

## eventi



■ Evento incentrato sul tema della sicurezza industriale, ICS Forum ha catturato l'attenzione di imprenditori, manager e tecnici di produzione e dei reparti IT, desiderosi di scoprire strategie e strumenti per orientare le proprie scelte d'innovazione.

# Cyber Security industriale

Oltre 500 partecipanti al primo vero approfondimento sul tema della sicurezza informatica nell'industria, che ha visto confrontarsi esperti tecnici, legali e assicurativi

a cura della Redazione

«La Cyber Security è un fattore di sviluppo, un asset critico per fare bene business, un servizio fondamentale per chi vuole investire in Italia»: questa frase del professor Stefano Panzieri, dell'Università degli Studi Roma Tre, riassume perfettamente quanto emerso lo scorso 30 gennaio a Milano in occasione di ICS Forum, Mostra convegno organizzata da Messe Frankfurt Italia in collaborazione con Innovation Post.

Un evento incentrato sul tema della sicurezza industriale, che ha catturato l'attenzione di oltre 500 imprenditori, manager e tecnici di

produzione e dei reparti IT, desiderosi di scoprire strategie e strumenti per orientare le proprie scelte d'innovazione.

«Siamo felici di aver saputo rispondere a un'esigenza d'informazione su un tema importante come quello della Cyber Security industriale che avevamo colto a più riprese nel corso dei tanti eventi dedicati al settore manifatturiero organizzati in questi anni. Anche a SPS IPC Drives Italia, la fiera italiana dell'automazione e del digitale per l'industria, la sicurezza informatica sarà tra i temi caldi», ha commentato Donald Wich, Amministrato-

re Delegato di Messe Frankfurt Italia che ha aperto la giornata con il suo saluto di benvenuto, insieme a Fabio Massimo Marchetti, Presidente del Gruppo Software di ANIE Automazione.

Enzo Maria Tieghi, Presidente dello Steering Committee e CEO di ServiTecnò, ha introdotto la giornata soffermandosi sul legame tra Cyber Security e continuità operativa. Subito dopo è intervenuto con un video messaggio Andrea Zapparoli Manzoni, esperto di Cyber Security e membro del consiglio direttivo del Clusit, che si è soffer-



■ Enzo Maria Tieghi, Presidente dello Steering Committee e CEO di ServiTecno, ha introdotto la giornata, soffermandosi sul legame tra Cyber Security e continuità operativa

mato sulle principali minacce per un'industria sempre più connessa, ma non protetta, e suggerendo alle aziende d'investire in tecnologie testate e sicure "by design".

### Tra tecnologie e fattore umano

Dal primo momento plenario – la tavola rotonda di esperti del settore Raoul Brenna (CEFRIEL), Domenico Billè (Oracle), Roberto Zuffada (Siemens), Massimo Scanu (ABB), Fabio Sammartino (Kaspersky), Antonio Mado-

glio (Fortinet), Giuseppe Cardinale Ciccotti (UniquID) – è emersa l'importanza assoluta del fattore umano come chiave di volta per una cultura diffusa nell'impresa che metta la sicurezza al centro dei processi aziendali. Ci si è soffermati anche sulle tecnologie in grado di aiutare a rispondere alle cyber minacce, dal machine learning all'intelligenza artificiale fino alla blockchain.

Francesco Laera ha, poi, spiegato perché la Commissione Europea sta affrontando la que-

stione Cyber Security con l'istituzione di un'Agenzia, mentre Alvisè Biffi, di Assolombarda, ha illustrato che cosa si sta facendo in Italia per supportare anche le PMI in un percorso che parta, innanzi tutto, da una valutazione della propria posizione.

Durante la seconda tavola rotonda si sono susseguiti gli interventi di Stefano Mele e Andrea Maggipinto, che hanno parlato del GDPR, della Direttiva NIS (Network and Information Security) e della Direttiva 943/2016 sul segreto industriale, tutte di imminente applicazione anche in Italia, evidenziando tra l'altro come conformarsi a queste normative sia un'opportunità per le imprese prima ancora che un vincolo. Raffaele Esposito (Phoenix Contact) e Eugenio Rizzi (Bureau Veritas) hanno parlato di normative tecniche e standard come la IEC 62443 e la ISO 27001, sottolineando anche loro come l'adozione di sistemi sviluppati in conformità a una normativa internazionale possa aiutare le imprese a ridurre i rischi.

Cristiano Cerri (Zurich) e Cesare Burei (Margas) hanno, infine, spiegato perché un'assicurazione può contribuire letteralmente a salvare le aziende in caso di un cyber-incidente, incentivando, quindi, le organizzazioni a stipulare una polizza assicurativa e all'adozione di tecnologie di protezione.

### I protagonisti e le tecnologie per un'industria connessa e sicura

La sessione pomeridiana si è aperta con i key note speech del professor Stefano Panzieri, che ha presentato il progetto Atena, e di Alberto Volpato (Secure Network), che ha messo a nudo l'insicurezza dei sistemi SCADA. Questi interventi hanno introdotto due tavole rotonde nelle quali rappresentanti di aziende fornitrici di servizi e tecnologie come Manuel Alessi (Alascom), Andrea Argentin (Cyberark), Giuseppe Linati (Digital Innovation Hub Lombardia), Dario Amoroso e Giancarlo Castronovo (KPMG con ESA Automation), Roberto Motta (Rockwell Automation), Alessandro Galmuzzi (Schneider Electric), Marco Zanovello (Var Group) si sono confrontati con esponenti di imprese che hanno già avviato percorsi di messa in sicurezza dei propri asset: Chiara D'Epifanio (Barilla), Antonio Giustino (Solvay), Marco Scognamiglio (Saipem), Gian Luigi Pugni (Enel) e Ivan Basso (Fluid-o-Tech).

Molto apprezzati anche i workshop di Siemens, Phoenix Contact, Schneider Electric, Gruppo Sigla/Stormshield, Kaspersky, ESA Automation/KPMG, Fortinet e Servitecno che hanno rappresentato un'occasione in più per approfondire il tema.



■ L'intervento del professor Stefano Panzieri ha presentato il progetto Atena, che si propone di individuare tecnologie e architetture per la sicurezza dei sistemi SCADA