INNOVATIONPOST.IT

Dalla supply chain all'AI generativa: le nuove sfide della cybersecurity industriale

Indirizzo copiato La cybersecurity industriale evolve tra nuovi rischi di filiera, furto di credenziali e uso dell´AI generativa, imponendo modelli Zero Trust e maggiore governance della supply chain per garantire continuità produttiva Pubblicato il 10 ott 2025 La cybersecurity industriale sta attraversando una fase di profonda trasformazione, sospesa tra l´urgenza di proteggere filiere sempre più interconnesse e la sfida di integrare nuove tecnologie come l´intelligenza artificiale. Nel corso dell´intervento tenuto da Andrea Ferrazzi , Business Unit Director Cybersecurity, IT & Cloud di Relatech , durante l´evento L´insostenibile leggerezza dell´essere Cyber Vulnerabili nell´industria manifatturiera organizzato da Cefriel, è emersa una riflessione chiara: il vero punto critico oggi non è solo la tecnologia, ma la governance della supply chain , il modo in cui le imprese industriali gestiscono accessi, identità e rapporti con i propri fornitori. La cybersecurity industriale non è solo compliance Per Ferrazzi, la sicurezza non può più essere interpretata come un «centro di costo imposto dalle norme», ma deve diventare parte integrante della gestione operativa e strategica delle imprese. La Direttiva NIS 2 ha certamente alzato il livello di attenzione, obbligando molte aziende del settore manifatturiero a dotarsi di procedure più rigorose. Tuttavia, la conformità normativa non basta a garantire resilienza. Nel mondo industriale, spiega Ferrazzi, esistono «diversi punti critici che vanno dalla visibilità alla gestione delle vulnerabilità, fino al tema del Digital Twin», ma è la supply chain a rappresentare oggi l´elemento più delicato. La crescente convergenza tra ambienti IT e OT favorita dall´automazione e dalla necessità di accessi remoti ha sfumato i confini tra sistemi tradizionalmente separati, esponendo l´intero ecosistema produttivo a nuove forme di rischio. Supply chain sotto attacco: credenziali, accessi e vulnerabilità Uno degli aspetti più problematici è quello legato alla gestione delle credenziali e degli accessi privilegiati. Ferrazzi descrive una dinamica purtroppo frequente: «Io sono un cliente e do le credenziali amministrative a un mio fornitore. Il fornitore le usa sul suo dispositivo, naviga in rete, viene infettato da un malware Password Stealer e quelle credenziali finiscono in un leak sul dark web». Il risultato è che un semplice incidente nella filiera può compromettere la sicurezza dell´intera infrastruttura industriale Questo tipo di scenario, prosegue Ferrazzi, è aggravato dal fatto che Italia, Slovenia, Francia e Spagna sono stati nel 2024 tra i target principali di campagne di furto credenziali tramite stealer. Ciò significa che «molte delle nostre credenziali sono già disponibili su internet». Un ulteriore elemento di rischio è rappresentato dagli Initial Access Broker, gruppi criminali specializzati nell´acquisire e rivendere accessi privilegiati a terzi . La loro attività «accorcia il periodo di attacco», riducendo drasticamente il tempo che intercorre tra l´intrusione iniziale e l´esecuzione di azioni dannose. In questo contesto, anche strumenti di difesa consolidati possono rivelarsi inefficaci, poiché si trovano a operare in presenza di comportamenti apparentemente trusted. Dallo Zero Trust al disaccoppiamento degli accessi: mitigare il rischio nella filiera lunga Per fronteggiare questa complessità, Ferrazzi individua nell´ approccio Zero Trust e nella segregazione degli accessi due pilastri fondamentali. Tecnologie che consentono di disaccoppiare il comportamento dell´amministratore dal dispositivo fisico diventano essenziali per mantenere il controllo anche in filiere estese, dove monitorare ogni singolo endpoint è «sostanzialmente impossibile». Relatech collabora, spiega Ferrazzi, con diversi attori del settore, dai produttori di macchine ai sistemi di accesso remoto gestiti da player specializzati. Queste soluzioni permettono di governare l´autenticazione e i privilegi senza esporre direttamente le credenziali agli ambienti potenzialmente vulnerabili, riducendo la possibilità che vengano sottratte o riutilizzate. L´obiettivo non è solo tecnico, ma di governance : creare un ecosistema in cui la fiducia non sia implicita, ma verificata costantemente, e in cui la sicurezza non dipenda più dalla bontà del singolo fornitore o manutentore. In un ambiente produttivo in cui la supply chain è lunga e interdipendente, questa separazione dei ruoli e dei canali di accesso diventa il presupposto per la sopravvivenza stessa dell´impresa. AI generativa e mondo OT: due universi ancora distanti Oltre alla sicurezza della filiera, Ferrazzi ha affrontato un tema che sta ridefinendo molti ambiti industriali: l´ uso dell´intelligenza artificiale generativa . La sua visione è prudente e al tempo stesso realista. «AI generativa e OT sono quasi due cose antitetiche», afferma, sottolineando come nel mondo operativo la priorità rimanga la continuità dei processi e la stabilità dei sistemi, piuttosto che la sperimentazione di tecnologie ancora immature per questi ambienti. Relatech, in quanto integratore, utilizza l´intelligenza artificiale come strumento complementare più che come elemento strutturale. «Non facendo i costruttori di macchine, non integriamo logiche di AI all´interno dei dispositivi,

INNOVATIONPOST.IT

ma le utilizziamo a supporto», spiega Ferrazzi. Ciò non significa che l´AI sia assente: molte fabbriche la impiegano da anni, soprattutto nella computer vision e nei sistemi di controllo automatico. «Siamo stati in una fabbrica che muove robottini per spostare cassette di frutta, e tutto era modellato da AI», racconta. La novità è l´introduzione di modelli linguistici di grandi dimensioni (LLM) in contesti operativi. Relatech ha sperimentato, ad esempio, una soluzione che permette a un operatore di interrogare un libretto di istruzioni attraverso comandi vocali e ricevere risposte immediate, integrando il modello direttamente in campo anziché in un ambiente di test. «Abbiamo usato modelli LLM, ma l´unica declinazione che abbiamo trovato è stata quella di metterli in campo, non li vediamo ancora come qualcosa di strutturale nel mondo OT», chiarisce Ferrazzi. Verso una nuova cultura della sicurezza industriale Le parole di Ferrazzi delineano un quadro in cui la cybersecurity industriale non è più un comparto tecnico isolato, ma una funzione trasversale che unisce governance, tecnologia e consapevolezza. La difesa della supply chain non si riduce alla gestione dei rischi informatici, ma diventa una questione di fiducia digitale tra imprese, partner e fornitori. In un ´economia sempre più interconnessa, dove i confini tra IT e OT si dissolvono e dove la vulnerabilità di un singolo nodo può propagarsi a tutta la rete produttiva, il valore della sicurezza risiede nella capacità di prevedere, segmentare e reagire. Come ricorda Ferrazzi, «governare la filiera diventa complesso, ma è l´unico modo per evitare che le nostre credenziali diventino un punto d´ingresso per gli attaccanti».Una consapevolezza che riporta la cybersecurity industriale al suo significato più concreto: proteggere la continuità delle fabbriche, dei processi e, in definitiva, della competitività dell´industria europea. @RIPRODUZIONE RISERVATA Valuta la qualità di questo articolo L Mattia Lanzarone