Verifica della resilienza delle TIC delle infrastrutture critiche – attuazione dello standard minimo per i sistemi di controllo ferroviario

Ufficio federale dei trasporti, ferrovia Lausanne-Echallens-Bercher, Trasporti pubblici friburghesi, Zentralbahn e Ferrovia retica

L'essenziale in breve

Le infrastrutture critiche (IC) garantiscono l'approvvigionamento della Svizzera in beni e servizi indispensabili. Al fine di proteggere queste IC occorre mantenere condizioni che garantiscano un funzionamento permanente. In questo contesto, la resilienza delle tecnologie dell'informazione e della comunicazione (TIC), ovvero la protezione delle infrastrutture critiche (PIC) contro le ciberminacce, riveste una grande importanza. L'8 dicembre 2017, il Consiglio federale ha varato la Strategia nazionale per la protezione delle infrastrutture critiche (PIC) per il periodo 2018–2022, nella quale rientra il traffico ferroviario. La Confederazione spende circa 4,5 miliardi di franchi all'anno per il mantenimento della qualità delle infrastrutture ferroviarie e l'ampliamento della rete.

In occasione di una verifica trasversale presso quattro imprese ferroviarie[1], il Controllo federale delle finanze (CDF) ha esaminato se i requisiti minimi per la protezione delle TIC contro i ciberattacchi fossero osservati. A questo scopo è stato utilizzato lo «standard minimo per migliorare la resilienza delle TIC», concepito dall'Ufficio federale per l'approvvigionamento economico del Paese (UFAE). Questo standard ricopre sostanzialmente i cinque settori tematici seguenti: «identificare», «proteggere», «individuare», «reagire» e «ripristinare» e prevede una serie di misure concrete da attuare. L'UFAE raccomanda ai gestori di IC di applicare questo standard minimo per le TIC.

Grandi differenze in materia di sicurezza delle informazioni

Secondo la verifica, la protezione attuale dei dati è molto eterogenea: il suo livello è compreso tra «nettamente sotto il valore minimo raccomandato» e «valore minimo chiaramente superato». Per quanto concerne l'attuazione della sicurezza delle informazioni, sussiste necessità di intervento per tutte le imprese verificate.

Già nel settore dell'organizzazione della sicurezza delle informazioni, è risultato che per tre delle quattro imprese la definizione dei ruoli necessari è insufficiente o mancante. Anche la percezione dei rischi connessi alle TIC da parte dei collaboratori differisce molto.

Un inventario completo dei sistemi e delle informazioni da proteggere costituisce la base principale per attuare la sicurezza TIC. Le imprese ferroviarie ne sono coscienti e tengono un inventario dei propri valori. Questi valori si trovano in parte ancora in diverse fonti di dati senza essere collegati tra di loro. Diversi progetti si prefiggono di migliorare la situazione in futuro.

[1] Ferrovia Lausanne-Echallens-Bercher, Trasporti pubblici friburghesi, Zentralbahn e Ferrovia retica

La gestione degli accessi deve essere migliorata presso tre imprese ferroviarie. Riguardo ad alcuni aspetti, si riscontrano gravi lacune sia nella gestione dei conti utente che nell'assegnazione dei diritti di accesso. I clienti devono avere il controllo degli accessi remoti dei fornitori, che dovrebbero essere documentati in modo chiaro. Al riguardo sussiste una considerevole necessità di intervento per le imprese ferroviarie interessate.

In generale, occorre prestare maggiore attenzione alla sicurezza fisica e ambientale. In un caso, l'accesso alla centrale di gestione non è sicuro e quindi, dal punto di vista tecnico, i sistemi TIC al suo interno non sono protetti da accessi indebiti. I dispositivi per la manutenzione del materiale rotabile sono sbloccati e accessibili in alcuni casi. Per quanto concerne la protezione antincendio vengono attuate misure molto diverse tra loro. Mentre diverse cabine di manovra non dispongono di sistemi antincendio o di rilevamento del fumo e non hanno mezzi estinguenti per il primo intervento, il CDF ha constatato sistemi ridondanti di estinzione automatica negli impianti critici di un'impresa ferroviaria.

La metà delle imprese ferroviarie verificate gestisce diverse centrali operative in luoghi diversi, al fine di non compromettere l'esercizio dell'impianto in caso di guasto.

Sarebbe opportuno prevedere un processo continuo con l'obiettivo di testare scenari d'emergenza e procedure di ripristino. Ciò garantirebbe che, in caso di incidente, i sistemi e i processi continuino a funzionare. Rimane ancora molto da fare per alcune imprese ferroviarie prima di raggiungere un livello adeguato in questo settore.

Prescrizioni sulla sicurezza delle informazioni: una grande sfida per le piccole imprese ferroviarie

La verifica trasversale ha dimostrato che le imprese ferroviarie di maggiori dimensioni sono meglio organizzate in materia di sicurezza TIC rispetto a quelle piccole. A tale riguardo, le piccole imprese devono invece affrontare un'importante sfida in termini finanziari e di personale. Tuttavia, una stretta collaborazione con imprese ferroviarie più grandi e l'acquisto di servizi esterni possono sortire effetti positivi.

Nell'anno in oggetto, l'Ufficio federale dei trasporti (UFT) ha rivisto e adottato le disposizioni d'esecuzione dell'ordinanza sulle ferrovie. Per la prima volta, gli aspetti della sicurezza delle informazioni sono esplicitamente affrontati. Con l'entrata in vigore delle nuove disposizioni d'esecuzione, dal 1° novembre 2020 tutte le imprese ferroviarie sono tenute a sviluppare e attuare un sistema di gestione della sicurezza delle informazioni. Tuttavia, le disposizioni non specificano né i requisiti minimi né il termine da rispettare per l'attuazione. L'UFT sarebbe di grande aiuto alle imprese ferroviarie se precisasse le sue aspettative e mettesse a disposizione strumenti di lavoro adeguati.

Testo originale in tedesco