L'AI al servizio della sicurezza industriale

Fonte: foto Shutterstock

Il monitoraggio continuo consente di rilevare tempestivamente variazioni impreviste che potrebbero indicare un tentativo di manomissione o un malfunzionamento del dispositivo

Se la connettività non viene adeguatamente protetta, può trasformarsi in un punto di debolezza, offrendo ai criminali informatici un'agevole via d'accesso ai sistemi di controllo industriale. Il caso Nozomi Networks e Bosch Rexroth

Giovanni Dini Gentilini

L'Industria 4.0, con la sua crescente interconnessione di dispositivi e sistemi, promette una rivoluzione nell'efficienza e nell'automazione dei processi produttivi. Tuttavia, questa trasformazione digitale porta con sé nuove sfide in termini di sicurezza informatica. L'aumento dei dispositivi connessi estende significativamente la superficie d'attacco per i criminali informatici, aumentando i rischi a cui le aziende sono esposte. In questo contesto, l'intelligenza artificiale emerge non solo come tecnologia per migliorare la produttività, ma anche come strumento cruciale per proteggere le infrastrutture critiche e garantire la continuità operativa.

Controllo e monitoraggio

I prodotti di Nozomi Networks sfruttano l'AI attraverso modelli predittivi che potenziano la capacità di rilevare anomalie di sicurezza in ambienti industriali di qualsiasi dimensione. Inoltre, l'AI viene utilizzata per suggerire modifiche ai sistemi, al fine di ridurre significativamente i rischi con interventi rapidi ed efficaci. Un esempio concreto dell'efficacia dell'approccio di Nozomi Networks è rappresentato dalla ricerca sui Nexo Nutrunner e dalla conseguente collaborazione con Bosch Rexroth per la sicurezza dei sistemi di avvitatura. I Bosch Rexroth Nexo Nutrunner sono avvitatori industriali ampiamente utilizzati nelle moderne linee di produzione. Dotati di funzionalità avanzate di controllo e monitoraggio, questi dispositivi sono progettati per connettersi alla rete aziendale, consentendo di caricare rapidamente impostazioni differenti (come il valore di coppia o la direzione di rotazione) indipendentemente dalla posizione del dispositivo. Offrono anche funzionalità di raccolta dati, che vengono trasmessi sulla rete aziendale. Tuttavia, se la connettività non viene adeguatamente protetta, può trasformarsi in un punto di debolezza, offrendo ai criminali informatici un'agevole via d'accesso ai sistemi di controllo industriale. L'analisi condotta da Nozomi Networks sui Nexo Nutrunner ha evidenziato potenziali vulnerabilità legate alla gestione delle credenziali di accesso e alla comunicazione tra i componenti del sistema. In particolare, è emersa la possibilità di accedere ai Nutrunner senza autenticazione, una falla che potrebbe permettere a malintenzionati di manipolare i parametri di funzionamento, compromettendo la qualità del prodotto finale o causando danni fisici. Inoltre, la mancanza di crittografia nella comunicazione tra il Nutrunner e il controller rappresenta un ulteriore rischio, esponendo il sistema all'intercettazione e alla modifica dei dati trasmessi. Queste vulnerabilità, se sfruttate, potrebbero avere conseguenze significative, interrompendo la produzione e causando perdite economiche.

Comportamenti anomali?

Comprendendo l'importanza di una sicurezza robusta per i propri prodotti, Bosch Rexroth ha scelto di collaborare con Nozomi Networks attraverso un processo di responsible disclosure, per ga-

rantire un livello avanzato di sicurezza e informare il pubblico. Il produttore ha prontamente sviluppato aggiornamenti di sicurezza, rendendoli disponibili a tutti i propri clienti. Le soluzioni di Nozomi Networks, che utilizzano vari approcci di intelligenza artificiale e machine learning, offrono una risposta efficace a queste minacce. Attraverso l'analisi continua del traffico di rete, degli applicativi sugli endpoint e delle comunicazioni wireless, gli algoritmi di Nozomi Networks possono individuare in tempo reale comportamenti anomali, come tentativi di accesso non autorizzati o modifiche sospette ai parametri di configurazione. L'apprendimento automatico consente al sistema di adattarsi dinamicamente alle mutevoli tattiche d'attacco dei cybercriminali, garantendo una protezione costante contro le nuove minacce. Inoltre, la capacità di Nozomi Networks di analizzare una vasta gamma di dispositivi permette di riconoscere potenziali falle di sicurezza prima che vengano sfruttate, prevenendo attacchi disastrosi come nel caso degli avvitatori. Nel caso specifico dei Nexo Nutrunner, l'implementazione delle soluzioni Nozomi Networks ha permesso di monitorare costantemente i parametri di funzionamento, come la coppia di serraggio e la velocità di rotazione. Questo monitoraggio continuo consente di rilevare tempestivamente variazioni impreviste che potrebbero indicare un tentativo di manomissione o un malfunzionamento del dispositivo. Inoltre, l'analisi del traffico di rete tra il Nutrunner e il controller, effettuata dalla piattaforma di Nozomi Networks, identifica tentativi di intercettazione, modifiche dei dati o anomalie di processo, garantendo l'integrità delle informazioni e la sicurezza operativa.

Protezione a tutto tondo

Grazie a questa collaborazione, Bosch Rexroth ha potuto rafforzare la sicurezza dei Nexo Nutrunner, proteggendo non solo i dispositivi ma anche l'intero processo produttivo dei propri clienti. L'utilizzo dei prodotti di Nozomi Networks basati sull'AI offre numerosi vantaggi per la sicurezza dei dispositivi industriali. L'automazione dell'analisi e del monitoraggio riduce significativamente i tempi e i costi necessari per garantire la sicurezza dei sistemi, liberando risorse preziose. Inoltre, tali soluzioni sono in grado di identificare minacce complesse e sofisticate che sarebbero difficili da rilevare con metodi tradizionali. La capacità di intervenire rapidamente per mitigare le vulnerabilità e prevenire gli attacchi minimizza i danni potenziali, proteggendo le aziende da perdite economiche e danni reputazionali.

L'AI si sta affermando come strumento indispensabile per garantire la sicurezza dei dispositivi connessi nell'ambito dell'Industria 4.0. Il caso dei Nexo Nutrunner, protetti dalle soluzioni Nozomi Networks, dimostra l'importanza di una ricerca approfondita e offre un esempio concreto dell'uso dell'intelligenza artificiale nell'identificazione e mitigazione delle vulnerabilità. L'adozione di soluzioni specializzate come quelle offerte da Nozomi Networks rappresenta un investimento strategico per le aziende che desiderano proteggere i propri asset, garantire la continuità operativa e prosperare nell'era dell'Industria 4.0.

Nozomi Networks - www.nozominetworks.com

Fonte: foto Shutterstock

Bosch Rexroth ha rafforzato la sicurezza dei dispositivi e dell'intero processo produttivo dei propri clienti