Verifica concernente l'efficacia della gestione degli incidenti nella protezione dell'informatica federale dai ciber-rischi

Centro nazionale per la cibersicurezza

L'essenziale in breve

Il Centro nazionale per la cibersicurezza (NCSC), in qualità di servizio specializzato della sicurezza TIC (TIC è l'acronimo di tecnologie dell'informazione e della comunicazione), emana direttive sulla cibersicurezza in seno all'Amministrazione federale, ne verifica il rispetto e sostiene i fornitori di prestazioni nell'eliminazione di vulnerabilità.

L'ordinanza sulla protezione contro i ciber-rischi nell'Amministrazione federale, licenziata dal Consiglio federale, è in vigore dal 1° luglio 2020 e costituisce la base giuridica per l'istituzione e il potenziamento dell'NCSC. Disciplina la struttura, i compiti e le competenze delle autorità coinvolte. Essa autorizza l'NCSC, previa consultazione dei servizi interessati, ad assumersi la responsabilità principale della gestione di un ciberincidente se questo minaccia il corretto funzionamento dell'Amministrazione federale.

Nel quadro della presente verifica, il Controllo federale delle finanze (CDF) ha esaminato l'efficacia del processo. In particolare, ha controllato se lo scambio di informazioni tra le fonti e l'NCSC avviene in tempo reale e ha analizzato il modo in cui tali informazioni vengono integrate nei risultati della propria sorveglianza. Sono inoltre stati valutati l'individuazione di un ciberincidente, la tempestiva dell'attuazione di misure e il flusso di informazioni verso gli uffici interessati.

Il processo per la gestione degli incidenti è stato definito, pubblicato e viene applicato. In linea di principio i ruoli e le responsabilità sono stati attribuiti, ma il ruolo dell'incaricato della sicurezza informatica a livello di unità organizzativa (ISIU) deve essere rafforzato. Conviene altresì precisare l'elenco degli attori nel caso in cui sono interessati fornitori di prestazioni esterni. Le condizioni quadro sono adeguate, ma i canali di comunicazione e l'attualità delle notifiche devono essere migliorate.

Maggiore rapidità nel segnalare un ciberincidente

Per poter stimare i rischi ed effettuare un'analisi generale, è importante che i ciberincidenti siano segnalati immediatamente. In tal modo si può ridurre o evitare, nel migliore dei casi, il pericolo di una propagazione laterale nell'intera Amministrazione federale. Nel quadro della sua verifica, il CDF ha constatato che la comunicazione all'NCSC deve essere sviluppata ulteriormente. Ad esempio, la gestione a livello orizzontale, in particolare lo scambio di informazioni tra i fornitori di prestazioni, non è ancora garantita ovunque. Inoltre, gli incaricati della sicurezza informatica presso i dipartimenti devono essere informati con maggiore rapidità.

Un'altra sfida consiste nella classificazione dei ciberincidenti, che bisognerebbe coordinare o armonizzare quando riguardano più unità amministrative. In caso contrario vi è il rischio che le diverse unità amministrative attribuiscano all'incidente un grado di priorità diverso.

Una situazione di questo tipo potrebbe comportare anche una comunicazione non coerente con terzi.

Rafforzamento del ruolo dell'ISIU e creazione di un elenco dei fornitori di prestazioni esterni

Gli ISIU rivestono un ruolo importante nella notifica dei ciberincidenti: in qualità di beneficiari di prestazioni segnalano i ciberincidenti alla propria unità amministrativa, che provvede a informare l'NCSC. Poiché il livello di maturità dei beneficiari di prestazioni cambia a seconda delle loro dimensioni, non sempre è stata definita una supplenza. In caso di assenza dell'ISIU, la segnalazione di un ciberincidente può subire ritardi e quindi anche la conseguente segnalazione all'NCSC. Questa situazione deve essere corretta senza indugio.

In caso di ciberincidente è impossibile stabilire in tempi brevi quali siano le applicazioni e i servizi toccati, quale sia il fornitore e quale l'unità amministrativa per cui quest'ultimo li gestisce. In altre parole, in caso di segnalazione di un incidente relativo alla sicurezza informatica riguardante un fornitore di prestazioni esterno, le unità amministrative interessate non possono essere informate tempestivamente, cosa che rende l'Amministrazione federale più vulnerabile. Di conseguenza, si dovrebbe prendere in considerazione la creazione di un elenco completo.

Uso più efficiente degli strumenti

Per non impiegare strumenti di vigilanza differenti con funzionalità identiche o simili, il loro acquisto dovrebbe essere armonizzato a livello di Amministrazione federale ed effettuato centralmente. In tal modo si sfrutterebbero i possibili effetti di scala per quanto riguarda i costi e lo sviluppo del know-how.

Ottimizzazione del modello di clausola contrattuale

La Conferenza degli acquisti della Confederazione ha creato un modello di clausola contrattuale concernente i ciber-rischi. I punti relativi alla sicurezza informatica vanno nella giusta direzione. Tuttavia, poiché i termini per segnalare i ciberincidenti non sono specificati in maniera uniforme, bisognerebbe prevederne una definizione praticabile. Inoltre, la clausola dovrebbe poter essere rinegoziata nel caso dei contratti pluriennali.

Testo originale in tedesco