Luglio 2015 | www.odic.admin.ch

Stratégie nazionale per la protezione della Svizzera contro i cyber-rischi SNPC

Rapporto annuale 2014 del comitato direttivo della SNPC

Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Dipartimento federale delle finanze DFF
Organo direzione informatica della Confederazione ODIC
Centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI

Pubblicazione: 5 luglio 2015

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

Primo rapporto annuale (disponibile in francese e tedesco) all'indirizzo:
http://www.isb.admin.ch/themen/01709/01891/index.html?lang=it

Sommario

Premessa **4**

1 Sintesi **5**

2 Collaborazione **6**

2.1 Livello nazionale **6**
2.2 Livello internazionale **6**

3 Stato dei lavori di attuazione della SNPC 2014 ..... **7**

3.1 Prevenzione **8**
3.1.1 Misura 2: Analisi dei rischi e della vulnerabilità 9
3.1.2 Misura 3: Analisi della vulnerabilità delle infrastrutture TIC dell'Amministrazione federale sulla base di un piano di verifica 9
3.1.3 Misura 4: Elaborazione della rappresentazione e dell'evoluzione della situazione 9

3.2 Reazione **10**
3.2.1 Misura 5: Analisi ed elaborazione di eventi 10
3.2.2 Misura 6: Documento programmatico per una panoramica dei casi penali e il coordinamento dei casi di portata intercantonale 11
3.2.3 Misura 14: Misure attive per l'identificazione degli autori 11

3.3 Gestione della continuità operativa e delle crisi **11**
3.3.1 Gestione della continuità operativa (M12) 11
3.3.2 Misura 13: Gestione delle crisi 12
3.3.3 Misura 15: Documento programmatico per procedure e processi di condotta cibernetici 12

3.4 Processi di sostegno **12**
3.4.1 Misura 1: Identificazione di cyber-rischi attraverso la ricerca 13
3.4.2 Misura 7: Panoramica delle offerte di formazione 13
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 14
3.4.4 Misura 9: Internet governance 14
3.4.5 Misura 10: Cooperazione internazionale in materia di sicurezza cibernetica 15
3.4.6 Misura 11: Iniziative internazionali e processi di standardizzazione nel settore della sicurezza 15
3.4.7 Misura 16: Necessità di modificare le basi legali 15

3.5 Attività di attuazione nell'esercito **16**
3.6 Attività di attuazione nei Cantoni **16**

4 Controlling strategico **17**

5 Verifica dell'efficacia **17**

6 Considerazioni finali **18**

7 Allegati **19**

7.1 Documenti basilari della SNPC **19**
7.2 Riepilogo degli interventi parlamentari concernenti i cyber-rischi **19**
7.3 Elenco delle abbreviazioni **21**

Premessa

Nel corso del 2014 si sono ripresentati eventi e attacchi attribuiti a diversi Paesi e attuati con strumenti tecnologicamente avanzati. È stato necessario prendere atto anche delle sofisticate capacità dei criminali cibernetici e le lacune ampiamente diffuse hanno svolto un ruolo importante. Il mondo ha così acquisito la consapevolezza non solo delle opportunità offerte da una digitalizzazione sempre più estesa, ma anche di quanto siano vulnerabili Internet e, quindi, i propri dati, la sfera privata e la fiducia nella tecnologia della rete. Per contrastare tutto ciò, rafforzare la protezione contro i cyber-rischi e rispondere all'esigenza di affidabilità dell'infrastruttura, la Svizzera percorre con coerenza la propria strada: l'attuazione della «Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC)» è pertanto proseguita raggiungendo i primi, importanti obiettivi. Questo secondo rapporto annuale sullo stato di attuazione della SNPC fornisce una panoramica dettagliata dell'attuale situazione di minaccia, delle misure avviate secondo la strategia SNPC e del loro stato di attuazione.

La Svizzera non è la sola a dover affrontare le sfide per la protezione della rete, poiché le minacce non conoscono confini. Pertanto le cooperazioni internazionali sono più importanti che mai. Nel quadro della presidenza elvetica dell'Organizzazione per la sicurezza e la cooperazione in Europa (OSCE) sono state sviluppate misure di rafforzamento della fiducia che rivestono un'enorme importanza per una comprensione condivisa del concetto di sicurezza in Internet. Con diversi Paesi sono stati conclusi accordi concernenti lo scambio di informazioni sulle lacune a livello di sicurezza e sugli eventi e sono state rafforzate le collaborazioni esistenti. Ciò ha consentito di ottimizzare la reciproca informazione sugli eventi inerenti ai cyber-rischi.

Anche all'interno della Svizzera la lotta richiede un impegno comune, le conoscenze devono essere condivise. Per questo motivo, su iniziativa della centrale MELANI, è stata costituita la rete di competenza «Swiss Cyber Experts» in collaborazione con il settore delle TIC e i partner della ricerca.

Sono stati raggiunti risultati importanti, ma i lavori per l'attuazione della SNPC sono ben lungi dall'essere conclusi. Anche nel 2015 avvieremo tutte le misure necessarie affinché la Svizzera possa continuare a utilizzare Internet come uno spazio sicuro e libero da censure per l'economia, le autorità e i cittadini. Questa è e rimane l'esigenza di tutti nell'habitat digitale.

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 (PA SNPC). La SNPC, articolata in 16 misure, è incentrata sull'identificazione precoce dei rischi e delle minacce nel settore cibernetico nonché sul rafforzamento della capacità di resistenza delle infrastrutture critiche. Persegue inoltre l'obiettivo di una generale riduzione delle cyber minacce, in particolare lo spionaggio, il sabotaggio e la criminalità nel settore.

Per l'attuazione delle singole misure è stato di volta in volta nominato, in qualità di capofila, un Ufficio federale. Al fine di coordinare i lavori di attuazione, il Consiglio federale ha incaricato il servizio di coordinamento SNPC (SC SNPC), che è aggregato alla Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) in seno all'Organo direzione informatica della Confederazione (OSIC). Il Consiglio federale ha inoltre incaricato un comitato direttivo SNPC (CC SNPC) di seguire l'attuazione con un controlling strategico.

Le 16 misure interessano quattro settori: prevenzione, reazione, continuità e processi di sostegno. Lo scorso anno sono stati raggiunti importanti obiettivi in tutti i settori, tra l'altro grazie anche a una stretta collaborazione e una proficua comunicazione.

Nell'ambito della prevenzione, in sei sottosettori critici sono state svolte o avviate analisi delle vulnerabilità (tecnologia dell'informazione, traffico stradale, approvvigionamento di gas naturale, autorità, organizzazioni di primo intervento, protezione civile) ed è stato approntato un progetto a livello federale per rilevare le vulnerabilità delle tecnologie dell'informazione e della comunicazione (TIC). Ai fini dell'individuazione dei rischi è imperativo conoscere le minacce attuali e avere un quadro completo della situazione. Per quest'ultimo è stato preparato un quadro tecnico, che fornisce una visione d'insieme delle infrastrutture critiche in Svizzera, consentendo così ai gestori di localizzare tempestivamente i dispositivi infetti nella propria rete. Le principali minacce informatiche nel 2014 sono rilevate e illustrate dal rapporto semestrale MELANI e dal rapporto annuale SCOCI.[1]

Nel settore della reazione, lo scorso anno sono stati ampliati i centri di competenza per l'analisi dei software nocivi (p.es. GovCERT.ch, CISIRT-UFIT, milCERT-DDPS), nell'intento di garantire una disponibilità permanente. Nel caso di eventi inerenti ai cyber-rischi complessi e tecnicamente difficili, in futuro sarà possibile attingere anche alle conoscenze specialistiche dell'associazione «Swiss Cyber Experts», grazie a un accordo di collaborazione stipulato tra la suddetta associazione e MELANI nel 2014.

Nell'ambito della continuità, sulla base di un'analisi conclusa delle vulnerabilità dei sottosettori critici sono state adottate misure per istituire una gestione della continuità operativa e delle crisi. L'obiettivo è un accordo di settore, nel quale le imprese determinanti ai fini dell'approvvigionamento si impegnino a prestarsi assistenza reciproca nel caso di eventi cibernetici.

Nei processi di sostegno è stata rafforzata la collaborazione internazionale a livello bilaterale e multilaterale. Per quest'ultimo la Svizzera, che lo scorso anno aveva la presidenza dell'OSCE, ha preso parte alle sue misure di rafforzamento della fiducia. A livello bilaterale sono stati instaurati nuovi contatti e intensificati quelli esistenti.

Per verificare la validità delle 16 misure, a partire dal 2015 sarà approntato un esame dell'efficacia i cui risultati serviranno come base per le decisioni del Consiglio federale in merito al futuro sviluppo della strategia dopo il 2017.

[1] Il 2014 è stato contrassegnato in primo luogo dall'individuazione e dalla scoperta di cavalli di troia e lacune nella sicurezza che hanno avuto e continueranno ad avere ripercussioni sull'attuazione della SNPC. Nello specifico si è trattato di: «Heartbleed», lacuna di sicurezza in una delle principali librerie crittografiche, «Cryptolocker», insidioso ransomware in forte diffusione, «Regin», sofisticato programma di spionaggio informatico.

2 Collaborazione

Nel presente capitolo sono riportati alcuni importanti parametri nell'ambito della collaborazione nazionale e internazionale.

2.1 Livello nazionale

Il 20 marzo 2014 la seconda «Cyber-Landsgemeinde» della Rete integrata Svizzera per la sicurezza (RSS) ha ulteriormente rafforzato la collaborazione e i contatti tra la Confederazione e i Cantoni. Circa 70 interessati della Confederazione e dei Cantoni sono intervenuti all'incontro, dedicato ai progetti in corso a livello cantonale e all'informazione in merito allo stato attuale dell'attuazione della «Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC)».

Il 26 marzo 2014 è stata fondata l'associazione «Swiss Cyber Experts» con la partecipazione della centrale MELANI e il 17 dicembre è stato firmato l'accordo di collaborazione tra l'associazione e MELANI. Su questa base viene coordinato l'accesso ad altre risorse specialistiche nell'eventualità di gravi incidenti cibernetici.

L'obiettivo della prima conferenza SNPC del 20 novembre 2014 è stato lo scambio di informazioni sulle attività dell'amministrazione e dell'economia volte a ridurre i cyber-rischi in Svizzera, in particolare per le infrastrutture critiche, nonché sullo stato attuale dell'attuazione della SNPC. Circa 150 esponenti della Confederazione, dei Cantoni e dell'economia sono intervenuti all'evento.

Dal 3 al 21 novembre 2014 si è svolta l'esercitazione della Rete integrata Svizzera per la sicurezza 2014 (ERSS 14) che, prevedendo lo scenario «Pandemia e penuria di energia elettrica», ha verificato la collaborazione tra i partner della Rete. All'esercitazione hanno partecipato 26 Cantoni, Uffici federali dei sette Dipartimenti, l'esercito, le organizzazioni di crisi e l'economia privata. L'esercitazione era focalizzata sul livello politico-strategico, dalla gestione delle crisi fino al processo decisionale politico. La ERSS 14 ha già consentito a tutti i partecipanti di trarre preziosi insegnamenti, che saranno sottoposti a ulteriori valutazioni.

In futuro le periodiche riunioni di coordinamento dirette dall'OIC MELANI (SIC) serviranno ai diversi attori per scambiarsi opinioni, al fine di garantire un'analisi globale delle minacce in atto. Questa analisi sarà quindi schematizzata graficamente (radar della situazione delle minacce globali nel settore della cibernetica).

2.2 Livello internazionale

Con la nomina di Thomas Schneider (Ufficio federale delle comunicazioni, UFCOM) alla presidenza del Government Advisory Committee (GAC) della Internet Corporation for Assigned Names and Numbers (ICANN, l'organismo incaricato della registrazione degli indirizzi Internet a livello mondiale) nel mese di ottobre del 2014, la Svizzera ha la possibilità di esercitare un'influenza diretta sulla conduzione di una risorsa fondamentale di Internet. Sino ad allora Schneider era stato rappresentante del Governo svizzero in seno al GAC e vicepresidente, oltre ad avere la responsabilità dell'attuazione della misura 9 della SNPC. Il GAC è l'organo consultivo dei Governi per ICANN.

Dal 3 al 6 novembre 2014 si è svolta a Linz la seconda edizione della European Cyber Security Alpen Cup, un concorso internazionale al quale partecipano studenti provenienti da Svizzera, Austria e Germania e diretto da Cyber Security Austria con la partecipazione dell'associazione Swiss Cyber Storm e il patronato della Centrale d'annuncio e d'analisi per la sicurezza dell'informazione (MELANI) della Confederazione e dell'associazione Swiss Police ICT. L'obiettivo del concorso è scoprire, sfruttare ed eliminare i punti deboli dei sistemi informatici.

Alla Conferenza dell'OSCE tenutasi a Vienna il 7 novembre 2014 e presieduta dalla Svizzera, gli esponenti dell'economia privata, della società civile e della scienza, insieme con i rappresentanti di Governo, hanno riflettuto sullo stato dell'attuazione del primo pacchetto di misure di rafforzamento della fiducia (Confidence Building Measures, CBM). Hanno inoltre identificato altre esigenze e idee per il secondo catalogo di misure. La SNPC svizzera ha potuto essere presentata nell'ambito della CBM 7 (strategie e programmi cibernetici nazionali).

Dal 18 al 20 novembre 2014 i Paesi della NATO hanno voluto mettere alla prova le loro capacità di difesa contro gli attacchi informatici con un'esercitazione ad ampio raggio. I testi hanno riguardato la collaborazione nella gestione degli attacchi provenienti da Internet e il coordinamento. Sono stati invitati sette Paesi non appartenenti alla NATO, tra cui la Svizzera.

Nel mese di dicembre del 2014 l'ENISA ha pubblicato lo studio: «Framework for Evaluating National Cyber Security Strategies».[2] La Svizzera ha preso parte al «Cyber Expert Working Group» dell'ENISA, che ha l'obiettivo di confrontare le strategie cibernetiche nazionali identificandovi le «*best practice*» e la «guida». In questo gruppo di lavoro, oltre alla Svizzera, sono rappresentati diciotto Stati membri dell'UE e sette Stati non appartenenti all'UE.

A livello multilaterale la Svizzera ha preso parte attiva al Sino-European Cyber-Dialog, che si è svolto una volta a Ginevra e una volta a Pechino. La Svizzera ha illustrato il processo OSCE e ha proposto di elaborare misure di rafforzamento della fiducia tra gli Stati europei partecipanti e la Cina. In seno all'ONU la Svizzera si è impegnata in particolare per la protezione dei diritti umani nello spazio cibernetico, tra l'altro come membro del gruppo centrale sull'iniziativa «The Right to Privacy in the Digital Age», che cerca di rafforzare la tutela della sfera privata nello spazio cibernetico.

3 Stato dei lavori di attuazione della SNPC 2014

La SNPC è una strategia integrale, che con le sue 16 misure persegue un approccio globale per proteggere la Svizzera dalle cyber minacce. Le 16 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 due anni e per la maggior parte delle misure i lavori si trovano in uno stadio molto avanzato. In questo capitolo è spiegato il quadro generale dell'attuazione. Il servizio di coordinamento SNPC ha definito concretamente gli obiettivi e le tappe delle rispettive misure con tutti gli uffici responsabili rappresentandoli in una roadmap (cfr. fig. 1). Ogni ufficio responsabile dell'attuazione presenta sinteticamente lo stato attuale dell'attuazione della(e) rispettiva(e) misura(e). I lavori di attuazione di alcune misure SNPC sono svolti in collaborazione con i responsabili della «Strategia del Consiglio federale per una società dell'informazione in Svizzera» e della «Strategia nazionale per la protezione delle infrastrutture critiche».

[2] https://www.enisa.europa.eu/media/enisa-en-francais/

Roadmap SNPC

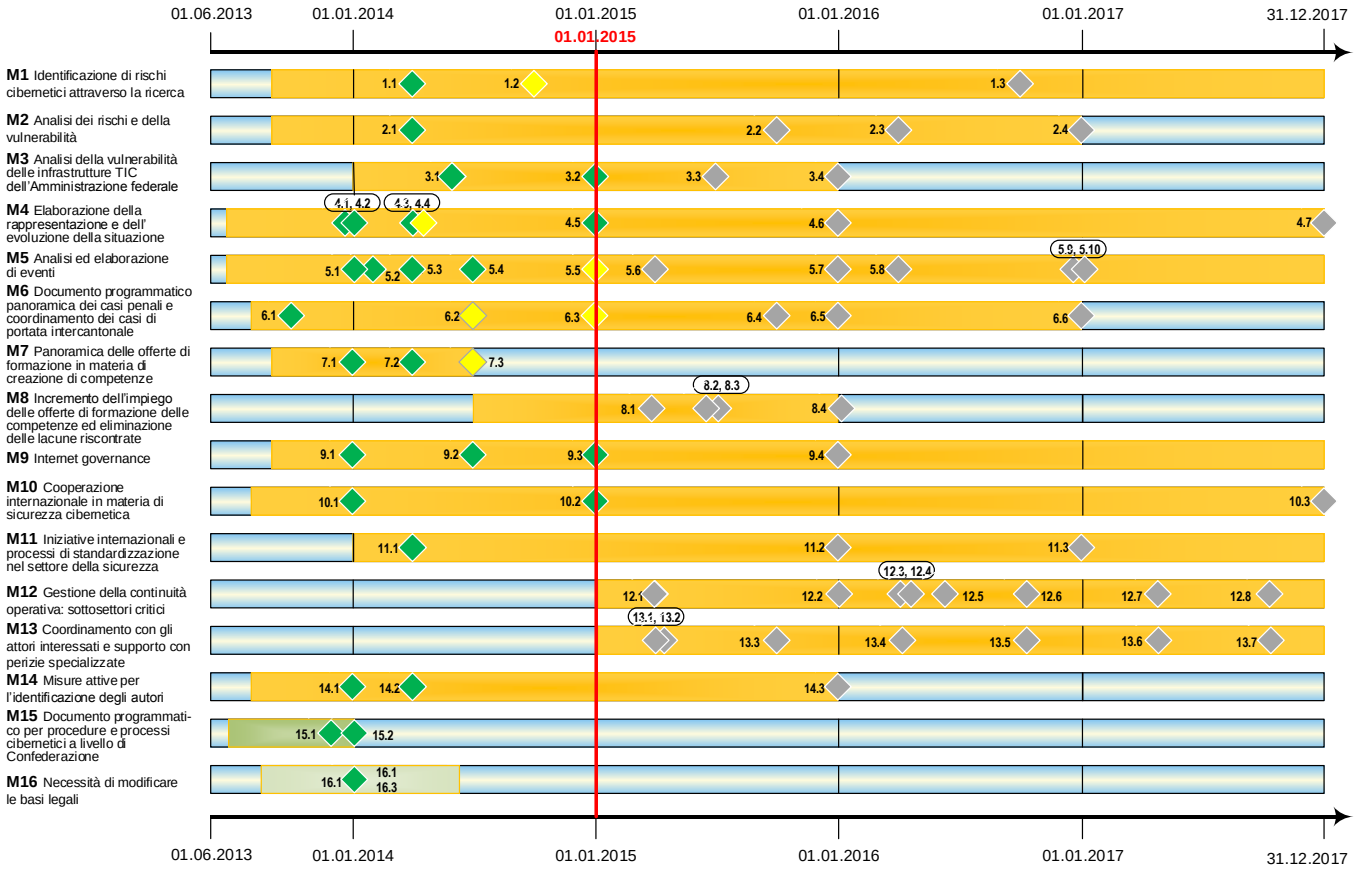

Figura 1: Roadmap SNPC

Legenda: stato di avanzamento delle tappe principali

- Tappa principale compromessa
- Tappa principale ritardata
- Tappa principale attuata secondo il piano
- Attuazione della tappa principale non ancora cominciata

3.1 Prevenzione

La prevenzione riguarda le misure dell'analisi dei rischi e delle vulnerabilità, della verifica delle vulnerabilità delle infrastrutture TIC a livello di Confederazione e della rappresentazione della situazione (misure M2, M3 e 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 di 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).

Stato attuale

Per il primo gruppo dei sottosettori sono state svolte analisi delle vulnerabilità all'interno dell'Ufficio federale per l'approvvigionamento economico del Paese (UFAE) e dell'Ufficio federale della protezione della popolazione (UFPP). Per l'approvvigionamento di gas naturale l'analisi si è conclusa (UFAE, ottobre 2014). I lavori nei sottosettori tecnologie dell'informazione e traffico stradale (UFAE) hanno raggiunto uno stadio molto avanzato. Le analisi concernenti i sottosettori Parlamento, Governo, giustizia e amministrazione, protezione civile e organizzazioni di primo intervento (UFPP) sono cominciate e proseguono secondo il piano di attuazione.

Il processo di svolgimento delle analisi e il conseguente coordinamento tra gli esponenti coinvolti dell'economia e dell'amministrazione sono stati sintonizzati.

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 gli Uffici federali devono verificare le vulnerabilità delle proprie infrastrutture TIC considerando i fornitori di prestazioni TIC come pure i fornitori di sistemi. L'Organo direzione informatica della Confederazione (ODIC) è stato incaricato di predisporre un piano per verificare periodicamente le vulnerabilità sistemiche, organizzative e tecniche delle infrastrutture TIC dell'Amministrazione federale.

Stato attuale

In una prima tappa è stata analizzata l'assegnazione dei compiti procedendo a delimitare il campo d'applicazione del piano di verifica previsto dalla M3. Nella seconda tappa sono state identificate le analisi delle vulnerabilità svolte sinora nell'Amministrazione federale, le interfacce con progetti analoghi e le responsabilità. È stata elaborata un'analisi dei rischi per l'attuazione del piano di verifica secondo la misura 3 e per l'identificazione delle principali tematiche. Su questa base è stata allestita la prima bozza del piano di verifica.

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 settore e descriva i rischi e i danni potenziali degli attacchi per i rispettivi settori critici oltre che la loro rilevanza per la Svizzera.

L'obiettivo della SNPC è di allestire un quadro unitario della situazione in stretta collaborazione con tutti gli attori. Nel quadro della situazione confluiscono le rilevanti informazioni evinte dalle analisi tecniche e attinte dal servizio delle attività informative e dalla polizia.

Stato attuale

I lavori di attuazione per allestire un quadro unitario della situazione sono cominciati ed è stato approntato un prototipo per riprodurre la situazione di minaccia. Sono stati registrati anche l'inventario e la verifica dei processi in atto per riprodurre la situazione di minaccia, i processi organizzativi nonché le responsabilità. È stato pure rilevato il conseguente fabbisogno di processi e regole considerando le priorità.

L'approntamento del quadro della situazione ha consentito di raggiungere una tappa importante, con la stesura di un rapporto sullo stato attuale della rappresentazione della situazione dal punto di vista tecnico. In questo modo è stato possibile, da un lato, risalire ai dispositivi infetti e, dall'altro, fare il punto della situazione sulle infezioni sotto il profilo tecnico.

Per la fine del 2014, secondo l'attuazione della misura 4 l'OIC della centrale MELANI assume la direzione del coordinamento degli attori individuali, operativi e tecnici (GovCERT, BAC-CEO CNO, Cyber SIC, UFIT-CSIRT, MilCERT e Cyber SIM) al fine di realizzare un'analisi complessiva della situazione di minaccia e coordinare la gestione degli eventi.

3.2 Reazione

Nell'ambito della reazione deve essere svolta un'analisi coordinata dell'evento con la successiva rielaborazione per porvi rimedio al più presto possibile. La SNPC prevede un rafforzamento delle capacità e un potenziamento della capacità di reazione di tutte le organizzazioni e degli attori interessati. 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).

3.2.1 Misura 5: Analisi ed elaborazione di eventi

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

Il team GovCERT, aggregato alla centrale MELANI, opera da anni nel settore dell'analisi dei malware. La SNPC si prefigge di ampliare queste capacità tecniche e le conoscenze specialistiche, tra l'altro aumentando i tempi di disponibilità e la capacità di reazione di tutti i team CERT nonché le loro interconnessioni. Per contestualizzare meglio gli eventi e valutare la loro rilevanza, è stato potenziato l'OIC della centrale MELANI. Nell'ambito degli eventi rilevanti per la protezione dello Stato, la SNPC può ora avvalersi delle necessarie risorse e capacità con la creazione del Cyber SIC.

Stato attuale

È stata aumentata la disponibilità nel GovCERT e garantita l'ottimale disponibilità nel funzionamento normale. Avvalendosi degli stretti contatti e del collegamento con gli uffici affini (altri CERT nell'Amministrazione federale) potrebbero essere coinvolti ulteriori specialisti dell'Amministrazione federale per superare un'eventuale crisi. Inoltre è ora possibile ricorrere anche agli esperti della neocostituita associazione «Swiss Cyber Experts». Nell'ambito dell'elaborazione degli eventi rilevanti per la protezione dello Stato, nel SIC è stata creata una nuova unità attribuendole le risorse contemplate dalla SNPC.

Tra la BAC (MilCERT e Computer Network Operations (CNO)), il SIC (Cyber NDB), il SIM (Cyber Defence), l'UFIT (CSIRT) è stata ulteriormente sistematizzata la collaborazione a livello operativo nella gestione degli eventi all'interno dell'Amministrazione federale ampliando gli strumenti disponibili per lo scambio di informazioni con una riunione periodica di coordinamento diretta dalla centrale MELANI. L'esercito ha rafforzato i propri strumenti di rilevamento e di analisi.

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 in grado di lottare contro la criminalità informatica. A tale scopo, nella misura 6 della SNPC è stato sancito che il servizio SCOCI aggregato al 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

Alla fine di giugno del 2014 è stato approntato l'inventario per la lotta alla criminalità cibernetica in Svizzera con un questionario sottoposto alla polizia e alle procure pubbliche a livello di Confederazione e di Cantoni. Sono stati inoltre verificati i processi esistenti, le procedure organizzative nonché le responsabilità delle autorità di perseguimento penale della Confederazione e dei Cantoni. Gli aspetti giuridici hanno potuto essere chiariti, creando una base solida per la bozza del documento programmatico. È stata preparata una prima bozza per ottenere una panoramica dei casi penali.

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 capacità del servizio delle attività informative della Confederazione (SIC) per identificare gli autori (analisi degli attori e del contesto e sviluppo di strumenti tecnici). Anche qui è necessaria una stretta collaborazione dei rilevanti attori (MELANI, SIC, SCOCI, Cyber SIC e, a titolo sussidiario, dell'esercito).

Stato attuale

Il settore Cyber, costituito il 1° gennaio 2014 in seno al SIC, è responsabile di elaborare le informazioni rilevanti per il servizio delle attività informative. Ha avviato i lavori, è pienamente funzionante e ha già occupato l'80 per cento dei posti di lavoro. Le tappe principali della SNPC sono dunque attuate nel rispetto dei tempi previsti presso il Cyber SIC. Sono state create le interfacce con l'OIC della centrale MELANI ed è stato istituito lo scambio di informazioni. L'integrazione delle capacità tecniche della BAC a supporto del Cyber SIC è avvenuta con la firma del Service Level Agreement (SLA) che disciplina la relativa collaborazione.

3.3 Gestione della continuità operativa e delle crisi

La gestione mirata 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 (M12, M13, M15).

3.3.1 Gestione della continuità operativa (M12)

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

Sulla base dei risultati dell'analisi dei rischi e delle vulnerabilità (misura 2) l'UFAE in qualità di capofila e l'UFPP definiscono le misure necessarie a garantire la continuità operativa insieme con le imprese rilevanti e i responsabili servizi specialistici.

Stato attuale

Le tappe principali per il futuro svolgimento della misura 12 sono state stabilite fino al 2017 e visualizzate nella roadmap. Le misure M12 e M13 sono elaborate contestualmente. In una fase iniziale lo svolgimento viene sperimentato con i primi sottosettori e la relativa metodologia è definita e convenuta dall'UFPP e dall'UFAE.

L'UFAE è riuscito ad avviare misure concrete per istituire una gestione della continuità operativa con gli esponenti dell'industria del gas. L'obiettivo è la firma di un accordo di settore, con il quale le imprese rilevanti per l'approvvigionamento si impegnano al supporto reciproco in presenza di cyber-rischi. L'accordo deve riguardare in particolare le dipendenze, individuate nell'analisi delle vulnerabilità, dai mezzi di comunicazione e dalla manodopera qualificata. Una bozza dell'accordo è in consultazione presso l'industria del gas (ottobre 2014).

3.3.2 Misura 13: Gestione delle crisi

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

Con la misura 13 le infrastrutture critiche e la Confederazione devono definire i processi necessari ad affrontare una situazione straordinaria causata da cyber-rischi. I lavori si basano sugli insegnamenti evinti dalle analisi dei rischi e delle vulnerabilità (misura 2). Nella gestione delle crisi occorre distinguere tra il livello strategico e quello operativo. L'UFAE e l'UFPP sono responsabili di definire i processi a livello strategico, la centrale MELANI quelli a livello operativo. Occorre inoltre considerare che la misura 13 è complementare alla misura 12 e deve essere intesa nel senso del «Business Continuity Management (BCM)» e non nella gestione delle crisi tradizionale.

Stato attuale

Le tappe fondamentali per le azioni future della misura 13 sono state definite fino al 2017 e visualizzate nella roadmap. Le due misure 12 e 13 sono elaborate contestualmente. L'UFAE ha già avviato misure concrete per istituire una gestione della continuità operativa e delle crisi in collaborazione con gli esponenti dell'industria svizzera del gas naturale (v. sopra).

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

Responsabilità: CF

La misura 15 intende integrare la gestione generale delle crisi con gli aspetti cibernetici.

Stato attuale

Il documento programmatico per procedure e processi di condotta cibernetici è stato allestito ed è in fase di attuazione; è stato inoltre approvato dal comitato direttivo SNPC (CD SNPC) nel mese di febbraio del 2014.

Il documento programmatico concernente la misura 15 è stato allestito ed è stato ampliato ai Cantoni nel gruppo di lavoro 3 dell'MCC RSS: *Gestione delle crisi*. Sulla base di un opportuno scenario dovrà essere valutata l'efficacia di questo documento programmatico, eventualmente modificandolo (v. n. 3.6).

3.4 Processi di sostegno

Per fornire le basi e i processi atti ad affrontare le problematiche cibernetiche occorrono cooperazioni internazionali di vasta portata, lo scambio di esperienze nell'ambito della formazione e della ricerca e un eventuale adeguamento delle basi giuridiche (M1, M7, M8, M9,

M10, M11, M16). A tale scopo sono stati creati i seguenti pacchetti di misure:

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

Inoltre il neocostituito gruppo specialistico Cyber-International consente di ottenere una panoramica delle diverse attività, dei processi e delle iniziative di portata internazionale e di incentivare il flusso di informazioni tra i Dipartimenti.

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

Responsabilità: SEFRI; SC SNPC

Con l'aiuto della ricerca dovranno essere evidenziati i cyber-rischi rilevanti per il futuro, nonché i cambiamenti intervenuti nel panorama delle minacce, al fine di prendere decisioni tempestive e mirate nella politica e nell'economia. Con questo intento viene incentivata la ricerca (la ricerca di base e quella applicata) nell'ambito della protezione dai cyber-rischi. La SEFRI è responsabile dell'attuazione in collaborazione con il SC SNPC.

Stato attuale

La SEFRI ha istituito un comitato direttivo «Ricerca nell'ambito della protezione contro i cyber-rischi». Tale comitato fornisce l'orientamento generale per la ricerca, definisce i criteri dell'assegnazione di progetti di ricerca e tiene una banca dati dei ricercatori sulle tematiche dei cyber-rischi.

Per acquisire le necessarie conoscenze specialistiche ai fini della ricerca nell'ambito dei cyber-rischi, il comitato di ricerca nominerà un pool di esperti in materia (scegliendoli tra i rappresentanti del mondo della ricerca e selezionati esponenti dell'economia), che fornisca consulenza al comitato direttivo nelle tematiche specialistiche e, in particolare, contribuisca a identificare i temi della ricerca stabilendone le priorità.

3.4.2 Misura 7: Panoramica delle offerte di formazione

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

Per aumentare la resilienza della Svizzera nel settore cibernetico, 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 sintonizzata sull'attuazione della «Strategia del Consiglio federale per una società dell'informazione in Svizzera» e con il DFAE.

Stato attuale

In una prima fase è stata allestita una panoramica delle attuali offerte di formazione in materia di creazione di competenze per la protezione contro i cyber-rischi. L'obiettivo di tale panoramica è avere una base che serva a identificare gli esempi di *best practice* (migliore prassi) per i gruppi target definiti dell'economia, dell'amministrazione e della popolazione. È stato inoltre redatto un rapporto sintetico per identificare le offerte di qualità nella formazione di competenze sulla scorta delle raccomandazioni degli esperti. Sono state identificate le possibilità di pubblicare le offerte identificate (ev. in collaborazione con terzi). Su incarico della Confederazione le lacune a livello di offerta in vista della gestione dei cyber-rischi sono state identificate dall'International Institute for Management in Technology dell'Università di Friburgo (iimt). Il rapporto sarà pubblicato nel 2015.

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, DATEC-UFCOM, DFAE-DP, DFI-UFAS

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. L'obiettivo è incentrato sulle offerte in materia di creazione di competenze rilevanti per i gestori di infrastrutture critiche. I lavori di attuazione si svolgono tuttavia d'intesa con i responsabili della «Strategia del Consiglio federale per una società dell'informazione in Svizzera». L'OC SNPC è responsabile dell'attuazione in collaborazione con SEFRI, DATEC, DFAE e UFAS.

Stato attuale

La misura 8 si basa sui risultati della misura 7. Con la conclusione della misura 7 sono state definite le tappe principali per colmare le lacune riscontrate nell'ambito delle offerte entro il mese di dicembre del 2015, visualizzandole nella roadmap. Il comitato direttivo «Ricerca nell'ambito dei cyber-rischi», diretto dalla SEFRI (cfr. 3.4.1), insieme con il pool di esperti nominati, aiuta a identificare ulteriori lacune e a creare le offerte per colmare le lacune presenti.

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'Ufficio federale delle comunicazioni (UFCOM), in qualità di capofila, prende parte ai rilevanti processi nazionali e internazionali.

Stato attuale

L'UFCOM ha allestito una panoramica delle principali manifestazioni, iniziative e dei principali organismi internazionali correlati all'Internet governance[3] e un rapporto concernente le priorità della Svizzera in materia e i rilevanti attori da coinvolgere.

La Svizzera partecipa attivamente ai lavori della Internet Cooperation for Assigned Names and Numbers (ICANN). Dalla fine di ottobre il Comitato consultivo governativo (GAC) di ICANN è presieduto da un cittadino elvetico[4].

L'UFCOM coadiuva inoltre la preparazione e lo svolgimento dell'«Internet Governance Forum (IGF)», è copromotore e co-organizzatore del forum europeo di dialogo IGF «EuroDIG (European Dialog on Internet Governance)» e prende parte attiva al gruppo di esperti del Consiglio d'Europa e della «Commission on Science and Technology for Development (CSTD)».

A livello nazionale l'UFCOM organizza regolarmente la piattaforma di discussione «Piattaforma tripartita per il follow up del VMSI[5]», 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. È stata inoltre costituita la Geneva Internet Platform (GIP) in collaborazione con il DFAE e la DiploFoundation[6].

[3] Questa panoramica è stata pubblicata su CH@World e viene aggiornata periodicamente.

[4] Thomas Schneider, UFCOM

[5] Vertice mondiale sulla società dell'informazione (World Summit on the Information Society)

[6] http://www.giplatform.org/about-gip

3.4.5 Misura 10: Cooperazione internazionale in materia di sicurezza cibernetica

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

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

Stato attuale

Le attività del 2014 sono state imperniate sulla promozione delle misure di rafforzamento della fiducia (Confidence Building Measures) nello spazio cibernetico per aumentare la sicurezza, la trasparenza e la prevedibilità delle minacce in materia. La Svizzera, alla presidenza dell'OSCE, è riuscita a promuovere l'attuazione del primo pacchetto di misure e a divulgarlo in altri forum. La Svizzera ha, tra l'altro, presentato la propria strategia nazionale e ha incaricato di svolgere un'analisi approfondita delle terminologie esistenti in materia. È proseguito lo sviluppo del catalogo di misure, elaborando con la Germania nuove proposte mirate a rafforzare la cooperazione.

Nell'ambito dell'ONU la Svizzera si impegna soprattutto per la protezione della sfera privata nello spazio cibernetico. Nell'ambito della creazione delle capacità la Svizzera si è adoperata affinché i Paesi in via di sviluppo possano partecipare ai processi internazionali in materia di sicurezza cibernetica.

Sono inoltre intensificati gli scambi nell'ambito delle consultazioni bilaterali per promuovere gli interessi della Svizzera.

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-MELANI

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

Stato attuale

Nell'ambito dell'attuazione della misura 11 della SNPC l'UFCOM ha allestito due tabelle ricapitolative. La prima elenca gli attori della misura 11 che seguono e influenzano gli avvenimenti in seno agli organismi internazionali e alle iniziative in materia di sicurezza cibernetica. La seconda tabella contiene gli organismi internazionali e le iniziative che gli attori della misura 11 giudicano importanti. Nel primo processo di elaborazione sono stati invitati gli esponenti di 34 autorità, uffici specialistici ed enti regolatori e, in base ai loro riscontri, altre 90 imprese dell'economia privata, associazioni e istituti di formazione. Il risultante elenco non è tuttavia ancora concluso. Di conseguenza tutti i partecipanti sono chiamati in qualunque momento a nominare altri esperti nazionali e organismi internazionali, ritenuti rilevanti ai sensi della misura 11.

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

Sono state individuate le rilevanti basi giuridiche e la misura è stata recepita dal comitato direttivo SNPC (CD SNPC) nel mese di agosto del 2014. Il servizio di coordinamento SNPC ha approntato con tutti i responsabili Uffici federali un compendio delle rilevanti basi giuridiche nei settori che tengano conto degli aspetti cibernetici anche accertando la necessità di legiferare o di rivedere le basi legali con la massima priorità. La necessità attualmente riconosciuta di legiferare è trattata nella corrente procedura legislativa ordinaria. Non esiste una necessità prioritaria di legiferare oltre. Occorre tuttavia considerare che si tratta soltanto di una rilevazione dello stato attuale e che in futuro il mutevole scenario dei rischi può rendere nuovamente necessario intervenire sulle leggi.

3.5 Attività di attuazione nell'esercito

L'esercito rientra tra le infrastrutture critiche del Paese per le quali lo spazio cibernetico e le minacce in questo ambito hanno assunto un ruolo centrale. Con il rapidissimo sviluppo e la crescente importanza dello spazio cibernetico si presentano nuove opzioni operative, che devono essere considerate nelle operazioni militari. 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 loro capacità d'intervento e la libertà d'azione.

In base alle suindicate esigenze l'esercito dispone di notevoli competenze e capacità, di cui se necessario i responsabili Uffici federali possono avvalersi in via sussidiaria, a condizione che non occorrano contemporaneamente all'esercito stesso, per il quale rimangono prioritari l'esclusione dal campo di applicazione della SNPC dei casi di guerra e di conflitti (cfr. n. 3.4) e il suo incarico di prepararsi a questi eventi specifici.

Stato attuale

In base allo studio concettuale sulla difesa cibernetica («Konzeptionsstudie Cyber-Defence» KS CYD) del 2013 è stata creata una base teorica che consenta di definire un concetto unitario in seno all'esercito e con i suoi partner dei compiti da svolgere nello spazio cibernetico. Sono stati posti e vengono continuamente sviluppati i principi metodologici di una moderna gestione dei cyber-rischi e di un'efficace gestione delle crisi. La collaborazione dell'esercito con i suoi partner critici e fornitori di prestazioni si è evoluta al punto da consentire di realizzare tappe importanti nell'ambito dell'anticipazione e della rappresentazione della situazione nel settore cibernetico.

Nel 2015 sono previsti lo sviluppo delle risorse dedicate e la concretizzazione del piano di attuazione della SNPC. Non è ancora stato possibile precisare la definizione esatta in termini di politica di sicurezza delle prestazioni che l'esercito è chiamato a fornire a favore delle autorità civili e dei gestori di infrastrutture critiche né la sua responsabilità in caso di conflitto e di guerra.

3.6 Attività di attuazione nei 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 necessari Uffici federali. Dirige quattro sottoprogetti che comprendono quattro 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

In riferimento alla misura 3 della SNPC è stato redatto un questionario per l'autoverifica dei cyber-rischi.

È stata elaborata una descrizione dei processi per trattare gli eventi cibernetici. È stato approntato uno dei cinque sottoprocessi. Nelle descrizioni dei processi si è interpellato un pool di esperti specialisti sotto forma di collaborazione tra settore pubblico e privato («Swiss Cyber Experts, cfr. n. 2.1). Il gruppo di lavoro ha inoltre formulato una definizione di un evento concernente la sicurezza cibernetica.

Il documento programmatico della misura 15 della SNCP «Documento programmatico per procedure e processi cibernetici per l'Amministrazione federale» è stato esteso ai Cantoni. Questo documento programmatico dovrà essere verificato mediante sequenze didattiche e di esercizi. Sono stati elaboratori possibili scenari di crisi con aspetti cibernetici, che dovranno essere trattati nel quadro di un seminario strategico.

È stata inoltre predisposta la bozza di un documento programmatico per la tenuta di una panoramica dei casi (casi penali) a livello nazionale e per il coordinamento di casi intercantonali complessi ed è stato allestito un documento programmatico per la formazione del corpo di polizia sul tema della criminalità cibernetica.

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, che deve 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)» ed è tenuto a riferire al Consiglio federale tramite la Conferenza dei segretari generali (CSG). Il servizio di coordinamento SNPC (SC SNPC) ha definito gli obiettivi, le tappe principali e i tempi delle sedici misure SNPC insieme con i responsabili Uffici federali.

5 Verifica dell'efficacia

Il Consiglio federale ha incaricato il comitato direttivo della SNPC (CD SNPC) di sottoporgli un esame dell'efficacia (EdE) nella primavera del 2017 (pag. 10 del piano di attuazione). L'incarico di svolgere questo esame è stato affidato a una società esterna. Dall'esame dovrà risultare:

- fino a che punto le misure della strategia sono state attuate nell'ottica dei contenuti e dell'organizzazione e quale contributo è legittimo attendersi da esse ai fini del raggiungimento degli obiettivi della SNPC;
- se l'Amministrazione federale si è avvalsa delle risorse umane e finanziarie previste per l'attuazione della strategia e se, soprattutto in un'ottica futura, si presenterà un ulteriore fabbisogno di risorse;
- se dai risultati dell'esame emerge la necessità di intervenire per adeguare la SNPC.

In vista dell'elaborazione di questo esame sono state elaborate due fasi con i seguenti contenuti: nel documento programmatico preliminare, interpellando i principali attori è stato sviluppato un concetto comune dei punti cardine (ad es. capisaldi tematici, portata, organizzazione ecc.) dell'esame. Nella stesura dettagliata il documento programmatico viene reso operativo. Sono cominciati i lavori per elaborare la versione dettagliata.

6 Considerazioni finali

Da quando è stato approvato il piano di attuazione della SNPC nel mese di maggio del 2013 sono trascorsi quasi due anni. L'attuazione di alcune misure comporta una procedura articolata e dispendiosa in termini di tempo. Il consolidamento della procedura e l'inventario con i principali attori hanno talora richiesto tempi lunghi. Le risorse limitate e le rispettive priorità attribuite dagli uffici coinvolti nonché gli estesi accertamenti delle basi giuridiche hanno in parte ritardato i lavori di attuazione. Inoltre diversi lavori, che hanno un carattere sequenziale, non consentono di essere svolti contestualmente. Fatte salve poche eccezioni, i lavori di attuazione rientrano comunque nei tempi previsti, pertanto il bilancio per la fine del 2014 è senz'altro positivo.

La SNPC ha portato a instaurare una collaborazione con i Cantoni orientata al futuro e improntata sulla fiducia. Ciò aiuta a incentivare il continuo scambio di conoscenze e di esperienze tra Confederazione e Cantoni e favorisce una migliore collaborazione con altri uffici, che corrisponde all'idea di fondo dell'approccio decentralizzato del piano di attuazione della SNCP. Questa collaborazione ha dato vita a uno scambio di *best practice* che riduce il dispendio per i relativi Cantoni e può aumentare l'efficacia delle loro misure. È stata affrontata l'impostazione della collaborazione con l'esercito in vista del suo supporto in via sussidiaria. È stato intensificato lo scambio di informazioni tra gestori di infrastrutture critiche, fornitori di prestazioni TIC, fornitori di sistemi, associazioni, organismi nazionali di normazione, autorità specializzate ed enti regolatori. Gli interessi della piazza economica Svizzera possono anche confluire ed essere rappresentati in modo coordinato negli organismi internazionali privati e statali nell'ambito della sicurezza, della salvaguardia e della normazione.

La SNPC ha avviato un processo e deve adeguarsi continuamente alle nuove minacce. È dunque importante mantenere anche in futuro la collaborazione, la cooperazione e la comunicazione tra i principali attori, coinvolgendone altri se ve ne sarà l'esigenza.

7 Allegati

7.1 Documenti basilari della SNPC

«Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (SNPC)»:
http://www.isb.admin.ch/themen/01709/01710/index.html?lang=it

«Piano di attuazione della Strategia nazionale per la protezione della Svizzera contro i cyber-rischi (PA SNPC)»:
http://www.isb.admin.ch/themen/01709/01711/index.html?lang=it

«Rapporto annuale SNPC 2013»: (solo in francese e tedesco)
http://www.isb.admin.ch/themen/01709/01891/index.html?lang=fr

7.2 Riepilogo degli interventi parlamentari concernenti i cyber-rischi

Intervento Ip. = Interpellanza; Mo. = Mozione; Po. = Postulato; I = Interrogazione	Depositato il:	Stato al 31.12.2014:
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), rapporto della CPS-CN dell'11.1.2011 nonché deliberazioni del Consiglio degli Stati del 15.3.2011 (BU CS 15.03.2011)	29.06.2010	liquidato
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
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
13.3692 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	accolto
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 protezione della Svizzera contro i cyberrischi e di attuare le 16 misure concrete entro la fine del 2016.»)	05.11.2013	liquidato
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	non ancora trattato nel plenum
13.4308 Po. Graf-Litscher «Migliorare la sicurezza e l'indipendenza del settore informatico	13.12.2013	non ancora trattato nel plenum

svizzero»		
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

7.3 Elenco delle abbreviazioni

AE	Approvvigionamento economico del Paese
BAC	Base d'aiuto alla condotta
BAC CEO	Base d'aiuto alla condotta – Centro operazioni elettroniche
CBM	Confidence Building Measures (Misure di rafforzamento della fiducia)
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
CF	Cancelleria federale
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-POLSIC	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
DPS	Divisione politica di sicurezza
EAPC	Consiglio di partenariato euro-atlantico
EdE	Esame dell'efficacia
ENISA	European Network and Information Security Agency
ERSS	Esercitazione della Rete integrata Svizzera per la sicurezza

Fedpol	Ufficio federale di polizia
FGI	Forum sulla governance di Internet
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, organismo incaricato della registrazione degli indirizzi Internet a livello mondiale
ICT	Information and Communication Technology
IG	Internet governance
LSI	Legge sul servizio informazioni
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	North Atlantic Treaty Organization
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
TIC	Tecnologie dell'informazione e della comunicazione
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