Verifica trasversale della sicurezza IT nell'Amministrazione federale
Rapporto all'attenzione del Consiglio federale

L'essenziale in breve

Conformemente alla decisione del 4 giugno 2010 del Consiglio federale, il 24 giugno 2010 il Controllo federale delle finanze (CDF) ha ricevuto dal «delegato per la strategia informatica della Confederazione» una richiesta scritta di verifica dello stato di attuazione delle misure volte a potenziare la sicurezza informatica. Il 27 agosto 2010 il CDF ha accettato la richiesta dichiarandosi disposto a effettuare una verifica trasversale per il 2011. Mediante la nota d'informazione del 2 dicembre 2011, il Dipartimento federale delle finanze (DFF) ha trasmesso il rapporto di revisione per conoscenza ai membri del Consiglio federale.

Nel programma di verifica per l'anno 2011 il CDF ha stabilito le misure da sottoporre a esame, il loro ordine di priorità e il loro grado di approfondimento in relazione a tale esame, nonché i settori dell'Amministrazione federale interessati. I temi scelti riguardavano il rispetto dei requisiti delle password, l'eliminazione tempestiva delle lacune di sicurezza e il rafforzamento della sorveglianza della rete. La verifica è stata effettuata presso sette fornitori di prestazioni informatiche dell'Amministrazione federale. Il CDF ha inoltre condotto un sondaggio scritto tra 71 beneficiari di prestazioni riguardo al rispetto dei requisiti delle password, all'eliminazione tempestiva delle lacune di sicurezza e al miglioramento della gestione dell'informazione. Questi temi costituiscono l'oggetto delle misure immediate decise dal Consiglio federale il 16 dicembre 2009.

Le verifiche hanno permesso di trarre le seguenti principali conclusioni.

In ambiente Windows non sono stati rilevati punti deboli significativi. Dalla verifica è emerso che i fornitori di prestazioni esaminati hanno raggiunto un buon grado di rispetto sia dei requisiti delle password sia dei termini che garantiscono una tempestiva eliminazione delle lacune di sicurezza dei nuovi sistemi Windows.

In ambiente non Microsoft sussistono importanti lacune di sicurezza. Il CDF individua notevoli punti deboli nell'eliminazione tempestiva delle lacune di sicurezza presenti in prodotti non Microsoft che operano su sistemi operativi Windows. Il problema risiede in parte nelle dipendenze da applicazioni specifiche che non consentono più l'aggiornamento di componenti fondamentali del sistema. Sono state constatate inoltre lacune nella definizione delle competenze relative alla manutenzione dei prodotti. Anche i vecchi sistemi sono a rischio in termini di sicurezza, poiché non soddisfano i requisiti delle password e per alcuni di essi non si dispone più degli aggiornamenti necessari per colmare le attuali lacune di sicurezza.

I beneficiari di prestazioni gestiscono sistemi e applicazioni nella consapevolezza delle lacune di sicurezza e i fornitori di prestazioni non riescono ad imporsi. Sulla base di esempi è emerso che spesso gli utenti attribuiscono un basso grado di priorità alle questioni di sicurezza:

- vi sono sistemi di postazioni di lavoro con diritti di accesso privilegiati (diritti di amministratore locali) che sono stati impostati su richiesta degli utenti registrati;
- i settori di attività continuano a gestire applicazioni e sistemi obsoleti pur sapendo che questi presentano lacune di sicurezza o impediscono l'aggiornamento di componenti critici dal punto di vista della sicurezza;

- le regole concernenti le password sono state disattivate a livello di direzione di un dipartimento. I meccanismi esistenti dell'escalation non hanno evidentemente funzionato in presenza di un siffatto ordine;
- tutt'ora la responsabilità per i temi in materia di sicurezza è spesso equiparata alla responsabilità meramente tecnica dei fornitori di prestazioni. Non c'è una sufficiente consapevolezza della ripartizione dei compiti e delle responsabilità tra fornitori e beneficiari di prestazioni;
- alcuni fornitori di prestazioni affermano che molte volte non hanno la possibilità di imporsi sui beneficiari di prestazioni, dato che non esistono regolamentazioni vincolanti o sufficientemente specifiche. A questo proposito sarebbe necessario precisare le direttive di sicurezza.

Le sinergie tra i fornitori di prestazioni sono considerate frutto del caso. Nel quadro delle verifiche il CDF ha constatato che in diversi settori sono state trovate buone soluzioni. Secondo il CDF queste conoscenze non vengono sufficientemente condivise tra i fornitori di prestazioni e le sinergie non vengono sfruttate abbastanza. Ne consegue che ogni singolo fornitore tende a sviluppare (o a far sviluppare) soluzioni proprie.

Sono in corso numerose attività per la sorveglianza intensificata della rete. I fornitori di prestazioni interessati hanno attuato i primi progetti e stanno raccogliendo le relative esperienze. Sono previste ulteriori tappe, segnatamente per la gestione e l'analisi del flusso di dati. Non tutti i fornitori di prestazioni sono d'accordo sul termine di conservazione di due anni richiesto per i file di registro. Benché esista la volontà di ottimizzare la sicurezza, non bisogna attendersi miglioramenti a breve termine.

La sicurezza delle reti cantonali rimane la «grande incognita». In assenza di una base contrattuale l'Ufficio federale dell'informatica e della telecomunicazione (UFIT) non può accertare la qualità della sicurezza delle reti dei Cantoni collegati né adottare le necessarie contromisure. Con la prevista firma del Service Level Agreement (SLA), rielaborato insieme ai Cantoni, la situazione dovrebbe cambiare entro la fine dell'anno. In diversi Cantoni l'attuazione del SLA, ovvero la garanzia e la prova della sicurezza delle reti cantonali, sarà possibile soltanto a medio termine.

I riscontri pervenuti al CDF lasciano supporre che le applicazioni critiche per la protezione dell'informazione non siano state ovunque completamente identificate dai beneficiari di prestazioni.

Il CDF ha trasmesso, in considerazione del livello gerarchico, diverse raccomandazioni al Consiglio informatico della Confederazione (CIC) e all'Organo direzione informatica della Confederazione (ODIC), come pure ai vari fornitori di prestazioni. Le raccomandazioni indirizzate all'ODIC e al CIC riguardavano la precisazione di direttive, l'intensificazione della collaborazione tra i fornitori di prestazioni nonché la formazione in materia di sicurezza. Dai pareri espressi in forma scritta risulta che le raccomandazioni del CDF sono state accettate.

Testo originale in tedesco