Verifica della sicurezza informatica
RUAG MRO Holding SA

L'essenziale in breve

Il 21 marzo 2018 il Consiglio federale ha deciso di riunire le unità operative dell'ex RUAG, attive quasi esclusivamente per l'Esercito svizzero, in una nuova società del gruppo, la RUAG MRO Holding SA (MRO CH), ovvero la società affiliata RUAG SA. Lo scopo era scorporare tali unità dal resto del gruppo RUAG (RUAG International), che svolge attività sia civili che militari a livello internazionale. Con questa decisione, il Consiglio federale ha perseguito l'obiettivo di aumentare la sicurezza informatica e garantire all'esercito una fornitura di prestazioni solida, trasparente e ottimizzata sotto il profilo dei costi. La MRO CH dovrebbe continuare ad adempiere al suo scopo sancito dalla legge, ovvero garantire l'equipaggiamento dell'esercito, e nel contempo avere l'opportunità di svilupparsi ulteriormente negli altri ambiti di attività.

Lo scorporo interessava anche le tecnologie dell'informazione e della comunicazione (TIC) di RUAG. È stato deciso di affidare la responsabilità delle TIC di RUAG SA al Dipartimento federale della difesa, della protezione della popolazione e dello sport. L'intera infrastruttura e i sistemi TIC sono stati riorganizzati e i dati ripresi nel perimetro di sicurezza della Base d'aiuto alla condotta (BAC) dell'esercito. Di conseguenza, i requisiti in materia di sicurezza TIC della Confederazione devono essere soddisfatti. Secondo una stima di settembre 2020, il progetto di scorporo comporta costi dell'ordine di 81–86 milioni di franchi. Dei costi totali pari a 57 milioni di franchi sostenuti fino a fine settembre, 34 milioni sono attribuibili allo scorporo delle TIC. Il progetto ha interessato circa 2500 collaboratori di MRO CH attivi in oltre 20 sedi in Svizzera.

La presente verifica è incentrata sulla sicurezza dei sistemi TIC, ovvero sul trasferimento monitorato in RUAG SA e nel perimetro di sicurezza della BAC.

Dalla verifica è emerso che il trasferimento dei sistemi e dei dati è ampiamente riuscito, nonostante i progetti successivi ancora in sospeso. La governance e l'organizzazione in materia di sicurezza delle TIC sono adeguate, ma necessitano ancora di importanti interventi successivi. La collaborazione con la BAC funziona, ma è ancora in fase di rodaggio.

Lo scorporo delle TIC è stato concluso con successo, malgrado l'elevata complessità del progetto e i ritardi

Dopo lo scorporo delle TIC (prima fase), i servizi standard della BAC dovrebbero essere utilizzati in futuro. Per questo motivo, i collaboratori di RUAG SA sono stati dotati di nuovi apparecchi di burotica della BAC. Il trasferimento nel nuovo ambiente, previsto per il 1° gennaio 2020, non ha potuto essere attuato a causa di diverse circostanze. La migrazione è quindi stata posticipata alla Pasqua 2020. Alla fine di aprile 2020 è stato completato il cambiamento di sistema *(cutover)* e la relativa prima fase è stata conclusa entro fine giugno 2020. Gli obiettivi del progetto sono stati raggiunti.

Il trasferimento dei dati ha rappresentato una grande sfida. Per evitare la diffusione di malware, non era permesso copiare dati direttamente dai sistemi dell'ex RUAG in quelli della BAC. Pertanto, i dati sono stati trasferiti in un'area di quarantena della BAC attraverso un

canale appositamente predisposto, dove vengono sottoposti a un'analisi antivirus prima di essere trasferiti nei nuovi sistemi.

Per ripulire i dati dai vecchi sistemi, MRO CH ha lanciato un altro progetto come parte della seconda fase del processo di scorporo. In questo processo, i dati rilevanti e confidenziali in ambito militare devono essere cancellati dai vecchi sistemi o resi irriconoscibili. È quindi di fondamentale importanza che anche gli archivi e i backup dei dati vengano ripuliti. Il progetto è condotto in stretta collaborazione con RUAG International. In qualità di detentrice dei dati, la loro pulizia spetta a RUAG SA.

Nella seconda fase, che si concluderà entro fine 2021, verrà messa in sicurezza anche l'infrastruttura tecnico–scientifica. In tale ambito, la responsabilità e l'esercizio competono a RUAG SA.

La nuova organizzazione della sicurezza di RUAG SA è strutturata in modo mirato

L'organizzazione della sicurezza di RUAG SA è adeguata. Siccome l'organizzazione include gli incaricati della sicurezza negli ambiti specializzati, lo scambio continuo di informazioni è garantito. I diversi settori parziali sono ben coordinati fra loro e gli scambi con la direzione garantiti. Vi sono inoltre scambi regolari con l'organizzazione della sicurezza della BAC.

La creazione di un sistema di gestione della sicurezza delle informazioni, comprese le attività di verifica, contribuiscono alla sicurezza sostenibile delle informazioni. La gestione dei rischi e quella della continuità operativa sono in fase di realizzazione. La gestione della continuità operativa verrà attuata soltanto nel 2023. Al riguardo, RUAG SA dovrebbe elaborare una soluzione più rapida, perlomeno per i processi aziendali più importanti.

Alcuni aspetti della sicurezza operativa devono essere migliorati

Dopo la migrazione, l'esercizio dei sistemi di RUAG SA spetta alla BAC. La vigilanza sulla sicurezza è garantita dal Centro operativo di sicurezza *(Security Operations Center)*. Tuttavia, all'atto dell'integrazione dei sistemi nel nuovo ambiente, non sono state effettuate verifiche della conformità in materia di sicurezza su ampia scala. Ne consegue un notevole rischio, in particolare per le applicazioni con accesso a Internet. La BAC dovrebbe eseguire sistematicamente verifiche della conformità in materia di sicurezza.

Con il passaggio della sua governance all'Amministrazione federale, RUAG SA soggiace alle direttive della Confederazione. Per determinati casi d'applicazione, è stato quindi necessario chiedere delle deroghe alla protezione di base delle TIC. Laddove possibile, queste deroghe devono essere eliminate o essere almeno ancora formalizzate.

Le raccomandazioni del CDF formulate nei precedenti rapporti sono ampiamente attuate

Le raccomandazioni formulate dal CDF nei rapporti 18517 e 19418 sono state ampiamente attuate, nella misura in cui interessano MRO CH. Per quanto concerne le due raccomandazioni ancora da attuare al momento della verifica, sono state create organizzazioni di progetto e i lavori sono in corso. La pulizia degli incarti della sicurezza (raccomandazione 19418.002) ha raggiunto il 60 per cento e dovrebbe concludersi entro fine 2020. Riguardo al trasferimento dell'infrastruttura tecnico–scientifica in un perimetro di sicurezza (raccomandazione 19418.003), sono state definite l'architettura finale e le prestazioni di servizio. Il necessario centro di calcolo è operativo e il progetto dovrebbe essere concluso entro fine 2021.

Testo originale in tedesco