Cybersecurity ai tempi delle Reti OT: come e perché gestire le vulnerabilità di dati e processi nell'interconnessione con reti IT

Author : Igor Serraino

Date : 15 novembre 2018

L’era della Smart Factory 4.0 è entrata pienamente nella fase 2, quella dell’implementazione e dell’entrata in funzione dei nuovi processi di automazione industriale. In tale contesto, il corretto partizionamento tra risorse IT (Information Technology) e risorse OT (Operational Technology) assume particolare rilevanza dal punto di vista semantico, tecnico e giuridico.

Premessa doverosa è definire adeguatamente la differenza tra i due contesti: il dominio IT è accademicamente molto ampio e include l’intero spettro di tecnologie deputate alla gestione dell’informazione, comprensive di software, hardware, infrastrutture di comunicazione e servizi correlati. Si tratta del dominio orientato alla gestione dei dati, ed è per questo “data-centric”.

Il dominio OT è, invece, di sviluppo relativamente recente ed è per definizione orientato agli eventi e al controllo di stato di beni fisici che ad esso appartengono. Nel contesto OT rientrano aspetti quali il monitoraggio di eventi o i cambiamenti di stato delle entità su di esso attestate, nonché il controllo di devices fisici e dei relativi processi/eventi generati.

Il focus negli ultimi due anni si è inevitabilmente spostato sul contesto OT, in considerazione dell’evoluzione tecnologica e normativa che ha portato le imprese a puntare con decisione sull’interconnessione di beni e sistemi industriali, presentando all’infrastruttura del sistema informativo già presente nuovi attori dotati di caratteristiche hardware e software decisamente differenti da tutti gli altri apparati attestati sulla tipica rete IT.

Se nell’ambito IT il tradizionale parametro R-I-D sui dati viene enfatizzato nell’ordine in cui le lettere dell’acronimo sono riportate (Riservatezza-Integrità-Disponibilità), nelle reti di tipo operazionale (OT) l’ordine è esattamente invertito, dando assoluta priorità alla disponibilità dei dati necessari per implementare una gestione degli eventi solida ed efficace, oltre che in tempo reale. Così, il nuovo parametro diventa (C)-D-I-R, con al top il “Controllo”, e presuppone l’esistenza di policies di cybersecurity modellate *ad hoc* per garantirne il soddisfacimento, e con il giusto grado di priorità.

L’oggetto della tutela in ambito operazionale deve essere il processo: arrivando da scenari in cui il dato rappresenta il focus di ogni analisi sulla sicurezza, si può commettere il grave errore di seguire un approccio “a strati” (layers) anche per la realtà operazionale, strutturando i gradi di difesa azione/reazione su livelli potenzialmente infiniti come l’IT propone. Le applicazioni che operano sulla protezione dei dati, tipicamente coprono singoli contesti di vulnerabilità, e anche ove esse offrano suite applicative più ampie, l’approccio è sempre di tipo settoriale, arrivando a proteggere aree semantiche di rischio ben definite. Sistemi di autenticazione web, ad esempio, vengono resi solidi attraverso tecniche che minimizzino a livello algoritmico la possibilità di intercettare le chiavi di accesso o infiltrare entità software intermedie che possano bypassare il sistema software di verifica credenziali e farne le veci.

Il dinamismo del contesto IT impedisce qualunque altro tipo di approccio che non sia a strati: il numero di variabili da considerare nell’analisi del rischio è potenzialmente infinito.

I sistemi OT vedono attestati sulla propria infrastruttura entità che generano eventi, ben definiti e costituiti da una sequenzialità di operazioni (definite spesso da “ricette” o ordini di produzione), e dalla forte connotazione deterministica. Un’operazione di fresatura effettuata da una macchina interconnessa su una porzione di materia prima, solo per fare un esempio, modifica irreversibilmente la materia prima; se il sistema di controllo del processo è alterato da un attacco operazionale in grado di modificare il controllo numerico della macchina, il danno sarà irreversibile.

La separazione, spesso adottata dalle aziende lungimiranti, tra la porzione IT della rete aziendale e quella OT, deriva dalla necessità di fornire ai potenziali attaccanti un numero minore di punti di ingresso, privilegiando l’isolamento della sezione operazionale e, al contempo, rafforzando gli accessi alla rete esistenti e imprescindibili.

Si consideri l’esempio di applicazioni DCS (Distributed Control Systems) o MES (Manufacturing Execution System): esse, per definizione, devono essere in grado di alterare lo stato dell’impianto attraverso l’inoltro di comandi ben definiti e circoscritti a quelle che sono le reali esigenze di produzione, controllo e monitoraggio dell’azienda, esigenze peraltro spesso amplificate in virtù di aspetti normativi connessi all’Impresa 4.0. La presenza di istruzioni di controllo direttamente interpretabili dalla macchina pone il sistema a rischio di attacco nel momento in cui lo stato macchina sia “ready”, ove una eventuale compromissione porterebbe minacce fisiche agli operatori a bordo macchina (ad esempio surriscaldamento, interruzioni forzate, sovratensioni) e contemporaneamente danni irreversibili al ciclo di produzione.

Gli attacchi contro i sistemi di controllo di supervisione e acquisizione dati (SCADA) hanno subìto incrementi notevoli negli ultimi tre anni, secondo i dati di ricerca redatti dalle più importanti compagnie IT su scala mondiale. La Finlandia è stata l'obiettivo principale di questi attacchi, seguita da strutture nel Regno Unito e negli Stati Uniti, paesi nei quali i sistemi SCADA connessi a Internet sono più diffusi e le policies di separazione tra contesto IT e OT non sono ancora così rigide e definite da costituire un ostacolo concreto alla diffusione di attacchi.

Le statistiche rilevano inoltre una sostanziale differenza di gestione tra le vulnerabilità scoperte in ambito IT e quelle in ambito OT, poiché mentre le società sono tenute a segnalare violazioni

dei dati che coinvolgono informazioni personali o di pagamento, gli attacchi SCADA spesso non vengono segnalati, con il risultato di rendere difficoltoso il censimento dei data breaches in tale ambito e ostacolare il rinnovamento tecnologico.

L'età delle apparecchiature è davvero una sfida significativa per quanto riguarda gli hack di tipo operazionale. Sebbene la minimizzazione del rischio per gli attacchi sistemi OT esposti alla rete WAN (internet) sia attività complessa, a causa dell'elevato numero di gateway esistenti, la tecnica suggerisce di verificare entry points su canali non esclusivi del protocollo TCP/IP, come porte USB, porte seriale e dispositivi Bluetooth che, in molti casi, risultano presenti sui macchinari industriali, di fabbrica o come moduli aggiuntivi. Parallelamente, ancorché la segnalazione dei breaches su rete OT non sia ad oggi sistematica, la condivisione degli attacchi e dei relativi dettagli tecnici tra la comunità di sviluppatori e sistemisti industriali potrebbe aiutare a limitare il fenomeno.

Appare infine fondamentale, nel tentativo di trovare una convergenza tra sistema orientato ai dati e sistema operazionale orientato ai processi, l'individuazione di strategie già consolidate in ambito IT replicandole opportunamente, per quanto possibile, anche in contesti OT:

- Identificazione e autenticazione di tutti i dispositivi e macchine all'interno del sistema, sia all'interno degli impianti di produzione, sia sul campo, per garantire che dispositivi e sistemi approvati siano gli unici autorizzati a comunicare tra loro. Ciò ridurrebbe il rischio di dispositivi non affidabili inseriti da hacker per assumere il controllo del sistema;
- Crittografia di tutte le comunicazioni tra i dispositivi convergenti IT/OT per garantire la riservatezza dei dati trasmessi;
- Garantire l'integrità dei dati generati da questi sistemi, attraverso l'applicazione di metodi di analisi intelligente (euristica, predittiva) nell'adozione di Internet industriale, adottando criteri matematico statistici al fine di ottenere precisione assoluta;
- Supponendo che i prodotti fabbricati contengano software o firmware embedded, consentire la possibilità di eseguire aggiornamenti remoti e garantendo l'integrità di tali aggiornamenti. Non è un caso che tale criterio sia ripreso anche dal Piano Industria 4.0 nell'allegato A dei beni abilitati a iperammortamento (Rif. Circolare ministeriale 4/e del 30 marzo 2017), ove si legge che tra i criteri richiesti vi è il monitoraggio remoto o teleassistenza.

La strada da seguire per soddisfare la crescente esigenza di sicurezza nel contesto dell'impresa altamente interconnessa porta a considerare una sinergia di metodi e di tecniche tra i due scenari IT e OT, valorizzando opportunamente le loro sostanziali differenze, senza aspettarsi che misure consolidate nel primo scenario possano necessariamente funzionare anche nel nuovo contesto operazionale.

Un'ultima notazione.

L'uomo è e resta al centro anche di scenari di "cyber insicurezza". Per questo motivo occorre preparare la propria azienda non solo dal punto di vista tecnologico e organizzativo, ma anche sotto il profilo delle competenze e della valorizzazione del capitale umano. L'adozione di specifiche policies aziendali e di percorsi di formazione continua potrà incrementare i livelli di

sicurezza a protezione dei dati aziendali, sempre più rilevanti e preziosi in contesti di Industria 4.0; ma non solo. L'industria (o l'impresa) altamente interconnessa porta inevitabilmente con sé implicazioni anche lato privacy, con particolare riguardo alla sicurezza dei sistemi e dei processi e, in definitiva, dei dati personali accessibili attraverso di essi. Non va dunque dimenticata l'importanza di adottare e mantenere nel tempo - anche e soprattutto in sistemi OT di supervisione e controllo - quelle misure di sicurezza *adeguate al rischio* fortemente volute dal GDPR (General Data Protection Regulation) e imposte ad ogni titolare in ossequio al principio di *accountability*.

Articolo a cura di **Igor Serraino** e **Andrea Maggipinto**