Verifica trasversale concernente le misure in caso di guasti al sistema delle applicazioni specialistiche

Ufficio federale della dogana e della sicurezza dei confini, Amministrazione federale delle contribuzioni, Ufficio federale dell'informatica e della telecomunicazione

L'essenziale in breve

La gestione della continuità operativa (Business Continuity Management, BCM) serve a garantire la continuità delle attività operative di un'organizzazione in caso di evento dannoso. Ciò include la preparazione, la gestione e il follow-up di un evento. Nella primavera del 2017 è stata adottata e messa in vigore dai dipartimenti e dalla Cancelleria federale una regolamentazione concernente il BCM.

Il Controllo federale delle finanze (CDF) ha verificato lo stato di attuazione del BCM presso l'Ufficio federale della dogana e della sicurezza dei confini (UDSC) e l'Amministrazione federale delle contribuzioni (AFC), utilizzando un framework per determinarne il livello di maturità.

Poiché il backup e il ripristino dei dati dopo un evento rappresentano una componente importante del BCM, l'applicazione di sicurezza «NetBackup», messa a punto dall'Ufficio federale dell'informatica e della telecomunicazione, è stata sottoposta a una verifica parallela. In questo contesto, sono stati esaminati la sicurezza dell'esercizio e l'affidabilità dei processi di backup e ripristino.

Il sistema BCM dell'UDSC dispone di un elevato livello di maturità

La documentazione e i piani inerenti al BCM dell'UDSC presentano un grado di dettaglio elevato. Sono stati individuati i processi aziendali critici e la procedura in caso di sinistro è descritta dettagliatamente. Le misure previste sono comprensibili e adeguate all'UDSC. I mezzi informatici che supportano questi processi sono mezzi informatici ridondanti ad alta disponibilità.

Il collaudo e la messa in pratica delle misure BCM sono stati trascurati negli ultimi anni a causa di vari fattori. È disponibile un elenco dettagliato delle esercitazioni previste, che dovranno coprire nei prossimi anni tutti i settori inerenti al BCM.

L'AFC ha compiuto progressi significativi, ma occorre fornire ancora ulteriori lavori

Rispetto all'ultima valutazione del 2016, il BCM dell'AFC ha compiuto importanti progressi. I documenti richiesti sono disponibili, ma alcuni sono troppo generici. Ad esempio, i processi aziendali critici individuati nell'analisi d'impatto sull'operatività (business impact analysis) non vengono seguiti in modo sistematico nella pianificazione.

Non esiste un piano di testing sovraordinato che definisca i vari tipi di test e i gruppi di destinatari. Tuttavia sono stati elaborati piani separati per le singole esercitazioni. L'anno scorso è stata effettuata con successo una prova di evacuazione.

La protezione contro i ransomware ha la massima priorità

I sistemi per la fornitura della prestazione di mercato «backup e recovery» dell'UFIT sono sistemi ridondanti ad alta disponibilità. Le misure di sicurezza implementate soddisfanno i requisiti attuali.

Tuttavia i tempi di ripristino convenuti per contratto non possono essere completamente garantiti per le grandi banche dati a causa delle loro dimensioni.

Uno dei maggiori rischi odierni connesso alla disponibilità dei sistemi e delle banche dati sono i ransomware. Nei sistemi di backup non è ancora stata implementata una protezione specifica contro questo tipo di malware. L'UFIT ha affrontato il problema ed è prevista anche una valutazione esterna per proteggere i backup contro i ransomware. Occorre prioritizzare questa problematica e attuare tempestivamente le eventuali misure.

Testo originale in tedesco