VERIFICA

Protezione delle infrastrutture critiche – rapporto di sintesi sulle precedenti verifiche incentrate sulla ciber-resilienza

Ufficio federale della protezione della popolazione, Ufficio federale della cibersicurezza, Segreteria di Stato della politica di sicurezza

L'ESSENZIALE IN BREVE

Le infrastrutture critiche sono essenziali per il buon funzionamento dell'economia e per preservare le basi vitali della popolazione. Tra di esse rientrano, ad esempio, l'approvvigionamento elettrico, l'assistenza medica o le telecomunicazioni. La protezione delle infrastrutture critiche (PIC) è di grande importanza.

Oggigiorno non è più possibile assicurare il funzionamento delle infrastrutture critiche senza l'impiego delle tecnologie digitali interconnesse. Questo aumenta tuttavia il rischio di subire ciberattacchi, ragion per cui la cibersicurezza gioca un ruolo chiave nella PIC. Alla luce di quanto precede, il Controllo federale delle finanze (CDF) ha analizzato una selezione di nove verifiche precedenti (vedi allegati 4 e 5) correlate alla PIC e incentrate sulla ciber-resilienza. In base a queste verifiche, il CDF ha desunto sette fattori di successo per una cibersicurezza efficace e per la relativa vigilanza:

Fattori di successo per la cibersicurezza	Fattori di successo per la vigilanza
Definire chiaramente ruoli e responsabilità	Elaborare direttive vincolanti con il coinvolgimento dei settori specialistici e di tutti i livelli federali
Consolidare ed eseguire gli aggiornamenti e il ciclo di vita dei sistemi nei contratti di manutenzione	Garantire la comunicazione e il flusso di informazioni in caso di eventi
Proteggere in modo adeguato le componenti critiche dagli accessi non autorizzati (fisici e digitali)	Sorvegliare e controllare le misure di resilienza in modo capillare
Svolgere esercitazioni per testare i piani di risposta e le organizzazioni per i casi di emergenza	

La cibersicurezza può essere migliorata da subito tramite misure semplici

Spesso semplici misure possono già contribuire sostanzialmente al miglioramento della ciber-resilienza. Ad esempio, un'organizzazione ben strutturata con ruoli e responsabilità chiaramente definiti può avere effetti positivi sull'attuazione dei processi rilevanti per la sicurezza. Una protezione adeguata contro gli accessi non autorizzati ai sistemi e/o alle componenti critiche consente di migliorare notevolmente la sicurezza. Infine, la preparazione a un eventuale attacco può rivelarsi un'ancora di salvezza, perché favorisce la ripresa rapida dell'esercizio delle infrastrutture critiche. I piani di risposta e le esercitazioni sono strumenti utili in tal senso.

I progetti e i periodi di utilizzo di lunga durata nonché le tecnologie obsolete mettono a rischio la cibersicurezza

I progetti di lunga durata e i periodi di utilizzo estesi degli impianti delle infrastrutture critiche rappresentano una sfida per la ciber-resilienza. I sistemi che durante la fase di pianificazione erano considerati all'avanguardia, risultano già obsoleti al momento dell'entrata in funzione. Mentre gli impianti delle infrastrutture critiche restano in uso per decenni, le componenti TIC vanno sostituite ogni tre o quattro anni. Le componenti software necessitano di una manutenzione costante e di aggiornamenti con patch di sicurezza. Un rinnovo costante può però rivelarsi particolarmente costoso e complesso, perciò spesso vi si rinuncia. Di conseguenza, è frequente trovare nelle infrastrutture critiche componenti obsolete e software non aggiornati che presentano note vulnerabilità. Tali sistemi sono bersagli facili per i ciberattacchi.

I gestori delle infrastrutture critiche sono incoraggiati a mantenere i loro impianti e le relative componenti TIC aggiornati tramite architetture di facile manutenzione, pianificazioni sistematiche e misure corrispondenti.

La protezione delle infrastrutture critiche è un compito congiunto e duraturo, ma le condizioni necessarie al suo svolgimento non sono abbastanza vincolanti

Le infrastrutture critiche sono suddivise in settori e settori parziali. Le responsabilità di vigilanza e di regolamentazione vengono assegnate alla Confederazione o ai Cantoni a seconda del settore. Inoltre, molte infrastrutture critiche sono gestite da imprese private. Di conseguenza, la sorveglianza dei gestori da parte delle autorità federali diventa più difficile. Nel caso di un evento concreto, il flusso di informazioni, la comunicazione e da ultima una risposta rapida ed efficace ne risultano ostacolati.

Le tecnologie digitali impiegate cambiano rapidamente. Lo sviluppo e la garanzia di una cibersicurezza solida rappresentano quindi un compito duraturo che però può essere svolto con successo solo se sussiste una collaborazione tra tutte le parti coinvolte. Attualmente, le direttive vigenti che disciplinano la PIC sono incomplete e talvolta non abbastanza vincolanti. Si raccomanda quindi alle autorità settoriali di vigilanza e di regolamentazione di precisare le direttive, affinché si possa richiedere ai gestori delle infrastrutture critiche di rispettare le misure di ciber-resilienza. Al momento della stesura del rapporto di sintesi, sono in atto sforzi da parte della Confederazione per esaminare le basi legali nel settore della PIC.