Schweizerische Eidgenossenschaft
Confédération suisse
Confederazione Svizzera
Confederaziun svizra

Sicurezza informatica della RUAG – Situazione nel 2021

Rapporto della Commissione della gestione del Consiglio nazionale del 18 febbraio 2022

Parere del Consiglio federale

del 30 marzo 2022

Onorevoli presidente e membri della Commissione,

conformemente all'articolo 158 della legge sul Parlamento vi presentiamo il nostro parere in merito al rapporto della Commissione della gestione del Consiglio nazionale del 18 febbraio 2022 sulla «Sicurezza informatica della RUAG – Situazione nel 2021».

Vogliate gradire, onorevoli presidente e membri della Commissione, l'espressione della nostra alta considerazione.

30 marzo 2022

In nome del Consiglio federale svizzero:

Il presidente della Confederazione, Ignazio Cassis
Il cancelliere della Confederazione, Walter Thurnherr

Parere

1 Situazione iniziale

La Commissione della gestione del Consiglio nazionale (CdG-N) ha pubblicato il 22 febbraio 2022[1] il suo rapporto «Sicurezza informatica della RUAG − Situazione nel 2021». Il rapporto verte in particolare sulla protezione dei dati militari nonché di altri dati sensibili nelle unità aziendali della RUAG e sulla comunicazione del Consiglio federale nonché del Dipartimento federale della difesa, della protezione della popolazione e dello sport (DDPS) e del Dipartimento federale delle finanze (DFF) in qualità di rappresentanti della proprietaria.

Il rapporto della CdG-N va messo in relazione con un reportage del programma «Rundschau» della televisione svizzera tedesca in cui si asseriva che alcuni pirati informatici sarebbero riusciti a penetrare la rete di RUAG International Holding AG (RUAG International); data l'esistenza di numerose connessioni con RUAG MRO Holding AG (RUAG MRO) sarebbe quindi stato possibile anche un accesso a dati sensibili dell'esercito.

La CdG-N giunge alla conclusione che, contrariamente a quanto sostenuto dal programma «Rundschau», non esiste invece alcuna prova fondata di un presunto ciberattacco a RUAG International nella primavera del 2021. Tuttavia RUAG International ha immediatamente eseguito verifiche in proposito e ha riconosciuto l'esistenza di lacune gravi nella sua sicurezza. Visto che sono state adottate subito misure correttive – sottoposte anche a test di resistenza dall'esterno – la Commissione ritiene che RUAG International abbia reagito in maniera adeguata. La CdG-N raccomanda comunque misure supplementari al fine di ridurre ulteriormente il rischio di fughe di dati.

Inoltre la CdG-N si è chiesta se, nel quadro di questo incidente, il DFF e il DDPS abbiano tutelato gli interessi della Confederazione e se il Consiglio federale e in particolare il DDPS l'abbiano informata in modo trasparente e corretto sullo stato di avanzamento dello scorporo e sulla sicurezza informatica della RUAG. La CdG-N attesta ai due dipartimenti di avere avuto una reazione adeguata al reportage del programma televisivo. Nel contempo la Commissione muove però la critica che la comunicazione nei suoi confronti in merito allo scorporo e alla sicurezza informatica andava curata in maniera più trasparente.

Nel complesso la CdG-N formula due raccomandazioni e chiede al Consiglio federale di presentare il proprio parere entro il 30 marzo 2022.

1 FF **2022** 491

2 Parere del Consiglio federale sull'attuazione delle raccomandazioni del 18 febbraio 2022

Il Consiglio federale presenta il suo seguente parere sulle raccomandazioni:

> *Raccomandazione 1 – Protezione dei dati militari e di altri dati sensibili*
>
> La CdG-N invita il Consiglio federale ad adottare le misure necessarie per garantire che, dopo la cancellazione pianificata dei dati, RUAG International non disponga effettivamente più di dati militari o di altri dati sensibili (neanche negli archivi o nei backup). Occorre valutare se la cancellazione debba essere verificata anche da esperti esterni. Va altresì esaminata l'opportunità di chiedere un controllo supplementare della situazione dei dati prima di ogni vendita di parti di RUAG International.

A titolo introduttivo va ribadito che uno degli scopi principali dello scorporo consiste nel fare in modo che soltanto la RUAG MRO abbia ancora accesso ai dati dell'esercito rilevanti per la sicurezza. La maggior parte dei dati sono stati migrati ad aprile 2020 nella prima tappa dello scorporo informatico, il cosiddetto «cutover». Questa migrazione dei dati nel perimetro di sicurezza della Base d'aiuto alla condotta (BAC) ha consentito a RUAG MRO di usufruire di uno standard di sicurezza più elevato e di iniziare la sua attività il più possibile in maniera indipendente rispetto alla rete di RUAG International.

Il Consiglio federale sottolinea a tale proposito che i dati dell'esercito rilevanti per la sicurezza oggi sono trattati soltanto ancora da RUAG MRO. Non sono più stati trattati dati residui, ancora salvati nei vecchi sistemi di RUAG International. Anzi, tali dati sono stati cercati in maniera mirata e cancellati singolarmente nell'ambito di un progetto separato, volto a esaminare manualmente nel dettaglio i sistemi. Nel 2021 il Controllo federale delle finanze (CDF) nel suo rapporto di verifica sulla sicurezza informatica di RUAG MRO[2] ha illustrato nel dettaglio questa procedura, quantificando anche il volume dei dati residui e classificandoli in base alla loro criticità. È tra l'altro giunto alla conclusione che il concetto per la cancellazione dei dati nei sistemi di RUAG International è «impostato in maniera adeguata allo scopo».

Il Consiglio federale è consapevole della pericolosità di una potenziale fuga di dati. Per questo il DFF e il DDPS seguono da vicino il progetto di scorporo in tutta la sua complessità. Gli enti proprietari hanno preteso sia da RUAG International sia da RUAG MRO (quest'ultima responsabile per la rettifica dei dati, in veste di loro proprietaria) che la rettifica definitiva dei dati venga eseguita con la massima accuratezza. Nella procedura è stato inevitabile definire una certa sequenza: ad esempio non è stato possibile eseguire la rettifica definitiva dei dati prima del «cutover». In seguito i dati migrati rilevanti per la sicurezza sono stati registrati, classificati sistematicamente e rettificati: quest'operazione comprendeva anche la registrazione e la rettifica dei dati

[2] CDF (2021): Verifica della sicurezza informatica RUAG MRO Holding AG del 22 febbraio 2021 (CDF-20431): www.efk.admin.ch/it > Pubblicazioni > Sicurezza e ambiente > Difesa ed esercito > Sicurezza informatica – RUAG MRO Holding AG

nei backup, negli archivi, negli «share» personali, nelle caselle di posta elettronica e nei «transfer share».

Inoltre RUAG MRO ha commissionato un audit esterno che si prefigge lo scopo di verificare l'autonomia e la funzionalità dei sistemi IT scorporati. Il CDF nel suo programma annuale 2022 ha altresì preannunciato un ulteriore controllo della sicurezza informatica di RUAG MRO[3].

In seno a RUAG International è stato nominato un nuovo «chief information security officer» che ha il compito di garantire il trattamento accurato dei dati nelle singole cessioni di partecipazioni. A tale proposito gli enti proprietari hanno esortato RUAG International, prima di singole vendite di parti dell'azienda, a fare appurare da parte di esperti esterni che la stessa RUAG International abbia adottato provvedimenti adeguati per impedire una trasmissione involontaria di dati sensibili.

Inoltre è di principio possibile affermare che le vendite di parti di RUAG International in ultima analisi riducono costantemente il rischio di fughe di dati, vista la riduzione della complessità dei sistemi IT ivi correlata.

Il Consiglio federale ritiene che in questo modo siano state adottate misure efficaci per proteggere i dati militari e altri dati sensibili. Considera quindi come attuata la raccomandazione 1.

Raccomandazione 2 – Comunicazione trasparente

La CdG-N invita il Consiglio federale ad adottare misure adeguate affinché il Collegio governativo, il DFF e il DDPS con i loro enti proprietari informino in futuro le commissioni di alta vigilanza in modo più trasparente e rapido sulle difficoltà incontrate durante lo scorporo di RUAG e, in particolare, nell'ambito dello sviluppo di RUAG International.

Il Consiglio federale si adopera costantemente per garantire la trasparenza nello scambio di informazioni con le commissioni di alta vigilanza e svolge questo compito al meglio delle sue possibilità. Proprio per quanto riguarda le sfide dello scorporo della RUAG, in questa sede sottolinea che il rapporto del Consiglio federale sul raggiungimento degli obiettivi strategici per BGRB Holding AG (RUAG) 2020[4] ha presentato in maniera precisa e chiara l'avanzamento dei lavori. Ad esempio è stata illustrata dettagliatamente l'attuazione dell'obiettivo strategico 2.1.3 in base al quale il Consiglio federale si aspetta che «la società partecipata: [...] porti avanti rapidamente i lavori dello scorporo ancora da eseguire e li concluda al massimo entro fine 2021».

Le pietre miliari cruciali dello scorporo sono state il trasferimento dell'informatica di RUAG MRO nel perimetro di sicurezza della BAC ad aprile 2020 e la «scissione del bilancio» avvenuta quasi contemporaneamente, con cui dopo la separazione operativa e giuridica di RUAG MRO e RUAG International sono stati suddivisi anche i loro

3 Programma annuale Controllo federale delle finanze 2022, pag. 12: www.efk.admin.ch/it > Pubblicazioni > Comunicazione istituzionale > Rapporti annuali > Rapporto annuale 2022.

4 Consiglio federale (2020): Rapporto del Consiglio federale sul raggiungimento degli obiettivi strategici per BGRB Holding AG (RUAG) nell'esercizio 2020 del 19 marzo 2020 (rapporto confidenziale).

attivi e passivi. Gli aggiustamenti e i passi ancora mancanti, come ad esempio il «rebranding», sono stati poi raggruppati a settembre 2020 in una «seconda tappa dello scorporo». Il motivo va ricercato nel fatto che tali operazioni rivestivano un'importanza subordinata nell'ottica dell'obiettivo di potere eseguire in un ambiente TIC sicuro i lavori a favore dell'esercito; inoltre da metà 2020 lo scorporo era ultimato nelle sue parti principali.

Oggi è lecito affermare che lo scorporo della RUAG come progetto è stato eseguito con successo. Anche il CDF ne fornisce una valutazione positiva, intitolando ad esempio il capitolo 2.1 del suo rapporto di verifica sulla sicurezza informatica di RUAG MRO in questo modo: «Gli obiettivi del progetto sono stati raggiunti qualitativamente e quantitativamente»[5].

Il Consiglio federale attribuisce grande importanza alla richiesta della CdG-N di una comunicazione trasparente e tempestiva sulle sfide legate alla RUAG; nella sua opera di rendicontazione sul raggiungimento degli obiettivi strategici della RUAG, come pure in ogni altra comunicazione concernente la RUAG, si impegna a informare in modo preciso sugli sviluppi importanti per la Confederazione.

D'ora in poi il Consiglio federale attribuirà un'attenzione ancora maggiore alla richiesta della CdG-N relativa a una comunicazione trasparente. A titolo riassuntivo, il Consiglio federale considera pertanto attuate entrambe le raccomandazioni.

5 Cfr. nota a piè di pagina 2