Atti del convegno

Industrial Network Security: come proteggere le infrastrutture 4.0?

L'evento LAPP dello scorso 21 giugno pone l'accento sulle misure necessarie per un'industria sempre più connessa e protetta

Si è svolto lo scorso 21 giugno, a Bologna, l'evento organizzato da **LAPP**, *leader nello sviluppo e produzione di soluzioni integrate nella tecnologia di connessione e cablaggio*, dedicato a **"Industrial Network Security: come proteggere le infrastrutture 4.0?"**. Grazie a un panel di relatori di spicco, tra cui esperti in materia di *Industrial Cyber Security* dell'**Università di Genova** e referenti di **Alleantia** e **Bureau Veritas Nexta**, i partecipanti hanno avuto modo di approfondire i potenziali rischi di sicurezza delle reti in ambito OT, ancora oggi troppo spesso sottovalutati e le opportune misure di prevenzione da adottare nelle **Smart Factory**.

Roberto Pomari, AD di **LAPP Italia**, ha aperto la giornata di lavori e ha specificato come l'Italia sia il secondo Paese in Europa, dopo la Germania, per quanto riguarda il mercato degli OEM. "*Essere riconosciuti come unico Partner per ogni esigenza di cablaggio e networking di fabbrica è il nostro obiettivo, che perseguiamo attraverso un'offerta qualificata e diversificata di soluzioni, anche personalizzate e servizi dall'elevato valore aggiunto. Il networking è nel nostro DNA, per connettere reti e persone. Per questo siamo felici di poter nuovamente organizzare eventi in presenza e continuare così a diffondere conoscenza su aspetti oggigiorno fondamentali, come quello dell'Industrial cyber security*".

Il moderatore **Rodolfo Zunino**, *Professore ordinario del Dipartimento di Ingegneria navale, elettrica, elettronica e delle telecomunicazioni presso l'Università di Genova*, ha poi introdotto i concetti di *Safety* e *Security*. "*Quest'ultima* – spiega Zunino – *è stata introdotta in un secondo tempo e tutt'ora è spesso trascurata nell'iter progettuale di alcuni sistemi industriali. Per fare Industria 4.0 e cogliere appieno le opportunità derivanti dalla digitalizzazione, occorre un cambio di paradigma, ovvero superare la classica distinzione tra le due sfere della sicurezza, che oggi sono diventate una cosa sola"* e continua *"Sono tre i pilastri della cyber security: la tecnologia, la governance e, forse il più rilevante, la formazione. Queste tre componenti, in realtà, sono rilevanti in egual misura. Ciò implica la necessità di un approccio integrato orientato alla sicurezza e volto, oltre all'adozione di tecnologie efficaci, anche alla loro gestione e alla formazione del personale, da cui deve emergere una maggiore consapevolezza. È anche per questo motivo che sono nate le certificazioni di Cyber Security in ambito OT*".

Il Prof. **Lorenzo Ivaldi**, *Dipartimento di ingegneria navale, elettrica, elettronica e delle telecomunicazioni dell'Università di Genova,* ha esplorato il concetto di sicurezza informatica

degli IACS (*Industrial Automation & Control System*), le cui linee guida sono definite dalla serie di standard **ISO/IEC 62443**. "*Al fine di predisporre un corretto piano di cyber security industriale, la norma richiede prima di tutto la mappatura di tutti gli impianti, con l'obiettivo di definirne l'attuale livello di sicurezza. Molto spesso, infatti, negli stabilimenti non si tiene traccia degli interventi di sostituzione, riparazione o modifica. Le zone e i flussi di dati devono quindi essere certi per procedere con l'analisi di business continuity, volta ad identificare il grado di protezione che si desidera raggiungere, in funzione delle vulnerabilità rilevate"* spiega **Ivaldi**. Il relatore è poi entrato nel merito della **IEC 62443-3-1**, relativa alla sicurezza delle reti e dei sistemi, specificando l'importanza del controllo degli accessi, sia impostando livelli di autenticazione e autorizzazione, che attraverso la segmentazione delle reti, per consentire al solo traffico ammesso di transitare da un'area all'altra. Un aspetto ancor più rilevante nelle aree produttive automatizzate dove sono presenti sistemi di gestione in *real-time.* La presentazione è stata completata da un'*overview* sulla **IEC 62443-4-2**, che si occupa delle caratteristiche dei componenti che vengono inseriti in un sistema industriale.

L'intervento di **Marco Artoli**, *Project Manager Industrial Communication* di **LAPP***,* ha ulteriormente analizzato la **segmentazione** e **segregazione** delle reti. "*Come evidenziato anche dagli speech precedenti, la trasformazione digitale espone le Aziende a maggiori possibilità di attacchi informatici, sia di tipo volontario, che involontario*" spiega **Artoli**, che continua "*Il livello base della norma 62443, infatti, riguarda la limitazione dei rischi legati a manomissioni e danni accidentali, causati da quelle che possiamo definire operazioni "maldestre" e che, nella realtà dei fatti, hanno probabilità più elevate di verificarsi rispetto all'attacco cyber. Come LAPP, ci siamo concentrati sull'aspetto fondamentale che riguarda la delimitazione di specifiche zone, con punti di accesso ben precisi, da cui possono transitare solo le informazioni necessarie e una serie di filtri su chi può accedervi".* Tutto questo si è tradotto nello sviluppo di un dispositivo, lo switch ETHERLINE ACCESS NAT/Firewall, in grado sia di creare tali filtri che di effettuare la traduzione degli indirizzi IP delle macchine alla rete di fabbrica (WAN), senza dover adattare i singoli nodi della rete.

ETHERLINE ACCESS NAT/Firewall di LAPP è stato altresì il protagonista dell'esempio pratico di attacco, sia involontario che volontario, eseguito da **Ulisse Quartucci**, del *Genoa Fieldbus Competence Centre (GFCC).* Nel primo caso, i partecipanti hanno avuto modo di osservare come la semplice interconnessione *plug and play* di due macchine tramite switch, possa causare il malfuzionamento della rete, in quanto gli indirizzi IP o i nomi dei dispositivi potrebbero essere duplicati. Il problema è stato risolto attraverso la funzionalità NAT *(Network Address Translation)* per la segregazione logica delle reti. Per quanto riguarda l'intervento volontario, **Ulisse Quartucci** ha simulato un attacco al PLC di una macchina connessa in rete, utilizzando un *exploit* facilmente accessibile da *searchsploit.* Come risultato, è stata dimostrata l'efficacia di uno stretto controllo dell'accesso alle reti per proteggere l'impianto, mediante un

firewall con regole dedicate, possibilmente attivabili su richiesta. In tal senso, il firewall ETHERLINE ACCESS N/F supporta la funzionalità di attivazione regole tramite input esterno: in questo modo, l'accesso può essere consentito solo attraverso il contatto con serratura a pannello.

Antonio Conati Barbaro, *Chief Operating Officer* di **Alleantia** – *Azienda specializzata nell'Industrial Internet of Things* – ha dapprima preso in considerazione i c.d. "Cyberincubi in Fabbrica", come il mancato utilizzo delle password, i sistemi operativi obsoleti che non possono essere aggiornati, il fatto che ogni costruttore fornisca una sua VPN e, ancora, la carenza sul mercato di esperti in sicurezza. L'intervento è proseguito con la descrizione dell'Industrial IoT come "Security Wrapper", ovvero come layer di protezione di macchine, dati e applicazioni IT e delle diverse possibilità di rinforzare tali strati IIoT con funzionalità integrate proprie di piattaforme di cyber security. Inoltre, l'Ing. **Conati Barbaro** ha illustrato la partnership con LAPP volta all'evoluzione del "cavo *as a service*" grazie a ETHERLINE GUARD. Un dispositivo in grado di monitorare, in tempo reale, lo stato di efficienza del cavo di rete collegato a un robot o in una catena portacavi. Informazioni che, oltre a concorrere alla definizione della Overall Equipment Effectiveness (OEE), sono utili per l'invio di alert di controllo o sostituzione e per l'eventuale integrazione con marketplace, per la richiesta automatica di un nuovo cavo LAPP.

In ultimo, ma non per importanza, **Paolo Lama**, *Industry Engineering & Consulting Business Developer* di **Bureau Veritas Nexta**, si è soffermato sui requisiti di sicurezza informatica della Direttiva 2006/42/CE e della proposta per il nuovo Regolamento Macchine che la sostituirà, una volta terminato l'iter di approvazione, con le relative ricadute in termini di marcatura CE. "*A differenza dell'attuale Direttiva, il Regolamento sarà applicabile senza ulteriore attuazione da parte dei singoli Paesi dell'UE. Attualmente, il nuovo testo è in fase di analisi da parte dei comitati tecnici. Una volta entrato in vigore, sarà predisposto un periodo transitorio di 2-3 anni per consentire ai costruttori di macchine di adeguarsi alla nuova legislazione*" spiega Lama, che continua "*Salvo sensibili modifiche prima della pubblicazione definitiva, tra le principali novità vi è la definizione di "componente di sicurezza" che, per la prima volta, introduce anche i componenti digitali, inclusi i software che svolgono funzioni di sicurezza immessi sul mercato separatamente, i quali dovranno essere marcati CE ai sensi del regolamento macchine ed essere accompagnati da una dichiarazione di conformità UE e dalle istruzioni per l'uso*".

A conclusione dei lavori, oggetto della tavola rotonda sono stati principalmente sia i requisiti del nuovo Regolamento Macchine, sia le sfide per gli OEM e gli End User nell'affrontare la materia. Tra i messaggi chiave trasmessi dai relatori a chi realizza macchine che saranno collegate all'interno di una rete di fabbrica e interconnesse, e a chi le utilizza, vi è la necessità

di passare da un approccio *security by obscurity,* a un concetto di *security by design,* fondato su una superiore consapevolezza, formazione e cultura di tutti gli attori coinvolti.

LAPP *www.lappitalia.com*

LAPP è leader nella fornitura di prodotti per la tecnologia di connessione e distribuisce cavi elettrici, pressacavi, connettori e accessori per un ampio campo di applicazioni industriali, anche in ambito Industry 4.0. Integratore di sistemi e soluzioni su misura, vanta, inoltre, un servizio qualificato che costituisce il valore aggiunto per il cliente.
LAPP, azienda a conduzione familiare sin dalla sua fondazione nel 1959, conta a livello mondiale oltre 4.600 dipendenti, 20 siti produttivi e oltre 43 filiali commerciali, per un fatturato di 1.423 milioni di euro nel 2020/2021.
La sede di Desio ospita un magazzino automatizzato collegato alle sedi logistiche europee del gruppo, per un totale di 40.000 referenze sempre disponibili, per consegne rapide e puntuali ovunque. LAPP opera in Italia nei seguenti settori: macchine e impianti, ingegneria industriale, industria alimentare, energia e mobilità.

Facebook: @lappitalia
Twitter: @lapp_italia
Youtube: LAPP ITA
LinkedIn: LAPP ITA

Per ulteriori informazioni:
Lbdi Communication
Silvia Vara – email: svara@lbdi.it
Deborah Amato – email: damato@lbdi.it
Ginevra Fossati – email: gfossati@lbdi.it
Tel. 02/43910069 – Cell. 3662694449