INNOVATION Post
Politiche e tecnologie per l'industria

Edge e cyber security nel futuro dell'industria

17 Novembre 2020 Stefano Casini

Due mondi – IT (Information technology) e OT (Operational technology) – devono sempre più convivere e collaborare in azienda, ma con paradigmi di funzionamento molto diversi. Proprio per far fronte alla crescente necessità di convergenza e di integrazione, tra i sistemi di livello business, largamente in cloud, e gli impianti di produzione con logiche prevalentemente locali ('on premise'), si sono sviluppate nuove tecnologie di confine, denominate **Edge computing**.

Tecnologie e soluzioni che – come tutte quelle connesse in rete e online – si intrecciano con le funzioni della **Cyber security aziendale**, che deve proteggerle dagli attacchi esterni, ma molto spesso anche dagli incidenti interni.

Di queste dinamiche e delle prospettive associate si è discusso nel corso della **tavola rotonda** dal titolo ***Edge e Security nell'industria***, organizzata dal gruppo Software Industriale di **Anie Automazione** in occasione della presentazione del white paper sull'intelligenza artificiale.

"Attraverso i sistemi Edge, veri e propri server standard con caratteristiche di elaborazione molto spinte e notevoli capacità di integrazione e di comunicazione, si stanno riformulando i criteri di progettazione di tutti i sistemi di conduzione aziendale", sottolinea **Mario Testino**, chief operating officer in **Servitecno**. Che rimarca: "**Il modello che si sta affermando è ibrido**: invece di trasferire grandi quantità di dati nel cloud per poter prendere decisioni, si effettuano aggregazioni e valutazioni locali, attraverso l'analisi e l'elaborazione di grandi quantità di dati in real-time, e si trasferiscono nel cloud solo le possibili alternative per la decisione finale". Il miglioramento dell'affidabilità del sistema complessivo e la **riduzione dei costi** – dato che l'elaborazione e la storicizzazione dei dati in cloud sono molto onerosi – sono rilevanti.

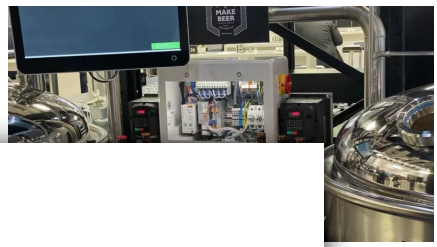
In più, lo sviluppo dell'intelligenza artificiale sta portando ulteriori miglioramenti a questo modello ibrido: attraverso l'AI associata alle tecnologie Edge "è possibile realizzare sistemi autonomi locali, ovvero che non supportano le decisioni ma decidono in autonomia, notificando solamente l'esito", spiega **Alberto Ascoli**, technology consultant di **Rockwell Automation**. "Dall'altro lato i sistemi in cloud liberano capacità elaborativa per dedicarsi alle decisioni più complesse e strategiche, ovvero quelle più legate all'andamento del business".

L'Eg
imp
aut
evid
di agire autonomamente in base alle circostanze è uno degli aspetti principali di **Industria 4.0**.

I PC industriali hanno un ciclo di vita più lungo rispetto ai PC consumer, devono essere robusti, adatti all'uso in ambienti difficili e con temperature molto elevate (o molto basse). Per questo la qualità e l'assistenza sono fattori fondamentali nella scelta del prodotto

Continua a leggere

AUTOMAZIONE



stato
il
processo di produzione della birra lavorando con Raspberry Pi e linguaggio Python. Grazie

Secondo Business Insider Intelligence, i dispositivi IoT arriveranno ad essere 40 miliardi entro il 2023. Risulta quindi difficile pensare che ci possa essere un'**infrastruttura cloud** in grado di processare in tempo reale la quantità di dati che questi dispositivi genererebbero, a causa sia delle limitazioni di banda che del tempo di latenza. Da qui la necessità di spostare quanta più intelligenza possibile dal cloud verso la parte periferica dell'infrastruttura IoT, vale a dire l'Edge.

Applicazioni di Edge computing in tutti i settori

Qualsiasi azienda in qualunque settore può utilizzare **tecnologie IoT e l'Edge computing** per sviluppare nuovi flussi di entrate, migliorare l'esperienza dei clienti e incrementare l'efficienza operativa. Con la crescita delle progettualità legate a Industria 4.0 e all'IoT, gli esempi di applicazione dell'Edge computing si stanno facendo più numerosi nei più disparati settori industriali: dai sistemi di monitoraggio della produzione ai droni utilizzati nella sorveglianza nei progetti in ambito smart city, fino alle applicazioni per la gestione dell'operatività dei datacenter.

Tutto ciò richiede "un'infrastruttura IT in grado di valutare grandi quantità di dati e di rispondere senza ritardi a eventi imprevisti. L'Edge computing risolve il problema della latenza attraverso l'elaborazione distribuita dei dati", sottolinea Ascoli, "le funzionalità Edge dell'IoT consentono alle macchine in produzione di acquisire capacità autonome di intelligenza, specialmente in due ambiti: la manutenzione predittiva e la riduzione automatica della dife dell più arch Edge. Più trasversalmente, le Pmi utilizzeranno l'Edge computing più rapidamente delle grandi imprese, con un tasso di crescita annuale previsto del 46%. La chiave, in questo caso, è **la riduzione dei costi** operativi garantita

PLCnext Technology di Phoenix Contact, microbirrifici e birrifici artigianali possono ora ottimizzare la produzione della birra e migliorare la qualità.

Continua a leggere

POLITICHE PER L'INDUSTRIA

LEGGI TUTTI ▶


Legge di Bilancio 2021, ecco le misure per imprese, innovazione e occupazione


L'Italia si dota di un Comitato Nazionale per la Produttività


World Manufacturing Forum, le quattordici lezioni della pandemia per il new normal


Enea Tech, ecco le nomine: Anna Tampieri presidente e Salvatore Mizzi amministratore delegato

CARICA ALTRI ▼

Danni informatici e conseguenze a lungo termine

Ma le reti e le connessioni online dei sistemi Edge chiamano subito e direttamente in causa anche il mondo della cyber security. "L'introduzione e l'integrazione di risorse IT fatta in modo non adeguato e non oculato è la causa di molte disfunzioni e inconvenienti a livello di operatività dei sistemi e aziendale", fa notare **Davide Pala**, specialista pre-sales Italy in **Stormshield**. Da qui, l'importanza "della security by-design, anche a livello di processo manifatturiero. E per trovare le soluzioni giuste è necessario avere delle tecnologie dedicate, che possano essere compatibili sia con il mondo IT sia con quello OT".

Molti malfunzionamenti e danni – fanno notare gli specialisti del settore cyber security – arrivano spesso dall'interno dell'azienda, causati involontariamente dai propri dipendenti e collaboratori. Ci sono poi le minacce esterne, gli hacker, i 'pirati informatici', sempre pronti a entrare nei sistemi sfruttandone falle e punti deboli. Tutto ciò porta non solo a problemi e danni immediati, come il blocco delle macchine e della produzione, ma provoca anche "conseguenze a lungo termine", fa notare Pala, "come ad esempio il **danno reputazionale** che ne può derivare, nei confronti del mercato, dei clienti o fornitori". E lo specialista in cybersecurity di Stormshield mette in guardia: "vedremo sempre più attacchi targetizzati su ambienti e sul mondo OT, prepariamoci".

I 3 rischi di una cybersecurity debole

Ma quali sono i rischi di essere esposti alle minacce e non proteggersi adeguatamente? Sono innanzitutto tre: c'è un **rischio di safety**, in quanto la violazione della cybersecurity può causare un danno fisico a persone e cose. C'è il **rischio economico** per l'azienda, in termini di perdita di ore di produzione per l'interruzione dell'operatività, della produzione, della continuità del business. E poi c'è un **danno di immagi**ziendale, che può risu

Anc
gli i
L'ob
aggiornamento tecnologico nelle aziende si devono ridurre".

Password, token fisici, certificati

PODCAST 1 – POLITICHE E INCENTIVI

Da oggi l'informazione di Innovation Post è disponibile anche in Podcast! Ascolta tutte le novità sugli incentivi e le politiche per Industria 4.0 - Impresa 4.0

PODCAST 2 – TECNOLOGIE

Diventa quindi vitale proteggere le singole apparecchiature da manipolazioni di terzi malevoli senza però compromettere le funzionalità dei devices e degli impianti. In questo quadro interviene anche la **normativa**, "con lo standard IEC 62443-4-2, che ha l'obiettivo di garantire la safety dell'impianto industriale, insieme alla riservatezza, disponibilità e integrità dei dati che vengono utilizzati", sottolinea il technology consultant di Rockwell Automation, "con il vantaggio di mitigare anche i rischi legati a manomissioni e danni anche accidentali".

Per garantire maggiore sicurezza, la normativa prevede uno schema di **controllo accessi diversificato su più livelli** (a differenza, per esempio, di molte vecchie installazioni, che prevedono il solo accesso come amministratore), e di attribuzione precisa dei comandi a ogni utente e ruolo previsto, in base alla **diversificazione dei compiti**. A parte il caso semplice di password, l'accesso può essere protetto mediante token fisici, certificati crittografici, biometria (nel caso di utente umano), anche in combinazione tra di loro.

Stefano Casini

Giornalista specializzato nei settori dell'Economia, delle imprese, delle tecnologie e dell'innovazione. Dopo il master all'IFG, l'Istituto per la Formazione al Giornalismo di Milano, in oltre 20 anni di attività, nell'ambito del giornalismo e della Comunicazione, ha lavorato per Panorama Economy, Il Mondo, Italia Oggi, TgCom24, Gruppo Mediolanum, Università Iulm. Attualmente collabora con Innovation Post, Corriere Innovazione, Libero, Giornale di Brescia, La Provincia di Como, casa editrice

COMPETENCE CENTER

Prorogata la scadenza per presentare i progetti per il bando del Competence Center Smact

Competence center, ecco i diciannove vincitori del secondo bando di

gie 4.0 di
r la
del
e Center
Bi-Rex

CARICA ALTRI ▼