PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 25 - numero 5332 di Venerdì 17 febbraio 2023

Infrastrutture critiche e utilizzo di Internet

Sono numerose le infrastrutture critiche che abbisognano, per funzionare correttamente, di efficienti collegamenti a Internet per esigenze di comunicazioni e operative. Uno studio mette in evidenza alcuni aspetti critici di questa funzionalità.

Le infrastrutture critiche nazionali fanno affidamento su sistemi elettronici, tra i quali si trova l'Internet of Things (IoT) e le tecnologie operative (OT).

IoT per solito fa riferimento a tecnologie ed apparecchiature che consentono le interconnessioni di rete e l'interazione con un gran numero di "oggetti", nel mondo delle infrastrutture del trasporto, delle abitazioni, delle costruzioni e simili.

Per contro, con l'espressione OT si fa riferimento a sistemi programmabili o apparecchiature che interagiscono con l'ambiente fisico, come ad esempio sistemi di automazione di edifici, movimentazioni ascensori, gestione di impianti di condizionamento e trattamento dell'aria e via dicendo.

Per aiutare le agenzie federali e gli enti privati a gestire i rischi di sicurezza informatica associati con questi due mondi, il Dipartimento della sicurezza nazionale, ed in particolare l'agenzia per la sicurezza informatica delle infrastrutture, ha pubblicato un prezioso documento e ha messo a disposizione risorse specifiche.

In particolare, vengono lanciati, quando appropriato, dei segnali di allerta per la presenza di criticità, che coinvolgano sia i sistemi IoT, sia i sistemi OT.

In particolare, gli investigatori hanno analizzato in profondità tre particolari categorie di infrastrutture critiche, rispettivamente legate alla gestione dell'energia, della salute pubblica e dei sistemi di trasporto.

Per quanto riguarda il settore dell'energia, sono stati avanzati suggerimenti afferenti alla messa sotto controllo dei sistemi di distribuzione dell'energia attraverso la rete, che permettono di aggirare interruzioni temporanee o potenziare l'invio di energia durante periodi di picco della richiesta.

Per quanto riguarda il settore della salute pubblica, gli specialisti hanno avanzato tutt'una serie di raccomandazioni, da trasmettere a tutti coloro che sviluppano apparati medici, come ad esempio apparati diagnostici, perché introducano dei criteri di sicurezza intrinseca, in grado di diminuire la probabilità che un attacco via Internet possa compromettere la funzionalità degli apparati.

Per quanto riguarda i sistemi di trasporto, è stata messa a punto una serie di strumenti, che possono mettere sotto controllo il rischio informatico, mettendo ad esempio sotto stretto monitoraggio gli aspetti meccanici dei dispositivi di trasporto, con particolare riferimento ai sistemi utilizzati nelle linee ferroviarie critiche.

Il documento è completato da alcuni esempi di tipi di attacchi informatici e della illustrazione delle modalità con le quali è possibile effettuare interventi di prevenzione e mitigazione del rischio.

Il documento, composto da 72 pagine, rappresenta una preziosissima guida per tutti gli esperti di sicurezza informatica, che operino nell'ambito di infrastrutture critiche, che facciano riferimento significativo alle due architetture informatiche illustrate.

Vedi allegato (pdf)

Adalberto Biasiotti

---

www.puntosicuro.it