Dossier

Fonte: foto Shutterstock

La cybersecurity non può mai essere sottovalutata, al contrario dovrebbe essere parte integrante della strategia aziendale

SICUREZZA 'CONVERGENTE'

PROTEGGERE E DIFENDERE UN SISTEMA INDUSTRIALE DOVREBBE ESSERE PARTE INTEGRANTE DELLA STRATEGIA AZIENDALE: UN INCIDENTE A UN IMPIANTO DI PRODUZIONE PUÒ AVERE RICADUTE SULL'INTERA COMUNITÀ

Aldo Di Mattia

La convergenza tra IT e OT è uno dei mantra dell'Industria 4.0, oltre che il fulcro della digital transformation, con l'obiettivo finale di permettere alle aziende di prendere le decisioni operative più vantaggiose, di ottimizzare i processi produttivi e di renderli più sostenibili sia sotto il profilo economico, sia sotto quello dell'impatto ambientale.

Ma cosa significa rete convergente? Significa abilitare lo scambio di informazioni e dati tra regioni OT e regioni IT. Se si immagina un impianto industriale, magari distribuito geograficamente su più siti, la regione OT comprende i sensori, gli attuatori, i PLC, le RTU, i sistemi Scada e quelli di controllo industriale (ICS), ovvero tutti i sistemi che sovrintendono il controllo operativo delle apparecchiature industriali. Tali sistemi raccolgono dati che devono essere processati. Si entra quindi nell'area dello storage e della computazione, ovvero nella regione IT che innesta su quei dati gli algoritmi di intelligenza artificiale (AI) atti a rendere virtuoso questo connubio e tradurlo nell'obiettivo finale di cui sopra. Gli ambienti OT sono però nativamente e storicamente meno protetti rispetto agli ambienti IT, perché pensati come ambienti isolati. Pertanto, tale convergenza deve garantire gli ambienti OT in termini di operatività, affidabilità, sicurezza operativa e gestione degli incidenti in modalità realtime e controllata. E questo soprattutto in ragione del fatto che un incidente in un impianto industriale di produzione potrebbe avere delle ricadute sull'intera comunità e, in ultima istanza, compromettere anche l'incolumità del singolo cittadino.

Dìvide et impera, ovvero segmentazione

Tornando al gergo tecnico, il modello spesso utilizzato per schematizzare l'interconnessione IT-OT è quello 'Purdue'. In questo contesto si inserisce lo standard internazionale IEC62443 per la sicurezza dei sistemi di controllo industriale (ICS). Si riprende, per così dire, una tecnica di epoca romana: il 'dìvide et impera' che in ambito rete si traduce nella segmentazione. L'obiettivo è quello di dividere la rete in una serie di reti più piccole, al fine di circoscrivere e definire un insieme di zone di sicurezza a differente livello di rischio. In questo modo è possibile limitare gli accessi esterni non autorizzati

e circoscrivere i potenziali danni. Ma questo non basta. Sebbene tale modello identifichi dei livelli di separazione tra la zona di produzione, quella di processamento e quella di controllo, per poi approdare nella regione IT, esso non è sufficiente.
Il modello di separazione, micro-segmentazione fisica e logica, di firewalling tra e all'interno dei layer di un modello Purdue deve infatti arricchirsi di quella intelligenza che permette di identificare e neutralizzare un possibile attacco cyber in ognuna delle sue fasi di esecuzione (Cyber Kill Chain).
Spieghiamo nel dettaglio cosa significa in termini di soluzioni tecnologiche.
In primo luogo, abbiamo accennato alla segmentazione: sia che si parli di regione IT che OT, essa deve essere controllata da un Next Generation Firewall (Ngfw) e attuata da switch e/o AP che raccolgano anche la platea di client dell'ambiente IIoT (Industrial Internet of Things). Il Ngfw è necessario in quanto aggiunge quell'intelligenza tecnologica in grado di identificare i sistemi e gli end point, e analizzare, nel dettaglio, lo scambio dati tra le diverse componenti di dialogo del sistema industriale. Il Ngfw riconosce se tale scambio è riconducibile a un pattern lecito o malevolo, tramite firme (signature) specifiche del mondo OT e alimentate da una 'threat intelligence' di complemento, che consente di accogliere, analizzare e classificare autonomamente le minacce con un alto grado di precisione. Il flusso di informazioni, così segmentato, controllato e ispezionato, può poi intervenire secondo due direttrici di traffico: dall'interno verso l'esterno (OT-to-IT) e viceversa. Nel primo caso, si tratta in genere di una raccolta di informazioni e dati da elaborare direttamente sul sito, o da trasportare all'esterno su un sito centrale o sul cloud. Il trasporto esterno al sito dovrà essere protetto da attacchi opportunistici tramite soluzioni di Secure SD-WAN, con edge di tipo Ngfw che consentano l'efficientamento e la sicurezza del trasporto tramite tunnel overlay protetti e cifrati. Se, invece, la direttrice di traffico è dall'esterno verso l'interno, per esempio accesso terze parti remote o personale operativo, allora occorre prevedere modalità di accesso di tipo Ztna (Zero Trust Network Access) e utilizzare tecniche di autenticazione di tipo MFA (Multi Factor Authentication). L'autenticazione e la successiva autorizzazione devono poi avvenire in modo granulare rispettando ruoli e responsabilità specifiche di chi, da dove e come sta accedendo al sistema (Role based access Control).
In questo modo abbiamo messo in sicurezza il transito e l'accesso, ma non basta. Occorre proteggere gli end point, i device, attraverso soluzioni di EPP (End Point Protection) ed EDR (Endpoint Detection and Response), nonché intervenire in modo proattivo sulla rete tramite soluzioni di tipo NDR (Network Detection and Response). Da notare, infatti, che difficilmente sarà possibile installare agent sugli end point OT, per cui nella maggior parte dei casi l'enforcement avverrà tramite il virtual patching di una soluzione NDR.

L'arte dell'inganno

La convergenza IT-OT deve essere anche operativa. Sarà quindi necessario utilizzare sistemi di 'risk management' per il controllo proattivo, come analizzatori di log, Siem e Soar. Tali sistemi saranno centralizzati (IT+OT) e dovranno interfacciarsi non solo con gli elementi della matrice di sicurezza menzionati in precedenza, ma anche con elementi a perimetro, che possano svolgere le funzioni di asset management o troubleticketing. E questi sistemi dovranno essere anche in grado di agire in maniera autonoma (actionable intelligence). I sistemi dovranno essere capaci di reagire a possibili comportamenti sospetti tramite enforcement sui singoli elementi di sicurezza attivi (Ngfw in primis, tramite API o in modalità nativa), al fine di rompere la catena di attacco e difendere il perimetro aziendale.

Fonte: foto Shutterstock

Gli ambienti OT sono meno protetti rispetto agli ambienti IT, pertanto la sicurezza OT deve garantire anche una gestione degli incidenti in modalità realtime e controllata

L'evoluzione di strategie di attacco mirate e sofisticate, dove la fase ricognitiva dell'attacco può durare mesi o anni, consiglia l'adozione di nuove tecniche per l'isolamento e il contenimento della minaccia, tecniche note come 'deception'.
La deception (arte dell'inganno) consente il posizionamento di dispositivi (decoy virtual machine) atti a fungere e contenere esche e trappole, al fine di creare una realtà target ad hoc assolutamente credibile, uno 'specchietto per le allodole'. Questo consente di deviare l'attaccante dai bersagli reali, intrappolandolo con l'inganno, per studiarne le mosse, vincere sul suo stesso terreno e velocizzare i tempi di mitigazione delle minacce. L'efficacia di queste tecniche è tanto maggiore in ambiente industriale OT, quanto più la dissimulazione dell'oggetto target è credibile: è quindi necessario disporre di esche e trappole conformi proprio a tali ambienti (Scada Decoy e Lures). Il contesto deve inoltre dotarsi di tecnologie in grado di prevenire minacce zero day e quindi Sandbox ma, anche qui, sandbox che dispongano di immagini Scada specifiche dell'ambiente OT che si vuole mettere in sicurezza.

Più sicurezza per l'industria

Questo, in sintesi, è quanto si può offrire a livello tecnologico per proteggere e difendere in maniera efficace un qualunque sistema di controllo industriale, dove la cybersecurity non può essere sottovalutata, ma al contrario dovrebbe essere parte integrante della strategia aziendale. Da un punto di vista normativo, la Direttiva NIS2 (vedi l'articolo pubblicato su *Fieldbus&Networks* - febbraio 2023, *https://automazione-plus.it/brochure/fn/114/14 - ndr*) va in questa direzione, aggiungendo a quanto già descritto la necessità di tecniche di crittografia integrate (firma digitale e crittografia) a protezione dei dati e dei messaggi scambiati tra le parti software o hardware che realizzano l'impianto industriale.

Fortinet - www.fortinet.com