Stefano Panzieri - Intervista al Forum ICT Security 2018

Author : Redazione

Date : 13 novembre 2018

Stefano Panzieri

Professor of Automatic Control at Department of Engineering of the University of Roma Tre

Negli ultimi anni il mondo industriale, come quello delle infrastrutture critiche, si è notevolmente modificato. La vecchia sala controllo oggi non esiste più, ci sono device che possono essere utilizzati sul campo che presentano aspetti informativi e operativi che gli addetti alla manutenzione o al controllo del processo utilizzano per poter operare correttamente sull'impianto. I perimetri non esistono più e di conseguenza è cambiato anche l'approccio alla sicurezza. Dove l'IoT introduce dispositivi più piccoli e quindi più "indifesi" è necessario fare un passo in più perché la maggior parte di questi non fa uso di criptazione, non fa uso di certificati ed è quindi in balia di qualsiasi attaccante.

Esistono da sempre dispositivi honey pot che fingono di essere qualcos'altro e consentono l'individuazione di un attacco, ma oggi se ne possono trovare alcuni che lavorano direttamente all'interno dei sistemi di controllo industriale fingendo di essere un controllore a logica programmabile, un PLC, oppure fingono di essere un intero sistema SCADA ingannando l'attaccante. Bisogna far lavorare insieme ingegneri informatici, dell'automazione, delle telecomunicazioni e di processo, ovvero gli esperti della parte fisica in grado di dire se i comandi che vengono inviati ai dispositivi sono buoni o meno

Domande:

1. Nell'odierna tavola rotonda si è parlato di IoT industriale e della sue interazioni con la sicurezza "fisica", potenzialmente devastanti in caso di attacco. Dove individuerebbe le principali vulnerabilità?

2. In questo scenario, quale ruolo giocano i dispositivi di campo ad hoc per la cyber security industriale?

Vai all'evento Forum ICT Security 2018