Verifica della sicurezza della banca dati INFOSTAR

Ufficio federale di giustizia e Centro servizi informatici del Dipartimento federale di giustizia e polizia

L'essenziale in breve

Infostar è il registro centralizzato per la registrazione elettronica degli eventi relativi allo stato civile (nascita, matrimonio, decesso ecc.) che la Confederazione mette a disposizione dei Cantoni dal 2005. Conta quasi 1200 utenti ripartiti in 142 uffici dello stato civile. L'applicazione è gestita dal Settore Infostar dell'Ufficio federale di giustizia (UFG) e dal Centro servizi informatici del Dipartimento federale di giustizia e polizia (CSI-DFGP). Attualmente è in corso un progetto di modernizzazione i cui costi ammontano a circa 23,7 milioni di franchi e che inizialmente si prevedeva di concludere nel 2023.

Nell'ambito della presente verifica, il Controllo federale delle finanze (CDF) esamina se la sicurezza delle informazioni è garantita quando viene utilizzata l'applicazione corrente. Verifica inoltre se il progetto di modernizzazione è in grado di colmare le lacune a livello di sicurezza e se la collaborazione nel trattamento dei ciberincidenti è efficace.

Nel complesso, le basi per la sicurezza delle informazioni sono state gettate nel quadro dell'utilizzo dell'applicazione corrente e del progetto di modernizzazione, in particolare tramite la loro integrazione nell'infrastruttura standard del CSI-DFGP. Tuttavia, sono state constatate delle lacune: la documentazione di sicurezza e l'analisi dei rischi dell'applicazione devono essere aggiornate. Il progetto «Infostar New Generation» si trova in una fase difficile: si devono apportare modifiche all'organizzazione e alla pianificazione come pure migliorare il processo di test. Infine, vi sono le basi per trattare i ciberincidenti, ma occorre rafforzare l'operatività e perfezionare la comunicazione.

Applicazione corrente: il funzionamento è stabile ma la documentazione di sicurezza è datata

Grazie alla sua integrazione nell'infrastruttura standard del CSI-DFGP, l'applicazione corrente beneficia di un'architettura di sicurezza comprovata. Questa comprende l'autenticazione degli utenti, i diritti di accesso, un traffico criptato delle informazioni e le ridondanze. I comitati di architettura seguono costantemente gli sviluppi.

Le attività di esercizio dell'applicazione e quelle tecnico-operative sono descritte e applicate in maniera adeguata. La gestione degli utenti, la protezione contro i malware, i backup di sicurezza, la sorveglianza dell'infrastruttura e i test periodici della sua stabilità sono assicurati da esperti. Il funzionamento della soluzione corrente è stabile, ma la sua manutenzione è difficile a causa della complessità dei programmi.

Esiste una governance della sicurezza, i ruoli sono definiti e assunti dai collaboratori nonché chiaramente delimitati l'uno dall'altro. Tuttavia, benché le esigenze di Infostar in termini di protezione delle informazioni siano maggiori, la documentazione di sicurezza è in gran parte datata. Ciò potrebbe portare i responsabili a sottovalutare i rischi cui è esposta la soluzione. La documentazione di sicurezza deve essere aggiornata e deve essere svolta e convalidata un'analisi dei rischi residui.

La modernizzazione incontra alcune difficoltà, l'organizzazione del progetto e dei test deve essere migliorata

Il progetto di modernizzazione di Infostar, lanciato nel 2018, è in fase di realizzazione. I lavori dovrebbero permettere di sfruttare gli sviluppi tecnici e fornire delle soluzioni alle difficoltà riscontrate nelle attività di manutenzione. Il progetto è condotto secondo una metodologia agile e sotto la responsabilità dell'UFG, che definisce le esigenze specifiche. Il CSI-DFGP è responsabile della realizzazione.

Da diversi mesi il progetto deve far fronte ad alcune difficoltà. Il ricambio di personale è molto frequente e il posto di capoprogetto è occupato ad interim. I responsabili sono consapevoli di questa situazione delicata e hanno definito misure immediate. È stata introdotta una nuova organizzazione e si cercano i profili necessari sul mercato del lavoro. Pertanto, si prevedono ritardi e sforamenti dei costi. Il CDF rinuncia a formulare una raccomandazione al riguardo, ma chiede alla nuova organizzazione di coinvolgere maggiormente gli specialisti della sicurezza e dell'esercizio.

La nuova applicazione viene realizzata nel quadro dell'architettura standard del CSI-DFGP e beneficia quindi delle sue solide componenti di sicurezza.

Tuttavia, il CDF ha constatato che la preparazione del processo di test non è ancora terminata. In particolare, chiede di rivalutare la profondità dei test e la loro automazione, la non regressione e il trattamento delle lacune.

Trattamento dei ciberincidenti e gestione della continuità: la collaborazione deve essere rafforzata

Le basi per il trattamento dei ciberincidenti sono definite in modo adeguato. I ruoli e le responsabilità in questo ambito sono assunti attivamente in seno al CSI-DFGP. I processi sono descritti, ma i beneficiari delle prestazioni non sono coinvolti a sufficienza nella loro attuazione. Il CSI deve migliorare questo aspetto. Deve inoltre rivalutare l'opportunità di elaborare dei modelli di risposta in base al tipo di incidente. Siccome al momento della verifica le modalità di gestione delle crisi erano in fase di aggiornamento, il CDF ha rinunciato a formulare una raccomandazione al riguardo.

I sistemi di gestione degli incidenti e le procedure di escalation sono implementati, come pure i servizi di contatto e i canali di comunicazione. Durante il trattamento degli incidenti, le azioni e le decisioni vengono documentate. Sono disponibili strumenti di monitoraggio e gli eventi vengono registrati e possono essere analizzati tramite appositi ausili.

Le modalità di gestione della continuità operativa sono definite all'interno di ciascuna unità amministrativa, ma il CDF teme che non siano sufficientemente integrate. Consiglia all'UFG di organizzare per Infostar degli esercizi di gestione della continuità che coinvolgano i beneficiari e i fornitori di prestazioni allo scopo di migliorare il coordinamento tra le parti interessate e individuare eventuali punti deboli nel processo.

Testo originale in francese