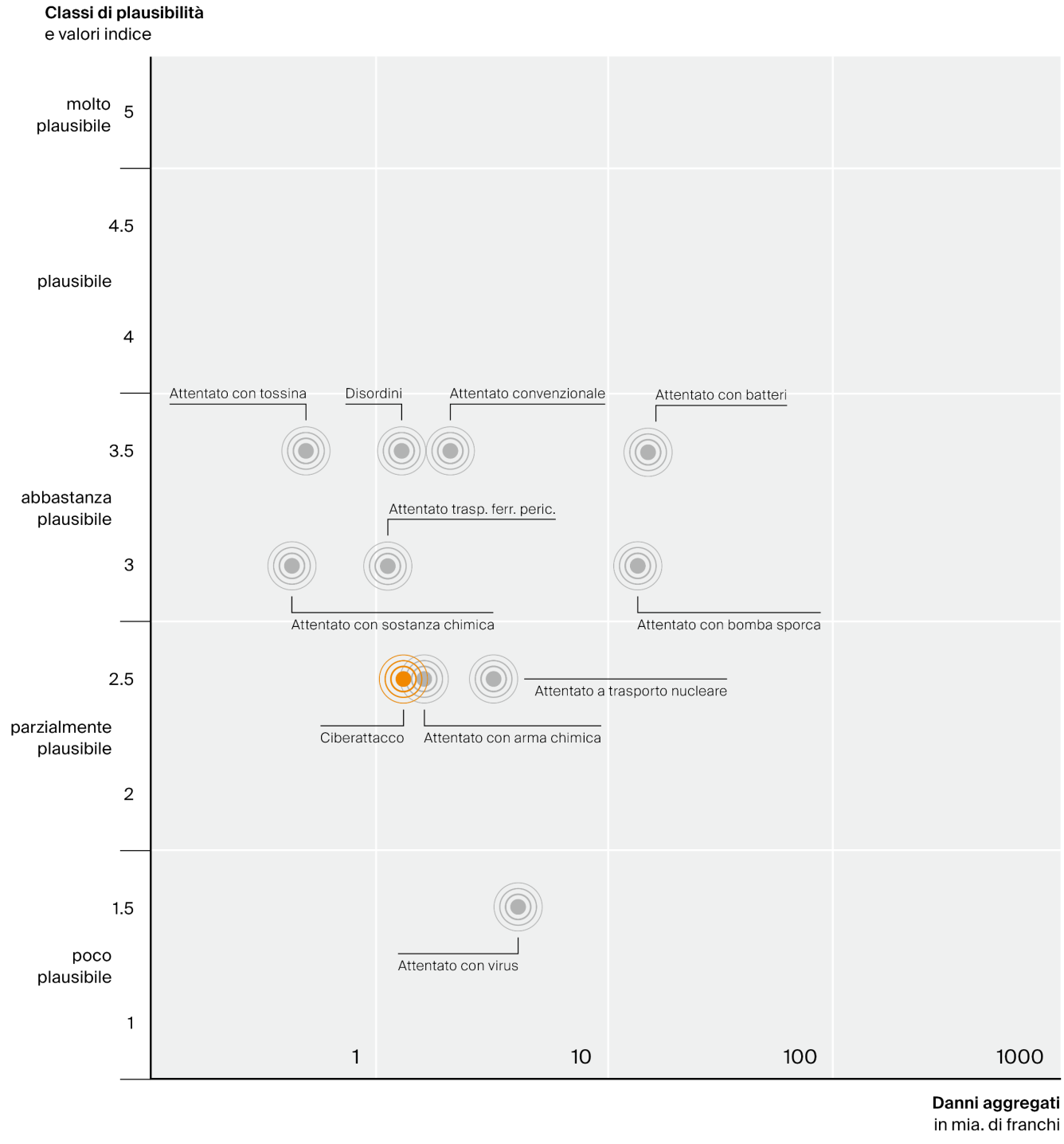
Gli attacchi creano insicurezza, ma non si verificano reazioni di panico. Per contro, la fiducia della popolazione svizzera nelle autorità e nelle istituzioni finanziarie è compromessa. Gli istituti finanziari colpiti assumono più personale di sicurezza privato per far fronte al forte afflusso di persone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

I media esteri riferiscono del ciberattacco e della sua gestione in modo oggettivo per alcuni giorni.

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 ciberspazio, 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 30 marzo 1911 di complemento del Codice civile svizzero (Libro quinto: Diritto delle obbligazioni); RS 220 — Legge federale del 19 giugno 1992 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 del 27 maggio 2020 sui ciber-rischi (OCiber); RS 120.73 — Ordinanza relativa alla legge federale del 14 giugno 1993 sulla protezione dei dati; (OLPD); RS 235.11
Altra base legale	— Council of Europe (2001): European Convention on Cybercrime.

Ulteriori informazioni

Sul pericolo

- Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) (vari anni): Sicurezza delle informazioni. La situazione in Svizzera e a livello internazionale. Rapporto semestrale. DFF e DDPS, Berna
- Check Point (2019): Cyber Attack Trends: 2019 Mid-Year Report
- 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 (2018): Strategia nazionale per la protezione della Svizzera contro i cyber-rischi 2018–2022. ODIC, Berna
- Il Consiglio federale (2017): Strategia nazionale per la protezione delle infrastrutture critiche 2018–2022. Berna
- Il Consiglio federale (2012): Strategia nazionale per la protezione delle infrastrutture critiche. Berna
- Il Consiglio federale (2012): Strategia nazionale per la protezione della Svizzera contro i rischi informatici. DDPS, Berna
- Ministry of Economic Affairs and Communications: Department of State Information Systems (2008): Information Technology in Public Administration of Estonia. Yearbook 2007. Tallinn

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