Rapporto annuale 2015

sullo stato di attuazione della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC)

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Eidgenössisches Finanzdepartement EFD
Informatiksteuerungsorgan des Bundes ISB
Melde- und Analysestelle Informationssicherung MELANI

Pubblicazione: 20.04.2016

Redazione: Servizio di coordinamento SNPC

Dipartimento federale delle finanze DFF

Organo direzione informatica della Confederazione ODIC
Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI

Schwarztorstrasse 59
CH-3003 Berna

Tel. +41 (0)58 462 45 38
e-mail: info@isb.admin.ch

Rapporto annuale SNPC: www.isb.admin.ch

Indice

Premessa

Il mondo digitale sta diventando sempre più importante, veloce e complesso. Occorre pertanto riconoscere e sfruttare al meglio le opportunità offerte alla Svizzera dalla digitalizzazione. In questo contesto non vanno tuttavia dimenticati i rischi. Anche nel 2015 vari eventi hanno mostrato che i rischi devono essere presi estremamente sul serio. Attività di spionaggio, nuove forme di malware, furto di dati e ricatti con attacchi DDoS hanno evidenziato la vulnerabilità del «motore» digitale dell'economia e della società. Ne sono stati esempi particolarmente emblematici le operazioni di spionaggio ai danni del Parlamento tedesco e in occasione dei negoziati condotti a Ginevra in vista dell'accordo sul nucleare con l'Iran.

Tali avvenimenti ci inducono a chiederci se in Svizzera stiamo facendo abbastanza per proteggerci dai cyber-rischi. Non esiste una risposta semplice a questa domanda. La natura stessa dei cyber-rischi, che sono in rapida evoluzione, ci obbliga a confrontarci costantemente con nuovi scenari e a verificare e adeguare di continuo le misure di protezione adottate. Dobbiamo inoltre rafforzare ulteriormente la cooperazione nazionale e internazionale. Possiamo tuttavia affermare con certezza che la Svizzera non è rimasta inattiva. Nel 2012 il Consiglio federale ha varato la «Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC)» e un anno più tardi ha approvato il relativo piano di attuazione. Ha definito come obiettivi strategici della SNPC l'identificazione precoce e puntuale dei cyber-rischi, la loro effettiva riduzione e il rafforzamento della capacità di resistenza della Svizzera a questi rischi.

Il rapporto annuale 2015 intende presentarvi una panoramica dello stato dei lavori nel terzo anno di attuazione della SNPC. In tutti i settori sono stati compiuti progressi importanti. A questo riguardo desidero sottolineare in particolare il rafforzamento della cooperazione tra tutte le parti coinvolte. Soltanto una collaborazione improntata alla fiducia tra la Confederazione, i Cantoni, l'economia e la società permetterà di proteggere meglio la Svizzera dai cyber-rischi. Già oggi uno dei successi della SNPC è l'intensificazione di questa collaborazione. Grazie alla SNPC, le responsabilità sono definite e tutti gli attori puntano nella stessa direzione.

Oltre a tracciare un bilancio dei risultati raggiunti, il rapporto delinea brevemente le prospettive future. Anche nel 2016 porteremo avanti a pieno ritmo l'attuazione della strategia. Daremo inoltre inizio ai lavori per l'ulteriore sviluppo della SNPC. La strategia attuale è in vigore sino alla fine del 2017. Il prossimo anno, nell'ambito di una valutazione, esamineremo i punti di forza e di debolezza della SNPC, in modo da poter sottoporre al Consiglio federale, nel 2017, una proposta relativa all'ulteriore modo di procedere.

Vi auguro una piacevole lettura del presente rapporto annuale. Sono lieto di poter portare avanti una proficua collaborazione con tutti i partner coinvolti affinché tutti noi possiamo sfruttare appieno i vantaggi della digitalizzazione senza che la sicurezza venga meno.

Peter Fischer
Delegato per la direzione informatica della Confederazione (ODIC)

1 Sintesi

Il 27 giugno 2012 il Consiglio federale ha approvato la «Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC)» e il 15 maggio 2013 il suo piano di attuazione. La SNPC, articolata in 16 misure, è incentrata sull'identificazione precoce dei cyber-rischi, sul rafforzamento della capacità di resistenza delle infrastrutture critiche e sulla riduzione delle cyber-minacce, in particolare lo spionaggio, il sabotaggio e la cyber-criminalità.

L'attuazione della SNPC è organizzata in modo decentralizzato. La responsabilità dell'attuazione è stata affidata a un Ufficio federale per ciascuna delle 16 misure. Per coordinare questi lavori, il Consiglio federale ha istituito un servizio di coordinamento (SC SNPC), aggregato alla Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) in seno all'Organo direzione informatica della Confederazione (ODIC). La responsabilità generale spetta al comitato direttivo (CD SNPC), incaricato di seguire i lavori di attuazione mediante un controlling strategico.

Le 16 misure interessano quattro settori: prevenzione, reazione, continuità e processi di sostegno. Negli anni scorsi sono stati raggiunti importanti obiettivi in tutti i settori, anche grazie a una stretta collaborazione e una proficua comunicazione con tutti gli attori coinvolti.

Nell'ambito della prevenzione, l'Ufficio federale della protezione della popolazione (UFPP) e l'Ufficio federale per l'approvvigionamento economico del Paese (UFAE) hanno condotto finora analisi dei rischi e della vulnerabilità in dieci sottosettori critici (approvvigionamento di gas naturale, traffico stradale, approvvigionamento elettrico, traffico aereo, approvvigionamento alimentare, assistenza medica e ospedali, banche, laboratori, media e protezione civile). Per individuare i rischi, è necessario non solo conoscere le vulnerabilità ma anche valutare bene le minacce attuali. A questo scopo MELANI ha sviluppato un radar interattivo della situazione che visualizza le diverse cyber-minacce nei confronti delle infrastrutture svizzere, indicandone inoltre la rilevanza. Una panoramica delle principali cyber-minacce nel 2015 è contenuta nel Rapporto semestrale MELANI e nel Rapporto annuale SCOCI.

Nel settore della reazione, anche nel 2015 sono stati ulteriormente potenziati i centri di competenze specialistiche per l'analisi dei software nocivi (ad es. GovCERT.ch, CISIRT-UFIT, milCERT-DDPS) e sviluppati numerosi prodotti. GovCERT ha realizzato e messo in servizio numerose piattaforme per lo scambio di informazioni tecniche. Queste servono a monitorare il malware e a cercare in modo semplice ed efficiente, per periodi di tempo prolungati, le prove di una manipolazione (cosiddetti «indicators of compromise») di sistemi informatici e reti. È così possibile informare rapidamente e proteggere le aziende e le organizzazioni interessate. Rientra nel settore della reazione anche l'identificazione degli autori. In questo settore la divisione specializzata Cyber del Servizio delle attività informative della Confederazione (SIC) ha acquisito conoscenze e competenze specialistiche che le consentono di analizzare gli obiettivi, i metodi e gli attori di un attacco e di identificare in tal modo i possibili autori.

Nell'ambito della continuità, nei due sottosettori critici «approvvigionamento di gas naturale» e «media» è stata elaborata, sulla base dell'analisi dei rischi e della vulnerabilità, una prima bozza delle diverse misure volte a migliorare la resilienza. Per gli altri sottosettori i rapporti sulle misure sono in elaborazione conformemente alla pianificazione.

Nei processi di sostegno l'accento è posto sui settori della ricerca e della formazione nonché sulla collaborazione internazionale. La Segreteria di Stato per la formazione, la ricerca e l'innovazione (SEFRI) ha istituito un comitato direttivo interdipartimentale che coordina e porta avanti a livello nazionale tutte le attività di ricerca e di formazione relative ai cyber-rischi.

La collaborazione internazionale è stata ulteriormente rafforzata ed ampliata a livello bilaterale e multilaterale sotto la direzione della Divisione politica di sicurezza (DPS) del Dipartimento federale degli affari esteri (DFAE) e dell'Ufficio federale della comunicazione (UFCOM). A livello bilaterale sono stati instaurati nuovi contatti e intensificati quelli esistenti. A livello multilaterale sono stati ulteriormente sviluppati i lavori relativi alle misure di rafforzamento della fiducia dell'OSCE.

Nel mese di gennaio del 2016 sarà avviato un esame dell'efficacia delle 16 misure, condotto da un servizio esterno e neutrale. I risultati saranno presentati al Consiglio federale nella primavera del 2017 come base per le decisioni relative all'ulteriore modo di procedere.

Principali cyber-minacce nel 2015

Il 2015 è stato caratterizzato principalmente dalle seguenti cyber-minacce:

- **spionaggio** (Duqu 2: intercettazione dei dialoghi sul programma nucleare iraniano. Carbanak: rapina elettronica a una banca, attacco di hacker al Parlamento tedesco);
- **furto di dati** (sottratti oltre 21 milioni di set di dati dall'ufficio di gestione del personale del governo degli Stati Uniti, Rex Mundi);
- **attacchi a sistemi di controllo industriali** («honeypot» centrale idroelettrica: 31 attacchi, AutoHack);
- **impiego di crimeware** (trojan bancario come Torpig, Dyre, Tinba, Gozi, Zeus);
- **attacchi DDoS** (TV5 Monde, Charlie Hebdo, cancellazione di voli di Polish Airlines);
- **ricatti** (Cryptolocker: Cryptowall 3.0, Teslascript);
- **defacement** (deturpamento di siti Web da parte di simpatizzanti islamisti in Francia e nella Svizzera francese dopo Charlie Hebdo);
- **social engineering e phishing** (attacchi a banche cantonali, dati delle carte di credito).

2 Attività

In questo capitolo sono riportate alcune importanti attività e manifestazioni svoltesi a livello nazionale e internazionale.

2.1 Contesto nazionale

Il 22 e il 23 aprile 2015 si è tenuta a Ginevra la «Cyber 9/12 Student Challenge». L'Atlantic Council e il Geneva Centre for Security Policy (GCSP) hanno ospitato la manifestazione, durante la quale studenti universitari provenienti da Stati Uniti, Gran Bretagna, Francia, Polonia, Ungheria, Finlandia, Estonia e Svizzera si sono dovuti preparare ad affrontare un grande cyber-attacco e a elaborare raccomandazioni operative adeguate. Il team svizzero è risultato vincitore del concorso.

Il 23 aprile 2015 si è svolta la terza «Cyber-Landsgemeinde». Circa 80 cyber-responsabili della Confederazione e dei Cantoni nonché alcuni partner della Rete integrata Svizzera per la sicurezza (RSS) hanno preso parte a questa manifestazione di networking. Come negli anni passati, l'evento era dedicato allo stato di avanzamento dei progetti realizzati a livello cantonale e nel quadro della SNPC.

Dal 19 al 22 ottobre 2015 si è tenuta a Lucerna la terza edizione dello «European Cyber Security Challenge». Nell'ambito di questa competizione internazionale allievi e studenti provenienti da Austria, Germania, Romania, Gran Bretagna, Spagna e Svizzera si sono cimentati nell'identificazione, nello sfruttamento e nell'eliminazione delle vulnerabilità dei sistemi informatici. La manifestazione è stata organizzata dall'associazione Swiss Cyber Storm, dal DFAE e dal Dipartimento federale delle finanze (DFF).

Il 2 novembre 2015 si è svolta la seconda conferenza SNPC con l'obiettivo di offrire ai rappresentanti dell'economia e della politica una panoramica dettagliata dello stato di attuazione delle misure della SNPC e di favorire lo scambio di informazioni tra tutti gli attori dell'amministrazione e dell'economia (in particolare i gestori di infrastrutture critiche).

2.2 Contesto internazionale

Il 16 e 17 aprile 2016 si è svolta all'Aia la «Global Conference on Cyberspace (GCCS)» che si è occupata della creazione di norme per la condotta degli Stati nel cyber-spazio. Nel suo discorso di apertura della conferenza, il consigliere federale Didier Burkhalter si è impegnato affinché anche nel cyber-spazio trovi applicazione una normativa di natura politica e giuridica.

Il 29 e 30 settembre 2015 si è tenuto il workshop della European Union Agency for Network and Information Security (ENISA) sulla sicurezza delle infrastrutture critiche nell'UE e in Svizzera. La Svizzera è l'unico Stato non membro dell'UE a essere rappresentato in questo gruppo di lavoro. L'obiettivo dell'evento era confrontare il livello di protezione delle infrastrutture critiche (processi, organizzazione, attori) in 15 Paesi dell'UE e in Svizzera. I risultati sono stati pubblicati sul sito Web dell'ENISA.

Nel 2015 la Svizzera ha preso parte per due volte al «Sino-European Cyber Dialogue», un dialogo multilaterale tra Stati europei e Cina finalizzato a comprendere meglio la rispettiva percezione delle minacce e a identificare le questioni da approfondire nel reciproco interesse.

Il 28 e il 29 ottobre 2015 si è tenuta a Belgrado, con la partecipazione della Svizzera, la Conferenza dell'OSCE presieduta dalla Serbia. La Conferenza era incentrata sulla prosecuzione dell'approccio multistakeholder in un contesto di politica della sicurezza. È stata di preziosa utilità per gli Stati che devono sviluppare cyber-strategie nazionali. Per la prima volta si è svolta inoltre un'esercitazione «tabletop» di DiploFoundation, volta a rafforzare la collaborazione fra Stati nell'ambito di un forum multilaterale. La Svizzera ha sostenuto la Conferenza

in modo sostanziale sia sul piano concettuale che finanziario.

Anche nel 2015 il gruppo specialistico «Cyber-International» ha continuato a garantire un flusso sistematico di informazioni tra i servizi federali interessati, allo scopo di migliorare la coerenza e l'efficacia della politica estera in materia di cyber-spazio.

3 Stato dei lavori di attuazione della SNPC nel 2015

La SNPC è una strategia integrale, che con le sue 16 misure (M1-M16) persegue un approccio globale per proteggere la Svizzera dalle cyber-minacce. Le misure si suddividono in quattro settori in base al loro sviluppo temporale e alle loro interdipendenze:

- prevenzione (M2, M3, M4);
- reazione (M5, M6, M14);
- continuità (M12, M13, M15);
- processi di sostegno (M1, M7, M8, M9, M10, M11, M16).

La SNPC è in atto da tre anni e per la maggior parte delle misure i lavori si trovano in uno stadio molto avanzato. In questo capitolo il quadro generale dell'attuazione è spiegato sulla base di una roadmap. Nei capitoli seguenti un breve rapporto del rispettivo Ufficio responsabile informa sullo stato attuale dell'attuazione delle singole misure nei quattro settori.

Roadmap SNPC

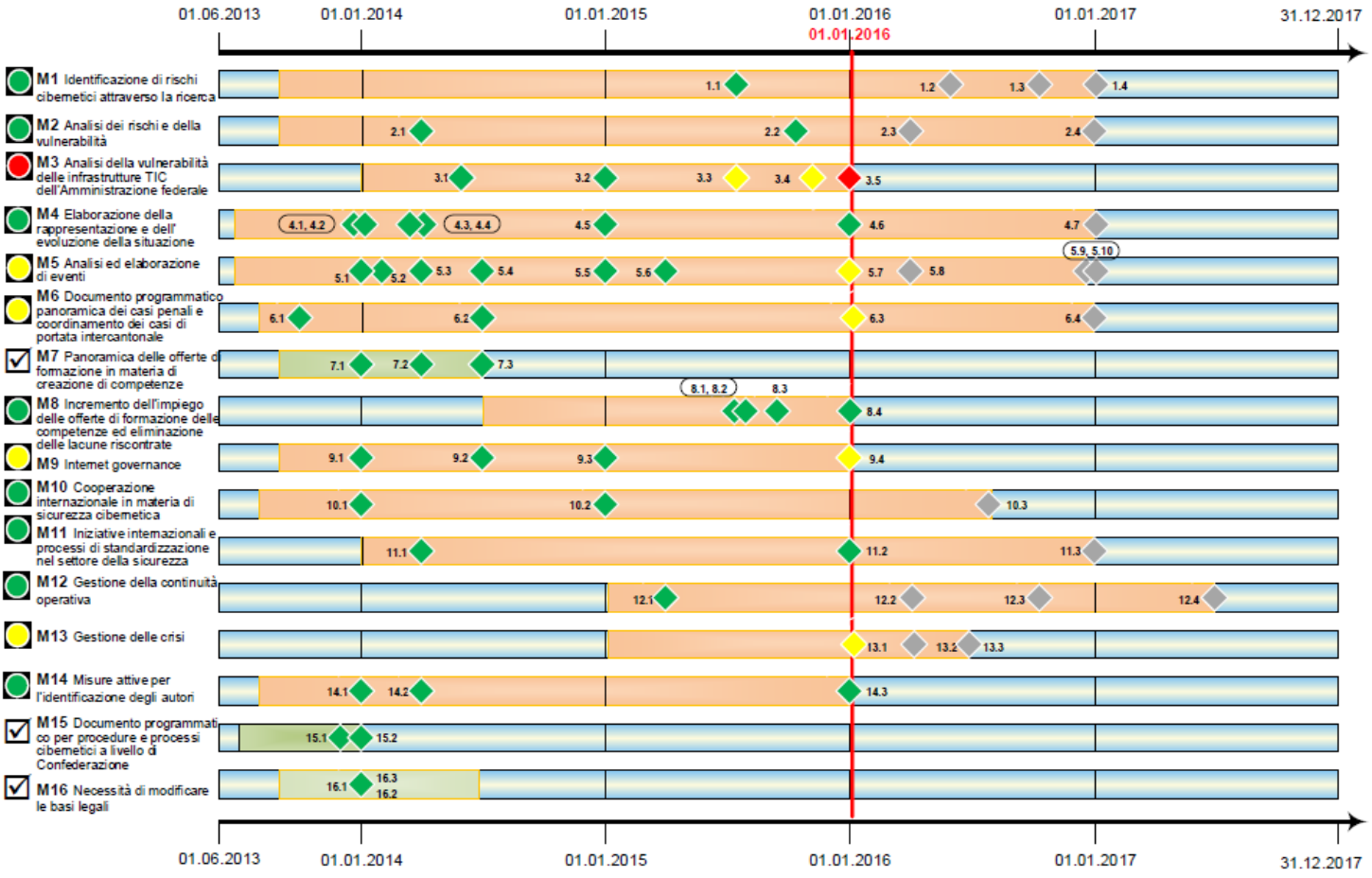
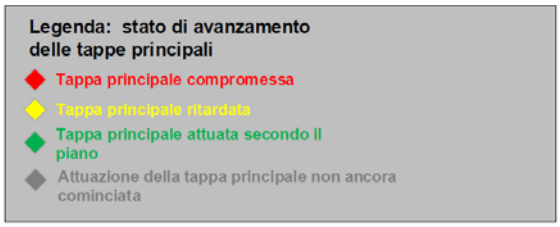


Figura 1: Roadmap SNPC



3.1 Prevenzione

La prevenzione riguarda le seguenti misure: analisi dei rischi e della vulnerabilità (M2), analisi della vulnerabilità delle infrastrutture TIC dell'Amministrazione federale (M3) e rappresentazione della situazione (M4).

3.1.1 Misura 2: Analisi dei rischi e della vulnerabilità

Responsabilità: DEFR-UFAE, DDPS-UFPP, autorità specializzate; DFF-MELANI

L'obiettivo dell'analisi dei rischi e della vulnerabilità è individuare i rischi per la Svizzera derivanti dalle vulnerabilità delle infrastrutture critiche TIC. I cyber-rischi si presentano quando queste vulnerabilità sono minacciate (ad es. attacchi informatici).

L'UFAE e l'UFPP si dividono i lavori nei 28 sottosettori complessivi della Svizzera e coordinano il loro modo di procedere. Nei singoli sottosettori le analisi dei rischi e della vulnerabilità si sono svolte in larga misura secondo i piani. In questo contesto sono stati consultati numerosi esperti delle aziende, delle associazioni di categoria e dei servizi federali competenti. Le analisi poggiano pertanto su un ampio consenso e nel contempo confermano il grande interesse dei servizi coinvolti.

Stato attuale

Nel mese di gennaio del 2016 le analisi dei rischi e della vulnerabilità erano concluse in dieci sottosettori: approvvigionamento di gas naturale, traffico stradale, approvvigionamento elettrico, traffico aereo, approvvigionamento alimentare, assistenza medica e ospedali, banche, laboratori, media e protezione civile. In sette sottosettori le analisi sono in corso: Parlamento, Governo, giustizia e amministrazione; esercito; organizzazioni di primo intervento; approvvigionamento idrico; acque di scarico; approvvigionamento di olio minerale.

3.1.2 Misura 3: Analisi della vulnerabilità delle infrastrutture TIC dell'Amministrazione federale sulla base di un piano di verifica

Responsabilità: DFF-ODIC; DFF-MELANI e UFIT, DDPS-BAC

Secondo la SNPC i servizi della Confederazione devono verificare le vulnerabilità delle proprie infrastrutture TIC coinvolgendo i fornitori di prestazioni TIC come pure i fornitori di sistemi. L'ODIC è stato incaricato di predisporre entro la fine del 2015 un piano per verificare periodicamente le vulnerabilità sistemiche, organizzative e tecniche delle infrastrutture TIC dell'Amministrazione federale.

Stato attuale

È stata elaborata una bozza del piano di verifica relativo all'analisi della vulnerabilità delle infrastrutture TIC dell'Amministrazione federale. Nel mese di agosto essa è stata presentata per la consultazione al comitato direttivo (CD SNPC). La principale divergenza emersa dalla consultazione riguarda il fatto che il piano propone un metodo di analisi dei rischi, mentre la misura 3 della strategia mira a fornire un metodo relativo all'analisi della vulnerabilità. Diversi membri del CD SNPC ritengono inoltre che l'attuazione comporti un ingente carico di lavoro e dubitano che il piano presentato possa produrre l'effetto sperato. In occasione della sua sesta seduta, prevista nel mese di febbraio del 2016, il comitato direttivo SNPC deciderà in merito all'ulteriore modo di procedere per quanto attiene alla misura 3.

Secondo il DFAE la principale divergenza risiede nel fatto che il piano propone un metodo di

analisi dei rischi, mentre la misura 3 della strategia mira a fornire un metodo di analisi della vulnerabilità.

3.1.3 Misura 4: Elaborazione della rappresentazione e dell'evoluzione della situazione

Responsabilità: DFF-MELANI, DDPS-SIC, DFGP-SCOCI; DDPS-BAC e SIM, DFF-UFIT

Per fronteggiare i cyber-attacchi occorre una rappresentazione della situazione che informi degli sviluppi in atto nel cyber-spazio e descriva i rischi e i danni potenziali degli attacchi in ogni settore critico oltre che la loro rilevanza per la Svizzera.

Tutte le informazioni rilevanti evinte dalle analisi tecniche e attinte dal servizio delle attività informative e dalla polizia devono confluire nella rappresentazione della situazione affinché questa sia per quanto possibile completa. A tal fine occorre definire i processi presso i singoli attori e tra di essi e assegnare le responsabilità. Fra gli attori figurano il Computer Emergency Response Team di MELANI all'interno dell'ODIC (GovCERT), l'Operation Information Center di MELANI nel SIC (MELANI OIC), il settore Cyber nel SIC e il Servizio informazioni militare (SIM). L'obiettivo della SNPC è elaborare una rappresentazione della situazione in stretta collaborazione con tutti gli attori rilevanti.

Stato attuale

I processi per elaborare una rappresentazione della situazione, definire le procedure organizzative, il ritmo di condotta e le responsabilità tra MELANI-ODIC/GovCERT, MELANI-OIC e Cyber SIC sono stati registrati. Il Cyber SIC, responsabile del trattamento di informazioni rilevanti per il Servizio delle attività informative, ha inoltre esteso le proprie competenze e conoscenze specialistiche (obiettivo e metodo di un cyber-attacco, analisi delle minacce, identificazione degli autori). Per sostenere il SIC si è fatto inoltre ricorso alle competenze tecniche della Base d'aiuto alla condotta (BAC) dell'esercito. Il relativo Service Level Agreement (SLA) è stato firmato. Sono stati inoltre definiti e introdotti processi tra MELANI e i servizi competenti dell'UFAE e dell'UFPP. Infine, gli adeguamenti a livello operativo resisi necessari nel quadro dei lavori relativi alla misura 15 (gestione delle crisi) sono prossimi alla conclusione; in tal modo sarà possibile testare a livello operativo i processi di gestione delle crisi in occasione di esercitazioni internazionali.

3.2 Reazione

Per poter reagire il più velocemente possibile in caso di eventi sono necessarie un'analisi coordinata dell'evento e la sua elaborazione. La SNPC prevede un ampliamento delle competenze e un potenziamento della capacità di reazione di tutte le organizzazioni e degli attori coinvolti. Ciò garantisce una rapida analisi degli eventi, un sollecito intervento delle autorità di perseguimento penale e la possibilità di identificare tempestivamente gli autori (M5, M6, M14). Nel settore della reazione sono previste le seguenti misure: analisi ed elaborazione di eventi (M5), panoramica dei casi penali e coordinamento dei casi di portata intercantonale (M6) nonché misure attive per l'identificazione degli autori (M14).

3.2.1 Misura 5: Analisi ed elaborazione di eventi

Responsabilità: DFF-MELANI, DDPS-SIC; DDPS-BAC e SIM, DFF-UFIT

La capacità di essere pronti ad affrontare cyber-eventi e di reagire ad essi è una condizione essenziale per la riduzione dei cyber-rischi. Secondo il piano di attuazione della SNPC le attività di analisi ed elaborazione di eventi devono essere ulteriormente sviluppate. I diversi Computer Emergency Response Team (CERT) (GovCERT, CISIRT-UFIT e milCERT-DDPS)

dovranno ampliare le competenze nell'ambito dell'analisi di malware affinché, in caso di evento, sia possibile analizzare e trattare i dati nonché adottare contromisure di natura tecnica. Per adempiere a questo mandato occorre in primo luogo ampliare le capacità tecniche e le conoscenze specialistiche e procedere in secondo luogo a un'analisi e a una valutazione esaustive delle minacce. È altresì necessario migliorare la capacità di resistenza, aumentare la capacità di reazione di tutti i CERT e creare una rete di questi ultimi.

Stato attuale

Nel 2015 il GovCERT ha realizzato e reso operative due piattaforme per lo scambio di informazioni tecniche sulle cyber-minacce. Entrambe si basano sull'Open Source Software MISP (piattaforma Malware Information Sharing).

Con alcuni membri selezionati della cerchia chiusa di clienti di MELANI (settori energetico e finanziario) è stato realizzato un progetto pilota che consente alle organizzazioni e al GovCERT di cercare in modo semplice ed efficiente, per periodi di tempo prolungati, eventuali manipolazioni (cosiddetti «indicators of compromise») di sistemi informatici e reti.

Sono state inoltre sviluppate ulteriormente diverse piattaforme che consentono il monitoraggio del phishing e degli attacchi di malware, al fine di informare e proteggere le aziende e le organizzazioni interessate. A questo proposito occorre citare in particolare il sito Web antiphishing.ch. Con l'aiuto di questo nuovo sito Web, cittadini e aziende possono segnalare a MELANI gli URL utilizzati per il phishing. Le informazioni così raccolte vengono trattate statisticamente e servono a elaborare una rappresentazione tecnica della situazione.

Grazie alla creazione di un posto di lavoro supplementare il GovCERT ha aumentato la sua capacità di analisi e di resistenza.

3.2.2 Misura 6: Documento programmatico per una panoramica dei casi penali e il coordinamento dei casi di portata intercantonale

Responsabilità: DFGP-SCOCI; DFF-MELANI

Per minimizzare i cyber-rischi in modo duraturo occorre un efficiente perseguimento penale nazionale e internazionale della criminalità informatica. A tale scopo, nella misura 6 della SNPC è stato sancito che il Servizio di coordinazione per la lotta contro la criminalità su Internet (SCOCI), aggregato all'Ufficio federale di polizia (fedpol) presso il Dipartimento federale di giustizia e polizia (DFGP), presenti, entro la fine del 2016, un documento programmatico «Panoramica dei casi penali e coordinamento dei casi di portata intercantonale» elaborato in collaborazione con i Cantoni.

Stato attuale

Nel 2015 il documento programmatico è stato elaborato e presentato per la consultazione alle autorità di perseguimento penale della Confederazione e dei Cantoni. Le osservazioni materiali fatte dagli Uffici consultati hanno potuto essere riprese nell'attuale bozza del documento programmatico.

Oltre a tale documento, in collaborazione con il Ministero pubblico della Confederazione il fedpol ha redatto un catalogo dei cyber-fenomeni comprendente 25 schede che descrivono le diverse forme di cyber-criminalità, i relativi autori, i mezzi utilizzati e il metodo di attacco adottato nonché gli obiettivi e la complessità tecnica degli attacchi. Questo catalogo ha un'influenza decisiva sulla definizione concreta della cyber-criminalità in Svizzera.

La consultazione ha confermato che le autorità di perseguimento penale privilegiano un rilevamento centralizzato degli atti di cyber-criminalità, affinché si possa elaborare una panoramica nazionale dei casi. I cyber-fenomeni catalogati nell'ambito della misura 6 sono stati

presi in considerazione negli attuali lavori del gruppo di lavoro per l'armonizzazione dell'informatica della polizia svizzera. Indipendentemente dai sistemi d'informazione di polizia utilizzati, in tal modo si garantisce un rilevamento unitario dei casi di cyber-criminalità.

In parallelo ai lavori concettuali relativi alla misura 6 della SNPC, la Conferenza dei comandanti delle polizie cantonali della Svizzera (CCPCS) e il fedpol stanno mettendo a punto una strategia nazionale globale relativa a tutti gli aspetti del perseguimento della cyber-criminalità. Questa strategia Cybercrime[1] dovrà includere il lavoro di indagine vero e proprio nonché questioni legate all'organizzazione, all'infrastruttura e alla formazione. Essa dovrà precisare, in quanto aspetti parziali, anche le modalità di attuazione delle misure e le stime del fabbisogno che costituiscono l'oggetto del mandato di base del SCOCI e del rapporto relativo alla misura 6.

3.2.3 Misura 14: Misure attive per l'identificazione degli autori

Responsabilità: DDPS-SIC; DFF-MELANI, DFGP-SCOCI, DDPS-SIM

La SNPC intende potenziare le competenze del Servizio delle attività informative della Confederazione (SIC) per quanto riguarda l'identificazione degli autori (analisi degli attori e del contesto e sviluppo di strumenti tecnici). Anche in questo caso è necessaria una stretta collaborazione degli attori coinvolti (MELANI, SIC, SCOCI, Cyber SIC e, a titolo sussidiario, l'esercito).

Stato attuale

Per disporre di conoscenze specialistiche e competenze relative al cyber-spazio, il SIC ha creato il settore Cyber SIC, con la BAC e il Servizio informazioni militare (SIM) quali fornitori di prestazioni. Sono state implementate le interfacce tra il Cyber SIC e MELANI ed è stato avviato lo scambio di informazioni tra questi servizi. Il Cyber SIC ha inoltre potuto maturare competenze e conoscenze e sviluppare una vasta rete di contatti e di fonti d'informazione. Questo nuovo bagaglio di conoscenze consente al Cyber SIC di rilevare in modo precoce, sia autonomamente che in collaborazione con la BAC e il SIM quali fornitori di prestazioni, cyber-attacchi diretti contro gli interessi della Svizzera. Tali scoperte confluiscono nell'analisi della situazione di minaccia condotta da MELANI. Grazie alla SNPC anche la BAC e il SIM hanno sviluppato competenze tecniche e analitiche e conoscenze in ambito militare-strategico relative al cyber-spazio.

3.3 Gestione della continuità operativa e delle crisi

La gestione di una crisi presuppone procedure e processi di condotta chiaramente definiti per l'evento. La gestione della continuità operativa garantisce che i processi operativi siano disponibili anche durante una crisi. La continuità comprende le seguenti misure: gestione della continuità volta a migliorare la resilienza dei sottosettori critici (M12), coordinamento delle attività con gli attori interessati e supporto attraverso perizie specializzate (M13) nonché documento programmatico per procedure e processi di condotta che include anche i cyber-aspetti (M15).

3.3.1 Misura 12: Gestione della continuità operativa: miglioramento della resilienza dei sottosettori critici

Responsabilità: DEFR-UFAE, DDPS-UFPP, autorità specializzate; DFF-MELANI

[1] Vedi anche n. 7.2.1.

Sulla base dei risultati dell'analisi dei rischi e della vulnerabilità l'UFAE in qualità di responsabile e l'UFPP definiscono le misure necessarie a garantire la continuità operativa insieme con le imprese interessate e i servizi specialistici competenti. Per ciascuno dei 28 sottosettori viene elaborato un rapporto sulle misure fondato sull'analisi dei rischi e della vulnerabilità.

Stato attuale

Nell'approvvigionamento di gas naturale è stata redatta una prima bozza di catalogo di misure che è stata sottoposta per un esame al servizio di coordinamento SNPC. Le imprese interessate istituiranno un servizio di picchetto comune attivo 24 ore su 24 e sette giorni su sette che potrà intervenire a breve termine in caso di eventi TIC. Le imprese si doteranno inoltre del sistema di comunicazione di emergenza «Polycom» e aderiranno alla cerchia chiusa di clienti di MELANI.

Nel traffico stradale la vulnerabilità è così limitata che per il momento non vengono proposte misure. Occorrerà invece osservare gli sviluppi in corso (ad es. le TIC nel veicolo) per rivalutarli nell'ambito delle analisi periodiche della vulnerabilità.

Nel settore media è prevista la creazione di un nuovo gruppo specialistico all'interno della cerchia chiusa di clienti di MELANI. Singole imprese stanno inoltre esaminando la costituzione di ubicazioni ridondanti. Bisognerà inoltre osservare l'evoluzione dinamica (relativa ad es. alle nuove tecnologie di diffusione) del panorama mediatico e valutarla periodicamente alla luce della vulnerabilità e dei rischi recenti.

Anche negli altri settori critici, in cui i lavori dovrebbero concludersi entro il mese di gennaio del 2016, l'analisi dei rischi e della vulnerabilità ha permesso di identificare le prime possibili misure. Queste sono attualmente all'esame dei servizi competenti e delle autorità specializzate e saranno descritte con maggior dettaglio nei rispettivi rapporti.

3.3.2 Misura 13: Coordinamento delle attività con gli attori direttamente interessati e supporto con perizie specializzate

Responsabilità: DEFR-UFAE, DFF-MELANI, DDPS-UFPP; DFAE-DP, DPGP-SCOCI

In caso di crisi MELANI fornisce agli attori interessati un supporto sussidiario mettendo a loro disposizione le proprie conoscenze e competenze. Lo scambio facoltativo di informazioni tra gestori di infrastrutture critiche, fornitori di prestazioni TIC e fornitori di sistemi viene assicurato al fine di rafforzare la continuità e la capacità di resistenza sulla base dell'autoaiuto. A questo scopo non sono stati soltanto garantiti, ma anche ulteriormente sviluppati i servizi attualmente disponibili.

Il DFAE viene informato nei casi in cui si presentano possibili implicazioni di politica estera ed è coinvolto nell'elaborazione della pianificazione preventiva.

Stato attuale

Per determinare le esigenze degli attori coinvolti, MELANI ha condotto un sondaggio online all'interno della cerchia chiusa di clienti. I risultati sono attualmente oggetto di analisi e costituiscono la base per l'ulteriore sviluppo e gli adeguamenti dei prodotti e dei servizi di MELANI. Il piano per il rafforzamento di MELANI quale piattaforma di scambio di informazioni è stato consolidato e adeguato e sarà ora ampliato e armonizzato con le esigenze dei sottosettori critici per quanto concerne la gestione della continuità operativa.

3.3.3 Misura 15: Documento programmatico per procedure e processi di condotta cibernetici

Responsabilità: CaF

La misura 15 intende integrare la gestione generale delle crisi con i cyber-aspetti.

Stato attuale

Questa misura è stata conclusa nel 2014.

La misura 15 è stata conclusa a livello di Confederazione con un documento programmatico per procedure e processi di condotta in situazioni di crisi che include anche i cyber-aspetti. Al contempo è stata ulteriormente sviluppata la collaborazione con i Cantoni e i gestori di infrastrutture critiche nell'ambito dell'attuazione della SNPC da parte della Rete integrata Svizzera per la sicurezza nel gruppo di lavoro 3 Gestione delle crisi. Le attività di questo gruppo di lavoro dovranno pertanto essere documentate anche nel rapporto annuale sull'attuazione della SNPC. I relativi dettagli sono riassunti al capitolo 3.6.

3.4 Processi di sostegno

Le cooperazioni internazionali, lo sviluppo di competenze attraverso la formazione e la ricerca ed eventualmente l'adeguamento delle basi legali costituiscono le basi e i processi necessari ad affrontare la cyber-problematica. A tale scopo sono stati creati i seguenti pacchetti di misure:

- ricerca e formazione delle competenze (M1, M7, M8);
- cooperazioni internazionali (M9, M10, M11);
- basi legali (M16).

3.4.1 Misura 1: Identificazione di cyber-rischi attraverso la ricerca

Responsabilità: SEFRI; SC SNPC

Con l'aiuto della ricerca dovranno essere identificati i cyber-rischi rilevanti per il futuro, nonché i cambiamenti intervenuti nel panorama delle minacce, affinché le decisioni politiche ed economiche possano essere prese in modo tempestivo e mirato. A tal fine viene incentivata la ricerca (la ricerca di base e quella applicata) nell'ambito della protezione contro i cyber-rischi. La responsabilità per l'attuazione spetta alla SEFRI in collaborazione con il servizio di coordinamento SNPC (SC SNPC).

Stato attuale

Nel mese di gennaio del 2015 la SEFRI ha istituito il comitato direttivo «Ricerca nell'ambito della protezione contro i cyber-rischi» (Comité de Pilotage Recherche et Formation Cyber - CoPIRFCyber). Il comitato è composto da rappresentanti di tutti gli organi dell'Amministrazione federale interessati alle questioni concernenti la ricerca e la formazione nel settore dei cyber-rischi. Esso mira a definire l'orientamento generale della ricerca e i principali temi di ricerca (di base e applicata) per i prossimi 5, 10 e 20 anni.

Per avvalersi di un sostegno specialistico il CoPIRFCyber ha istituito un gruppo di esperti composto da 14 specialisti dell'insegnamento, della ricerca e della pratica attivi nel settore dei cyber-rischi. Il gruppo di esperti inizierà il proprio lavoro nel mese di gennaio del 2016. La SEFRI organizza inoltre un convegno finalizzato a lanciare la ricerca nel campo dei cyber-rischi in Svizzera e a coinvolgere ulteriori specialisti nei lavori del gruppo di esperti. La Swiss Cyber Risk Research Conference (SCRRC) si terrà il 20 maggio 2016 presso lo Swiss Tech Convention Center del Politecnico federale di Losanna[2].

[2] Le informazioni sulla manifestazione saranno consultabili dal mese di febbraio del 2016 sul sito Web

3.4.2 Misura 7: Panoramica delle offerte di formazione

Responsabilità: SC SNPC; DATEC-UFCOM, DFAE-DP, DFI-UFAS

Per aumentare la cyber-resilienza della Svizzera, è necessario creare e potenziare competenze specifiche in modo mirato. Secondo la SNPC occorre allestire una panoramica che fornisca informazioni sulle attuali offerte di formazione, in modo da individuare e colmare eventuali lacune nell'offerta. L'attuazione di questa misura è coordinata con l'attuazione della «Strategia del Consiglio federale per una società dell'informazione in Svizzera» e con il DFAE.

Stato attuale
La misura ha potuto essere conclusa nel 2015 con la pubblicazione del rapporto «Kompetenzbildungsangebote im Umgang mit Cyber-Risiken»[3]. Il rapporto si basa su un sondaggio condotto tra 40 esperti e indica quali offerte sono utilizzate da quali gruppi di utenti e le lacune tutt'ora esistenti nell'offerta. Gli esperti hanno accennato in particolare alla mancanza di offerte nel settore della cultura della sicurezza e alla carenza di offerte nell'interfaccia tra specialisti della sicurezza delle TIC e il management. Riguardo ad alcuni settori specifici è stata inoltre citata l'assenza di offerte di formazione nel campo della sicurezza tecnica (ad es. per l'esercizio di un CERT). Nel settore giustizia e polizia numerosi esperti hanno evidenziato la mancanza di offerte di formazione combinate di scienza forense e diritto nonché in generale un'insufficiente sensibilizzazione nei confronti dei cyber-rischi.
Le lacune riscontrate nell'offerta saranno colmate nell'ambito della misura 8.

3.4.3 Misura 8: Incremento dell'impiego delle offerte di formazione in materia di creazione di competenze ed eliminazione delle lacune riscontrate nell'ambito delle offerte

Responsabilità: SC SNPC; SEFRI; DFAE-DP

La misura 8 intende, da un lato, accrescere le attuali offerte in materia di creazione di competenze concernenti la gestione dei cyber-rischi e, dall'altro, colmare le lacune riscontrate nell'ambito dell'offerta. La promozione della formazione avviene in stretto coordinamento con la promozione della formazione nel settore dei cyber-rischi e si basa sui risultati della misura 7.

Stato attuale

Nel 2015 il DFAE ha conferito l'incarico di condurre una ricerca settoriale sul tema della creazione di competenze nel settore della cyber-sicurezza all'estero (pubblicata all'indirizzo http://www.diplomacy.edu/cybersecurity). La ricerca illustra le diverse misure adottate da dieci Stati selezionati dell'OCSE per promuovere la creazione di competenze nel settore della cyber-sicurezza (ad es. nelle università, attraverso programmi di formazione continua ecc.) Gli approcci di soluzione identificati in questo contesto possono ispirare possibili attività da avviare in Svizzera nell'ambito della misura 8.

A fronte dello stretto legame che intercorre tra i temi della ricerca e della formazione la SEFRI ha deciso insieme al SC SNPC di occuparsi della formazione anche nel quadro del comitato direttivo interdipartimentale CoPIRFCyber (cfr. misura 1). L'obiettivo è promuovere, in parallelo alla ricerca, la formazione nelle università.

Sono inoltre in corso i lavori con l'associazione ICT-Formazione professionale Svizzera per

www.scrrc.ch.

[3] Il rapporto è disponibile alla pagina dedicata alla società dell'informazione in Svizzera: http://www.bakom.admin.ch//themen/infosociety/04837/index.html.

la promozione della formazione professionale. L'idea è creare un diploma federale di esperto in sicurezza delle TIC. I colloqui con le parti interessate sono iniziati e nella primavera del 2016 l'associazione ICT-Formazione professionale Svizzera deciderà sulla fattibilità di un diploma di questo tipo.

3.4.4 Misura 9: Internet governance

Responsabilità: DATEC-UFCOM; DFAE-DP, DDPS-POLSIC, DFF-MELANI, autorità specializzate

Con la misura 9 della SNPC la Svizzera (l'economia, la società, le autorità) deve impegnarsi attivamente e nel modo più coordinato possibile per una Internet governance, che sia conciliabile con gli ideali svizzeri di libertà e (auto)responsabilità, approvvigionamento di base, pari opportunità, diritti umani e stato di diritto. L'UFCOM, in qualità di Ufficio responsabile, prende parte attivamente ai pertinenti lavori internazionali e regionali, ad esempio nel quadro della CANN (Internet Cooperation for Assigned Names and Numbers), del VMSI, della Commissione dell'ONU per la scienza e la tecnologia al servizio dello sviluppo (CSTD), dell'IGF (UN Internet Governance Forum) e del Consiglio d'Europa.

Stato attuale

L'UFCOM ha partecipato attivamente ai lavori del Comitato consultivo governativo (Government Advisory Committee, GAC) dell'ICANN presieduto dalla Svizzera. I lavori, cui ha partecipato anche il DFAE, erano incentrati sul trasferimento della vigilanza sulle funzioni dello IANA e sull'inasprimento dell'obbligo di reporting (accountability). La Svizzera si è inoltre impegnata a favore di misure volte a rafforzare la sicurezza e la fiducia nel caso dei nuovi top-level domain. Nell'ambito della verifica dell'attuazione dei risultati del VMSI la Svizzera ha pure partecipato, con una delegazione composta da rappresentanti dell'UFCOM e del DFAE, ai lavori preparatori per l'incontro ad alto livello dell'Assemblea generale dell'ONU, tenutasi nel dicembre del 2015 a New York, con cui si sono conclusi i lavori.

L'UFCOM coadiuva inoltre la preparazione e lo svolgimento dell'«Internet Governance Forum (IGF)» come copromotore e coorganizzatore del forum di dialogo europeo sulla governance di Internet dell'IFG («European Dialog on Internet Governance EuroDIG»). Insieme al DFAE l'UFCOM è rappresentato nella Geneva Internet Platform e ne sostiene i lavori.

A livello nazionale l'UFCOM organizza regolarmente la piattaforma di discussione «Piattaforma tripartita per il follow-up del VMSI», che consente uno scambio di informazioni tra tutti i gruppi d'interesse (Amministrazione federale, società civile, mondo accademico) sulle tematiche e sugli sviluppi attuali in riferimento a Internet. Nel maggio del 2015 esso ha inoltre organizzato lo Swiss Internet Governance Forum, che ha riunito i gruppi d'interesse per un dialogo interattivo sulle questioni relative alla governance di Internet.

3.4.5 Misura 10: Cooperazione internazionale in materia di sicurezza cibernetica

Responsabilità: DFAE-DP; DDPS-POLSIC, DFF-MELANI, DATEC-UFCOM

La misura 10 concerne la salvaguardia degli interessi a livello della politica di sicurezza nel cyber-spazio nei confronti dell'estero. Avvalendosi di iniziative e delle sue relazioni internazionali la Svizzera si impegna affinché il cyber-spazio non sia utilizzato in modo abusivo con finalità criminali, di spionaggio, terroristiche e politiche.

Stato attuale

Nel 2015 la Svizzera ha continuato ad adoperarsi per la creazione di una normativa volta a disciplinare l'utilizzo e i confini del cyber-spazio con l'ausilio di strumenti politici e giuridici e a promuovere la propria visione di un cyber-spazio aperto, libero e sicuro.

Fra gli strumenti di carattere politico figura la creazione di una fiducia reciproca. La fiducia costituisce infatti il presupposto per la trasparenza, la collaborazione fra Stati e la stabilità nel cyber-spazio. La Svizzera ha contribuito attivamente a plasmare il processo dell'OSCE inteso a creare fiducia. Essa ha inoltre sostenuto la presidenza OSCE serba nell'organizzazione di una conferenza a livello di OSCE.

Nell'ambito della creazione di norme per la condotta degli Stati nel cyber-spazio la Global Conference on Cyberspace, svoltasi il 16 e il 17 aprile 2015 all'Aia, ha costituito l'aspetto centrale delle attività della Svizzera. Il consigliere federale Didier Burkhalter ha preso parte alla conferenza, insistendo sul fatto che la normativa tra Stati dovrà basarsi sul diritto internazionale vigente, applicabile anche nel cyber-spazio.

Grazie a una manifestazione organizzata dalla Svizzera a Ginevra è stato possibile confrontare, a titolo di contributo alla Global Conference on Cyberspace 2015, diversi approcci regionali e promuovere la collaborazione oltre i confini regionali.

Per consentire e facilitare la partecipazione dei Paesi in via di sviluppo ai processi internazionali la Svizzera ha finanziato progetti concreti per creare o sviluppare le capacità. Essa è inoltre membro fondatore del Global Forum on Cyber Expertise (GFCE), costituito nell'anno in rassegna, che ha lo scopo di promuovere ulteriormente lo sviluppo di capacità a livello globale.

Anche quest'anno la Svizzera ha partecipato attivamente al dialogo multilaterale tra gli Stati europei e la Cina volto a comprendere meglio la rispettiva percezione delle minacce e a identificare le questioni da approfondire nel reciproco interesse.

3.4.6 Misura 11: Iniziative internazionali e processi di standardizzazione nel settore della sicurezza

Responsabilità: DATEC-UFCOM; SC SNPC, autorità specializzate, DFAE-DP, DFF-ME-LANI

L'obiettivo della misura 11 consiste nel coordinamento e nella cooperazione degli esperti in cyber-sicurezza in Svizzera per ottimizzare l'impegno internazionale in seno agli organismi di normazione e altre opportune iniziative.

Stato attuale

Nel 2015, nel quadro dello scambio con gli attori coinvolti, sono stati definiti gli ambiti di intervento prioritari per il coordinamento della standardizzazione internazionale e delle iniziative nel settore della cyber-sicurezza e sono stati armonizzati i processi necessari per questa misura. I partecipanti attivi alla misura 11 intendono realizzare un workshop pubblico annuale e, all'occorrenza, organizzare progetti di coordinamento in seno a gruppi specialistici. I processi e gli ambiti di intervento prioritari sono stati documentati e segnalati al servizio di coordinamento SNPC.

3.4.7 Misura 16: Necessità di modificare le basi legali

Responsabilità: SC SNPC

La misura 16 prevede di verificare se il diritto applicabile contiene le basi necessarie alla protezione contro i cyber-rischi, eventualmente apportando le necessarie modifiche. Le unità amministrative devono individuare le rilevanti basi giuridiche per il loro ambito di attività e valutare la necessità di revisione e di integrazione.

Stato attuale

I primi chiarimenti sono stati effettuati nel 2014. Sulla base dei recenti sviluppi non si ravvisa la necessità generalizzata di una regolamentazione. Tale necessità è oggetto di continue valutazioni.

3.5 Attività di attuazione da parte dell'esercito

L'esercito rientra tra le infrastrutture critiche del Paese per le quali il cyber-spazio e le cyber-minacce sono diventati una sfida di capitale importanza. Con il rapidissimo sviluppo e la crescente importanza del cyber-spazio si presentano nuove opzioni operative in ambito militare da considerare. Tra i principali compiti immediati dell'esercito si annovera tuttavia la protezione dei suoi sistemi e delle sue infrastrutture TIC in ogni situazione, per garantire la sua capacità d'intervento e la sua libertà d'azione.

L'esercito dispone di considerevoli conoscenze e competenze, di cui se necessario i responsabili Uffici federali possono avvalersi in via sussidiaria, a condizione che non occorrano contemporaneamente all'esercito stesso.

A questo scopo l'esercito sviluppa costantemente le proprie conoscenze e competenze. I suoi compiti nel settore sussidiario e i suoi compiti in caso di guerra o di conflitto vengono al momento precisati. Nel settore del personale non è stato possibile reperire le risorse pianificate nel 2015; questo ritardo dovrebbe essere colmato nel 2016.

Stato attuale

I valori di riferimento dottrinali delle azioni militari nel cyber-spazio e i principi metodologici della gestione dei cyber-rischi sono stati definiti. Sono stati inoltre compiuti passi importanti per quanto riguarda l'anticipazione (ad es. creazione di una «cartografia» degli attori del settore accademico) e la rappresentazione della cyber-situazione. È stato anche istituito un comitato consultivo incaricato di seguire i lavori. Nel 2015 si è svolta l'esercitazione «CYBER-PAKT 15», che costituisce un'importante pietra miliare nell'ambito della gestione delle crisi e della collaborazione dell'esercito con i suoi partner. I processi per il trattamento di cyber-eventi hanno potuto essere confermati e verificati. Lo stato maggiore dell'esercito per la protezione della Svizzera contro i cyber-rischi ha dunque raggiunto la sua prontezza di base. Sono state pure condotte diverse iniziative di sensibilizzazione a favore delle unità amministrative e delle formazioni di milizia. Non appena le risorse lo consentiranno, dal 2016 sarà possibile mettere sistematicamente in atto il concetto per l'istruzione dell'esercito.

3.6 Attività di attuazione da parte dei Cantoni

Il meccanismo di consultazione e coordinamento nel quadro della Rete integrata Svizzera per la sicurezza (MCC RSS) è l'interfaccia della SNPC con i Cantoni. Il Gruppo specializzato Cyber (GS-C) dell'MCC RSS garantisce il coordinamento tra Confederazione e Cantoni nell'attuazione della SNPC in collaborazione con i Cantoni, i Comuni e i servizi federali interessati. L'MCC RSS dirige quattro sottoprogetti o gruppi di lavoro. Il servizio di coordinamento SNPC è membro del GS-C e a livello di Confederazione funge da ponte con i lavori di progetto che coinvolgono i Cantoni.

Stato attuale

Sulla base della misura 3 della SNPC (piano di verifica della vulnerabilità delle infrastrutture TIC) le organizzazioni coinvolte hanno effettuato un esame autonomo dei cyber-rischi. Quest'ultimo è stato valutato e sono state proposte misure volte a ridurre i rischi esistenti. In linea con le misure 4 e 5 della SNPC, il processo generale per il trattamento dei cyber-eventi è stato stabilito e suddiviso in cinque sottoprocessi. Sia i sottoprocessi che la definizione di un evento di cyber-sicurezza sono stati messi a disposizione dei Cantoni.

Il documento programmatico per procedure e processi a livello di Confederazione che include anche i cyber-aspetti (misura 15) è stato esteso ai Cantoni e alle infrastrutture critiche. Per verificare il documento programmatico è stato organizzato un seminario strategico con rappresentanti della Confederazione e della maggioranza dei Cantoni e con i gestori di infrastrutture

critiche. A questo scopo è stato elaborato un apposito scenario concernente un cyber-attacco al sistema previdenziale svizzero. I temi principali erano il rilevamento dei problemi, i processi, le strutture, le interfacce e le esigenze.

4 Controlling strategico

Il Consiglio federale ha incaricato il comitato direttivo della SNPC (CD SNPC) di seguire l'attuazione della strategia con un controlling strategico allo scopo di verificare a intervalli semestrali lo stato di avanzamento in termini di obiettivi e di tempistica delle misure della «Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC)». Secondo la decisione del Consiglio federale del 15 maggio 2013 relativa al piano di attuazione della SNPC, l'affare dovrà essere sottoposto al Consiglio federale tramite la Conferenza dei segretari generali (CSG). La quinta seduta del CD SNPC si è svolta il 20 agosto 2015.

5 Verifica dell'efficacia

Nel 2015 sono iniziati i lavori preparatori in vista della verifica dell'efficacia della SNPC. La verifica dovrà essere condotta nel 2016, in modo da poterne sottoporre i risultati al Consiglio federale nel mese di aprile del 2017. Su questa base il Consiglio federale potrà decidere in merito al proseguimento della SNPC.

Nella primavera del 2015 il SC SNPC ha elaborato, con il sostegno ricevuto dall'esterno, un piano dettagliato per la verifica dell'efficacia. L'obiettivo dei lavori consisteva nello sviluppo di un metodo rigoroso, nella definizione di questioni concrete e nell'identificazione dei soggetti da interpellare. Nella sua seduta del 20 agosto 2015 il CD SNPC ha approvato il piano dettagliato. Successivamente il SC SNPC ha conferito l'incarico a un'azienda qualificata nell'ambito di una procedura mediante invito. Nel dicembre si è svolta la prima riunione di progetto con i mandatari.

La verifica dell'efficacia può dunque essere iniziata per tempo e si basa su un piano ben elaborato. Permane invece la sfida di valutare l'efficacia della SNPC in un momento in cui molte delle misure sono ancora in fase di attuazione.

6 Considerazioni finali

In questo terzo anno è emerso nuovamente quanto l'attuazione della SNPC costituisca un compito ampio e complesso. Le minacce di oggi non corrispondono a quelle di domani, per cui si rende necessario strutturare la SNPC in modo flessibile, adattandola continuamente alle nuove minacce. Anche nel 2015 si è pertanto dovuto modificare la tabella di marcia e ridefinire alcuni compiti. Queste modifiche sono tuttavia sempre operate nell'intento di garantire l'alta qualità dei lavori di attuazione e dei prodotti della SNPC. Già oggi si ritiene che i risultati esplicheranno i loro effetti oltre l'orizzonte temporale del 2017. Sono stati definiti nuovi processi volti ad assicurare che la collaborazione, la cooperazione e la comunicazione tra gli attori, create attraverso la SNPC, proseguano anche in futuro e, all'occorrenza, consentano di coinvolgere altri attori. Questi fattori hanno causato lievi ritardi nel caso di alcune misure. Ciò nonostante i lavori di attuazione della maggior parte delle misure rispettano la tabella di marcia, per cui il bilancio è positivo anche alla fine del 2015.

L'aumento del numero di cyber-crimini registrato lo scorso anno ha sottolineato ancora una volta l'importanza della cooperazione a livello nazionale e internazionale. A livello nazionale

l'elemento centrale è una collaborazione basata sulla fiducia con i gestori di infrastrutture critiche, l'economia e i Cantoni. Anche con l'esercito si è instaurata una fruttuosa collaborazione. Per rafforzare la Svizzera occorre estendere ulteriormente lo scambio di informazioni con le organizzazioni di polizia e i pubblici ministeri nonché con i gestori delle infrastrutture critiche, i fornitori di prestazioni TIC, i fornitori di sistemi, le autorità specializzate e gli organi di regolamentazione.

Un altro elemento centrale è costituito dalla collaborazione e dallo scambio di informazioni rilevanti con altri Stati e organizzazioni internazionali. La fiducia reciproca deve essere promossa e regolamentata attraverso strumenti politici e giuridici, poiché costituisce il presupposto per la trasparenza, la cooperazione fra Stati e la stabilità nel cyber-spazio. Si intende così favorire ulteriormente la comprensione reciproca della cyber-sicurezza e la fiducia verso Internet.

Il 2016 porterà nuove sfide che ci obbligheranno a rafforzare la collaborazione e la cooperazione, coinvolgendo tutti gli attori rilevanti attuali e futuri.

7 Allegati

7.1 Documenti di base della SNPC

«Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC)»: https://www.isb.admin.ch/isb/it/home/ikt-vorgaben/strategien-teilstrategien/sn002-nationale_strategie_schutz_schweiz_cyber-risiken_ncs.html

«Piano di attuazione della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (PA SNPC)»: https://www.isb.admin.ch/isb/it/home/themen/cyber_risiken_ncs/umsetzungsplan.html

«Rapporto annuale SNPC 2013»: (solo in francese e tedesco) https://www.isb.admin.ch/isb/it/home/themen/cyber_risiken_ncs/jahresberichte_ncs.html

«Rapporto annuale 2014 sull'attuazione della SNPC»: https://www.isb.admin.ch/isb/de/home/themen/cyber_risiken_ncs/jahresberichte_ncs.html

7.2 Riepilogo degli interventi parlamentari concernenti i cyber-rischi

Intervento Ip. = Interpellanza; Mo. = Mozione; Po. = Postulato; I = Interrogazione	Depositato il	Stato al 31.12.2015
08.3050 Po. Schmid-Federer «Protezione dal bullismo elettronico»	11.03.2008	Liquidato
08.3100 Mo. Burkhalter «Strategia nazionale per combattere la criminalità su Internet»; con deliberazioni del Consiglio degli Stati del 2.06.2008 (BU CS 2.06.2008), rapporto della CPS-CN dell'11.11.2008 nonché deliberazioni del Consiglio nazionale del 3.06.2009 (BU CN 3.06.2009)	18.03.2008	Liquidato
08.3101 Po. Frick «Proteggere meglio la Svizzera dalla criminalità informatica»	18.03.2008	Liquidato
08.3924 Ip. Graber «Misure contro la guerra elettronica»	18.12.2008	Liquidato
09.3114 Ip. Schlüer «Sicurezza in Internet»	17.03.2009	Liquidato
09.3266 Mo. Büchler «Sicurezza della piazza economica Svizzera»	20.03.2009	Liquidato
09.3628 Po. Fehr HJ «Rapporto "Internet in Svizzera"»	12.06.2009	Liquidato
09.3630 Ip. Fehr HJ «Domande su Internet»	12.06.2009	Liquidato
09.3642 Mo. Fehr HJ «Osservatorio di Internet»	12.06.2009	Liquidato
10.3136 Po. Recordon «Valutazione della minaccia in materia di cyberguerra»	16.03.2010	Liquidato
10.3541 Mo. Büchler «Protezione contro gli attacchi cibernetici»	18.06.2010	Liquidato
10.3625 Mo. CPS-N «Misure contro gli attacchi informatici»; con deliberazioni del Consiglio nazionale del 2.12.2010 (BU CN 2.12.2010), rap-	29.06.2010	Liquidato

porto della CPS-CN dell'11.1.2011 nonché deliberazioni del Consiglio degli Stati del 15.3.2011 (BU CS 15.03.2011)		
10.3872 Ip. Recordon «Rischio di un black out di ampie dimensioni della rete elettrica svizzera»	01.10.2010	Liquidato
10.3910 Po. Gruppo liberale radicale «Centro di condotta e di coordinamento nell'ambito delle cyberminacce»	02.12.2010	Liquidato
10.4020 Mo. Glanzmann «MELANI per tutti»	16.12.2010	Liquidato
10.4028 Ip. Malama «Rischio di attacco di virus nelle centrali nucleari svizzere»	16.12.2010	Liquidato
10.4038 Po. Büchler «Capitolo sulla guerra cibernetica nel rapporto sulla politica di sicurezza»	16.12.2010	Liquidato
10.4102 Po. Darbellay «Concetto per la protezione delle infrastrutture digitali della Svizzera»	17.12.2010	Liquidato
11.3906 Po. Schmid-Federer «Legge quadro sulle TIC»	29.09.2011	Liquidato
12.3417 Mo. Hodgers «Mercati delle telecomunicazioni aperti. Strategie per la sicurezza digitale nazionale»	30.05.2012	Liquidato
12.4161 Mo. Schmid-Federer «Strategia nazionale contro il bullismo e il mobbing elettronici»	13.12.2012	Liquidato
13.3228 Ip. Recordon «Sistema federale di intercettazioni telefoniche e lacune generali della Confederazione in materia di informatica e telecomunicazioni»	22.03.2013	Liquidato
13.3229 Ip. Recordon «Portata della minaccia e misure di lotta contro la guerra e la criminalità cibernetiche»	22.03.2013	Liquidato
13.3558 Ip. Eichenberger «Spionaggio informatico. Valutazione e strategia»	20.06.2013	Liquidato
13.3677 Ip. Gruppo socialista «Atti di spionaggio della NSA e di altri servizi informazioni anche in Svizzera?»	11.09.2013	Liquidato
13.3692 Ip. Hurter «Mercato delle telecomunicazioni. Sono ancora attuali la legislazione e le misure di regolamentazione in vigore?»	12.09.2013	Non ancora trattato nel plenum
13.3696 Mo. Müller-Altermatt «Protezione dei dati anziché scudo protettivo per coloro che non pagano le imposte»	12.09.2013	Non ancora trattato nel plenum
13.3707 Po. Gruppo BD «Strategia globale per il ciberspazio al passo con i tempi»	17.09.2013	Non ancora trattato nel plenum
13.3773 Ip. Gruppo liberale radicale. «Legge sulle comunicazioni al passo con i tempi. Una strategia globale per il ciberspazio»	24.09.2013	Non ancora trattato nel plenum
13.3841 Mo. Rechsteiner «Commissione di esperti per il futuro del trattamento e della sicurezza dei dati»	26.09.2013	Adottato
13.3927 Ip. Reimann «Protezione dei bunker svizzeri per l'archiviazione dei dati»	27.09.2013	Non ancora trattato nel plenum
13.4009 Mo. CPS-CN «Attuazione della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi» («Il Consiglio federale è incaricato di accelerare l'attuazione della Strategia nazionale per la	05.11.2013	Liquidato

protezione della Svizzera contro i cyberrischi e di attuare le 16 misure concrete entro la fine del 2016.»)		
13.4077 Ip. Clottu «Spionaggio di dati e sicurezza su Internet»	05.12.2013	Liquidato
13.4086 Mo. Glättli «Programma nazionale di ricerca “Protezione idonea dei dati nella società dell’informazione”»	05.12.2013	Liquidato
13.4308 Po. Graf-Litscher «Migliorare la sicurezza e l’indipendenza del settore informatico svizzero»	13.12.2013	Non ancora trattato nel plenum
13.5224 Dom. Reimann «Zur Präsenz von US-Geheimdiensten und ihren Cyber-Schnüffelaktivitäten in der Schweiz»	10.06.2013	Liquidato
13.5325 Dom. Sommaruga Carlo «Verwendet der Nachrichtendienst des Bundes illegal von der NSA beschaffte Daten?»	11.09.2013	Liquidato
14.1105 I Buttet «Mezzi a favore della «cyber defense» nel quadro della politica di sicurezza della Svizzera»	10.12.2014	Depositato
14.3654 Ip. Derder «Sicurezza digitale. Abbiamo preso la direzione sbagliata?»	20.06.2014	Non ancora trattato nel plenum
14.4138 Ip. Noser «Prassi in materia di acquisti pubblici nel settore delle infrastrutture TIC critiche dell’amministrazione federale»	10.12.2014	Non ancora trattato nel plenum
14.4299 Ip. Derder «Vigilanza trasversale sulla rivoluzione digitale. È necessario istituire una segreteria di Stato della società digitale?»	12.12.2014	Non ancora trattato nel plenum
14.5569 Dom. Leutenegger Oberholzer «NSA. Ein Jahr Schnüffelstaat»	26.11.2014	Liquidato
15.1059 Interpellanza urgente Berberat «Aiuto finanziario urgente della Confederazione in seguito all’attacco informatico contro TV5 Monde»	10.09.2015	Liquidato
15.3359 Po. Derder «Per un esercito innovativo»	20.03.2015	Non ancora trattato nel plenum
15.3375 Ip. «Sottrazione di codici SIM da parte della NSA e del GCHQ presso la società Gemalto»	20.03.2015	Liquidato
15.3656 Ip. Munz «Pericolo per la centrale nucleare di Mühleberg a causa della manutenzione a distanza del sistema informatico. Discutibile sorveglianza da parte dell’IFSN»	18.06.2015	Non ancora trattato nel plenum
15.4073 Ip. Derder «L’esercito è realmente in grado di proteggere il cyberspazio svizzero?»	25.09.2015	Non ancora trattato nel plenum
15.5299 Dom. Leutenegger Oberholzer «Schutz vor NSA-Spionage»	09.06.2015	Liquidato

7.3 Elenco delle abbreviazioni

AE	Approvvigionamento economico del Paese
BAC	Base d’aiuto alla condotta
BAC COE	Base d’aiuto alla condotta – Centro operazioni elettroniche

CaF	Cancelleria federale
CBM	Confidence building measures
CCPCS	Conferenza dei comandanti delle polizie cantonali della Svizzera
CD SNPC	Comitato direttivo della strategia nazionale per la protezione della Svizzera contro i cyber-rischi
CDCGP	Conferenza dei direttori cantonali di giustizia e polizia
CdE	Capo dell'esercito
CERT	Computer Emergency Response Team
CNE	Computer Network Exploitation
CNO	Computer Network Operations
CSG	Conferenza dei segretari generali
CSIRT	Computer Security Incident Response Team
CSTD	Commission on Science and Technology for Development
CTI	Commissione per la tecnologia e l'innovazione
Cyber SIC	Settore Cyber nel Servizio delle attività informative della Confederazione
D	Difesa
DATEC	Dipartimento federale dell'ambiente, dei trasporti, dell'energia e delle comunicazioni
DDPS	Dipartimento federale della difesa, della protezione della popolazione e dello sport
DDPS-Sipol	Dipartimento federale della difesa, della protezione della popolazione e dello sport – Politica di sicurezza
DEFR	Dipartimento federale dell'economia, della formazione e della ricerca
DFAE	Dipartimento federale degli affari esteri
DFAE-DOI	Dipartimento federale degli affari esteri – Divisione organizzazioni internazionali
DFAE-DP	Dipartimento federale degli affari esteri – Direzione politica
DFF	Dipartimento federale delle finanze
DFGP	Dipartimento federale di giustizia e polizia
DFI	Dipartimento federale dell'interno
DSP	Divisione politica di sicurezza
EAPC	Consiglio di Partenariato Euro-Atlantico
ENISA	European Network and Information Security Agency
ERSS	Esercitazione della Rete integrata Svizzera per la sicurezza
fedpol	Ufficio federale di polizia
GAC	Government Advisory Committee
GCHQ	Government Communications Headquarters
GIP	Geneva Internet Platform
GovCERT	Swiss Governmental Computer Emergency Response Team
GS-C	Gruppo specializzato Cyber
GS-CI	Gruppo specializzato Cyber International
ICANN	Internet Cooperation for Assigned Names and Numbers
ICT	Information and Communication Technology
ICTec	Informazione, comunicazione, tecnologia
IG	Internet Governance
IGF	Internet Governance Forum
LAIn	Legge federale sulle attività informative
MCC RSS	Meccanismo di consultazione e coordinamento nel quadro della Rete integrata Svizzera per la sicurezza
MELANI	Centrale d'annuncio e d'analisi per la sicurezza dell'informazione
MilCERT	Computer Emergency Response Team militare
NATO	Organizzazione del Trattato dell'Atlantico del Nord
NSA	National Security Agency
ODIC	Organo direzione informatica della Confederazione

ODIC-SEC	Organo direzione informatica della Confederazione – Sicurezza
OIC MELANI	Operation Information Center della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione
ONU	Organizzazione delle Nazioni Unite
OSCE	Organizzazione per la sicurezza e la cooperazione in Europa
PA SNPC	Piano di attuazione della strategia nazionale per la protezione della Svizzera contro i cyber-rischi
RSS	Rete integrata Svizzera per la sicurezza
SC DC	Studio concettuale sulla difesa cibernetica
SC SNPC	Servizio di coordinamento della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi
SCOCI	Servizio di coordinamento per la lotta contro la criminalità su Internet
SDO	Organismo di normazione
SEFRI	Segreteria di Stato per la formazione, la ricerca e l'innovazione
SG-DDPS	Segreteria generale del Dipartimento federale della difesa, della protezione della popolazione e dello sport
SIC	Servizio delle attività informative della Confederazione
SIM	Servizio informazioni militare
SLA	Service level agreement
SNPC	Strategia nazionale per la protezione della Svizzera contro i cyber-rischi
Strategia PIC	Strategia per la protezione delle infrastrutture critiche
UFAE	Ufficio federale per l'approvvigionamento economico del Paese
UFAS	Ufficio federale delle assicurazioni sociali
UFCOM	Ufficio federale delle comunicazioni
UFCOM-IR	Ufficio federale delle comunicazioni – servizio Affari internazionali
UFE	Ufficio federale dell'energia
UFIT	Ufficio federale dell'informatica e della telecomunicazione
UFPP	Ufficio federale della protezione della popolazione
VMSI	Vertice mondiale sulla società dell'informazione