Sommario Rassegna Stampa

Pagina	Testata	Data	Titolo	Pag.
Rubrica	**Anie**			
46/47	Automazione Industriale	01/04/2015	*NON CI SARA' INDUSTRY 4.0 SENZA SICUREZZ*	2

Automazione Industriale
Mensile
Data 04-2015
Pagina 46/47
Foglio 1 / 2

Hot Topic Cybersecurity

Non ci sarà Industry 4.0 senza sicurezza

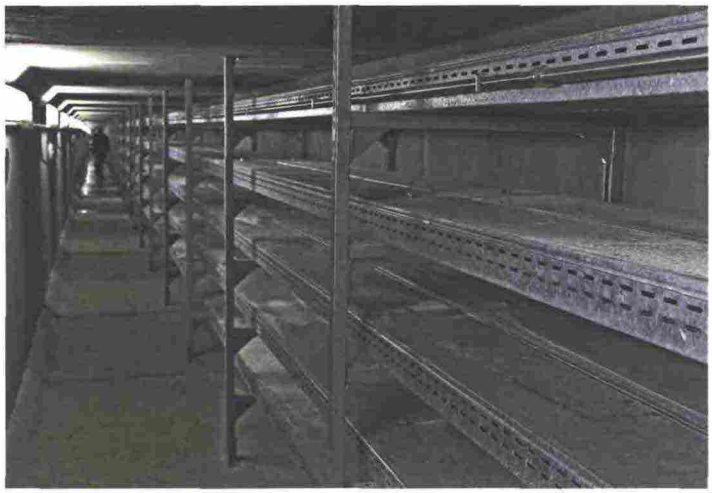
Di fronte al crescente numero di attacchi informatici, il mondo industriale è chiamato a riflettere su come fronteggiare una situazione che compromette anche la sicurezza fisica

di **Massimiliano Cassinelli**

L'integrazione tra i processi di automazione industriale e le tecnologie Ict potrebbe essere frenata dalle problematiche di sicurezza. Questo perché con l'apertura di reti e protocolli, i cyber-criminali hanno trovato una nuova opportunità di guadagno, in un settore in cui la cultura della security non è ancora radicata. Eppure, com'è emerso dall'annuale Rapporto Clusit sulla sicurezza Ict, gli attacchi informatici, a tutti i livelli, sono sempre più numerosi ma, soprattutto, sempre più pericolosi. Come si legge nel documento: "Non è più possibile utilizzare strumenti informatici senza, per questo stesso fatto, essere costantemente sotto attacco". I cyber-criminali, indipendentemente dalla loro natura e dai loro scopi, sono attratti da sostanziosi guadagni e appaiono in continuo aumento, oltre che sempre più organizzati. Sfruttano, inoltre, strumenti totalmente automatizzati, in grado di colpire milioni di sistemi in poche ore, indipendentemente dalla posizione geografica. Una situazione, si legge nel rapporto, aggravata dai possibili effetti sistemici: "Da un lato, sofisticate tecniche di attacco sviluppate da team governativi (anche queste poi 'riciclate' dall'underground criminale, come nel caso del malware Gyges) sono già usate su larga scala da un certo numero di nazioni con finalità di spionaggio e di infiltrazione dei sistemi altrui, allo scopo di fare 'pressione' sui bersagli e/o di poterli danneggiare o disattivare, e dall'altro strumenti analoghi stanno entrando nella disponibilità di organizzazioni terroristiche, che si approvvigionano di tramite gruppi cyber criminali".
Le possibili conseguenze di questa selvaggia corsa ai cyber-armamenti (ambito non normato a livello internazionale) sono devastanti, sia perché potrebbero essere prese di mira le infrastrutture critiche, sia "perché crescono i servizi erogati da aziende private e da pubbliche amministrazioni che, se resi indisponibili a seguito di un attacco, creerebbero enormi disagi alla popolazione e, in certi scenari, anche perdite di vite umane".

Problematiche da non rimandare

Quello della cybersecurity era quindi un tema che non poteva mancare nel corso della tavola rotonda 'Automazione 4.0: il futuro è già qui?', organizzata recentemente da Anie Automazione in vista di Sps Italia del prossimo maggio. Questo anche in considerazione del fatto che da una ricerca, condotta tra le aziende americane, solo il 14% delle realtà coinvolte ha dichiarato di avere una perfetta integrazione tra It e Operation. Ciò significa che, al di là del notevole lavoro da svolgere per sfruttare davvero le tecnologie informatiche, è necessaria una notevole attenzione anche a tutte le problematiche di security, che non possono più essere trascurate.
Del resto, Giambattista Gruosso, del Politecnico di Milano, ha rimarcato che l'industria, pur sfruttando sempre più le tecnologie informatiche, "ha notevoli esigenze in termini di sicurezza e affidabilità dei dati stessi, al punto che la sicurezza è stata una delle sfide identificate dal Governo tedesco, già in fase di stesura della roadmap sull'Industry 4.0".



Safety e security sono sempre più correlate nell'industria moderna

Safety e security non sono più divise

Il problema è ben noto anche alle industrie di settore, al punto che Roberto Motta di Rockwell Automation non ha esitato a rimarcare il notevole impatto delle nuove tecnologie: "Viviamo un cambio di approccio; le nuove macchine sono progettate tenendo conto di tutte le innovazioni tecnologiche esistenti, anche se questo implica la necessità di dover gestire, oltre alla sicurezza fisica delle persone, anche la security, ossia la sicurezza dei dati". Una situazione che, come dice sempre Motta, "impone un cambio culturale, non solo tecnologico".

Tale svolta, come sottolinea Luca Bogo di Pilz, sta cambiando anche il rapporto tra sicurezza fisica e logica. Del resto, in passato, le due tematiche erano sistematicamente separate, mentre ora si stanno sempre più sovrapponendo. È, infatti, immediato comprendere come una violazione dei sistemi di controllo potrebbe mettere a repentaglio anche l'incolumità delle persone. Ma Bogo va oltre, spiegando come l'Ict può contribuire alla sicurezza fisica, anche se bisogna prestare attenzione al rischio di mettere a repentaglio la privacy delle persone e i diritti dei lavoratori: "A volte, per garantire la sicurezza, è necessario limitare l'efficienza della persone e delle macchine. Per questa ragione stiamo usando le protesi tecnologiche di ogni persona per aumentarne la sicurezza. In particolare crediamo che l'IoT possa permettere a una macchina di riconoscere chi si avvicina e di settarsi in base al profilo delle persone presenti. É però necessario ricordare che si tratta di tecnologie molto specifiche, chiamate a identificare il ruolo e le competenze di una persona, ma non i suoi dati anagrafici, perché altrimenti si violerebbe la privacy dei lavoratori stessi".

Se il dato supera il prodotto

Malgrado i limiti, anche normativi, Marino Crippa di Bosch Rexroth si è spinto a esasperare il concetto: "La sicurezza logica è diventata un elemento chiave nei processi industriali, arrivando ad assumere un'importanza che può superare anche quella della sicurezza fisica". Anche per questa ragione, "servono standard che noi abbiamo scelto aperti, per supportare l'evoluzione tecnologica e cogliere subito le innovazioni del mondo IT; integrazione e conoscenza delle tecnologie sono sempre più essenziali oggi e, soprattutto, lo saranno nel prossimo futuro. La rivoluzione non è sfruttare Internet, magari reso più robusto, ma pensare il processo produttivo e il prodotto in modo che sappiano assecondare la volatilità del mercato".

Un cambio di paradigma realmente significativo, al punto che Motta ha spiegato come "uno degli aspetti più interessanti dell'Industry 4.0 sia legato al fatto di utilizzare, anche nel mondo industriale, una serie di dispositivi provenienti dal mondo Office e persino dal Consumer". Oltre allo smartphone impiegato nella supervisione dei processi industriali, Motta ha portato l'attenzione sul fenomeno Cloud: "L'industria è tra i maggiori collettori di dati che, proprio perché eterogenei, possono fornire le informazioni più svariate, che devono essere sfruttate in modo opportuno. Anche perché è cambiata la struttura delle informazioni legate a un processo industriale: in passato esisteva una struttura piramidale, con un flusso accuratamente predeterminato. Oggi, al contrario, lo scambio dei dati avviene come attraverso una ragnatela, eliminando le gerarchie tradizionali.

Da qui deriva la necessità di integrare, correttamente, tecnologie che provengono da un mondo diverso rispetto a quello dell'automazione e del manifatturiero". ■