PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4203 di Venerdì 23 marzo 2018

La sicurezza informatica delle infrastrutture critiche

É stata recentemente condotta negli Stati Uniti una analisi, nel febbraio 2018, sul livello di sicurezza delle infrastrutture critiche, a fronte di attacchi informatici. La situazione riscontrata non è soddisfacente ed occorre intervenire con urgenza.

Questo studio, che è stato condotto negli Stati Uniti dagli ispettori del General accounting Office, ha messo in evidenza alcune situazioni, che sono sicuramente riferibili non solo al mondo americano, ma anche al mondo europeo ed in particolare italiano.

Mentre infatti da tempo si stanno allestendo misure di sicurezza delle infrastrutture critiche, a fronte di attacchi terroristici con ordigni esplosivi e simili, siamo ancora indietro per quanto riguarda la messa a punto di efficienti ed efficaci sistemi di protezione delle infrastrutture informatiche.

Negli Stati Uniti è già stata pubblicato una preziosa normativa dall'istituto nazionale per le normative le tecnologie - NIST, chiamata "quadro di riferimento per migliorare il livello di sicurezza delle infrastrutture critiche da attacchi informatici".

Lo studio ha messo in evidenza come la cybersecurity lasci ancora molto a desiderare, mentre gli interventi fatti per la difesa fisica delle strutture sembrano soddisfacenti.

I problemi che sono stati messi in evidenza mettono in evidenza le seguenti aree, che temo purtroppo possano essere parimenti applicabili anche in Italia:

- Le infrastrutture critiche non sempre dispongono delle sufficienti risorse per attivare efficienti ed efficaci protezioni informatiche,
- Non sempre sono disponibili le conoscenze e le competenze necessarie per attuare misure di sicurezza informatica,
- Possono essere presenti leggi e regolamenti che potrebbero rallentare l'adozione delle misure di sicurezza informatica,
- Le infrastrutture devono fronteggiare anche altri scenari di rischio, che potrebbero avere priorità rispetto ai rischi legati alla sicurezza informatica.

Negli Stati Uniti il dipartimento della sicurezza nazionale richiede che tutti i responsabili di infrastrutture critiche riferiscano, a scadenza almeno annuale, sullo stato di attuazione di interventi di protezione delle infrastrutture stesse, indicando anche degli obiettivi temporali, entro i quali misure non ancora attuate dovrebbero essere attuate.

Tuttavia l'analisi ha messo in evidenza che nessuna delle 16 infrastrutture analizzate ha potuto rispettare questa indicazione, per motivi legati a uno o più dei problemi che sono stati illustrati in precedenza.

Ricordo che una infrastruttura critica include sistemi pubblici e privati, che trattino beni e servizi essenziali per la sicurezza nazionale, per la stabilità economica, per la sicurezza della salute pubblica ed altro. Ad oggi i coordinatori federali hanno individuato 16 settori critici, ivi inclusi i servizi finanziari, l'energia, i trasporti e le comunicazioni. Il motivo per cui questo studio può essere prezioso anche in Europa ed in Italia è legato al fatto che anche in Italia alcuni di questi settori sono stati già inseriti nei piani di sicurezza nazionale ed europea.

Ricordo che una infrastruttura critica europea, tale quindi che una sua indisponibilità più o meno lunga possa avere riflessi su almeno altri due paesi europei, è tale se opera nel settore dell'energia e dei trasporti. L'Europa si sta già attivando perché vengano introdotti anche altri settori, per i quali occorre sviluppare il piano di sicurezza dell'operatore, individuare un responsabile per l'interfacciamento con altri organi coinvolti e per tenere sotto controllo il piano di analisi dei rischi e di pianificazione delle misure di messa sotto controllo.

Per esperienza diretta, ad oggi l'attenzione posta alla difesa fisica delle infrastrutture critiche è decisamente superiore a quella posta alla difesa dei sistemi ICT, forse anche per la mancanza di specialisti del settore.

È del tutto probabile che la entrata in vigore a pieno ritmo del nuovo regolamento generale europeo sulla protezione dei dati 679/2016, che prevede stringenti regole per la protezione dati personali, possa portare benefici anche ad un miglioramento del livello generale di sicurezza dei sistemi informativi, che possono trattare anche aspetti funzionali ed operativi, comunque privi di dati personali.

Quando una misura di sicurezza è tale da proteggere in maniera efficace un dato personale, con ogni probabilità è in grado di proteggere in maniera altrettanto efficace anche un dato relativo ad un assorbimento energetico, o altro parametro legato alla funzionalità specifica della infrastruttura critica sotto controllo.

Per questa ragione metto a disposizione dei lettori la relazione effettuata dagli ispettori del General accounting Office, perché alcune preziose indicazioni possano essere recepite anche nel nostro paese.

Vedi allegato (pdf)

Adalberto Biasiotti

www.puntosicuro.it