Gruppo Software Industriale
di ANIE Automazione (*)

Cloud e big data: come proteggere la filiera del dato in ambito industriale

(*) ANIE Automazione, con oltre 100 aziende associate, rappresenta in Italia il punto di riferimento per le imprese fornitrici di tecnologie per l'automazione di fabbrica, di processo e delle reti. **https://anieautomazione.anie.it**

Big data, cloud, edge computing: in ambito manifatturiero permettono di controllare ogni aspetto dei processi produttivi e di introdurre nuovi controlli di qualità o di implementare servizi di manutenzione predittiva

Ormai da qualche anno il numero di attacchi informatici cresce a ritmi vertiginosi: a livello mondiale nel 2021 si è registrato un aumento su base settimanale del 50% rispetto al 2020, con un valore medio di 925 attacchi per settimana per azienda (fonte: Checkpoint Research). Il settore manifatturiero si conferma un settore particolarmente colpito dagli attacchi informatici: come riportato nell'IBM X-Force Threat Intelligence Index 2022, l'industria manifatturiera nel 2021 si è posizionata al primo posto nella lista dei settori economici più attaccati, superando i servizi finanziari. A ulteriore conferma c'è il dato secondo cui tra tutte le aziende "OT-Connected" che sono state compromesse, il 61% sono aziende manifatturiere.

Attacco ransomware

Tutti i report sulla cyber security sono concordi nell'indicare il ransomware come il tipo di attacco più diffuso: il ransomware è un tipo di attacco che limita l'accesso al dispositivo infetto, richiedendo un riscatto (ransom in inglese) per rimuovere la limitazione. Nel corso del 2021 si è registrata la comparsa di ransomware di nuova generazione, che all'attacco principale basato sull'encryption (criptaggio) dei dati aggiungono il furto dei dati (prima dell'encryption) e l'attacco di tipo Denial of Service (dopo l'encryption). Il phishing, lo sfruttamento di vulnerabilità software e i sistemi di accesso remoto sono i vettori di attacco più comunemente sfruttati per la fase iniziale di un attacco ransomware.

"Nel mondo industriale, parliamo di Industrial Cyber Security per intendere l'insieme delle soluzioni applicabili all'automazione di fabbrica per contrastare minacce e attacchi informatici diretti verso le infrastrutture, i dati e gli asset aziendali a supporto dei processi produttivi. Il problema della cyber security e della data protection è critico in particolare per le aziende che fanno uso di dispositivi interconnessi ad applicazioni e piattaforme cloud, essendo questa una delle tecnologie abilitanti più impattanti e di grande sviluppo per la transizione verso la digitalizzazione/interconnessione dei prodotti/processi dell'Industria 4.0.

Il rischio per l'industria

I sistemi di automazione e controllo industriale non sono immuni al rischio di attacco informatico, dato che, con la digitalizzazione e l'interconnessione dei sistemi industriali, la superficie di attacco è aumentata notevolmente. Nel 2021 il numero di vulnerabilità scoperto negli Industrial Control Systems ha avuto un aumento del 50% anno-su-anno a fronte di un aumento complessivo delle vulnerabilità dello 0,4%. Inoltre nei primi nove mesi del 2021 si è registrato un aumento del 2204% nelle attività di ricognizione malevola sulla porta TCP 502, riservata per il protocollo Modbus. Questo dato è un indicatore di un maggiore interesse dei cyber-criminali verso i sistemi che ne fanno uso allo scopo di comprometterli per chiedere un riscatto o prenderne il controllo e causare danni: data la mancanza di funzionalità di sicurezza nel protocollo Modbus, una volta trovato un dispositivo accessibile, un malintenzionato potrebbe inviare comandi dannosi al dispositivo e compromettere altri sistemi ICS collegati.

Occorre proteggere l'intera filiera del dato: generazione, trasmissione in Cloud, memorizzazione, elaborazione, fruizione dei risultati

Questa è però solo la classica "punta dell'iceberg": esistono decine di altri protocolli di comunicazione industriale non autenticati o crittografati (dove quindi manca totalmente sia la verifica di legittimità dei due endpoint che la cifratura del dato in transito). Pensiamo alle tecnologie nate a cavallo del 2000, quando le reti industriali erano totalmente chiuse, limitate in estensione e la minaccia cyber meno sentita – e la cui messa in sicurezza oggi, a meno di non affrontare un costoso revamping dell'impianto, si raggiunge solo lavorando sul perimetro con un'attenta e stretta segregazione delle reti.

Cloud e big data

Il danno

Il danno si traduce immediatamente nello stop alle linee produttive, e di conseguenza nella mancata produzione, così come nell'interruzione dell'erogazione da remoto dei servizi a valore da parte dei costruttori di macchinari o nell'interruzione del funzionamento delle supply-chain integrate. Le conseguenze possono essere molto serie per le aziende colpite: negli Stati Uniti si sono registrati i primi casi di aziende incorse nel fallimento a seguito di un attacco informatico.
Un altro trend emergente sono gli attacchi alle infrastrutture e ai servizi in Cloud, finalizzati principalmente al furto dei dati aziendali. Nella maggior parte dei casi la compromissione degli asset in Cloud sfrutta una compromissione degli asset on-prem, ma vengono utilizzate anche API configurate male o credenziali rubate in vendita sul web.

La Cyber security dev'essere progettata by-design perché può assicurare (o meno) il successo di un intero processo di trasformazione digitale

Big Data e Cloud

Secondo Gartner, i Big Data sono asset di informazioni ad altissimo volume, ad altissima rapidità e/o di altissima varietà che richiedono forme innovative di analisi e interpretazione capaci di migliorare gli insight, il decision making e l'automazione dei processi. In concreto i Big Data sono grandi quantità di dati, strutturati e non, generati da un numero crescente di fonti diverse (file, database, video, immagini, interazioni sui social, sensori, dispositivi connessi, ecc.), che vengono elaborati da algoritmi appositamente sviluppati allo scopo di ricavare informazioni con un livello di precisione e una profondità di analisi impensabili prima. Il Cloud Computing è la capacità di elaborazione nel "Cloud", un insieme di server ad elevata potenza di calcolo messi a disposizione da più fornitori di servizi. Cloud Computing e Big Data sono due tecnologie che si completano a vicenda: da un lato la potenza di calcolo e la capacità di storage del Cloud Computing sono i due fattori che permettono la fruizione dei Big Data a costi sostenibili e in tempi utili per il business, dall'altro i Big Data sono una delle applicazioni che maggiormente favoriscono l'adozione del Cloud Computing.

Edge Computing

Non va dimenticato il ruolo dell'Edge Computing, inteso come architettura di elaborazione distribuita in prossimità dei dispositivi che generano i dati. Edge e Cloud Computing non sono tecnologie alternative, ma complementari per una efficiente gestione del dato: i dati operativi utili nell'immediato sono mantenuti nei nodi di Edge Computing e si inviano invece al cloud i dati che vanno elaborati, archiviati o che servono per le fasi previsionali e predittive. Quando vengono applicate all'ambito manifatturiero, queste tre tecnologie sono in grado di cambiare significativamente i processi produttivi e i servizi che si possono offrire: permettono infatti di controllare ogni aspetto dei processi produttivi, rivelandone le eventuali inefficienze, di introdurre nuovi controlli di qualità o di implementare servizi di manutenzione predittiva, permettendo di gestire in modo proattivo eventi affrontati fino a oggi in modo reattivo.

Proteggere la filiera del dato

Da quanto detto finora emerge come i dati siano un asset fondamentale per le aziende impegnate nella trasformazione digitale e come rappresentino l'obiettivo primario degli attacchi informatici. Risulta quindi fondamentale proteggere l'intera filiera del dato, dalla generazione alla trasmissione in Cloud, dalla memorizzazione alla elaborazione fino alla fruizione dei risultati. In fase di generazione è fondamentale che solo le soluzioni di Edge Computing autorizzate siano in grado di estrarre il dato: il gateway deve essere opportunamente protetto e controllato, così da garantire la non compromissione del suo hardware e del suo sistema operativo. Tutti i flussi di comunicazione devono essere controllati e solo quelli legittimi devono essere permessi. L'applicazione di Edge Computing deve essere firmata digitalmente e il suo ciclo di vita gestito centralmente, in modo da evitare che possa essere alterata a scopi fraudolenti. Riconducendoci ai paragrafi precedenti, l'Edge Computing può anche essere inteso come un "firewall del dato" o – in altre parole "un nodo periferico sicuro di acquisizione", che mette in sicurezza ed isola il più vicino possibile un protocollo locale non sicuro prima dell'esposizione e trasmissione dei dati da esso generati.

Tutto il ciclo va protetto

La trasmissione del dato va messa in sicurezza con opportune forme di encryption, sia a livello applicativo che a livello di rete, in modo tale che anche in caso di intercettazione il traffico non sia intellegibile.
Giunto nel Cloud, il dato va memorizzato in modo criptato, meglio se con chiavi di encryption controllate direttamente dall'azienda cui appartiene l'informazione. Il dato va protetto anche mentre viene elaborato: molti Cloud provider offrono servizi di Confidential Computing, una tecnologia che grazie a specifiche funzionalità hardware garantisce l'integrità e la confidenzialità del dato (mentre viene elaborato) e l'integrità del codice applicativo. È fondamentale proteggere anche l'accesso all'informazione e ai risultati delle elaborazioni nel Cloud: l'accesso ai dati è importantissimo per la creazione di filiere integrate e le informazioni ottenute dal processing dei dati sono il valore principale di un progetto Big Data. E' pertanto necessario provvedere utenze individuali, disattivabili singolarmente in caso di necessità, cui vengono applicate opportune policy per la gestione delle password (tipi di caratteri necessari nella password, cambiamenti periodici, ecc.). L'autenticazione a due fattori è ormai diventata un requisito imprescindibile, in quanto contromisura efficace contro il furto delle credenziali. L'accesso ai dati tramite Application Programming Interface (API) è un altro punto critico da mettere in sicurezza: si tratta infatti di una funzionalità essenziale per automatizzare lo scambio dati in una filiera integrata e proprio per questo è una delle componenti più esposte agli attacchi. Per la protezione delle API vanno previste tecnologie di Web Application & API Protection (WAAP) e Cloud Analytics in grado di analizzare l'utilizzo delle API e rilevare comportamenti anomali nei flussi di traffico da/per il Cloud.

Conclusioni

Le aziende impiegano tecnologie innovative generando una crescente mole di dati che, se opportunamente sfruttati, permettono di digitalizzare processi e prodotti per una loro più efficiente ed efficace fruibilità, a supporto dell'adozione di nuovi e sempre più sostenibili modelli di business. D'altro canto, ogni anno si registrano nuovi record per gli attacchi informatici, in continuo aumento per intensità, sofisticazione e complessità. È pertanto essenziale che le soluzioni di cyber security diventino parte integrante di ogni progetto, servizio o prodotto che abbia una componente digitale: in altre parole, la cyber security deve essere ormai considerata by-design, ovvero una parte necessaria per garantire il successo del progetto di trasformazione digitale o il corretto funzionamento di un bene interconnesso o la persistente erogazione di un servizio.