Raccomandazioni per l'attuazione della ciber-organizzazione cantonale

12 gennaio 2021

Sicherheitsverbund Schweiz
Réseau national de sécurité
Rete integrata Svizzera per la sicurezza

Informazioni sul contenuto

Il presente documento tratta i seguenti temi:
– requisiti di una ciberorganizzazione a livello cantonale e relativi compiti, competenze, responsabilità e processi,
– interfacce con le ciberstrutture della Confederazione.

Le raccomandazioni sono state adottate dalla Conferenza delle direttrici e dei direttori dei dipartementi cantonali di giustizia e polizia (CDDGP) del 12 novembre 2020.

1. Riassunto

L'ambito ciber è un tema trasversale che interessa le autorità (amministrazione, tribunali ecc.), le infrastrutture critiche nonché altre istituzioni e la popolazione. In tale settore la prevenzione e la sensibilizzazione, ma anche la preparazione in caso di ciberincidente, sono quindi fondamentali. Un incidente di questo tipo, infatti, non può più essere gestito da una sola organizzazione. I ciberevenți richiedono un coinvolgimento intercantonale e transfrontaliero. È necessario riflettere e agire in modo interconnesso e, in caso di evento, anche rapidamente. In seguito a un attacco le misure immediate vanno attuate in modo tempestivo ed efficace. Il presente concetto ha carattere di raccomandazione e illustra le strutture e i compiti consigliati nell'ambito della prevenzione e per migliorare la cibersicurezza congiuntamente con altri attori cantonali.

L'attuazione del presente concetto comporta i seguenti vantaggi:

– un interlocutore per tutte le questioni cantonali in ambito ciber, che allo stesso tempo è anche a disposizione delle autorità cantonali come *Single Point of Contact (SPoC)*.
– Possibilità di ridurre o eliminare il furto e/o le fughe di dati.
– I mezzi di informazione e comunicazione restano in funzione o subiscono interruzioni solo in parte.
– I processi aziendali restano in funzione o subiscono interruzioni solo in parte.
– I costi per la gestione degli incidenti sono esigui, è possibile evitare ingenti danni finanziari e di immagine per l'Amministrazione.
– Si garantisce la connessione con altri servizi coinvolti, in particolare, con servizi dei Cantoni e della Confederazione.
– MELANI può fornire supporto all'amministrazione cantonale in caso di incidente.
– Le infrastrutture critiche sono protette.
– È possibile ripristinare dati e informazioni in modo rapido.
– È possibile ripristinare l'infrastruttura TIC (hardware e software inclusa la connessione).

2. Introduzione

Il presente concetto rientra nell'ambito dell'attuazione della Strategia nazionale per la protezione della Svizzera contro i ciber-rischi (SNPC) 2018–2022 e del relativo Piano di attuazione dei Cantoni. Nel quadro dell'elaborazione del Piano di attuazione i rappresentanti dei Cantoni si sono espressamente pronunciati a favore della misura per la creazione delle organizzazioni cantonali per la cibersicurezza, precisando che questa misura prevede la creazione di organizzazioni cantonali per la cibersicurezza in analogia con la struttura organizzativa nel settore ciber a livello di Confederazione[1]. Queste organizzazioni cantonali dovrebbero essere sovrane in materia di bilancio, con facoltà di impartire istruzioni e provvedono al monitoraggio della situazione, rappresentano il loro Cantone in tutte le questioni in ambito ciber, siedono nello Stato maggiore di condotta cantonale (SMCC) e garantiscono il coordinamento all'interno del Cantone, tra i Cantoni e con la Confederazione. La decisione del Consiglio federale del 30 gennaio 2019 sull'organizzazione della Confederazione nel settore dei ciber-rischi stabilisce inoltre ancora una volta in modo esplicito lo sviluppo e il rafforzamento della collaborazione con i Cantoni, il mondo economico e le università nell'ambito della protezione dai ciber-rischi. Il Consiglio federale ha inoltre deciso di creare un Centro nazionale per la cibersicurezza (NCSC). Le strutture previste per tale centro fungono da base per il modello cantonale. A complemento della SNPC il Consiglio federale ha adottato la Strategia nazionale per la protezione delle infrastrutture critiche (PIC)[2] per il periodo 2018–2022, alla quale fa riferimento anche il presente ciberconcetto.

Il presente concetto è stato elaborato da un gruppo di lavoro della Rete integrata Svizzera per la sicurezza con specialisti di diversi settori quali tecnologia dell'informazione, polizia e protezione della popolazione provenienti da tutta la Svizzera per l'implementazione del Piano di attuazione dei Cantoni sopracitato per il periodo fino al 2022. Le raccomandazioni sono state adottate dalla CDDGP del 12 novembre 2020. I capitoli seguenti sono da intendersi come strumento di ausilio per l'introduzione di una ciberorganizzazione cantonale e non hanno alcuna pretesa di esaustività; il concetto può quindi essere adeguato alle richieste ed esigenze di ogni Cantone.

1 Organo direzione informatica della Confederazione. *Piano di attuazione della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi 2018–2022,* p. 82.

2 Strategia nazionale per la protezione delle infrastrutture critiche 2018–2022 (FF **2018** 455).

3. Oggetto e campo d'applicazione

Il presente concetto può costituire la base per una decisione del Consiglio di Stato / per una normativa volta a implementare la ciberorganizzazione in un determinato Cantone. I compiti, le competenze e la responsabilità sono descritti in questo documento.

Il presente concetto serve da raccomandazione sia per tutta l'amministrazione cantonale che per altre organizzazioni quali ospedali, università ecc., in particolare quando queste sono collegate alla stessa rete delle autorità.

4. Obiettivi

- Evitare un ciberattacco attraverso misure adeguate, ad esempio mediante l'identificazione, la protezione, il rilevamento, la reazione e il ripristino.
- Ridurre al minimo i danni (finanziari e di immagine) dopo un attacco e riavviare il più rapidamente possibile i processi aziendali più importanti.
- Approvare, introdurre e sottoporre a esercitazioni un'adeguata organizzazione delle procedure e delle strutture.
- Garantire l'accesso alla formazione e alla sensibilizzazione a seconda del livello gerarchico per tutti i collaboratori dell'Amministrazione.

5. Organizzazione in ambito ciber

5.1 Organizzazione della Confederazione in ambito ciber[3]

– **Comitato per la cibersicurezza del Consiglio federale:** in esso siedono i capidipartimento del Dipartimento federale delle finanze (DFF), del Dipartimento federale di giustizia e polizia (DFGP) e del Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS); ha il compito di vigilare sull'attuazione della SNPC.

– **Delegato federale alla cibersicurezza:** il delegato è direttamente subordinato al capo del DFF ed è la persona di riferimento per gli attori politici, gli operatori dei media e la popolazione in caso di domande in materia di cibersicurezza. Dirige il neocostituito Centro nazionale per la cibersicurezza (NCSC), coordina gli organi interdipartimentali per migliorare la collaborazione nei progetti relativi ai ciber-rischi e rappresenta la Confederazione in altri organi.

– **Comitato ristretto ciber:** rafforza il coordinamento fra i tre ambiti della sicurezza, della difesa e del perseguimento penale, assicura una valutazione congiunta delle minacce in atto e vigila sulla gestione, da parte dei servizi della Confederazione, degli incidenti gravi verificatisi a livello interdipartimentale. Rappresentanti dei Cantoni possono essere invitati a parteciparvi in modo puntuale.

– **Comitato direttivo della SNPC (CD SNPC):** assicura l'attuazione coordinata e mirata delle misure definite nella SNPC ed elabora proposte per il suo ulteriore sviluppo. Questo organo è composto da rappresentanti sia della Confederazione che dei Cantoni (CDDGP e RSS) nonché del mondo economico e delle università.

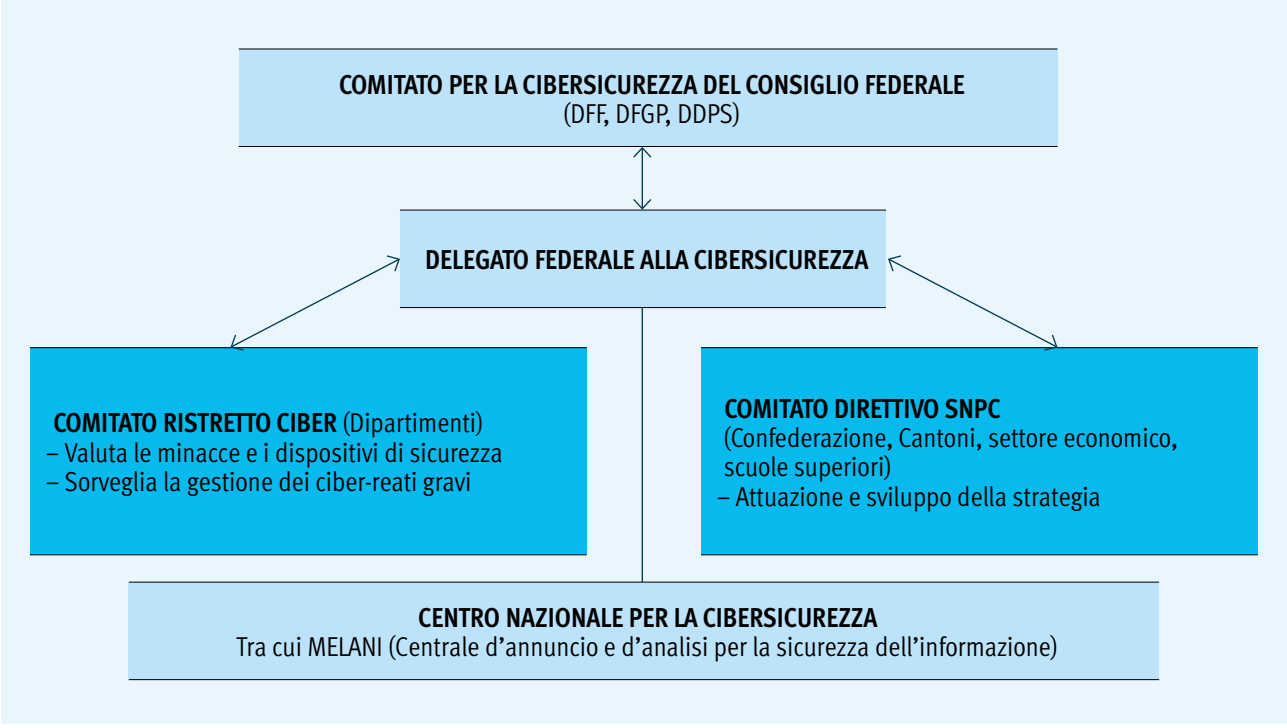

Figura 1: Organizzazione della Confederazione in ambito ciber[1]

3 Centro nazionale per la cibersicurezza (NCSC): https://www.ncsc.admin.ch/ncsc/it/home/ueber-ncsc/das-ncsc.html (stato: 07.01.2021).

– **Centro nazionale per la cibersicurezza (NCSC):** il centro si occuperà dei seguenti compiti:
  - Servizio nazionale di contatto per la segnalazione di incidenti e questioni relative ai ciber-rischi rivolto alle autorità, ai privati e alla popolazione.
  - Gestione, in quanto servizio tecnico, del Computer Emergency Response Team (GovCERT).
  - Direzione operativa della gestione degli incidenti in caso di ciberincidenti di ampia portata.
  - Segreteria del delegato federale alla ciberdifesa.
  - Servizio specializzato della sicurezza TIC della Confederazione.
  - Pool di esperti per fornire supporto agli uffici specializzati nello sviluppo e nell'attuazione degli standard di cibersicurezza.
  - Collaborazione con mondo economico e ricerca.
  - Cooperazione internazionale a livello specialistico.

Il Centro nazionale per la cibersicurezza è al momento in fase di realizzazione. I Cantoni potranno eventualmente mettere a disposizione del centro alcune prestazioni[4].

5.2 Altri organi federali competenti

Con l'introduzione della funzione del delegato federale alla cibersicurezza è stato creato anche un Single Point of Contact (SPOC), che tra le altre cose funge da interlocutore per le autorità federali. I partner principali a livello nazionale sono i seguenti:

– **Ufficio federale della protezione della popolazione (UFPP):** insieme all'Ufficio federale per l'approvvigionamento economico del Paese, l'UFPP promuove la resilienza (resistenza e capacità di rigenerazione) delle infrastrutture critiche con misure mirate. Un ruolo centrale l'assume la protezione delle infrastrutture di informazione e comunicazione[5].

– **Ufficio federale per l'approvvigionamento economico del Paese (UFAE):** in quanto organizzazione competente per l'approvvigionamento del Paese in beni e servizi d'importanza vitale in situazioni di grave penuria alle quali l'economia non è in grado di far fronte[6], l'UFAE ha emanato uno standard minimo per migliorare la resilienza delle TIC[7]. Le imprese e le organizzazioni sono direttamente responsabili della propria protezione, ma sussiste una responsabilità legale laddove sia in gioco l'operatività (regolare) delle infrastrutture critiche. Gli standard sono applicabili anche ad altri settori e imprese.

– **Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI):** il compito di MELANI consiste nell'individuare tempestivamente i pericoli e gestirli nonché fornire assistenza ai gestori di infrastrutture critiche durante la crisi. Per far ciò MELANI gestisce il Computer Emergency Response Team (GovCERT), che offre servizi quali analisi e informazioni tecniche su attacchi mirati a infrastrutture critiche, e l'Operation Information Center (OIC), competente per l'analisi della situazione. MELANI funge inoltre da servizio nazionale di contatto per la segnalazione di ciberin-

4 Nel quadro di un progetto sotto la direzione della Rete integrata Svizzera per la sicurezza, nei prossimi mesi verrà effettuato un bilancio delle prestazioni cantonali e si chiarirà come queste competenze possano essere messe a disposizione di altri beneficiari di prestazioni.

5 Bischof, Angelika P. «Sollecitati anche i gestori delle infrastrutture critiche», in: *Protezione della popolazione 27 (2017)*, pag. 13–15

6 Le basi legali dell'approvvigionamento economico del Paese si fondano sull'articolo 102 della Costituzione federale e sulla legge sull'approvvigionamento economico del Paese.

7 Ufficio federale per l'approvvigionamento economico del Paese (2018). *Standard minimo per migliorare la resilienza delle TIC,* consultabile al link: https://www.bwl.admin.ch/bwl/it/home/themen/ikt/ikt_minimalstandard.html (stato: 07.01.2021).

cidenti. Questo centro di contatto ha sede presso il Centro nazionale per la cibersicurezza, che funge da primo interlocutore per questioni nel settore dei ciber-rischi[8] .

– **Ministero pubblico della Confederazione (MPC):** l'MPC è competente da un lato per i classici reati contro la sicurezza dello Stato, ossia reati commessi contro la Confederazione o i suoi interessi. Dall'altro lato spettano all'MPC anche complessi casi intercantonali o internazionali di criminalità organizzata (compresi il terrorismo e il relativo finanziamento), riciclaggio di denaro e corruzione. Nel settore della criminalità economica i casi di portata nazionale o internazionale vengono trattati dall'MPC[9]. Per una lotta coordinata e unitaria alla cibercriminalità a livello operativo e strategico è stata creata la piattaforma comune «Cyberboard» (cfr. capitolo 6.2.6) grazie all'intermediazione dell'MPC e di fedpol, con la collaborazione delle autorità di perseguimento penale cantonali e nazionali nonché rappresentanti della prevenzione.
– **Ufficio federale di polizia (fedpol):** la sicurezza pubblica spetta in primo luogo ai Cantoni. fedpol si occupa tuttavia del coordinamento, dell'analisi e delle indagini nell'ambito di casi complessi e gravi di criminalità e di settori tematici transfrontalieri quali la criminalità su Internet. La nuova legge federale sulle misure di polizia per la lotta al terrorismo (MPT) prevede espressamente la collaborazione con i Cantoni nella lotta alla cibercriminalità[10]. fedpol funge inoltre da anello di congiunzione con l'estero, dal momento che la criminalità non si ferma ai confini. fedpol pubblica regolarmente sul proprio sito indicazioni sulla prevenzione e sui pericoli legati a Internet per la popolazione[11] .
– **Rete integrata Svizzera per la sicurezza (RSS):** il Delegato della Confederazione e dei Cantoni della Rete integrata Svizzera per la sicurezza funge da partner per il coordinamento dell'attuazione delle misure della SNPC (interfaccia tra Confederazione e Cantoni) e da interlocutore per gli sviluppi in ambito ciber a livello strategico.

5.3 Coinvolgimento dei Cantoni

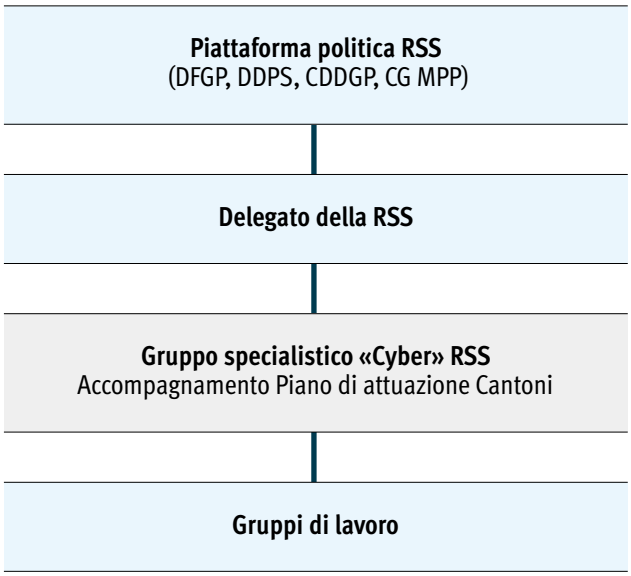

Figura 2: Organizzazione RSS[II]

I Cantoni possono essere coinvolti sia a livello politico-strategico che a livello operativo[12] Questa figura presenta gli organi paritetici della Rete integrata Svizzera per la sicurezza, nella quale siedono rappresentanti dei Cantoni[13]. Tali organi affrontano sfide comuni in materia di politica di sicurezza, tra le quali figura anche la tematica ciber.

8 https://www.ncsc.admin.ch/ncsc/it/home.html (stato: 07.01.2021).
9 https://www.bundesanwaltschaft.ch/mpc/it/home/die-bundesanwaltschaft/aufgaben-breit11.html (stato: 07.01.2021).
10 Il Parlamento ha approvato la legge sul MPT (FF 2020 6795) alla fine di settembre 2020.
11 https://www.fedpol.admin.ch/fedpol/it/home.html (stato: 07.01.2021).
12 La Conferenza delle direttrici e dei direttori dei dipartimenti cantonali di giustizia e polizia (CDDGP) e la Conferenza governativa per gli affari militari, la protezione civile e i pompieri (CG MPP) sono rappresentate.
13 Per un esempio concreto cfr. Allegato III.

5.4 Ciberorganizzazione cantonale

In linea generale in ogni Cantone sono possibili due tipi di organizzazione:

- una persona interna all'amministrazione viene designata cibercoordinatore, ad esempio l'incaricato della sicurezza delle informazioni o il responsabile dei servizi IT, e agisce all'interno delle strutture già esistenti; oppure
- su decisione del livello politico viene creata una ciberorganizzazione con un cibercoordinatore, come illustrato nell'esempio seguente.

Il potenziamento della ciber-resilienza e quindi della sicurezza integrale all'interno di un Cantone si basa su un'organizzazione ottimale dell'amministrazione e dei suoi partner. Lo schema sottostante funge da esempio e deve essere adeguato alla situazione del singolo Cantone.

5.4.1 Cibercoordinatore

Il valore aggiunto apportato dalla figura del cibercoordinatore consiste principalmente nella sua funzione di Single Point of Contact (SPOC) all'interno del Cantone ma anche nei confronti delle autorità a livello federale. Garantisce il contatto tra i diversi attori statali e privati. In caso di ciberincidente si occupa della gestione della situazione. Il delegato federale alla cibersicurezza può chiedere il supporto dello Stato maggiore cantonale di condotta (SMCC) / dell'organizzazione cantonale di crisi. A loro volta questi due organi possono coinvolgere il «Comitato operativo» in caso di incidente in materia di sicurezza. Le competenze devono quindi essere definite a priori. Di seguito si illustra nel dettaglio il portfolio dei compiti del cibercoordinatore. L'entità di tali compiti richiede risorse di personale per un totale stimato pari a un posto a tempo pieno, direttamente subordinato a uno o più consiglieri di Stato. Per coadiuvare il cibercoordinatore si consiglia un supporto amministrativo.

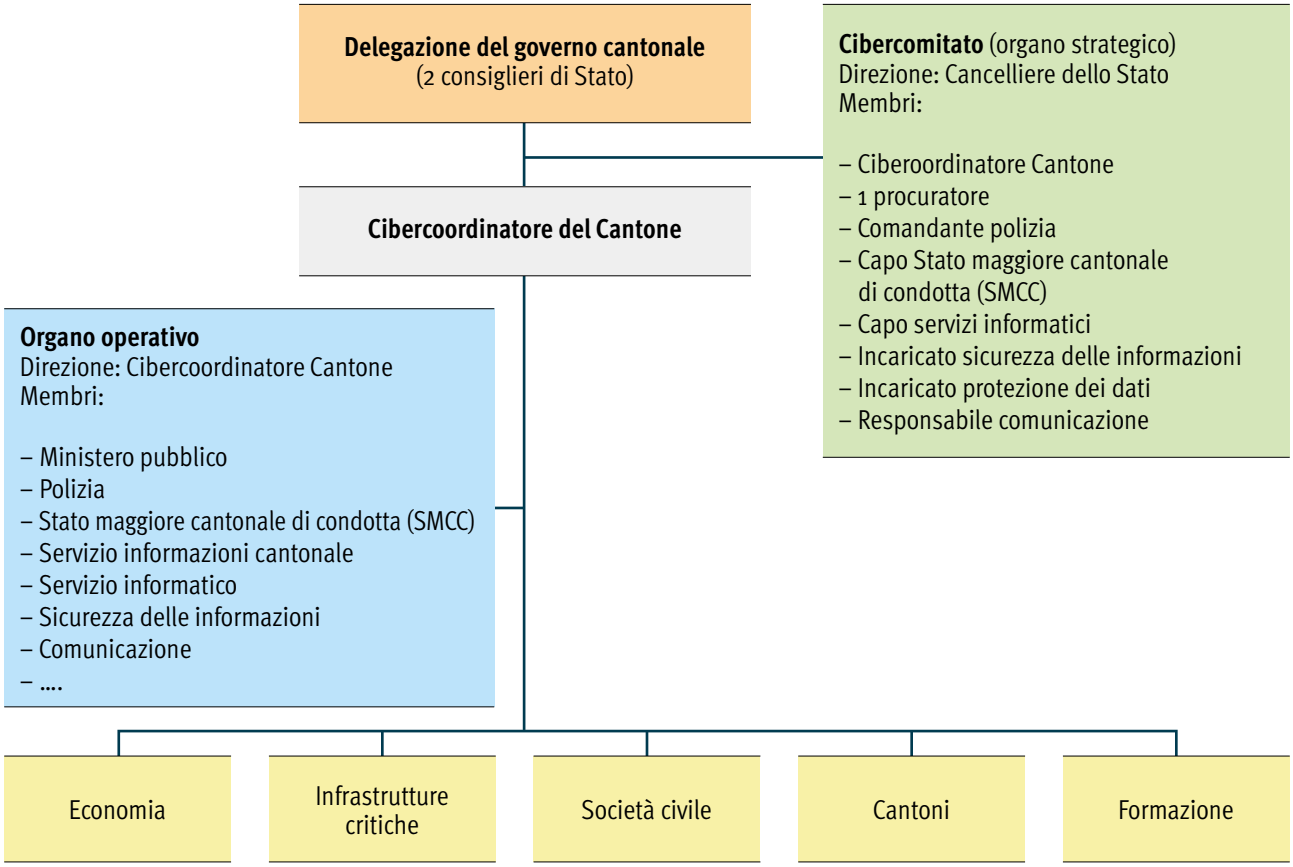

Figura 3: Ciberorganizzazione cantonale[III]

Compiti e competenze del cibercoordinatore: Questa lista non esaustiva contiene i possibili compiti e competenze del cibercoordinatore.

	N.	Tema	CA[14]	M[15]
Permanente		**Creazione delle organizzazioni cantonali per la cibersicurezza**		**8**
	1	Segue gli sviluppi in ambito ciber a livello strategico		
	2	Segue la situazione di minaccia in ambito ciber Internamente: Incident Management, monitoraggio e servizio informazioni cantonale Esternamente: OSINT, segnalazioni MELANI e Servizio delle attività informative della Confederazione	2	4
	3	Valuta il dispositivo di sicurezza		
	4	Responsabile della gestione dei rischi e del Business Continuity Management (BCM)		
	5	Ruolo di interfaccia con il delegato federale alla cibersicurezza e con la Conferenza svizzera sull'informatica (CSI), rappresenta il Cantone in tutte le questioni relative all'ambito ciber		
	6	Redige documenti didattici e tiene formazioni Sensibilizza l'amministrazione, le imprese e la popolazione	1	2
	7	Coordina l'attuazione delle misure della SNCP II all'interno del Cantone		
	8	Crea contatti con il mondo economico, in particolare con le infrastrutture critiche cantonali		
	9	Potenzia la resilienza dell'amministrazione, delle imprese e della popolazione	3	4
	10	Coordina le esercitazioni nello stato maggiore di crisi con le infrastrutture critiche cantonali	7	17
	11	Verifica la standardizzazione / regolamentazione; per es. sicurezza della rete	6	8
In modo puntuale	12	Avanza richieste sul piano politico. Es.: – elaborazione di disposizioni legali (legge e ordinanza in ambito ciber) – richiede il budget per l'attuazione delle misure volte a potenziare la cibersicurezza – chiede l'attuazione di misure		
	13	Vigila sui ciberincidenti, definisce misure immediate e trae insegnamenti dagli incidenti		
	14	Su richiesta fornisce supporto alle autorità di perseguimento penale		
	15	Su richiesta può fornire supporto alle autorità di perseguimento penale di un altro Cantone		

14 Campo d'azione secondo il Piano di attuazione della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) 2018–2022.

15 Misura secondo il Piano di attuazione della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) 2018–2022.

5.4.2 Delegazione del governo cantonale

Ella sarà composto da due a tre consiglieri di Stato.

Compiti:

- definisce a quale dipartimento viene subordinato il cibercoordinatore,
- orienta il Consiglio di Stato nella scelta del cibercoordinatore e del suo sostituto,
- approva gli obiettivi e verifica il raggiungimento degli obiettivi annuali, il rapporto annuale, il budget e il concetto d'impiego.

5.4.3 Cibercomitato

L'organo preposto alle questioni strategiche è presieduto dal Cancelliere dello Stato ed è composto dai seguenti membri:

- Cibercoordinatore
- Procuratore in rappresentanza dei procuratori
- Comandante di polizia in rappresentanza della polizia, coadiuvato dal capo analisi della situazione o dal capo della polizia giudiziaria
- Capo SMCC in rappresentanza dello Stato maggiore cantonale di condotta. Se presente, viene coadiuvato dal capo analisi della situazione
- Capo dei servizi informatici in rappresentanza degli interessi dei fornitori di prestazioni IT
- Incaricato della sicurezza delle informazioni
- Incaricato della protezione dei dati
- Responsabile della comunicazione

Compiti:

- approva il rapporto annuale del cibercoordinatore,
- controlla l'organo operativo attraverso gli obiettivi stabiliti e raggiunti,
- valuta la gestione dei ciberincidenti,
- valuta i nuovi vettori di attacchi, es. Internet delle cose (IoT), veicoli delle organizzazioni di pronto intervento,
- trae insegnamenti dai ciberincidenti delle proprie organizzazioni o a livello di ambiente,
- valuta il livello di formazione dell'organo operativo,
- definisce condizioni quadro/standard di sicurezza per le PMI,
- ...

5.4.4 Organo operativo

L'organo operativo è diretto dal cibercoordinatore. In tale organo siedono i rappresentanti dei seguenti servizi:

- Ministero pubblico[16]
- Polizia
- Stato maggiore cantonale di condotta
- Servizio informazioni cantonale
- Servizio informatico
- Sicurezza delle informazioni
- Rappresentanti delle infrastrutture critiche

Compiti:

- gestisce i ciberincidenti,
- valuta gli sviluppi in ambito ciber nei propri settori e le relative contromisure,
- garantisce che i collaboratori siano formati e sensibilizzati,

16 Il procuraotre pubblico che funge da SPOC del Ministero pubblico della Confederazione in caso di evento ciber dovrebbe far parte anche dell'organo operativo e viceversa.

– garantisce che le proprie organizzazioni dispongano delle risorse necessarie (collaboratori, hardware e software),
– ...

5.5 Collaborazione all'interno dei Cantoni

Il cibercoordinatore collabora in modo trasversale con tutti i dipartimenti e con i responsabili delle infrastrutture critiche nonché con altre organizzazioni.

5.6 Collaborazione intercantonale

Il cibercoordinatore collabora con i cibercoordinatori degli altri Cantoni.

5.7 Requisiti minimi

Affinché la ciberorganizzazione funzioni occorre creare i seguenti presupposti. La realizzazione di tali condizioni può essere avviata anche su iniziativa del cibercoordinatore.

– Trasmissione della formazione e delle conoscenze delle autorità cantonali e comunali nonché dei partner
– Panoramica dei processi aziendali, dell'infrastruttura, dei fornitori e dei prestatari di servizi: i processi aziendali più importanti dell'amministrazione cantonale e i processi dei partner nonché le interfacce con questi ultimi devono essere noti per poter applicare le misure di sicurezza[17]
– Avvenuta elaborazione e verifica del Business Continuity Management (BCM)
– Avvenuta elaborazione della gestione dei rischi
– Avvenuta elaborazione di un sistema di gestione della sicurezza delle informazioni
– Processi definiti e documentati per la gestione di un ciberattacco

17 Nel quadro della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) 2018–2022 i Cantoni procedono, tramite un tool sviluppato dalla RSS, a un'autovalutazione dei propri ciber-rischi.

6. Ciber-rischi e ciberminacce

Esistono diversi tipi di ciber-rischi. A titolo esemplificativo si descrivono di seguito tue tipologie di pericoli.

6.1 Ciber-rischi

6.1.1 Guasto mezzi TIC

Secondo l'Ufficio federale della protezione della popolazione si parla di guasto di mezzi TIC quando «mezzi tecnici atti all'elaborazione o alla trasmissione di informazioni risultano temporaneamente non disponibili. Tenendo conto del vasto utilizzo dei mezzi TIC, un guasto di questo tipo può comportare gravi conseguenze. L'entità del danno dipende dalla durata, dalla tipologia delle tecnologie interessate, dal numero e dall'importanza dei servizi e degli utenti coinvolti nonché dal danneggiamento di dati. Anche guasti a sistemi specifici possono comportare gravi danni, ad esempio quando sono coinvolti i sistemi di controllo basati sulle TIC delle infrastrutture critiche (centrali elettriche, sistemi di trasporto ecc.). Dal momento che molte infrastrutture dipendono da un sistema TIC funzionante e sono connesse tra loro grazie a quest'ultimo, un guasto delle TIC può innescare una serie di altri pericoli. Un guasto alle TIC può essere provocato da diversi eventi, come ad esempio malfunzionamenti o guasti di componenti, errori umani, eventi naturali (es. terremoti), azioni criminali (cibercriminalità, terrorismo informatico) o avarie tecniche (blackout)»[18].

6.1.2 Esternalizzare le prestazioni informatiche

I dati possono andare persi o essere rubati non solo dai sistemi personali. L'esternalizzazione delle prestazioni (informatiche), come succede ad esempio nel settore dell'approvvigionamento idrico, si porta spesso dietro una perdita di controllo. Questo perché non è chiaro quali misure di sicurezza e procedure debbano adottare i partner nella gestione degli incidenti. Il rischio aumenta quando diverse prestazioni vengono esternalizzate; in questo caso il Cantone o il Comune si assume un cosiddetto «grande rischio». La Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) raccomanda quindi di stabilire a livello contrattuale che i partner adottino misure di sicurezza adeguate, anche se ciò implica maggiori controlli[19].

6.2 Ciberminacce

6.2.1 Ciberattacco

Nel Rapporto sulla politica di sicurezza 2016 si definisce ciberattacco un atto intenzionale illecito commesso da una persona o da un gruppo nel ciberspazio al fine di compromettere l'integrità, la riservatezza o la disponibilità di informazioni e dati. A seconda del tipo di attacco, un simile atto può avere anche conseguenze fisiche[20].

---

18 Ufficio federale della protezione della popolazione (2015). *Analisi nazionale dei pericoli – Dossier pericoli «Interruzione delle infrastrutture d'informazione e di comunicazione» (non tradotto in italiano)*. Consultabile al link https://www.babs.admin.ch/it/aufgabenbabs/gefaehrdrisiken/natgefaehrdanalyse/gefaehrddossier.html (stato: 07.01.2021).

19 NCSC (2019). *Rapporto semestrale 2019/1 (gennaio–giugno)*, pag. 32. https://www.ncsc.admin.ch/ncsc/it/home/dokumentation/berichte.html (stato: 07.01.2021).

20 Dipartimento federale della difesa, della protezione della popolazione e dello sport (2016). *RAPOLSIC 2016: La politica di sicurezza della Svizzera – Rapporto del Consiglio federale*, pag. 7101. https://www.vbs.admin.ch/it/tematiche/politica-sicurezza/rapporti-politica-sicurezza/rapporto-politica-sicurezza-2016.detail.document.html/vbs-internet/it/documents/politicadisicurezza/rapolsic2016/SIPOL-B-2016-i.pdf.html (stato: 07.01.2021).

6.2.2 Cibercriminalità

Nel Rapporto sulla politica di sicurezza 2016 si definisce cibercriminalità l'insieme dei reati e delle omissioni punibili commessi nel ciberspazio[21] La dottrina iniziale[22] distingueva tra cibercrimine in senso stretto e in senso lato. Con cibercrimine in senso stretto si intendevano i cosiddetti «reati informatici»; dall'acquisizione di dati ai sensi dell'articolo 143 CP fino all'abuso di un impianto per l'elaborazione di dati ai sensi dell'articolo 147 CP. Il cibercrimine in senso lato comprendeva invece tutti i reati in cui il computer costituiva un fatto o un mezzo di prova. Oggi tale distinzione è da considerarsi superata, tanto più che la maggior parte dei ciberfenomeni è il risultato della combinazione di diversi reati di cui sopra. Secondo gli studi più recenti[23] occorre fare una distinzione in base alla complessità del fenomeno e delle indagini necessarie per chiarire le dinamiche:

1. Crimini Hightech da parte di gruppi internazionali che perpetrano crimini professionali in modo il più possibile anonimo. Gli accertamenti richiedono l'impiego mirato di misure di sorveglianza segrete nell'ambito di procedure operative onerose.

2. Cibercrimini: comprendono le classiche forme di estorsione e frode per le cui indagini sono necessari grandi oneri ma non misure di sorveglianza in tempo reale.

3. Criminalità digitale: questa categoria include infine tutti i reati nei quali un dispositivo o un supporto EED costituisce un fatto o un mezzo di prova e per i quali è possibile determinare l'autore del reato attraverso semplici misure di assistenza giudiziaria o verifiche della proprietà della connessione. La criminalità digitale, più che a una tipologia di reati, corrisponde quindi a un insieme di metodi di indagine per l'identificazione degli autori dei reati su Internet e Darknet.

Ai fini di una comprensione uniforme e per il coordinamento a livello giuridico occorre definire i fenomeni più ricorrenti, per i quali sono state create le cosiddette schede esplicative nell'ambito della SNPC 2012–2017. Le autorità possono richiedere il catalogo dei diversi ciberfenomeni presso l'Ufficio federale di polizia.

21 Ibidem, pag. 7101.
22 Allianz der schweizerischen Strafverfolgung zur Bekämpfung der Cyberkriminalität, verbale della prima seduta del 2 settembre 2016.
23 Staatsanwaltsakademie, Università di Lucerna, Corsi Cybercrime I-III, Kompetenzzentrum Cybercrime, Cantone di Zurigo.

6.2.3 Criteri di valutazione

Per valutare un evento occorre necessariamente tenere conto dei seguenti aspetti[24] tra loro interdipendenti.

Fonte del pericolo	– Caratteristiche degli autori (ideologia, inclinazione alla violenza, capacità e know-how, livello di organizzazione, risorse, infrastrutture controllate / già disponibili) – Atteggiamento di uno Stato o di organizzazioni con sede nel Paese (di natura criminale o parastatale) – Vulnerabilità dei sistemi (permeabilità, misure di protezione, interfacce/punti di accesso, Social Engineering, integrazione lacunosa della sicurezza delle informazioni nei processi di sicurezza strategici e integrali)
Data	– Solitamente legata a decisioni e sviluppi economici, politici e/o sociali – I mezzi e le infrastrutture rilevanti possono essere già stati preparati in un altro contesto. – Il sistema informatico può essere stato manipolato in modo illecito prima del ciberattacco vero e proprio, che a seconda delle circostanze può essere molto breve
Luogo ed entità	– Ampiezza e caratteristiche dell'oggetto dell'attacco (obiettivo isolato, ambito, settore, livello di collegamento dei settori, tecnologia specifica ecc.) – Provenienza dell'attacco (luogo in cui si trovano l'autore e i suoi complici) – Infrastrutture utilizzate (reti, interfacce, protocolli ecc.)
Svolgimento dell'evento	– Margine di preavviso del guasto – Efficacia delle misure preventive, compresa la prassi legale – efficacia delle contromisure specifiche adottate – Decorso dell'attacco (con eventuali livelli di escalation) – Comportamento delle organizzazioni interessate, delle forze d'impiego e delle autorità competenti – Reazione della popolazione e del mondo politico

24 UFPP (2015). *Analisi nazionale dei pericoli – Dossier pericoli «Attentato informatico» (non tradotto in italiano)*. Consultabile al link https://www.babs.admin.ch/it/aufgabenbabs/gefaehrdrisiken/natgefaehrdanalyse/gefaehrddossier.html#ui-collapse-420 (stato: 07.01.2021).

6.2.4 Gruppi di aggressori

La presente tabella illustra la probabilità e il livello di professionalità degli attacchi nello spazio virtuale contro persone, aziende, banche, infrastrutture critiche, polizia, sanità, pompieri, ospedali ecc. e organismi pubblici.

La freccia blu rappresenta la professionalità degli aggressori. La freccia grigia indica il grado di probabilità di un attacco.

Esempio: gli aggressori «Attori statali» dispongono di ampie conoscenze e grandi risorse finanziarie per perpetrare attacchi mirati e con un compito preciso. La probabilità che ciò si verifichi è tuttavia molto bassa. Al contrario è molto più probabile un attacco a opera di vandali con mezzi molto limitati.

	Aggressore	Conoscenze	Obiettivi	Mezzi	Procedure	Probabilità
Mirato	– Attori statali – Servizi segreti	Molto elevate	– Informazione – Spionaggio – Lotta – Terrorismo/ criminalità – Danni	– Grandi disponibilità finanziarie – Focus sull'utilità più che sui costi	– Acquistare know-how e formare specialisti – Attacchi non appariscenti e a lungo termine	Molto bassa
	Terroristi	Elevate	– Danni – Attenzione – Manipolazione, influenza sulla politica	– Disponibilità finanziaria media, impiegata per attacchi fisici e logici	– Acquistare know-how sul mercato nero – Attacchi fisici e logici	Bassa
	Criminalità (organizzata)	Medie	Denaro	– Business – Guadagnare denaro a lungo termine – Costi e utilità devono essere proporzionati	– Bande già esistenti – Bande di specialisti organizzate in modo spontaneo – Corruzione	Media
Opportunistico	Attivisti, gruppi	Esigue	– Attenzione – Danni – Stigmatizzazione della vulnerabilità dei sistemi	– Risorse esigue – Grande portata	– Professionisti e dilettanti molto motivati – Sviluppare l'iniziativa personale spontanea	Elevata
	Vandali, Script Kiddies	Molto esigue	Fama e visibilità	– Risorse esigue – Conoscenze minime	Utilizzo di strumenti disponibili	Molto elevata

Figura 4: Gruppi di aggressori[IV]

6.2.5 Diagramma delle ripercussioni

Il diagramma rappresenta gli eventi e gli sviluppi descritti nel «Catalogo dei pericoli» dell'Ufficio federale della protezione della popolazione[25], che potrebbero causare o essere provocati da un guasto all'infrastruttura TIC: la fornitura di prestazioni può risultare lievemente difficoltosa o essere completamente bloccata; l'attività commerciale può presentare problemi a breve o lungo termine; è possibile che ne derivi un danno di immagine, in alcuni casi addirittura a livello internazionale.

Come si può evincere dal grafico, l'economia è molto toccata dalla cibercriminalità. A livello globale si calcola una perdita pari a 600 miliardi di dollari per l'economia[26]. Dal sondaggio internazionale sulla criminalità economica nel 2018 di PricewaterhouseCoopers è emerso[27], che in Svizzera la cibercriminalità costituisce il secondo reato economico in ordine di frequenza (44 %, contro il 31 % a livello mondiale). I danni che ne derivano per la Svizzera sono dunque corrispondentemente elevati. Le tecniche di attacco più comuni risultano essere il phishing (42 %) e i malware (31 %). Allo stesso tempo solo il 54 per cento delle aziende svizzere dispone di un programma di cibersicurezza pronto all'impiego. La cibercriminalità verrà percepita anche in futuro come il rischio più importante. La cibersicurezza resterà quindi una priorità per i dirigenti aziendali e occorrerà un impegno adeguato in tal senso.

All'interno della categoria dei ciberattacchi viene descritto a titolo di esempio un atto intenzionale com-

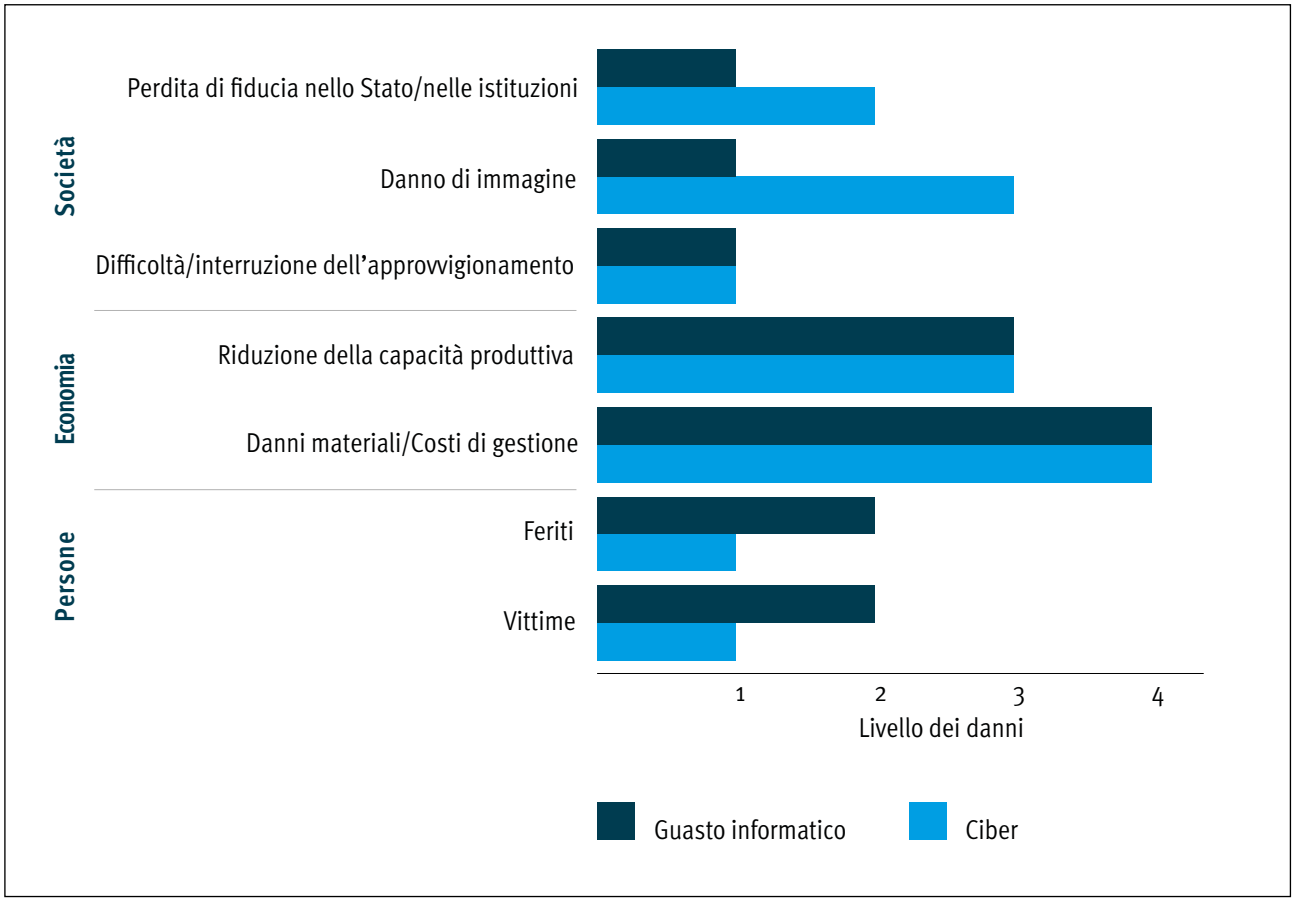

Figura 5: Diagramma delle ripercussioni[v]

25 UFPP (2013). *Katalog möglicher Gefährdungen. Grundlage für Gefährdungsanalyse (il documento non più disponibile in italiano).* Consultabile al link http://www.alexandria.admin.ch/bvo01492631.pdf (stato: 07.01.2021).

26 McAfee (2018). *Economic Impact of Cybercrime— No Slowing Down.* https://www.mcafee.com/enterprise/en-us/assets/reports/restricted/rp-economic-impact-cybercrime.pdf (stato: 07.01.2021).

27 PricewaterhouseCoopers (2018). *Globale Umfrage zur Wirtschaftskriminalität 2018 – Schweizer Erkenntnisse.* https://www.pwc.ch/de/publications/2018/globale-umfrage-zur-wirtschaftskriminalitaet-2018.pdf (stato: 12.10.2020).

prendente i seguenti reati: sabotaggio di edifici, ambienti e mezzi TIC, furto e divulgazione di informazioni o di mezzi TIC; gli aggressori tentano di introdurre malware nell'ambiente TIC e di sfruttare le falle nella sicurezza dei sistemi di gestione e dei software. Le conseguenze che ne derivano sono le seguenti: riduzione o interruzione delle prestazioni; accesso non autorizzato a edifici, ambienti, dati, informazioni e mezzi TIC; furto di valori e informazioni.

La tabella consente di visualizzare il valore del rischio del presente esempio, mostrando le ripercussioni della probabilità che si verifichi un determinato evento e l'entità massima dei danni che può provocare.

I danni vengono valutati sulla base di tre ambiti:

- danni finanziari;
- interruzione di processi aziendali critici;
- interruzione di processi aziendali non critici.

Nel nostro esempio l'ambito «Interruzione di processi aziendali critici» («Ausfall von kritischen Geschäftsprozessen») viene valutato come prioritario e riceve quindi un valore pari a 4. In questo esempio il valore del rischio (che si ottiene moltiplicando la probabilità per i danni massimi) ammonta quindi a 20.

Una gestione globale dei rischi è imprescindibile per poter gestire i ciberattacchi e le conseguenze che ne risultano.

	Effetti			Valore di rischio = Impatto x Probabilità di accadimento					
Livello	**Impatto finanziario (in Mio CHF)**	**Fallimento dei processi aziendali critici (in giorni)**	**Perdita di processi aziendali non critici (in giorni)**						
molto elevate **6**	› 10	**›14**		6	12	18	24	30	36
elevate **5**	1 – 10	**7 – 14**		5	10	15	20	25	30
essenziale **4**	0.5 – 1	**3 – 7**		4	8	12	**16**	**20**	24
moderato **3**	0.1 – 0.5	**0.5 – 3**	**›3**	3	6	9	**12**	15	18
esigue **2**	**0.01 – 0.1**	**0.5**	1 – 3	2	4	6	8	10	12
molto esigue **1**	‹ 0.01		‹ 1	1	2	3	4	5	6
				molto improbabile **1 più di 10 anni**	improbabile **2 ogni cinque o dieci anni**	raramente **3 ogni 3 a 5 anni**	possibile **4 ogni 2 a 3 anni**	probabilmente **5 ogni 1 a 2 anni**	molto probabilmente **6 Più volte all'anno**
				Probabilità di accadimento					

Figura 6: Matrice del rischio[VI]

Esempio di lettura

Passo 1	Valutazione del rischio finanziario	Valutazione dei fallimenti dei processi aziendali			
	La perdita finanziaria è tra 0,01 e 01,1 milioni di CHF. Livello 2				
Passo 2		Si valuta il tempo massimo di inattività dei processi aziendali critici			
		Il fallimento dei processi aziendali critici può durare al massimo 7 giorni. **Livello 4**			
Passo 3			Si valuta il tempo massimo di inattività dei processi aziendali non critici		
			Il fallimento di processi aziendali non critici può durare più di 3 giorni. Livello 3		
Viene applicato il livello massimo di impatto. In questo esempio il valore è **4**					
Passo 4				**Viene valutata la probabilità di accadimento**	
				Il guasto si verifica ogni 1–2 anni **Livello 5**	
	Il valore del rischio (Effeti (4) x Probabilità di accadimento (5) = **20**				
Passo 5	Attuazione di misure di riduzione del rischio	Poiché il valore del rischio è **20**, le misure di riduzione del rischio devono essere attuate entro 1 mese.		Protezione di base Valori 1 a 4	Non è necessario attuare misure di riduzione del rischio.
				Maggiore necessità di protezione Valori 5 a 15	Le misure di riduzione del rischio devono essere attuate entro 6 mesi.
				Molto alto Necessità di protezione Valori 18 a 36	Le misure di riduzione del rischio devono essere attuate entro 1 mese.

Fonte: In conformità con le direttive dell'Organo direzione informatica della Confederazione (ODIC)
P042 – Piano per la sicurezza dell'informazione e la protezione dei dati (SIPD) – Versione 4.3

6.2.6 Lotta alla cibercriminalità

La lotta alla cibercriminalità è un classico compito congiunto delle autorità di perseguimento penale della Confederazione e dei Cantoni. Per questo motivo nel 2018 è stato creato un «Concetto cyberboard». Il cyberboard consente un coordinamento rafforzato nel quadro dei compiti congiunti per trattare i casi intercantonali e internazionali. Il cyberboard funge da piattaforma basata sul mantenimento delle strutture e delle competenze esistenti. Non vi sono modifiche nell'ambito delle competenze e non vengono create nuove autorità. Il cyberboard si suddivide in un livello operativo e un livello strategico: Cyber-CASE, CyberSTATE e Cyber-CORE lavorano in ambito operativo, Cyber-STRAT in ambito strategico.

- **Cyber-STRAT:** è responsabile della gestione e dell'orientamento strategici del settore operativo del Cyberboard.
- **Cyber-CORE:** questo organo è l'interfaccia del settore operativo del Cyberboard. Determinati compiti del Cyber-CORE vengono svolti da collaboratori del MPC; finora tuttavia l'organo non è stato istituzionalizzato.
- **Cyber-CASE:** casistica nazionale, scambio di esperienze tra Cantoni/autorità, discussione di casi attuali ecc.
- **Cyber-STATE:** garantisce una valutazione del quadro della situazione consolidata a livello nazionale (e non solo all'interno del Cantone). Finora anche il Cyber-STATE non è stato istituzionalizzato (volutamente), dal momento che MELANI è rappresentata nel Cyber-CASE come fornitrice centrale di input per la situazione.

Cyberboard

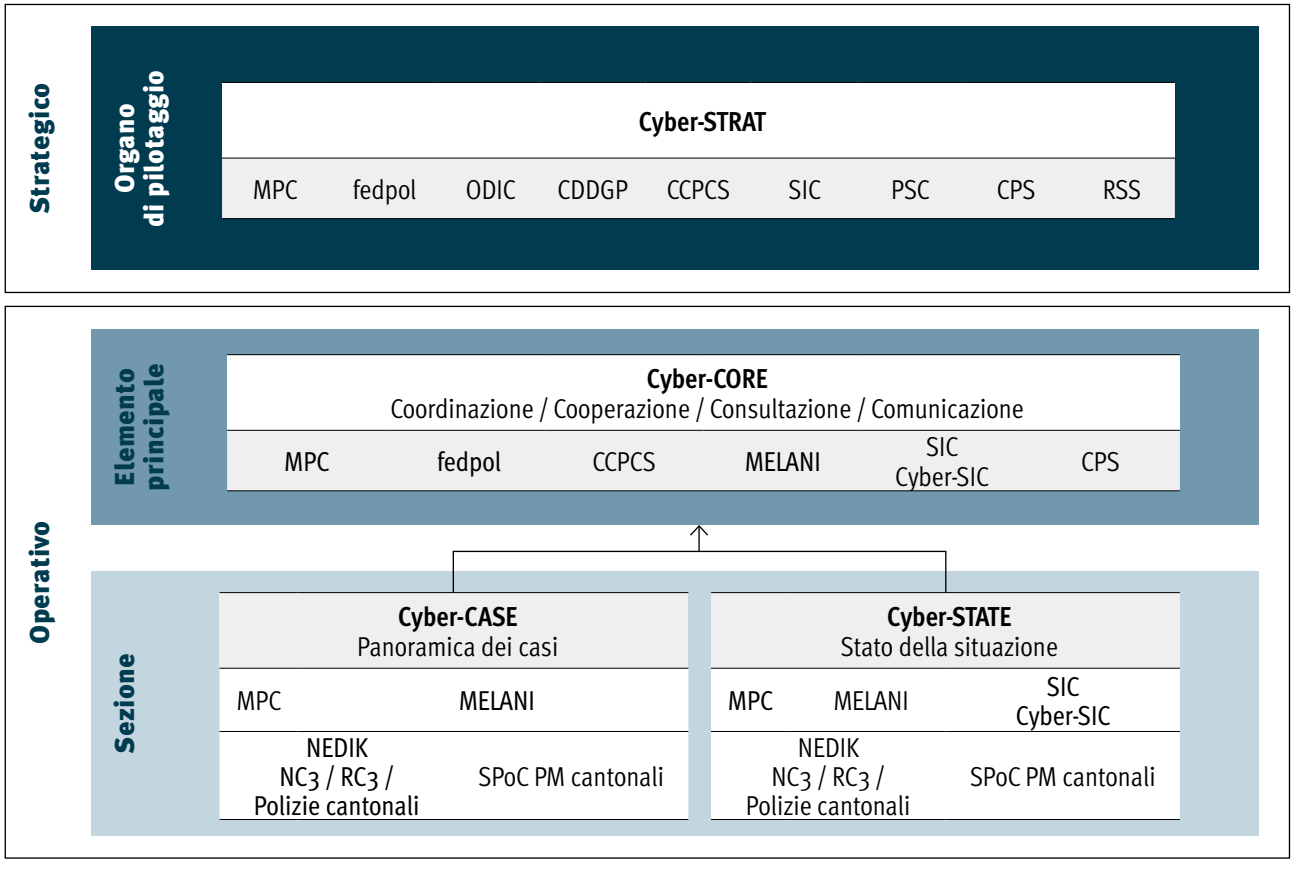

Figura 7: Cyberboard[VII]

7. Strategie e standard

Il presente concetto si basa sui seguenti standard e strategie, alcuni dei quali prevedono esplicitamente l'elaborazione di questo concetto per la ciberorganizzazione cantonale e la relativa attuazione. Attraverso l'applicazione di determinati standard si garantisce inoltre la possibilità di effettuare controlli adeguati.

7.1 Documenti di base a livello di Confederazione

- Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) 2018–2022[28]
- Strategia nazionale per la protezione delle infrastrutture critiche (PIC) 2018–2022[29]
- Ordinanza sulla protezione contro i ciber-rischi nell'Amministrazione federale 27.05.2020[30]
- Piano di attuazione della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi 2018–2022[31]
- Standard minimo per migliorare la resilienza delle TIC 2018[32]
- Analisi di rischio e di vulnerabilità e misure di resilienza 2018[33]

7.2 Documenti di base a livello cantonale

- Cybersecurity Core Framework/ NIST Standard 2018[34]
- Network Security Policy (NSP) 2017[35]
- Piano d'attuazione dei Cantoni relativo alla Strategia nazionale per la protezione della Svizzera contro i cyber-rischi 2018–2022[36]
- Leitlinien der Kantone zur Digitalen Verwaltung 2018[37]
- Strategie/documenti del Cantone[38]

28 https://www.bk.admin.ch/bk/it/home/digitale-transformation-ikt-lenkung/ikt-vorgaben/strategien-teilstrategien/sno02-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html (stato: 12.01.2021).
29 https://www.babs.admin.ch/it/aufgabenbabs/ski/nationalestrategie.html (stato: 15.07.2020).
30 https://www.admin.ch/opc/it/classified-compilation/20200291/index.html (stato: 15.07.2020).
31 https://www.ncsc.admin.ch/ncsc/it/home/strategie/umsetzungsplan.html (stato: 12.01.2021).
32 https://www.bwl.admin.ch/bwl/it/home/themen/ikt/ikt_minimalstandard.html (stato: 15.07.2020).
33 Questi documenti si possono reperire su richiesta presso l'Ufficio federale della protezione della popolazione.
34 National Institute of Standards and Technology (2018). *Framework for Improving Critical Infrastructure Cybersecurity.* https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf (stato: 05.11.2020).
35 Conferenza svizzera sull'informatica (CSI): https://intranet.sik.ch/dokumentation/ITEmpfehlungen/ITEmpfehlungen/Forms/AllItems.aspx?RootFolder=%2Fdokumentation%2FITEmpfehlungen%2FITEmpfehlungen%2FNSP%20Network%20Security%20Policies&FolderCTID=0x0120004325A2A049A4D545B893CFF7CD3EC2F9&View=%7b9FD8BBC0-634A-4D17-B788-1D3F75D21ABD%7d *(non tradotto in italiano)* (stato: 12.01.2021).
36 https://www.svs.admin.ch/it/temi/cybersicherheit/cybersicherheit-kantone.html *(non tradotto in italiano)* (stato: 09.07.2020).
37 https://kdk.ch/uploads/media/Leitlinien-E-Government_20180927.pdf *(non tradotto in italiano)* (stato: 09.07.2020).
38 Aggiunte tratte dai documenti del singolo Cantone.

8. Basi legali e altre direttive

Il presente concetto si fonda sulle basi legali o sulle direttive seguenti[39]:

Tali direttive devono essere verificate regolarmente, ovvero circa una volta all'anno; a seconda di quanto emerge di volta in volta, occorre modificare di conseguenza l'organizzazione.

Abbreviazioni delle leggi e delle ordinanze	Legge	Ordinanza	Istruzioni	Altre prescrizioni	Titolo	Data di entrata in vigore
LOA (es.)	X				Legge sull'organizzazione dell'amministrazione (es.)	12.01.2007
OOGC (es.)		X			Ordinanza sull'organizzazione cantonale di gestione delle crisi (es.)	05.09.2018
OCiber		X			Ordinanza sui ciber-rischi	27.05.2020
I-DMI (es.)			X		Misure volte ad assicurare la disponibilità dei mezzi informatici (es.)	03.05.2004
D-AMI (es.)				X	Direttive sugli acquisti di mezzi informatici (es.)	02.06.2015

39 Queste indicazioni servono da esempio. Tali basi possono essere completate e/o modificate ai fini della creazione delle singole organizzazioni cantonali in ambito cyber.

9. Situazione iniziale

9.1 Interventi parlamentari relativi a misure preventive in ambito ciber

Gli interventi parlamentari costituiscono una base importante per l'attuazione dell'organizzazione cantonale in ambito ciber. Questa tabella serve da modello per istituire una lista degli interventi cantonali di ogni Cantone. È stato inserito un intervento a titolo esemplificativo.

Numero dell'oggetto	Data	Titolo	Nome	Tipologia	Stato – mandato – in elaborazione – liquidato
16.5128	12.02.2020	Cibercriminalità	Marina Muster	Interpellanza	In elaborazione

9.2 Incidenti

Come illustrato negli esempi seguenti, tenere una lista degli eventi verificatisi nel Cantone consente di avere una visione sistematica degli attacchi con i relativi danni/costi generati (e che potrebbero ripetersi anche in futuro). Esempi:

Data	Titolo	Descrizione	Costi totali stimati
12.06.2019	Ransomware	Cifratura di informazioni	200'000 CHF
25.09.2019	Fuga di dati	Fuga di dati dal dipartimento x	1'000'000 CHF
15.09.2019	Diritti	Diritti amministrativi utilizzati da persone non autorizzate	30'000 CHF

La cibersicurezza è fondamentale per evitare questi eventi; la creazione di una ciberorganizzazione cantonale contribuisce a rafforzare la cibersicurezza.

9.3 Misure di sicurezza adottate in ambito organizzativo, informatico e della protezione delle informazioni

La tabella sottostante riporta un esempio delle misure adottate da un Cantone e fornisce una panoramica nonché una base per la valutazione della ciber-resilienza. La tabella deve essere costantemente aggiornata.

Tema	Attuazione completata al
Entrata in vigore delle istruzioni sulla sicurezza delle informazioni del Cantone in questione	100%
Attuazione delle misure per la protezione dell'amministrazione	50%
Attuazione delle misure per la protezione di base e la protezione avanzata dei mezzi TIC	75%
Attuazione della sicurezza delle reti (progetto, realizzazione e verifica)	80%
Attuazione del Business Continuity Management (BCM) inclusa la gestione dei rischi e delle emergenze	70%
Scenari concernenti l'ambito ciber e l'ambito delle emergenze informatiche nell'organizzazione cantonale di gestione delle crisi	20%

9.4 Il Business Continuity Management (BCM) e la prevenzione delle emergenze informatiche

Il Business Continuity Management (BCM) e la prevenzione delle emergenze informatiche sono due elementi importanti della gestione di un ciberattacco. L'amministrazione dovrebbe creare e verificare il BCM con il supporto del servizio informatico (nel quadro dell'IT-Service Continuity Management).

9.5 Approccio integrale

I seguenti elementi hanno un'influenza sul sistema informatico:

- Amministrazione cantonale
- cittadini
- infrastrutture critiche
- edifici e ambienti
- mezzi di informazione e di comunicazione (TIC) e informazioni (es. banche dati)
- fornitori (di prestazioni) interni ed esterni
- Centro nazionale per la cibersicurezza (NCSC)

I rispettivi dati consentono di istituire una visione globale della situazione. I dati acquisiti consentono di elaborare misure (immediate) per la riduzione dei rischi.

10. Allegati

I. Standard raccomandati

Il Cantone dovrebbe stabilire uno degli standard seguenti per la propria cibersicurezza e sicurezza delle informazioni.

Norma o raccomandazione	Titolo
ISO/IEC 27001	Tecnologia delle informazioni – Tecniche di sicurezza – Sistemi di gestione della sicurezza delle informazioni – Requisiti
ISO/IEC 27002	Tecnologie Informatiche – Tecniche di sicurezza – Codice di pratica per la gestione della sicurezza delle informazioni
ISOI/EC 31000	Gestione dei rischi
ISO/IEC 22301	Gestione della continuità operativa
BSI-Standards	Raccomandazione del Bundesamt für Sicherheit in der Informationstechnik tedesco
NIST 800-82	Standard per la sicurezza delle informazioni applicato nello standard minimo TIC dell'Ufficio federale per l'approvvigionamento economico del Paese (UFAE)

II. Documenti referenziati

I riferimenti devono essere adattati per ogni cantone.

N.	Titolo	Autore	Data/ Versione
[1]	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) 2018	Consiglio federale	
[2]	Strategia nazionale per la protezione delle infrastrutture critiche (PIC) 2018	Consiglio federale	
[3]	Piano di attuazione della «Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC) 2018–2022»	Consiglio federale	
[4]	Strategia in ambito cyber Cantone + *Nome del Cantone*	*Nome del Cantone*	
[5]	Politica di sicurezza delle reti (NSP) 2017		
[6]	Altri documenti del Cantone		
[7]	Altri documenti del Cantone		
[8]	Altri documenti del Cantone		

III. Esempi di ciberincidenti

Esempio 1: Amministrazione della città di Berna

Nel suo Rapporto semestrale 2019/1 (gennaio–giugno)[40] la Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) e il responsabile della sicurezza della tecnologia dell'informazione e della comunicazione dell'amministrazione comunale di Berna Martin Müller constatano che i software nocivi come i trojan di crittografia rappresentano un importante pericolo in ambito ciber per le autorità e le imprese. Gli aggressori inoltrano una richiesta di riscatto e in cambio promettono il ripristino dei dati che sono stati crittografati. Tuttavia non vi sono garanzie in merito al recupero dei dati. L'Amministrazione comunale di Berna ha subito attacchi di questo tipo nel 2017 e nel 2019. L'aspetto inquietante è che oggi attacchi di questo tipo possono essere sferrati senza disporre di particolari conoscenze o mezzi. Le misure preventive di sicurezza a livello tecnico come i firewall e una gestione dei backup risultano quindi fondamentali. Müller sostiene però che la formazione e la sensibilizzazione dei collaboratori rappresenti la misura più importante per garantire la sicurezza nel settore TIC.

Esempio 2: Postfinance

A inizio dicembre 2010 Postfinance aveva bloccato il conto del fondatore di Wikileak Julian Assange a causa di dati falsi sul suo domicilio forniti al momento dell'apertura del conto. Julian Assange aveva infatti indicato Ginevra come luogo di domicilio, informazione rivelatasi poi falsa durante la verifica dei dati. In reazione a questo avvenimento i suoi seguaci lanciarono attacchi hacker mirati che bloccarono il sito di Postfinance per diverse ore[41].

Esempio 3: Ospedale Wetzikon

Nell'ottobre del 2019 l'ospedale di Wetzikon subì l'attacco di un trojaner molto aggressivo. L'attacco venne lanciato attraverso un'e-mail che riproduceva in modo estremamente verosimile una comunicazione interna nella quale si chiedeva al destinatario di aprire l'allegato (un documento word) e di attivare una macro. In questo modo l'aggressore si procurava l'accesso al sistema senza che l'interessato se ne accorgesse. Un attacco di questo tipo si suddivide in diverse fasi, con l'obiettivo di identificare il maggior numero possibile di sistemi e crittografare i backup e i sistemi online. In seguito arriva la richiesta di riscatto, grazie al quale l'interessato può ottenere di nuovo l'accesso ai propri dati. Tuttavia l'ospedale di Wetzikon ha avuto fortuna: un informatico si accorse in tempo di alcune irregolarità nel firewall. La perdita fu quindi solo parziale, poiché si riuscì a bloccare gli attacchi e riparare i danni. Un attacco come questo potrebbe però avere esiti molto negativi in diversi ospedali, dal momento che varie infrastrutture del sistema sanitario svizzero non soddisfano gli standard minimi di sicurezza informatica[42].

---

40 Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (2019). *Rapporto semestrale 2019/1 (gennaio–giugno),* pag. 5. https://www.ncsc.admin.ch/ncsc/it/home/dokumentation/berichte.html (stato: 07.01.2021).

41 ATS (2010). «Postfinance-Webseite lahmgelegt»: *Neue Zürcher Zeitung,* 08.10.2020, https://www.nzz.ch/postfinance-website_lahmgelegt-1.8594103?reduced=true (stato: 12.01.2021).

42 Jenni, Thier (2020). «Wir hatten ein Riesenglück. Das Spital Wetzikon wurde von einem Trojaner angegriffen – viele Krankenhäuser unterschätzen die Gefahr»: *Neue Zürcher Zeitung*, 28.01.2020, https://www.nzz.ch/digital/wir-hatten-ein-riesenglueck-ld.1536678?reduced=true (stato: 07.01.2021).

Riferimenti delle illustrazioni

I Fonte: NCSC

II Fonte: RSS

III Fonte: RSS

IV Swisscom SA (2015). *Cyber Security: Die aktuelle Bedrohungslage und ihre Entwicklung.* https://www.swisscom.ch/content/dam/swisscom/de/about/unternehmen/portraet/netz/sicherheit/documents/cyber-security-report-2015.pdf.res/cyber-security-report-2015.pdf (stato: 18.08.2020).

V UFPP (2015). *Analisi nazionale dei pericoli – Dossier pericoli «Interruzione delle infrastrutture d'informazione e di comunicazione» (non tradotto in italiano)*. Consultabile al link https://www.babs.admin.ch/it/aufgabenbabs/gefaehrdrisiken/natgefaehrdanalyse/gefaehrddossier.html (stato: 12.01.2021).

VI Illustrazione: RSS

VII Fonte: Ministero pubblico della Confederazione

Rete integrata Svizzera per la sicurezza RSS
Tel. +41 58 462 20 29, www.svs.admin.ch

80.252.d 02.21