Sicurezza informatica in seno al Servizio delle attività informative della Confederazione

Rapporto della Delegazione delle Commissioni della gestione (riassunto)

del 30 agosto 2013

Rapporto

1 Introduzione

Il 30 maggio 2012 il direttore del Servizio delle attività informative della Confederazione (SIC) ha comunicato al presidente della Delegazione delle Commissioni della gestione (DelCG) che un collaboratore del suo servizio aveva sottratto una considerevole quantità di dati classificati ed era stato in seguito arrestato.

Dopo aver effettuato vari accertamenti sul caso, il 15 ottobre 2012 la DelCG ha deciso di eseguire un'ispezione formale sulla sicurezza informatica in seno al SIC. Dopo averne parlato con il capo del Dipartimento della difesa, della protezione della popolazione e dello sport (DDPS), il 16 ottobre 2012 ha reso pubblica la vicenda (attraverso un comunicato stampa[1] e una conferenza stampa).

Da novembre 2012 a febbraio 2013 la DelCG ha condotto diversi interrogatori nell'ambito della sua ispezione e nel dicembre 2012 ha fatto visita al servizio informatico del SIC. Durante la seduta di fine aprile 2013 ha avuto un ultimo incontro in merito alla vicenda con il capo del DDPS.

All'inizio di giugno 2013 la DelCG ha invitato i dipartimenti interessati a pronunciarsi sul progetto del suo rapporto di ispezione. Il 2 luglio 2013 ha analizzato con una delegazione del Consiglio federale i risultati dell'ispezione e il giorno seguente ha trasmesso al Consiglio federale il rapporto di ispezione insieme a undici raccomandazioni[2].

Volendo evitare che con la pubblicazione di alcune informazioni riguardanti il Servizio delle attività informative venissero violati gli interessi superiori dello Stato, la DelCG ha preferito non pubblicare la versione completa del rapporto di ispezione. Per informare l'opinione pubblica ha redatto questo breve rapporto e lo ha corredato delle raccomandazioni e di un riassunto dei risultati più importanti emersi dall'ispezione.

2 Istituzione del servizio informatico del SIC

Al di fine di attuare le disposizioni della legge federale del 3 ottobre 2008[3] sul servizio informazioni civile (LSIC), nel marzo 2009 il Consiglio federale aveva deciso di riunire in un unico ufficio federale il SAP (Servizio di analisi e prevenzione) e il SIS (Servizio informazioni strategico). Su proposta del DDPS la fusione doveva essere effettuata all'inizio del 2010 «senza ulteriori risorse». Ciò significava che il futuro SIC poteva disporre soltanto delle risorse informatiche di quello che sino ad allora era il SIS, in quanto il DDPS aveva assorbito il SAP, prima appartenente al Dipartimento federale di giustizia e polizia (DFGP), senza il personale competente per le attività informatiche. Poiché non si è sopperito a tale mancanza né

1 Informatiksicherheit im Nachrichtendienst des Bundes, comunicato stampa della DelCG del 16 ottobre 2012.
2 Inspektion der GPDel: Informatiksicherheit im NDB, comunicato stampa della DelCG del 3 luglio 2013.
3 RS **121**

nella fase di concezione del SIC né in una fase successiva, il Servizio ha dovuto gestire con scarse risorse un sistema informatico complesso e sempre più vasto.

Per le banche dati del SIC questo significava che, in caso di assenza dell'unico amministratore interno delle banche dati, la sicurezza dell'attività poteva essere garantita soltanto finché non sarebbero sorti gravi problemi. In seguito alla fusione, diversi sistemi che il SIC aveva acquisito dovevano essere sostituiti o adattati. Tuttavia la mancanza di personale informatico disponibile ha limitato il numero di progetti che il SIC ha potuto realizzare.

Secondo il rapporto che il DDPS ha pubblicato l'11 aprile 2013 sul furto di dati in seno al SIC, il Servizio si è ritrovato a dover gestire una quantità molto più elevata di sistemi e applicazioni e un numero quasi raddoppiato di utenti, con un numero invariato di unità di personale[4]. Secondo la DelCG questo è stato il risultato di un'insufficiente pianificazione che risaliva al maggio 2008, quando il Consiglio federale aveva deciso di trasferire il SAP al DDPS. Il 25 marzo 2009 il Consiglio federale, su proposta del DDPS, aveva deciso di istituire il SIC a partire dai due servizi già esistenti e utilizzando unicamente le risorse a disposizione. Il DDPS avrebbe dovuto porre rimedio alle carenze che ne erano conseguite all'interno del servizio informatico, se non durante il lavoro di concezione del SIC almeno dopo la sua istituzione.

Nella primavera 2011 il SIC ha richiamato per la prima volta l'attenzione della DelCG sulla situazione venutasi a creare in termini di personale. Prima del furto di dati il SIC non aveva tuttavia mai dichiarato che vedeva minacciata la sicurezza informatica a causa della suddetta situazione. Anche la Delegazione delle finanze (DelFin) non aveva ricevuto alcuna informazione che avrebbe potuto rivelare la necessità di agire[5].

Ad avviso della DelCG né il trasferimento del SAP al DDPS né la successiva istituzione del SIC sono stati predisposti in maniera sufficientemente accurata. In vista della nuova legge sul servizio informazioni, la Delegazione ritiene perciò indispensabile che il DDPS valuti le esigenze future in termini di risorse di personale basandosi su un'analisi inconfutabile della situazione ideale e di quella reale.

Raccomandazione 1

La DelCG raccomanda al Consiglio federale di incaricare il DDPS di eseguire un'analisi approfondita e dettagliata delle risorse di personale necessarie per l'adempimento degli ulteriori compiti previsti dalla nuova legge sul servizio informazioni.

3 Gestione dei rischi in seno al SIC

La sicurezza informatica in seno al SIC non era stata integrata in un processo di gestione dei rischi che avrebbe permesso di individuare le conseguenze della carenza

4 Fuga di dati evitata in seno al Servizio delle attività informative della Confederazione, rapporto del DDPS dell'11 aprile 2013 (riassunto).
5 Lettera della DelFin alla DelCG del 5 giugno 2013, p. 2.

di personale nel servizio informatico e di giungere a una mirata riduzione dei rischi. Negli ultimi anni il SIC ha intensificato il proprio impegno nell'ambito del reporting dipartimentale sui rischi[6], ma nell'ambito della gestione interna dei rischi – anche nel settore informatico – i rischi non sono stati né definiti e valutati né attribuiti a determinati responsabili. L'ispezione della DelCG non ha fornito indizi in base ai quali la direzione del SIC avrebbe proceduto attivamente, prima del furto di dati, a una gestione sistematica dei rischi all'interno del Servizio.

Il documento approvato in materia di protezione e sicurezza dei dati, citato nel rapporto del DDPS dell'11 aprile 2013[7], regolava in modo incompleto le responsabilità in materia di gestione dei rischi ed era stato inoltre approvato soltanto all'interno del SIC. Sarebbe necessario che il SIC allinei la propria gestione dei rischi alle disposizioni della Confederazione e fissi in un proprio documento unicamente le deroghe e i complementi riguardanti in maniera specifica il Servizio.

Basandosi sulla politica di gestione dei rischi definita nel 2004, il Consiglio federale ha emanato nel 2010 le Istruzioni sulla politica della Confederazione in materia di gestione dei rischi[8], seguite, nell'autunno 2011, dalle direttive dell'Amministrazione federale delle finanze (AFF) sulla gestione dei rischi presso la Confederazione. Queste direttive sono state completate da un manuale di gestione dei rischi in seno alla Confederazione[9].

Raccomandazione 2

La DelCG chiede al Consiglio federale di assicurarsi che, entro giugno 2014, il DDPS gli riferisca sullo stato della gestione dei rischi in seno al SIC e illustri in che modo il SIC applica adeguatamente le disposizioni della Confederazione in materia.

4 Provvedimenti per la sicurezza informatica in seno al SIC prima del furto di dati

L'ordinanza del 9 dicembre 2011 sull'informatica nell'Amministrazione federale[10] e le Istruzioni del Consiglio informatico della Confederazione (CIC)[11] contengono diverse disposizioni in materia di sicurezza informatica. Il DDPS ha inoltre emanato una propria direttiva e il servizio specialistico Protezione delle informazioni e delle opere (PIO), incaricato della sicurezza informatica, ha pubblicato in qualità di orga-

6 Rapporto sui rischi all'attenzione del Consiglio federale e del Consiglio degli Stati. Rapporto della CdG-N/S del 28 maggio 2010 (FF **2010** 4973).
7 Rapporto del DDPS dell'11 aprile 2013, p. 11.
8 Istruzioni del 24 settembre 2010 sulla politica della Confederazione in materia di gestione dei rischi (FF **2010** 5759).
9 La documentazione è disponibile sul sito Internet dell'AFF: www.efv.admin.ch/i/dokumentation/finanzpolitik_grundlagen/risiko_versicherungspolitik.php
10 Ordinanza del 9 dicembre 2011 concernente l'informatica e la telecomunicazione nell'Amministrazione federale (OIAF; RS **172.010.58**).
11 Istruzioni del Consiglio Informatico della Confederazionne (CIC) sulla sicurezza dell'informatica nell'Amministrazione federale del 27 settembre 2004, disponibili sul sito Internet della SFI: www.isb.admin.ch/themen/sicherheit/00150/00836/index.html?lang=it

no esecutivo e di controllo un manuale sulla sicurezza informatica, che è rimasto tuttavia incompleto rispetto allo standard richiesto.

La DelCG è giunta alla conclusione che, prima del furto di dati, il SIC non aveva adottato diverse misure tecniche e organizzative che avrebbero dovuto rientrare nel sistema di protezione informatica di base e che in parte erano prescritte dalla Confederazione e dal DDPS.

Inoltre non disponeva di personale a sufficienza per adempiere alla funzione di incaricato della sicurezza informatica dell'unità organizzativa e questo rendeva impossibile un'adeguata gestione dei rischi in ambito informatico. I concetti di sicurezza prescritti per le applicazioni e i sistemi erano per la maggior parte insufficienti o mancavano del tutto.

Le password dei conti non nominativi degli amministratori venivano gestite internamente al servizio e il loro utilizzo non era controllato. Considerata la carenza di personale, tale procedura agevolava l'attività informatica, ma dava agli informatici interessati diritti di accesso illimitati e questo non permetteva più di individuare successivamente chi ne aveva fatto uso.

Mentre alcune attività del sistema per motivi di sicurezza venivano registrate, la DelCG non è riuscita a dimostrare che i protocolli delle attività di sistema (file di log) erano stati sistematicamente analizzati. Durante i cinque mesi del 2012 precedenti alla segnalazione, arrivata dall'esterno, su un eventuale furto di dati non è stata effettuata alcuna analisi. Non esisteva per di più alcun piano d'emergenza da attuare in caso di sospetto di minaccia ai sistemi o ai loro dati. Infine il SIC non disponeva del personale necessario per amministrare un sistema di sorveglianza efficace.

In seguito al furto di dati la direzione del SIC ha provveduto con l'urgenza necessaria affinché il Servizio assumesse a tempo pieno un incaricato della sicurezza informatica (nel novembre 2012) e soddisfacesse in tal modo le disposizioni della Confederazione. Tuttavia solo in seguito si è riconosciuta l'importanza dei concetti di sicurezza per la gestione dei rischi legati ai sistemi informatici. Per tale ragione il SIC ha cominciato soltanto alla fine del 2012 a esaminare, con la collaborazione del PIO, quali concetti erano necessari e come potevano essere migliorati.

L'obiettivo del concetto di sicurezza dell'informazione e protezione dei dati (concetto SIPD) è proprio di valutare i rischi della sicurezza di un sistema e di decidere, su questa base, quali misure tecniche, organizzative o di altro tipo adottare per ridurre tali rischi. L'approccio basato sul rischio impedisce l'adozione di misure che, tenuto conto della diversità dei rischi e delle risorse disponibili, non condurrebbero ad una efficace riduzione del rischio.

Raccomandazione 3

La DelCG chiede al DDPS di provvedere affinché l'incaricato della sicurezza informatica del Dipartimento verifichi entro la fine del 2014 che tutte le applicazioni e i sistemi del SIC siano corredati di un valido concetto di sicurezza che preveda una valutazione dei rischi fondata e completa. Per rimediare a eventuali carenze sarà elaborato un piano di provvedimenti vincolante.

L'ispezione ha mostrato che la direzione del SIC non aveva esaminato con la necessaria attenzione la questione riguardante le disposizioni che il servizio doveva osservare nell'ambito della sicurezza informatica. Solo in questo modo si spiega perché la disposizione contenuta nell'articolo 7 capoverso 1 dell'ordinanza del 4 dicembre 2009[12] sui sistemi di informazione del Servizio delle attività informative della Confederazione (OSI-SIC) che chiede di criptare il sistema di comunicazione interno al SIC (SiLAN) non è mai stata attuata, anche se, al momento dell'istituzione del nuovo servizio nel 2009, la direzione del SIC si era dichiarata favorevole a una simile misura e aveva proposto al Consiglio federale di emanare una norma corrispondente per via d'ordinanza.

Raccomandazione 4

La DelCG chiede al Consiglio federale di incaricare il DDPS di verificare entro la fine del 2013 se la disposizione dell'articolo 7 capoverso 1 OSI-SIC relativa alla crittazione del SiLAN può essere applicata in modo che gli oneri siano proporzionati agli utili per la sicurezza informatica del SIC. In base al risultato di questo esame la disposizione dovrà essere applicata in tempo utile o altrimenti immediatamente abrogata.

5 Controlli di sicurezza relativi alle persone

Le due organizzazioni preesistenti al SIC dovevano osservare disposizioni differenti nell'ambito dei controlli di sicurezza relativi alle persone (CSP). Nel SIS tutti gli impiegati venivano sottoposti a un CSP, mentre nel SAP le persone che svolgevano ad esempio funzioni puramente amministrative ne erano escluse. Il livello più alto di CSP, ossia il controllo di sicurezza ampliato con audizione, secondo l'articolo 12 dell'ordinanza del 19 dicembre 2001[13] sui controlli di sicurezza relativi alle persone (OCSP), non veniva tuttavia applicato a tutti i collaboratori del SIS, ad esempio non a quelli del servizio informatico.

Dopo la fusione del SAP e del SIS, si è deciso di sottomettere ai CSP soltanto i nuovi impiegati e coloro che dovevano ripetere il controllo di cui all'articolo 12 OCSP dopo un periodo di cinque anni. Considerate le limitate capacità del servizio specializzato CSP e d'intesa con il PIO, si è tuttavia preferito non anticipare i controlli la cui ripetizione non era stata ancora fissata.

In seguito alla revisione totale dell'OCSP[14], avvenuta nel 2011, il 1° aprile 2012 il DDPS ha prescritto mediante l'ordinanza OCSP-DDPS[15] di sottoporre a controllo tutti i membri del SIC conformemente all'articolo 12 OCSP. Secondo le disposizioni transitorie il nuovo controllo doveva essere avviato per tutte le persone alle quali era ormai imposto un livello di controllo più elevato, entro un mese dall'entrata in

12 RS **121.2**
13 RU **2002** 377
14 Ordinanza del 4 marzo 2011 sui controlli di sicurezza relativi alle persone (OCSP; RS **120.4**).
15 Ordinanza del DDPS del 12 marzo 2012 sui controlli di sicurezza relativi alle persone (OCSP-DDPS; RS **120.423**).

vigore dell'ordinanza. Come risulta dall'ispezione della DelCG, il SIC non ha adempiuto alle suddette disposizioni e nel febbraio 2013 un terzo dei collaboratori non era stato ancora controllato in conformità all'articolo 12 OCSP. Di questi ultimi un quarto era costituito dal personale informatico.

A causa del crescente numero di progetti informatici, che rappresenta un'ulteriore conseguenza della fusione del SAP e del SIS, il SIC è diventato sempre più dipendente da informatici esterni. Questi non sono tuttavia sottoposti al livello più alto dei controlli di sicurezza relativi alle persone, che è invece prescritto a tutti i collaboratori del Servizio. L'ispezione della DelCG non ha fornito inoltre alcuna risposta definitiva alla domanda riguardante il servizio responsabile di avviare il CSP per i collaboratori esterni e il livello di tale tipo di controllo.

La DelCG ritiene che i servizi federali che sono i destinatari finali delle prestazioni fornite da terzi dovrebbero garantire di lavorare soltanto con aziende e collaboratori esterni su cui sono stati effettuati gli appropriati controlli di sicurezza. Gli uffici interessati dovrebbero perciò avere una visione d'insieme di tutti i propri collaboratori esterni ma, secondo le indagini della Delegazione, non sembra ancora essere il caso.

Raccomandazione 5

La DelCG raccomanda al Consiglio federale di fare in modo che, mediante una revisione della OCSP, vengano definite per i collaboratori esterni le stesse condizioni di CSP degli impiegati della Confederazione che assolvono compiti identici. Il servizio federale che è il destinatario finale della prestazione fornita da aziende e collaboratori esterni si assume la responsabilità di far loro osservare le pertinenti disposizioni.

Il problema di un'adeguata esecuzione dei CSP in seno al SIC o ad altri servizi non può essere trattato indipendentemente dalla questione della carenza di risorse di personale che da anni sussiste nel servizio specializzato CSP del PIO. In base al rapporto dell'Ispettorato del DDPS del 21 dicembre 2012 il numero di CPS pendenti è aumentato a 1500 alla fine del 2012. Sebbene nel novembre 2012 il capo del DDPS abbia temporaneamente potenziato il servizio specializzato CSP, ad avviso dell'Ispettorato del DDPS non sarà possibile smaltire le pratiche arretrate prima di cinque anni. Questa situazione è problematica, tanto più che una grande parte dei controlli pendenti riguarda casi che presentano un rischio potenzialmente più elevato e richiedono perciò un lavoro più intenso.

Poiché il CSP deve essere ripetuto periodicamente, il problema della carenza di personale non può essere risolto in modo duraturo tramite impieghi supplementari temporanei. Inoltre negli ultimi anni il numero dei mandati d'esame da parte dei dipartimenti è aumentato costantemente. Si pone dunque la questione se la Confederazione preveda tendenzialmente troppo poco personale per l'esecuzione dei CSP o se i dipartimenti abbiano prescritto il massimo livello di controllo per troppe funzioni. Questo avviene ad esempio perché i superiori delegano la propria responsabilità, invece di adempiere effettivamente al proprio ruolo dirigenziale.

La DelCG è pienamente convinta della necessità di eseguire i CSP, che costituiscono una sorta di protezione di base nell'ambito della sicurezza delle informazioni. I

risultati della sua ispezione, tuttavia, sottolineano l'imprescindibilità di una gestione effettiva del personale che, nel caso del furto di dati in seno al SIC, invece non è stata garantita per settimane, nonostante i tempestivi segnali di avvertimento.

La tendenza a porre l'accento sui CSP per garantire la sicurezza, piuttosto che sulla responsabilità in termini di gestione, emerge anche dalla reazione ufficiale del DDPS di fronte al furto di dati. Nel suo rapporto dell'11 aprile 2013 il DDPS sostiene che anche un CSP ampliato con audizione non avrebbe comunque consentito di formulare riserve sulla prosecuzione dell'attività dell'amministratore delle banche dati.[16] Ciò detto, e senza tenere conto della questione delle risorse disponibili, il DDPS auspica l'aumento del livello di controllo e del ritmo dei controlli, al fine di ridurre ulteriormente i rischi in tutta l'Amministrazione federale.

Più i controlli saranno allargati e generalizzati su tutte le funzioni possibili in seno all'Amministrazione federale, tanto più ci sarà il pericolo che i dirigenti rinuncino ad adottare approcci diversificati nella gestione dei rischi e a utilizzare gli strumenti previsti dal diritto del personale.

Raccomandazione 6

La DelCG raccomanda al Consiglio federale di spiegare in modo dettagliato nel suo messaggio concernente la legge sulla sicurezza delle informazioni quali ruoli rivestono il controllo di sicurezza relativo alle persone e la gestione del personale nell'ambito della sicurezza informatica e di differenziarli chiaramente l'uno dall'altro. Parallelamente, in un rapporto separato deve essere fornita una stima delle risorse di personale che la Confederazione dovrebbe impiegare per l'esecuzione dei CSP e una descrizione del contributo che essa intende apportare alla protezione delle informazioni.

6 Furto di dati avvenuto nel maggio 2012

La DelCG constata che il SIC a causa delle scarse risorse di personale del servizio informatico e dell'inadeguata gestione dei rischi non si è sufficientemente adoperato per garantire la disponibilità, l'integrità e la confidenzialità dei dati, che rappresentano l'obiettivo principale della sicurezza informatica.

Nell'aprile 2012 una nuova assenza per malattia dell'unico amministratore delle banche dati aveva esposto, secondo i suoi superiori, a un rischio crescente la sicurezza di esercizio delle banche dati del SIC. La collaborazione con questo impiegato era stata sentita una volta di più come problematica. La direzione del servizio informatico aveva perciò ritenuto necessario agire al livello gerarchico superiore segnalando, il 26 aprile 2012, la possibilità che, a determinate condizioni, l'amministratore delle banche dati compromettesse anche l'integrità dei programmi delle banche dati. Concretamente si proponeva di togliere all'amministratore i diritti di accesso ai sistemi da lui gestiti.

La direzione della divisione, di cui fanno parte il servizio informatico, la cellula di sicurezza, il servizio giuridico e il servizio del personale, si è trovata di fronte a un

16 Rapporto del DDPS dell'11 aprile 2013, p. 18.

dilemma: sospendere l'amministratore delle banche dati e mettere così in pericolo la disponibilità dei sistemi o mantenere il suo posto di lavoro e correre il rischio di compromettere l'integrità e – come poi avvenne – anche la confidenzialità dei dati.

Sebbene al capodivisione competente fosse stata fornita una chiara valutazione dei rischi, egli lasciò trascorrere una settimana prima di parlare, il 7 maggio 2012, con i propri diretti subordinati delle possibili opzioni di intervento. Anche allora non prese provvedimenti nei confronti dell'amministratore delle banche dati, ma attese tre giorni prima di decidere di convocarlo.

In questa fase critica è mancata una linea di condotta e di gestione rigorosa nei confronti dell'amministratore delle banche dati. Soltanto un'ora dopo il colloquio del 16 maggio 2012, a cui non si è presentato, l'amministratore ha potuto trattenersi a lungo sul proprio posto di lavoro, senza che questo abbia suscitato una benché minima reazione da parte della direzione della divisione.

La mancata reazione della divisione in materia di gestione del personale e di gestione dei rischi ha alla fine reso possibile il furto di dati avvenuto nel maggio 2012. Il direttore del SIC venne a conoscenza dei rischi individuati nell'aprile 2012 soltanto quando il 18 maggio 2012 arrivò una segnalazione dall'esterno su un comportamento sospetto dell'amministratore delle banche dati.

Secondo la DelCG non è esatto sostenere che il diritto federale in materia di personale non avrebbe permesso al SIC alcuna azione efficace nei confronti dell'amministratore delle banche dati. Il SIC avrebbe dovuto prendere in considerazione in tempo utile le possibilità definite dall'articolo 103 dell'ordinanza del 3 luglio 2001[17] sul personale federale (OPers), che regola la sospensione o l'attribuzione di una diversa occupazione degli impiegati della Confederazione. Poiché il SIC non aveva documentato i problemi sorti già da tempo con questo collaboratore, non aveva elementi su cui basarsi durante la fase critica, per predisporre ad esempio una sua sospensione a causa di irregolarità comprovate e ripetute conformemente all'articolo 103 capoverso 1 lettera b OPers.

La DelCG non condivide la valutazione del SIC, secondo cui il Servizio avrebbe reagito in modo sufficiente, in base ai problemi rilevati nell'aprile 2012, al fine di risalire autonomamente e in tempo utile al furto di dati anche senza segnalazioni esterne. Quando l'identificazione dell'amministratore delle banche dati con l'aiuto della grande banca svizzera che aveva segnalato il suo comportamento sospetto tardava ad arrivare, il SIC non ha pensato ad esempio a verificare i file di log connessi alle interfacce esterne, attraverso le quali l'amministratore avrebbe potuto copiare i dati. In questo lasso di tempo non è stata verificata neanche la fondatezza del sospetto in base al quale l'amministratore potrebbe aver compromesso i programmi delle banche dati. Questi due esami sono stati effettuati soltanto dopo la verifica definitiva da parte del SIC della segnalazione della grande banca.

La DelCG non ha motivo di ritenere che il dispositivo di sorveglianza e controllo presente nel servizio informatico e che nel migliore dei casi era incompleto avrebbe permesso da solo di scoprire il furto di dati.

17 RS **172.220.111.3**

7 Misure adottate dal SIC dopo il furto

Secondo la DelCG, dopo il furto dei dati il direttore del SIC non si è preoccupato della sorveglianza in maniera sufficientemente sistematica e non ha affidato la responsabilità dei controlli interni alle persone giuste. In particolare, la decisione di affidare la discussione interna del caso al capo divisione, responsabile di tutti i settori che avevano determinato il modo di procedere del SIC prima del furto dei dati, è stata problematica.

Il capo divisione ha poi concentrato la propria analisi sull'amministratore delle banche dati, tralasciando di ricercare nell'organizzazione e nelle procedure del SIC altre possibili cause del furto. Inoltre nessuno ha controllato se il SIC avesse adottato le misure di sicurezza prescritte in ambito informatico. In un secondo tempo il controllo è stato affidato al capo della sicurezza, il quale, tuttavia, non era la persona adatta per giudicare se la responsabilità gestionale nei confronti dell'amministratore delle banche dati fosse stata usata correttamente, ovvero per giudicare l'operato del proprio capo divisione.

La DelCG, come la Sorveglianza delle attività informative, ritiene problematica l'annessione della cellula di sicurezza a una divisione operativa. Il caso del furto dei dati ha mostrato che gli interessi divergenti dei settori sicurezza, esercizio informatico e gestione del personale hanno ostacolato un intervento deciso nell'interesse della sicurezza. Data la situazione, le decisioni necessarie andavano prese da un organo superiore.

Raccomandazione 7

La DelCG raccomanda al capo del DDPS di provvedere affinché il SIC ricollochi la cellula di sicurezza in modo che essa non sia più subordinata alla divisione Supporto alla condotta e all'impiego (NDBU). Allo stesso tempo bisogna riflettere sulla ripartizione dei compiti relativi alla gestione dei rischi in seno al Servizio.

La DelCG giudica positivamente il fatto che il SIC abbia reagito all'incidente prendendo alcune misure immediate, per esempio nella gestione delle password. Con il tempo, tuttavia, il numero crescente di misure prese dalla direzione del Servizio ha destato l'impressione che il Servizio volesse perlopiù dimostrare la propria capacità di superare le conseguenze del furto di dati. L'enfasi sulle misure in atto o previste ha messo in secondo piano la questione delle cause dell'incidente.

Le misure atte ad aumentare la sicurezza sono state decise senza basarsi su un processo di gestione dei rischi. Il direttore del SIC ha persino approvato misure che poi non sono mai state applicate o che si sono rivelate tecnicamente irrealizzabili. Secondo la DelCG, per adottare misure di sicurezza adeguate e fissare il loro giusto ordine di priorità è necessaria una gestione dei rischi efficiente.

Siccome il SIC ha trascurato l'analisi delle cause sistemiche del furto dei dati, al problema delle risorse del personale non è stata riservata per troppo tempo l'attenzione dovuta. Solo dopo la metà di ottobre 2012 la direzione del Servizio si è dichiarata pronta a impegnarsi per più di un semplice aumento minimo delle risorse di personale in ambito informatico.

Il fabbisogno di personale per la sicurezza informatica nel SIC è stato infine confermato con la decisione del Consiglio federale del 1° maggio 2013 (11 posti di lavoro supplementari). La DelCG approva questa decisione, anche se è stata presa un anno dopo il furto di dati, ma deplora il fatto che l'aumento del personale convenuto avverrà in parte solamente a partire dal 2014 e in parte dal 2015. In questo modo la critica situazione del personale nel settore informatico del SIC durerà più a lungo di quanto in realtà la sensibilità dei dati del Servizio permetterebbe di tollerare.

Raccomandazione 8

La DelCG raccomanda al DDPS di fare in modo che il SIC possa occupare i posti di lavoro di informatico attingendo alle riserve di personale del Dipartimento già nel 2013, sebbene il Consiglio federale abbia dato la propria autorizzazione per il 2014.

8 Accertamenti sulla sicurezza delle informazioni su mandato del Consiglio federale

A seguito del furto di dati in seno al SIC, il 24 ottobre 2012, il Consiglio federale ha deciso, su proposta del DDPS, di richiedere un'analisi dei pericoli per la sicurezza delle informazioni a livello federale. Un gruppo di lavoro che, sotto la direzione del professor Markus Müller (Università di Berna) stava già elaborando la futura legge sulla sicurezza delle informazioni (LSIn), doveva individuare entro la fine di febbraio 2013 le lacune nella sicurezza delle informazioni e proporre misure immediate per rimediarvi. Tuttavia questo termine si è rivelato troppo breve e l'oggetto d'esame è stato limitato al furto di dati commesso da alcuni collaboratori interni.

Il 1° marzo 2013 il DDPS ha presentato il rapporto del gruppo di lavoro al Consiglio federale, invitandolo formalmente a prenderne atto. Il Consiglio federale vi ha provveduto il 15 marzo 2013 e ha deciso di dare seguito, dall'autunno 2013, alla raccomandazione in esso contenuta che mira a formare e sensibilizzare i quadri dell'Amministrazione federale in materia di prevenzione di atti illeciti interni.

Il gruppo di lavoro ha inoltre sottolineato la necessità di applicare senza restrizioni le disposizioni federali in vigore nell'ambito della sicurezza informatica e delle informazioni. Oltre a ciò, dovranno essere applicate rigorosamente le misure destinate al miglioramento della sicurezza informatica, che il Consiglio federale aveva ordinato per tutta l'Amministrazione federale nel dicembre 2009 e nel giugno 2010 a seguito degli attacchi perpetrati contro il settore informatico del Dipartimento federale degli affari esteri (DFAE). Alcune di queste misure sono state esaminate dal Controllo federale delle finanze (CDF) negli anni 2011 e 2012 su mandato del Consiglio federale.

A questo riguardo, va detto che l'Organo direzione informatica della Confederazione (ODIC)[18] stila ogni anno un rapporto sulla sicurezza informatica in seno alla Confederazione destinato al Consiglio federale, in cui fa il punto della situazione riguardo all'applicazione delle misure di sicurezza informatica (cfr. art. 11 cpv. 2 e 3 OIAF).

18 Prima del 2012 l'ODIC si chiamava Organo strategia informatica della Confederazione.

Finora, inoltre, il PIO redigeva un rapporto annuale sulla protezione delle informazioni in seno alla Confederazione all'attenzione della Delegazione Sicurezza del Consiglio federale (DelSic). Tuttavia a seguito della revisione del 1° maggio 2013 dell'ordinanza sulla protezione delle informazioni (OPrI), il rapporto in questione sarà stilato solo ogni due anni e destinato alla Conferenza dei segretari generali.

Entrambi i rapporti si basano sulle indicazioni fornite dai dipartimenti. Affinché essi riflettano lo stato effettivo della sicurezza informatica e della protezione di informazioni, sarebbe necessario verificare le indicazioni ricevute, come è il caso, in parte, per le misure di sicurezza informatica decise nel 2009 e 2010 dal Consiglio federale.

Viste le procedure già istituzionalizzate, la DelCG reputa che il mandato al gruppo di lavoro del professor Müller sia una misura isolata che il DDPS ha proposto senza tenere conto degli strumenti già disponibili a livello federale.

Secondo la DelCG il rapporto annuale sulla sicurezza informatica in seno alla Confederazione redatto dall'ODIC e le misure atte a migliorare la sicurezza informatica, decise dal Consiglio federale nel 2009 e nel 2010 su richiesta del DFF, costituiscono una punto di partenza ideale per avviare un processo duraturo volto a migliorare la sicurezza informatica a livello federale. Il rapporto dell'ODIC che oggi si basa principalmente sulle dichiarazioni spontanee dei dipartimenti potrebbe essere trasformato in un sistema di controlling. Inoltre, il controllo delle misure di sicurezza decise dal Consiglio federale, svolto ad hoc dal CFF, potrebbe essere istituzionalizzato in una forma adeguata.

La DelCG ritiene inoltre che le conclusioni risultanti dal controllo della sicurezza informatica dovrebbero confluire, in modo appropriato, nelle direttive e nelle esigenze valide per la sicurezza informatica in seno alla Confederazione. Infine, la gestione informatica a livello federale dovrebbe essere organizzata in maniera tale che in sede di pianificazione e acquisizione degli strumenti informatici si possa tenere conto per tempo delle direttive in materia di sicurezza informatica e delle esperienze fatte.

Raccomandazione 9

La DelCG raccomanda al Consiglio federale di elaborare delle proposte al fine di migliorare il processo di controllo dello stato della sicurezza informatica in seno alla Confederazione. Le misure devono permettere al Consiglio federale di identificare i rischi legati alla sicurezza informatica in modo tempestivo, di adottare le misure richieste per ridurre tali rischi e di monitorare la loro applicazione nel quadro di un processo istituzionalizzato.

9 Sorveglianza da parte del capo del DDPS

Nei primi tre mesi successivi alla scoperta del furto di dati, il capo del DDPS si è basato sulla valutazione dell'incidente che aveva ricevuto dal SIC. Quest'ultima, tuttavia, era principalmente incentrata sulla persona incaricata di amministrare le banche dati e non conteneva indicazioni su altre concause del furto di dati.

Solo verso la fine di agosto 2012 il capo del DDPS ha chiesto a un organo esterno al SIC di chiarire la situazione del furto di dati e di analizzare la reazione del Servizio. Il 24 agosto 2012 anche la Sorveglianza delle attività informative interna al Dipartimento e a ottobre 2012 il servizio specialistico PIO hanno ricevuto mandati in tal senso.

Il 22 ottobre 2012 il PIO ha elaborato una valutazione sulla sicurezza informatica in seno al SIC per il capo del DDPS. Secondo il servizio specialistico, le risorse di personale del Servizio nei settori dell'informatica e della sicurezza erano insufficienti. In un rapporto complementare elaborato su richiesta del capo del DDPS, il PIO giunge alla conclusione che per poter garantire la doppia occupazione di posti e dunque di funzioni particolarmente sensibili del servizio informatico andrebbero creati, oltre al posto di incaricato della sicurezza informatica dell'unità organizzativa, due posti supplementari nei settori della sicurezza e dai cinque ai dieci posti a tempo pieno.

Per migliorare la capacità di reazione del SIC nell'ambito della gestione e del personale, il PIO ha suggerito di ampliare le possibilità di esonerare rapidamente dal servizio un impiegato che occupa una funzione sensibile in termini di sicurezza. Tale misura dovrebbe tuttavia essere accompagnata da garanzie di tipo finanziario o di altro tipo a favore dell'impiegato coinvolto. Il PIO ha inoltre proposto che, in caso di sospensione immediata, il collaboratore continui a ricevere il salario per un periodo più lungo o che gli venga proposta un'attività equivalente in un settore meno sensibile.

Secondo il PIO, andrebbe comunque verificato se queste proposte sono fattibili dal punto di vista del diritto in materia di personale. In vista del suo rapporto finale dell'11 aprile 2013, il DDPS non ha tuttavia colto l'occasione per chiarire le questioni giuridiche e presentare modelli di condizioni di impiego corrispondenti.

Raccomandazione 10

La DelCG raccomanda al Consiglio federale di creare un gruppo di lavoro interdipartimentale, posto sotto la direzione dell'Ufficio federale del personale (UFPER), con il compito di elaborare delle condizioni di impiego particolari che permettano di migliorare le possibilità di reazione degli organi di gestione del personale di fronte a rischi di attacchi interni. Per ottenere il necessario consenso dai collaboratori interessati, andrebbero esaminate in particolare anche misure di compensazione finanziaria o di altro tipo. Il Consiglio federale è invitato a esprimersi sui risultati ottenuti dal gruppo di lavoro entro la fine del 2014.

A settembre 2012 la Sorveglianza delle attività informative ha fornito al capo del DDPS un primo rapporto intermedio, e, in previsione dell'incontro di metà ottobre 2012 fra il capo del DDPS e la DelCG, un secondo rapporto intermedio. Quindi il capo del DDPS ha pregato la Sorveglianza delle attività informative di concludere entro la fine di novembre 2012 le varie indagini che aveva ordinato a partire da agosto 2012.

Come appreso dalla DelCG, a fine ottobre 2012 prima di chiedere e ottenere l'approvazione da parte del capo del DDPS, il SIC aveva rifiutato di fornire alla Sorveglianza delle attività informative la propria analisi sul potenzale di rischio dei

dati rubati. Alla DelCG non risulta che nella legge in vigore ci sia una disposizione che giustifichi una tale riserva da parte del Servizio.

La DelCG attribuisce grande significato a questo incidente perché il SIC aveva già rifiutato di informare la Sorveglianza delle attività informative su un altro affare che non aveva alcuna relazione con l'ispezione della Delegazione, e l'aveva fatto con il consenso del capo del DDPS. La Delegazione ne è venuta a conoscenza in occasione di un incontro con il professor Koller in cui si è discusso delle sue conclusioni concernenti la sorveglianza interna del Dipartimento. Secondo la DelCG il capo del Dipartimento non può permettere, e tantomeno approvare, che il SIC decida quali informazioni fornire o meno all'organo di sorveglianza.

Raccomandazione 11

La DelCG chiede al capo del DDPS di vigilare sul rispetto incondizionato dei diritti all'informazione garantiti alla Sorveglianza delle attività informative dalla legge (art. 8 LSIC in combinato disposto con l'art. 26 cpv. 1 LMSI) e dall'ordinanza (art. 33 cpv. 1 O-SIC). Il SIC non può limitare questi diritti all'informazione né di sua propria iniziativa, né in accordo con il capo del Dipartimento.

Nei suoi due rapporti intermedi per il capo del DDPS la Sorveglianza delle attività informative ha formulato cinque raccomandazioni e le ha poi riprese nel proprio rapporto finale di fine novembre 2012.

Per la DelCG non è chiaro come mai il capo del DDPS si sia pronunciato solo nell'aprile 2013 su tali raccomandazioni e le abbia trasmesse al SIC affinché le mettesse in pratica, tanto più che queste raccomandazioni figuravano già nel secondo rapporto intermedio della Sorveglianza delle attività informative, pubblicato sei mesi prima.

Complessivamente la DelCG constata che il modo in cui il capo del DDPS ha esercitato il suo dovere di sorveglianza è stato fonte di ambiguità per ciò che concerne la ripartizione dei ruoli tra la Sorveglianza delle attività informative e il SIC.

Il 19 novembre 2012 il capo del DDPS ha incaricato il professor Heinrich Koller, ex direttore dell'Ufficio federale di giustizia (UFG), di effettuare un'indagine sulla Sorveglianza delle attività informative perché, visto il furto di dati, intendeva disporre di un esame di tutti gli attori del DDPS coinvolti[19]. I risultati sono stati forniti a fine marzo 2013 e riguardo alla questione della sicurezza informatica in seno al SIC non è emerso nulla di nuovo.

Visto l'obiettivo fissato dal Dipartimento per l'indagine del professor Koller, alla DelCG non è chiaro perché il capo del DDPS abbia limitato questa indagine alla Sorveglianza delle attività informative. Secondo la Delegazione, dopo il furto di dati in seno al SIC sarebbe stato logico, ma anche opportuno, controllare anche il PIO, poiché quest'ultimo non ha solo un ruolo di sorveglianza, ma anche il compito di approvare i concetti SIPD del Servizio.

A ottobre 2012 la DelCG ha appreso che il capo del DDPS intendeva redigere un rapporto finale sulla base dei risultati dell'incidente che contenesse degli insegna-

19 Rapporto del DDPS dell'11 aprile 2013, p. 16.

menti per tutta l'Amministrazione federale. Contrariamente alle affermazioni del capo del Dipartimento, il Consiglio federale non gli ha però mai affidato un mandato del genere.

Il DDPS ha concluso il rapporto l'11 aprile 2013 e l'ha presentato al Consiglio federale per la sua seduta del 24 aprile 2013 sotto forma di una semplice nota informativa. Il 30 aprile 2013 il rapporto è stato pubblicato in occasione di una conferenza stampa del Dipartimento.

Il DDPS è giunto alla conclusione che il SIC non è nemmeno lontanamente l'unico servizio dell'Amministrazione federale a conservare dati degni di particolare protezione e che nel caso di un furto di dati in un altro servizio, il potenziale di danno sarebbe altrettanto grande[20]. Il DDPS è inoltre convinto che, con le 40 misure adottate dopo il furto di dati, il SIC ha svolto un lavoro di base che potrebbe rivelarsi utile per tutta l'Amministrazione federale. Il Dipartimento ha addirittura proposto di verificare in che misura sarebbe opportuno applicare queste misure al di fuori del SIC.

Nei documenti su cui si basa il rapporto finale del DDPS non ci sono indicazioni concrete riguardo al potenziale di danno in seno al settore informatico dell'Amministrazione federale. La DelCG non esclude però che alcune delle misure decise dal SIC possano contribuire al miglioramento della sicurezza informatica in uno o più servizi della Confederazione. Gli altri servizi della Confederazione non dovranno però ripetere l'errore del SIC e quindi focalizzarsi su una lista di misure prima di avere identificato e ponderato i rischi rilevanti. Solo successivamente si dovrà decidere quali sono le misure appropriate e quali devono essere adottate per ridurre i rischi riscontrati.

20 Rapporto del DDPS dell'11 aprile 2013, p. 18.

10 Fase successiva della procedura

Il 3 luglio 2013 la Delegazione della gestione ha inviato il proprio rapporto di ispezione al Consiglio federale pregandolo di esprimersi sul rapporto e sulle raccomandazioni in esso contenute entro la fine di ottobre 2013. Le raccomandazioni sono state riprese in modo integrale nel presente riassunto del rapporto.

30 agosto 2013

In nome della Delegazione delle Commissioni della gestione:

Il presidente
Pierre-François Veillon, consigliere nazionale

La segretaria
Beatrice Meli Andres

Le Commissioni della gestione del Consiglio degli Stati e del Consiglio nazionale hanno preso atto del rapporto e approvato la sua pubblicazione.

4 settembre 2013

In nome delle Commissioni della gestione:

Il presidente della Commissione della gestione del Consiglio degli Stati
Paul Niederberger, consigliere degli Stati

Il presidente della Commissione della gestione del Consiglio nazionale
Ruedi Lustenberger, consigliere nazionale

La segretaria
Beatrice Meli Andres

Abbreviazioni

AFF	Amministrazione federale delle finanze
CDF	Controllo federale delle finanze
CdG	Commissioni della gestione del Consiglio nazionale e del Consiglio degli Stati
CIC	Consiglio informatico della Confederazione
Concetto SIPD	Concetto di sicurezza dell'informazione e protezione dei dati
CSP	Controlli di sicurezza relativi alle persone
DDPS	Dipartimento federale della difesa, della protezione della popolazione e dello sport
DelCG	Delegazione delle Commissioni della gestione
DelFin	Delegazione delle finanze
DelSic	Delegazione Sicurezza del Consiglio federale
DFAE	Dipartimento federale degli affari esteri
DFGP	Dipartimento federale di giustizia e polizia
FF	Foglio federale
LMSI	Legge federale del 21 marzo 1997 sulle misure per la salvaguardia della sicurezza interna (RS *120*)
LSIC	Legge federale del 3 ottobre 2008 sul servizio informazioni civile (RS *121*)
LSIn	Legge sulla sicurezza delle informazioni (avamprogetto)
NDBU	Divisione Supporto alla condotta e all'impiego del SIC
OCSP	Ordinanza del 19 dicembre 2001 sui controlli di sicurezza relativi alle (RS *120.4*)
OCSP-DDPS	Ordinanza del DDPS del 12 marzo 2012 sui controlli di sicurezza relativi alle persone (RS *120.423*)
ODIC	Organo direzione informatica della Confederazione
OIAF	Ordinanza concernente l'informatica e la telecomunicazione nell'Amministrazione federale (Ordinanza sull'informatica nell'Amministrazione federale; RS *172.010.58*)
OPers	Ordinanza sul personale federale del 3 luglio 2001 (RS *172.220.111.3*)
OPrl	Ordinanza del 4 luglio 2007 sulla protezione delle informazioni della Confederazione (Ordinanza sulla protezione delle informazioni; RS *510.411*)
O-SIC	Ordinanza del 4 dicembre 2009 sul Servizio delle attività informative della Confederazione
OSI-SIC	Ordinanza del 4 dicembre 2009 sui sistemi d'informazione del Servizio delle attività informative della Confederazione (RS *121.2*)
PIO	Protezione delle informazioni e delle opere
RS	Raccolta sistematica
SAP	Servizio di analisi e prevenzione
SIC	Servizio delle attività informative della Confederazione

SiLAN	Sicurezza LAN (Local Area Network)
SIS	Servizio informazioni strategico
UFG	Ufficio federale di giustizia
UFPER	Ufficio federale del personale