Differenza tra sicurezza IT e OT

A ottobre 2018, Daniel Ehrenreich, esperto di sicurezza della “tecnologia operativa” (OT), ha pubblicato un breve articolo su LinkedIn con l’immagine che accompagna questo articolo.

In sostanza dice che chi si occupa di sicurezza informatica (orientata alla difesa di riservatezza, integrità e disponibilità) non può riutilizzare gli stessi concetti legati alla sicurezza della tecnologia “operativa”.

Il termine OT (Operational technology) è definito, dal sito Gartner, come “l’insieme di hardware e software che rileva o causa cambiamenti attraverso il monitoraggio o il controllo diretto di dispositivi fisici, processi ed eventi di un’impresa”. È usato per elencare un vasto insieme di strumenti, inclusi quelli ICS (Industrial Control Systems) e SCADA.

Daniel Ehrenreich asserisce che la sicurezza per OT si concentra sulla difesa di sicurezza fisica (safety), affidabilità (reliability) e produttività (productivity), parametri evidentemente diversi da quelli della sicurezza informatica. Per questo la “convergenza di sicurezza IT e OT” non è realizzabile e la promuovono solo consulenti di sicurezza IT che cercano di estendere il proprio mercato senza averne le competenze.

Caratteristiche della sicurezza OT

È necessario ricordare che la sicurezza OT deve includere elementi ignorati da chi si occupa dei sistemi informatici “di ufficio”.

Per esempio, quando si tratta di sistemi OT è necessario considerare elementi come:

- comportamento del sistema in caso di assenza di alimentazione;
- comportamento del sistema in fase di avvio o riavvio e in fase di spegnimento;
- separazione completa dei sistemi di sicurezza fisica dagli altri sistemi;
- presenza sulla rete di dispositivi obsoleti e non più mantenuti dal produttore;
- condivisione dei macchinari tra più operatori;
- necessità di accesso in situazioni di emergenza;
- protezione dai fattori ambientali (polvere, calore, eccetera).

Al di là della complessità tecnica, è importante riconoscere la differenza di sensibilità necessaria per affrontare le due materie.

Un classico esempio, forse una leggenda metropolitana, è fornito da un esperto di “sicurezza informatica” che voleva fosse impostata una password nel sistema di blocco in emergenza di un macchinario. Inutile specificare perché avesse torto.

Più complesso è comprendere che le tecnologie usate possono essere molto diverse rispetto a quelle IT e così le architetture da realizzare per assicurare la sicurezza ed efficienza dei sistemi OT.

Conclusione

Il post su LinkedIn esprime forse concetti troppo estremi. Infatti, anche la sicurezza OT deve considerare la riservatezza, per esempio delle ricette e dei progetti, che possono essere recuperati dalle macchine.

È innegabile, però, che, per affrontare bene una materia, è necessario capirne la cultura di fondo. Questo vale, per esempio, quando si tratta di sicurezza delle informazioni

(orientata alla protezione di un'organizzazione), di sicurezza dei dati personali (orientata alla protezione degli interessati) o di qualità del servizio informatico (orientata alle aspettative del cliente). Ogni materia ha le sue peculiarità e queste vanno capite e apprezzate prima di farle "convergere".

Nota

L'articolo di Daniel Ehrenreich si trova all'URL https://www.linkedin.com/pulse/itot-cyber-security-experts-daniel-ehrenreich.

L'immagine di copertina è di SCCE – Daniel Ehrenreich.

Articolo a cura di **Cesare Gallotti**

Lavora dal 1999 nel campo della sicurezza delle informazioni, della qualità e della gestione dei servizi IT.

Ha condotto progetti di consulenza per la pubblica amministrazione e per il settore privato. Opera, sia in Italia che all'estero, come Lead Auditor ISO/IEC 27001, ISO 9001, ISO/IEC 200000 e ISO 22301. Ha progettato ed erogato corsi di Quality Assurance e di certificazione Lead Auditor ISO/IEC 27001 e ITIL Foundation.

Tra gli attestati si segnalano: le certificazioni AICQ SICEV Lead Auditor ISO/IEC 27001, IRCA Lead Auditor 9001, CISA, ITIL Expert e CBCI, la qualifica come Lead Auditor ISO/IEC 20000 e il perfezionamento postlaurea in "Computer Forensics e investigazioni digitali".

E' capodelegazione del WG1 del comitato italiano ISO/IEC SC27 in UNINFO.

Ha pubblicato il libro, aggiornato nel 2017, "Sicurezza delle informazioni: valutazione del rischio; i sistemi di gestione;

la norma ISO/IEC 27001:2013”.

Cura la pubblicazione, dal 2008, della newsletter “IT Service management news” (http://www.cesaregallotti.it/Newsletter.html).

Web: www.cesaregallotti.it; Blog: blog.cesaregallotti.it

https://www.ictsecuritymagazine.com/articoli/differenza-tra-sicurezza-it-e-ot/