Politecnico di Torino

Corso di Laurea Magistrale in Ingegneria della Produzione Industriale e dell'Innovazione Tecnologica

Anno Accademico 2023/2024

Testi di Laurea Magistrale

Cybersecurity nelle Infrastrutture Critiche: Strategie e Sfide per il Settore Industriale

Relatore:
Prof. Abdollah Saboori

Candidato:
Alice Ribelli

Ottobre 2024

Tavola dei contenuti

Introduzione

La trasformazione digitale, spesso associata alla Quarta Rivoluzione Industriale, ha portato alla nascita di un nuovo paradigma produttivo noto come Industria 4.0. Questa evoluzione tecnologica si fonda sull'integrazione avanzata di tecnologie come l'Internet delle Cose (IoT), l'intelligenza artificiale (AI) e i sistemi di automazione industriale, che insieme abilitano la cosiddetta "manifattura intelligente." Attraverso la connessione e la collaborazione in tempo reale tra macchine, processi e dati, le fabbriche stanno diventando più efficienti, flessibili e personalizzabili.

Tuttavia, questa digitalizzazione crescente comporta sfide significative, soprattutto in ambito di sicurezza informatica. L'adozione massiccia di dispositivi interconnessi e di sistemi operativi come SCADA, DCS e PLC ha aumentato la vulnerabilità di tali infrastrutture, esponendole maggiormente agli attacchi informatici. Episodi come quelli che hanno coinvolto Colonial Pipeline e Norsk Hydro hanno evidenziato la fragilità di questi sistemi critici e la necessità di implementare strategie di cybersecurity mirate al contesto industriale.

Il presente lavoro si pone l'obiettivo di esaminare in dettaglio il ruolo della cybersecurity nell'Industria 4.0, concentrandosi in particolare sui sistemi di tecnologia operativa (OT) e sugli ambienti industriali complessi e interconnessi. Saranno analizzate le principali minacce e vulnerabilità che interessano i sistemi di controllo industriale (ICS) e l'Industrial Internet of Things (IIoT), insieme alle normative e ai regolamenti che disciplinano la sicurezza informatica in tale ambito. Particolare attenzione sarà rivolta alle best practices per l'implementazione di un'architettura di sicurezza a più livelli, con l'analisi di casi studio reali per evidenziare rischi e soluzioni adottate.

Attraverso l'esame di normative, standard di sicurezza specifici, incidenti reali e tendenze di mercato, questa tesi esplorerà le implicazioni pratiche della cybersecurity industriale, con l'obiettivo di delineare strategie efficaci e tecnologie chiave per la protezione delle infrastrutture critiche in un contesto sempre più esposto a minacce cyber.

Trasformazione digitale e Industria 4.0

La trasformazione digitale sta ridisegnando il panorama economico globale, influenzando profondamente tutti i settori, dalla manifattura ai servizi. Non si tratta solo di adottare nuove tecnologie, ma di un complesso cambiamento che coinvolge processi operativi, modelli di business e, soprattutto, la cultura e l'organizzazione aziendale. L'integrazione di tecnologie come l'Internet of Things (IoT), l'intelligenza artificiale (AI), il cloud computing e l'analisi dei Big Data sta rivoluzionando il modo in cui le aziende operano, creando nuove opportunità volte a migliorare l'efficienza, personalizzare prodotti e servizi, e accrescere il valore offerto ai clienti.

Secondo l'International Data Corporation (IDC), nel 2023 la spesa globale per la trasformazione digitale è stata di circa 2.2 trilioni di dollari e si prevede che raggiungerà quasi 4 trilioni di dollari entro il 2027. In questo contesto, l'AI emerge come uno dei principali motori di questi investimenti, con una crescita annua stimata del 16,2% tra il 2022 e il 2027. (IDC, 2024)

La produzione discreta (ovvero la produzione di beni distinti come automobili, computer e telefoni) sarà il settore che vedrà i maggiori investimenti nella trasformazione digitale (DX) nel periodo di previsione 2022-2027, con una spesa globale che raggiungerà quasi mezzo trilione di dollari nel 2024. Questa spesa crescerà fino a superare i 700 miliardi di dollari nel 2027, con l'Omni-Experience Engagement e la Sostenibilità che saranno le priorità strategiche in più rapida crescita tra le aziende di Discrete Manufacturing. (IDC, 2024)

Nonostante i progressi, la trasformazione digitale rappresenta ancora una sfida significativa per molte organizzazioni, in particolare per le piccole e medie imprese, che spesso devono affrontare ostacoli come la mancanza di competenze digitali, la resistenza al cambiamento e la necessità di investimenti consistenti. Tuttavia, le prospettive per il futuro sono positive. Il sostegno delle politiche pubbliche, unito all'impegno del settore privato, sta creando un ambiente favorevole per l'innovazione digitale, aprendo nuove frontiere di crescita e competitività a livello globale. In un mondo sempre più interconnesso e competitivo, la trasformazione digitale è ormai una necessità ineludibile per tutte le aziende, indipendentemente dal settore o dalle dimensioni.

Questa trasformazione si inserisce nel contesto della "quarta rivoluzione industriale", nota come Industria 4.0. Il concetto ha avuto origine in Germania con l'iniziativa "Industrie 4.0", una strategia promossa dal governo tedesco per rilanciare il settore manifatturiero attraverso l'integrazione di tecnologie digitali e sistemi di automazione avanzati. Presentata ufficialmente alla fiera di Hannover nel 2011, questa iniziativa ha segnato l'inizio di una nuova era industriale, destinata a rivoluzionare la produzione su scala globale.

Questo nuovo paradigma mira alla creazione di fabbriche intelligenti, interconnesse e altamente flessibili, capaci di sfruttare al massimo tecnologie come l'Internet of Things (IoT), l'intelligenza artificiale, la robotica e l'analisi dei Big Data per ottimizzare i processi produttivi e rispondere rapidamente alle esigenze del mercato.

Tale cambiamento si inserisce nella tradizione delle precedenti rivoluzioni industriali, ciascuna delle quali ha portato innovazioni epocali. La prima, spinta dall'invenzione del motore a vapore, ha avviato la produzione meccanizzata su larga scala, trasformando radicalmente l'economia. La seconda ha introdotto l'uso dell'elettricità e le catene di montaggio, permettendo la produzione di massa. La terza, con l'avvento dei computer e dell'automazione, ha inaugurato la rivoluzione digitale, migliorando la gestione e l'efficienza delle attività industriali. Ora, l'Industria 4.0 si basa su queste fondamenta, integrando tecnologie digitali avanzate per creare sistemi cyberfisici che fondono il mondo fisico con quello digitale.

Diverse tecnologie giocano un ruolo fondamentale nel ridefinire i processi manifatturieri e nell'innovare il settore produttivo. Nello specifico, la società di consulenza Boston Consulting Group, (BCG, 2023) ha individuato le nove tecnologiche che costituiscono la base dell'Industria 4.0 e cambiano i tradizionali rapporti di produzione tra fornitori, produttori e clienti, nonché tra uomo e macchina, portando a una maggiore efficienza:

1. *Big Data e Analytics*: In uno scenario Industry 4.0, i Big Data vengono raccolti da una vasta gamma di fonti. Questo include, ovviamente, la raccolta di dati provenienti da beni, attrezzature e dispositivi abilitati all'IoT. Le fonti di dati si estendono anche al di fuori del piano di produzione, fino ad altre aree dell'azienda e del mondo. Le analisi supportate da AI e machine learning vengono applicate ai dati in tempo reale, e le

intuizioni vengono sfruttate per migliorare il processo decisionale e l'automazione in ogni area della produzione e della gestione della supply chain.

2. *Integrazione Orizzontale e Verticale*: Un framework essenziale di Industry 4.0 è l'integrazione orizzontale e verticale. Con l'integrazione orizzontale, i processi sono strettamente integrati a livello "di campo" – sul piano di produzione, tra più impianti produttivi e lungo l'intera supply chain. Con l'integrazione verticale, tutti i livelli di un'organizzazione sono collegati – e i dati fluiscono liberamente dal piano di produzione fino ai livelli più alti e di nuovo verso il basso. In altre parole, la produzione è strettamente integrata con i processi aziendali come R&D, qualità, vendite e marketing e altri dipartimenti – riducendo i silos di dati e conoscenze e semplificando le operazioni.

3. *Cloud Computing*: Il cloud computing è il "grande abilitante" di Industry 4.0 e della trasformazione digitale. Consiste nella fornitura di servizi di computing, quali software, database, server e reti, tramite connessione a Internet. Ciò dà la possibilità agli utenti finali di accedere a dati e applicazioni ovunque si trovino. La tecnologia cloud odierna rappresenta la base per la maggior parte delle tecnologie avanzate – dall'AI e machine learning all'integrazione dell'IoT – fornendo piattaforme scalabili e flessibili per l'archiviazione, l'elaborazione e l'analisi di grandi quantità di dati generati dai dispostivi IoT e dagli altri sistemi industriali.

4. Realtà *Aumentata* (AR): La realtà aumentata sovrappone tipicamente contenuti digitali a un ambiente reale. Con un sistema AR, i dipendenti utilizzano occhiali intelligenti o dispositivi mobili per visualizzare dati IoT in tempo reale, parti digitalizzate, istruzioni di riparazione o assemblaggio, contenuti formativi e altro – tutto mentre osservano un oggetto fisico come un pezzo di attrezzatura o un prodotto.

5. *Internet delle Cose Industriale (IIoT):* L'Industrial Internet of Things si riferisce a sensori, strumenti e altri dispositivi interconnessi e collegati in rete con computer per applicazioni industriali, tra cui la produzione e la gestione dell'energia. La maggior parte degli oggetti fisici in Industry 4.0 – dispositivi, robot, macchinari,

attrezzature, prodotti – utilizza sensori e tag per fornire dati in tempo reale sul loro stato, prestazioni o posizione. Questa tecnologia consente alle aziende di gestire supply chain più fluide, progettare e modificare rapidamente prodotti, prevenire i tempi di inattività delle attrezzature, tracciare prodotti e inventario e molto altro.

6. *Manifattura Additiva:* La manifattura additiva, o stampa 3D, inizialmente utilizzata come strumento di prototipazione rapida, ora offre una gamma più ampia di applicazioni, dalla personalizzazione di massa alla produzione distribuita. Con la stampa 3D, parti e prodotti possono essere conservati come file di design in inventari virtuali e stampati su richiesta al punto di utilizzo – riducendo sia i costi sia la necessità di produzione fuori sede.

7. *Robot Autonomi*: Con Industry 4.0, sta emergendo una nuova generazione di robot autonomi. Programmati per eseguire compiti con minima interazione umana, i robot autonomi variano notevolmente per dimensioni e funzione, dai droni per la scansione dell'inventario ai robot mobili autonomi per operazioni di prelievo e posizionamento. Dotati di software all'avanguardia, AI, sensori e visione artificiale, questi robot sono capaci di eseguire compiti difficili e delicati – e possono riconoscere, analizzare e agire in base alle informazioni che ricevono dall'ambiente circostante.

8. *Simulazione/Digital Twins*: Un digital twin è una simulazione virtuale di una macchina, prodotto, processo o sistema del mondo reale basata sui dati dei sensori IoT. Questo componente fondamentale di Industry 4.0 consente alle aziende di comprendere meglio, analizzare e migliorare le prestazioni e la manutenzione dei sistemi e dei prodotti industriali. Un operatore di asset, ad esempio, può utilizzare un digital twin per identificare una parte specifica malfunzionante, prevedere potenziali problemi e migliorare il tempo di attività.

9. *Cybersecurity*: Con l'aumento della connettività e l'uso dei Big Data, diventa sempre più essenziale garantire canali di comunicazione affidabili e sistemi di accesso sofisticati, per prevenire o mitigare attacchi informatici. La Industrial Cybersecurity mira alla messa in sicurezza dei sistemi di controllo industriali (PLC, SCADA e HMI),

cuore pulsante dei processi produttivi, da eventuali manomissioni che comporterebbero conseguenze catastrofiche.

L'applicazione integrata di queste tecnologie avanzate apre le porte a nuove frontiere di innovazione nel settore manifatturiero. Una delle aree più promettenti è rappresentata dalla robotica collaborativa (cobot), che consente agli operatori umani di lavorare fianco a fianco con i robot in modo sicuro e sinergico. I cobot sono progettati per agire come assistenti intelligenti, in grado di svolgere compiti complessi e ripetitivi in modo rapido ed efficiente, senza compromettere la sicurezza dei lavoratori. Grazie all'apprendimento automatico e all'integrazione di sensori avanzati, questi robot collaborativi possono adattarsi alle esigenze specifiche dei lavoratori, migliorando la produttività e l'ergonomia dei processi.

Oltre alla robotica, l'Industria 4.0 sta trasformando anche il modo in cui le aziende progettano e sviluppano i propri prodotti. La realtà aumentata (AR) e la realtà virtuale (VR) stanno rivoluzionando i processi di progettazione, consentendo agli ingegneri di creare modelli digitali tridimensionali e di simulare i prodotti in ambienti virtuali prima della produzione fisica. Questa capacità di prototipazione rapida e iterativa accelera i tempi di sviluppo, riduce i costi di progettazione e permette una personalizzazione più agile dei prodotti in risposta alle esigenze del mercato.

Con il continuo avanzamento tecnologico e il cambiamento delle aspettative dei consumatori, è emersa una nuova fase di sviluppo: Industry 5.0. Questo nuovo approccio rappresenta una naturale evoluzione di Industry 4.0, spostando l'accento dalla pura automazione alla collaborazione sinergica tra uomo e macchina e alla personalizzazione avanzata dei prodotti. In questa fase, l'obiettivo è non solo migliorare l'efficienza, ma anche arricchire l'esperienza umana e rispondere alle esigenze individuali. Questo passaggio segna un cambiamento verso una produzione più sostenibile e orientata al valore aggiunto per l'umanità. Con l'Industria 5.0, l'attenzione si sposta ulteriormente verso un equilibrio tra efficienza tecnologica e benessere umano, enfatizzando la sostenibilità e la resilienza. Questa fase non solo sfrutta le tecnologie avanzate dell'Industria 4.0, ma le integra in un contesto che pone l'accento sull'essere umano e sulle pratiche di produzione sostenibili.

Espansione e Prospettive del Settore della Manifattura Intelligente

Il mercato globale della manifattura intelligente, che integra tecnologie digitali avanzate nei processi industriali, ha visto una crescita significativa, con un valore stimato tra i 283 e i 292 miliardi di dollari nel 2023.
Le proiezioni future sono altrettanto promettenti: entro il 2032 il mercato potrebbe raggiungere un valore tra i 658 e gli 880 miliardi di dollari, con un tasso di crescita annuale composto (CAGR) compreso tra il 10% e il 14,8% durante il periodo di previsione (Straits Research, 2023) (Market.us, 2024).
Secondo il rapporto McKinsey sui trend tecnologici del 2024, l'adozione di tecnologie come l'intelligenza artificiale generativa, il computing edge e le soluzioni di cybersecurity sarà determinante per il futuro della manifattura intelligente. L'intelligenza artificiale generativa, ad esempio, è destinata a crescere con un CAGR del 30%, mentre il mercato del computing edge dovrebbe toccare i 250 miliardi di dollari entro il 2025. Allo stesso modo, gli investimenti in cybersecurity potrebbero superare i 200 miliardi di dollari entro il 2025, in risposta alla crescente necessità di protezione dei dati. (Lareina Yee, 2024)

L'implementazione di queste tecnologie comporta notevoli vantaggi in termini di efficienza e innovazione, ma espone anche le organizzazioni a nuove sfide in ambito di sicurezza informatica. La fiducia digitale, in questo contesto, diventa un fattore chiave, con un'attenzione sempre maggiore verso l'approccio "security by design" e la cyber resilienza. Questi concetti non solo puntano a prevenire e mitigare le minacce, ma anche a garantire che i sistemi e le infrastrutture siano in grado di riprendersi rapidamente da eventuali attacchi o compromissioni.
Secondo lo stesso rapporto di McKinsey, circa il 30% delle aziende ha già implementato o sta espandendo l'adozione di tecnologie legate alla fiducia digitale e alla cybersecurity, mentre oltre il 60% ha effettuato investimenti significativi in queste aree. Le società di servizi finanziari sono tra le più attive, spinte dalla crescente complessità delle minacce informatiche e da normative sempre più rigorose. (Lareina Yee, 2024)

Cybersecurity: Fondamenti e Tendenze

Introduzione alla Cybersecurity

La sicurezza informatica è l'arte di proteggere reti, dispositivi e dati dall'accesso non autorizzato o dall'uso criminale, e la pratica di garantire la riservatezza, l'integrità e la disponibilità delle informazioni.
Questo approccio è ottimizzato in base ai livelli definiti dai leader aziendali, che devono bilanciare le risorse necessarie con l'usabilità e la gestibilità, oltre a considerare il livello di rischio da mitigare. All'interno del vasto panorama della cybersecurity, è possibile identificare diverse sottocategorie, tra cui la sicurezza IT, la sicurezza IoT, la sicurezza delle informazioni e la sicurezza OT. Ognuna di queste aree svolge un ruolo cruciale nel garantire la protezione complessiva dell'infrastruttura digitale di un'azienda, contribuendo a mantenere al sicuro i dati e i sistemi critici in un contesto di minacce sempre più sofisticate.

Un'efficace strategia di cybersecurity si basa su tre componenti essenziali: *persone, processi* e *tecnologie*, il cui coordinamento è essenziale per garantire la protezione completa di informazioni e sistemi.
- *Persone*: Le organizzazioni devono assumere professionisti della cybersecurity adeguatamente formati per progettare e implementare framework di sicurezza efficaci. È fondamentale formare i dipendenti affinché possano riconoscere truffe di phishing e tecniche di ingegneria sociale. Infatti, le persone rappresentano spesso il punto più vulnerabile nella resilienza informatica di un'organizzazione.
- *Processi*: I processi e le politiche forniscono le linee guida per la governance della cybersecurity. Questi processi comprendono piani di risposta agli incidenti, analisi delle minacce, definizione delle priorità degli asset e interventi in tempo reale in caso di crimine informatico, permettendo di identificare ed eliminare eventuali intrusi.
- *Tecnologia*: La tecnologia si riferisce all'infrastruttura IT, sia hardware che software, utilizzata dalle organizzazioni per raggiungere i propri obiettivi di cybersecurity. Esempi includono software antivirus e intelligenza artificiale difensiva, in grado di monitorare le reti informatiche alla ricerca di comportamenti anomali e di apprendere dagli attacchi precedenti.

Figura 1 - I tre pilastri della Cyber Security: Persone, Processo, Tecnologia

La cybersecurity è, dunque, cruciale per proteggere i dati e le risorse aziendali in un contesto digitale sempre più complesso. Al centro di questa disciplina vi è la triade CIA, che sintetizza i tre principi fondamentali su cui si basa la sicurezza informatica: *riservatezza, integrità* e *disponibilità*. Questi elementi operano sinergicamente per garantire la protezione delle informazioni sensibili, preservare l'accuratezza dei dati e assicurarne l'accessibilità in modo sicuro, contribuendo così a mantenere la continuità operativa dell'organizzazione.

Nello specifico, la *riservatezza* limita l'accesso alle informazioni sensibili dell'azienda, *l'integrità* garantisce che i dati e le apparecchiature dell'azienda rimangano affidabili e accurati, mentre la *disponibilità* fornisce accesso tempestivo ai dati e alle apparecchiature dell'azienda.

Figura 2 - La triade CIA

Altri attributi vengono talvolta aggiunti alla triade CIA, come la privacy e la sicurezza, ma questi sono i principi fondamentali generalmente accettati e che qualsiasi adottatore dell'Industria 4.0 dovrebbe considerare. (Toth P. , 2022)

L'importanza della Cybersecurity nelle Organizzazioni Moderne

La cybersecurity è un campo vasto e in continua evoluzione. Questo settore comprende numerose specializzazioni, ognuna delle quali gioca un ruolo cruciale nella creazione di un ecosistema digitale sicuro. Il processo di protezione dei dati digitali può essere articolato su sei elementi chiave, che proteggono i dati in tre stati principali: *memorizzati*, *elaborati* o *trasmessi*.

Il **Network Security** si concentra sulla protezione dei dati mentre viaggiano attraverso la rete aziendale o Internet. Questo livello introduce procedure per prevenire l'accesso non autorizzato ai dati degli individui dall'esterno del processo industriale. Ciò include:

- *L'autenticazione di ogni utente*: verifica l'identità di ogni utente tramite password robuste, autenticazione a due fattori, chiavi di sicurezza fisiche o certificati digitali, ecc.
- *Firewall di rete*: verificano le regole di accesso e consentono i servizi solo agli utenti autorizzati. Questi dispositivi o software filtrano il traffico di rete in entrata e in uscita, bloccando o consentendo le connessioni in base a regole prestabilite.
- *Antivirus e Antimalware*: questi programmi rivelano, bloccano e neutralizzano software dannosi come virus, trojan e ransomware, esaminando il contenuto dei programmi installati per rilevare e neutralizzare software dannoso.
- *Sistemi di rilevamento e prevenzione delle intrusioni* (IDS/IPS): Un IDS, Intrusion Detection System, monitora il traffico di rete per rilevare attività sospette e prevenire attacchi in tempo reale, mentre l'IPS, Intrusion Prevention System, previene attacchi in tempo reale, bloccando pacchetti di dati sospetti.

L'**Application Security** riguarda il processo di protezione delle applicazioni durante tutte le fasi del loro sviluppo e utilizzo. È particolarmente importante poiché le applicazioni sono un canale potenziale per gli attacchi. Le principali pratiche di sicurezza includono:

- *Analisi delle vulnerabilità*: si esaminano le applicazioni per l'identificazione e correzione delle vulnerabilità durante il ciclo di vita dello sviluppo del software.

- *Progettazione sicura:* vengono implementate pratiche che riducono al minimo le vulnerabilità, come l'uso di codifica sicura e il principio di privilegio minimo, fin dall'inizio dello sviluppo.
- *Test di penetrazione (Pen Testing*): si simulano attacchi contro l'applicazione per identificare le aree deboli che potrebbero essere sfruttate.
- *Crittografia dei dati*: consiste nella protezione dei dati sensibili all'interno delle applicazioni tramite algoritmi di crittografia robusti, rendendo i dati incomprensibili a chiunque non abbia la chiave di decrittazione.

La **Information/Data Security** protegge informazioni e documentazione (dati aziendali critici, documenti legali e altre informazioni sensibili), dati relativi ai prodotti (informazioni sul ciclo di vita dei prodotti, dalla progettazione alla produzione), nonché dati di dipendenti e clienti (informazioni personali e sensibili), da accessi non autorizzati, manomissioni e perdite. Le tecnologie e politiche di sicurezza implementate comprendono:

- *Gestione delle identità e degli accessi (IAM):* controlla chi ha accesso a determinate informazioni e quali operazioni possono essere eseguite. Questo implica l'uso di autenticazione forte e autorizzazioni granulari.
- *Politiche di sicurezza rigorose*: queste includono la gestione delle password, la classificazione dei dati, e l'uso di protocolli di backup e ripristino in caso di perdita o corruzione dei dati.
- *Crittografia dei dati:* si basa sull'uso di modelli matematici per codificae dati in modo tale che solo le parti che hanno la chiave per decodificarli possano accedervi.

La **Operations Security** si occupa della protezione dei processi aziendali e operativi. Essa mira a garantire che l'infrastruttura IT e i processi industriali funzionino in sicurezza e senza interruzioni. Gli elementi principali sono:

- *Protezioni dei processi industriali:* questo riguarda la sicurezza delle macchine, robot, sistemi di controllo industriale (ICS) e tutto ciò che supporta le operazioni. Il sabotaggio o la manomissione di questi sistemi può avere gravi conseguenze.
- *Infrastruttura IT*: include il monitoraggio continuo di server, dispositivi di rete e risorse critiche per identificare minacce o anomalie in tempo reale.

- *Risposta agli incidenti:* si occupa della pianificazione e implementazione di misure di risposta agli incidenti per mitigare i danni in caso di attacco. Quando si verifica una violazione della sicurezza, devono essere messe in atto misure per ridurre al minimo i danni, come la disconnessione di sistemi compromessi o il ripristino da backup sicuri.
- *Gestione del rischio:* identifica, analizza e mitiga i rischi per garantire che le operazioni continuino senza interruzioni anche durante un attacco.

Il **Cloud Security** è il processo di protezione dei dati e delle applicazioni memorizzate nel cloud da accessi non autorizzati. Mentre i fornitori di servizi cloud gestiscono l'infrastruttura, le organizzazioni che utilizzano i loro servizi devono adottare ulteriori precauzioni per garantire la sicurezza dei propri dati, attraverso:

- *Backup regolari:* la creazione di copie di sicurezza dei dati su base regolare assicura, in caso di perdita di dati, il ripristino rapido dell'operatività senza gravi interruzioni.
- *Piani di ripristino di emergenza:* include piani dettagliati per il ripristino dei dati in caso di guasti o attacchi, come ransomware o altre minacce.
- *Conservazione esterna dei dati*: consiste nell'archiviazione di dati sensibili in più luoghi, inclusi servizi di cloud storage, per ridurre il rischio di perdita permanente.

La **End point Security** riguarda la protezione dei dispositivi degli utenti finali, come computer, smartphone e tablet, che rappresentano spesso il punto più vulnerabile in una rete. Le pratiche chiave per la sicurezza di questi dispositivi includono:

- *Adozione di pratiche sicure:* utilizzo di password forti, installazione di software e antivirus aggiornamenti regolari per garantire che tutte le patch di sicurezza siano applicate.
- *EndPoint Detection and Response (EDR):* questi strumenti forniscono visibilità sugli endpoint, consentendo di individuare attività sospette in tempo reale e rispondere rapidamente agli attacchi, semplificando la gestione e automatizzando le attività di allerta e risposta.
- *Gestione dei dispositivi:* l'implementazione di soluzioni come il Mobile Device Management (MDM) consente alle organizzazioni di monitorare e gestire centralmente i dispositivi mobili e gli endpoint, garantendo che siano conformi alle

politiche di sicurezza aziendale

Con l'espansione dei dispositivi connessi a Internet, la **IoT Security** è fondamentale per proteggere apparecchi come smart home devices e sensori industriali. Le principali misure comprendono:

- *Scoperta e classificazione dei dispositivi:* Identificare e monitorare i dispositivi connessi alla rete per rilevare vulnerabilità o attività sospette.
- *Segmentazione della rete:* Separare i dispositivi IoT dal resto della rete aziendale per limitare la portata di eventuali compromissioni.
- *Patch virtuali:* Implementare aggiornamenti rapidi per prevenire sfruttamenti di vulnerabilità note e sconosciute, senza richiedere l'installazione di patch ufficiali.

Tipologie di Attacchi Informatici

Nel panorama della sicurezza informatica, le minacce e gli attacchi evolvono costantemente, sfruttando la vulnerabilità dei sistemi e delle reti per compromettere dati e operazioni aziendali. Gli attacchi possono manifestarsi in diverse forme, ognuna con tecniche e obiettivi specifici. Tra i tipi più comuni di attacchi informatici ci sono:

- *Malware***:** Il malware, o software malevolo, è qualsiasi programma o codice creato con l'intento di danneggiare o ottenere accesso non autorizzato a computer, rete o server. È il tipo di attacco informatico più comune, poiché il termine include diverse sottocategorie di tipi di attacchi, tra cui:

- *Trojan horses:* Si mascherano da programmi utili o si nascondono all'interno di software legittimo per indurre gli utenti a installarli, creando una porta segreta sul dispositivo della vittima o installando ulteriori malware una volta che si è ottenuto un accesso iniziale.
- *Ransomware*: È un tipo di malware sofisticato che utilizza una forte crittografia per tenere in ostaggio dati o sistemi. I criminali informatici richiedono poi un pagamento in cambio del rilascio del sistema e del ripristino delle sue funzionalità. Secondo l'Indice delle Minacce di IBM X-Force, il ransomware è il secondo tipo più comune di attacco informatico, rappresentando il 17% degli attacchi. (IBM X-Force, 2024)
- *Scareware:* Utilizza messaggi falsi per spaventare le vittime e indurle a scaricare malware o a fornire informazioni sensibili a truffatori.

- *Social engineering*: Gli attacchi di social engineering sfruttano la manipolazione psicologica per indurre le persone a compiere azioni dannose, come divulgare informazioni riservate, scaricare software nocivo o trasferire denaro ai truffatori. Il *Phishing* è uno dei metodi di social engineering più comuni, in cui vengono utilizzati e-mail o messaggi di testo falsificati per rubare credenziali, sottrarre dati sensibili o distribuire malware.

  Nel caso di una *compromissione dell'e-mail aziendale* (BEC), i truffatori si spacciano per dirigenti, fornitori o partner commerciali per indurre le vittime a trasferire denaro o a condividere dati sensibili. Secondo il report "Cost of a Data Breach", è la seconda causa più frequente di violazioni dei dati.
- *Denial-of-service attacks (DDos):* Gli attacchi di Denial-of-Service (DoS) e di Distributed Denial-of-Service (DDoS) inondano le risorse di un sistema con traffico fraudolento. Questo traffico sovraccarica il sistema, impedendo la risposta alle richieste legittime e riducendo la capacità del sistema di funzionare correttamente.

  Nello specifico, gli attacchi DoS utilizzano una sola fonte per generare traffico fraudolento, mentre gli attacchi DDoS impiegano più fonti.
- *Attacchi Man-in-the-Middle:* In un attacco man-in-the-middle (MitM), noto anche come "attacco di intercettazione," un hacker intercetta segretamente le comunicazioni tra due persone o tra un utente e un server. Gli attacchi MitM sono frequentemente eseguiti tramite reti Wi-Fi pubbliche non sicure, dove è relativamente facile per i malintenzionati spiare il traffico. In un attacco di *session hijacking*, l'hacker interrompe la connessione tra un utente e un server che ospita dati importanti, come un database aziendale riservato, e sostituisce il proprio indirizzo IP con quello dell'utente, facendo credere al server di essere un utente legittimo con una sessione valida.
- *Attacco SQL injection:* Gli aggressori utilizzano l'iniezione di linguaggio SQL per sfruttare le vulnerabilità e prendere il controllo di un database. Una query SQL è una richiesta di esecuzione di un'azione su un database e una richiesta malevola ben costruita può creare, modificare o cancellare i dati memorizzati nel database. Molti siti e applicazioni web memorizzano i dati in SQL e li utilizzano per condividere i dati degli utenti con i database. Se un aggressore individua una vulnerabilità in una

pagina web, può eseguire una SQL injection per scoprire le credenziali dell'utente e sferrare un attacco informatico.

- *DNS tunneling:* È un tipo di attacco informatico che sfrutta le vulnerabilità del Domain Name System (DNS), un protocollo che traduce gli indirizzi Web in indirizzi IP, per deviare il traffico web verso siti falsi. Il tunneling DNS è un attacco difficile da rilevare che instrada le richieste DNS verso il server dell'aggressore, fornendo a quest'ultimo un canale di comando e controllo di comunicazione che può essere utilizzato per rubare dati e svolgere altre attività dannose. Il DNS gode di ampia fiducia e, poiché non è destinato all'esfiltrazione di dati, spesso non viene monitorato per rilevare attività dannose.
- *Zero Day Attack:* Un exploit zero-day è un vettore di cyberattacco che sfrutta una falla di sicurezza sconosciuta o non risolta nel software, nell'hardware o nel firmware di un computer. Quando un aggressore individua una vulnerabilità del codice, crea un exploit per infiltrarsi nel sistema di un'organizzazione, prima che questa si accorga del problema. Una volta all'interno, l'aggressore può raccogliere dati sensibili e rubare le credenziali degli utenti senza essere scoperto.

Evoluzione e Tendenze nel Panorama delle Minacce Informatiche

Nel contesto attuale della Cybersecurity, i criminali informatici stanno adottando tattiche sempre più sofisticate e mirate, evidenziando un'evoluzione preoccupante nelle minacce e nei metodi di attacco. Le statistiche recenti rivelano tendenze chiave che le organizzazioni devono affrontare per migliorare la loro sicurezza.

Nel 2023, per la prima volta, l'abuso di account validi è emerso, insieme al phishing, come il vettore di accesso predominante per i criminali informatici, rappresentando il 30% degli incidenti segnalati da IBM X-Force. Questo segna un incremento del 71% rispetto all'anno precedente, riflettendo una crescente disponibilità di credenziali compromesse, spesso facilmente reperibili nel dark web. Questa tendenza suggerisce che i criminali informatici stanno trovando più semplice sfruttare credenziali legittime piuttosto che effettuare attacchi complessi.

Gli attacchi di phishing, sebbene ancora rappresentino il 30% degli incidenti, hanno visto una riduzione del 44% rispetto al 2022. Questo calo potrebbe riflettere l'efficacia delle

tecniche di mitigazione del phishing e un cambiamento verso l'utilizzo di credenziali compromesse come metodo preferito di accesso iniziale.

Un'altra tendenza preoccupante è l'aumento dell'utilizzo degli infostealers, un tipo di malware progettato per raccogliere informazioni sensibili in modo furtivo. Nel 2023, si è registrato un'impressionante impennata del 266% nell'uso di questo malware. Questa tendenza al rialzo ha probabilmente contribuito all'aumento dell'abuso di account validi, il principale vettore di accesso iniziale osservato da X-Force. Gruppi di minacce che in passato si concentravano prevalentemente su attacchi ransomware stanno ora diversificando le loro attività, investendo nello sviluppo di software specificamente progettati per la sottrazione di dati.

Secondo IBM X-Force 2023, la distribuzione di malware rimane una delle azioni più comuni, rappresentando il 43% di tutti gli incidenti segnalati. Di questi, il 20% sono stati casi di ransomware. Al secondo posto, il 32% degli incidenti vede l'uso dannoso di strumenti legittimi per il furto di credenziali, l'accesso remoto e l'esfiltrazione dei dati.

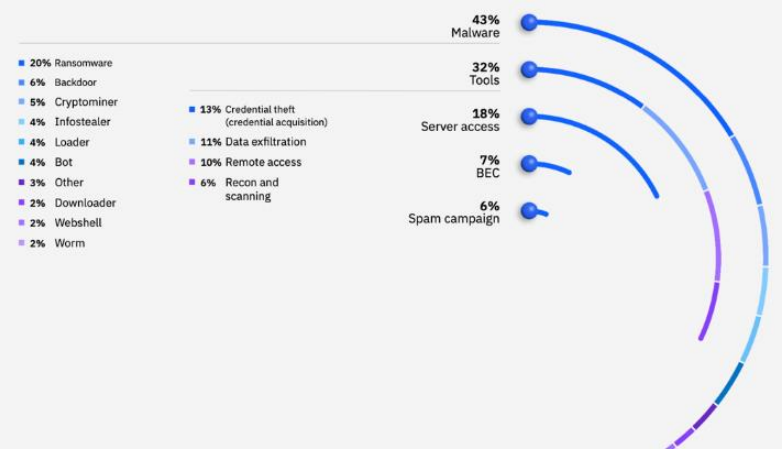

Figura 3 - Principali attacchi informatici 2023

Nel 2023, il furto e la perdita di dati sono diventati l'impatto principale per le organizzazioni, rappresentando il 32% degli incidenti gestiti da IBM X-Force, un notevole incremento rispetto al 19% registrato nel 2022. Questo aumento è coerente con la crescita nell'attività degli infostealer e nell'uso di strumenti legittimi per esfiltrare dati sensibili.

Inoltre, nel 2023, gli episodi di estorsione sono aumentati di oltre il doppio, con la percentuale di incidenti classificabili come estorsioni che è salita dal 21% del 2022 al 24% del 2023. Come già menzionato, gli attacchi di estorsione si sono confermati tra le principali cause della criminalità informatica nel 2023, con i criminali informatici che hanno sfruttato diverse tipologie di attacco per raggiungere i loro scopi di estorsione. (IBM X-Force, 2024)

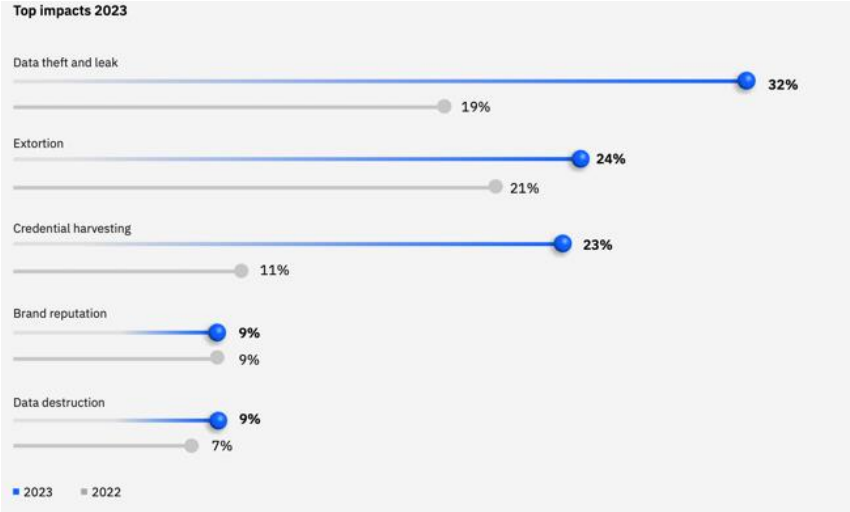

Figura 4 - Principali impatti 2023

Gli attacchi basati sull'estorsione continuano a essere una delle forze trainanti del crimine informatico. I criminali informatici stanno adottando diverse modalità per raggiungere i loro obiettivi di estorsione, spesso utilizzando tattiche che non prevedono il ransomware tradizionale. Invece di criptare i dati, i criminali possono minacciare di esporre dati sensibili rubati per esercitare pressione sulle vittime e ottenere pagamenti. Questo approccio, meno impegnativo in termini di risorse rispetto ai metodi di attacco basati su ransomware, dimostra come le tattiche di estorsione siano sempre più efficaci nel costringere le vittime a pagare.

Ad oggi l'uso crescente dell'intelligenza artificiale (AI) rappresenta una nuova frontiera sia per la difesa che per gli attacchi informatici. Anche se al momento non ci sono conferme definitive sull'uso di AI generativa nelle campagne malevoli, l'interesse dei criminali informatici per questa tecnologia è evidente. Strumenti come FraudGPT e WormGPT, promossi su forum e canali Telegram, indicano che alcuni gruppi di

cybercriminali stanno esplorando l'AI come potenziale risorsa per attività illecite, come la creazione di e-mail di phishing e altre forme di attacco. Si prevede che gli strumenti di intelligenza artificiale generativa (GenAl) permetteranno a determinati attaccanti di creare e-mail di phishing e siti web credibili in modo più rapido e semplice. Inoltre, si ritiene che tecnologie come Deep Voice e Deepfake Video possano essere utilizzate come mezzo di accesso iniziale.
Nonostante l'assenza di dati concreti su campagne di attacco basate su AI fino ad oggi, X-Force ha registrato una crescente discussione sull'AI e sui modelli linguistici generativi (GPT) in oltre 800.000 post su mercati illeciti e forum della dark web nel 2023. Questo segnale suggerisce un crescente interesse tra i criminali informatici per l'adozione di queste tecnologie. X-Force ha effettuato un'analisi approfondita delle tecniche e delle tecnologie utilizzate dai criminali, rilevando che le tecnologie che raggiungono una dominanza di mercato possono diventare obiettivi privilegiati per attacchi su larga scala. Con l'adozione aziendale dell'AI in continua espansione, è previsto che i criminali informatici inizieranno a sfruttare l'AI nelle loro operazioni man mano che la tecnologia matura.

A livello geografico, nel 2023, l'Europa è diventata la regione più colpita dagli attacchi informatici, con il 32% degli incidenti gestiti da X-Force, seguita dal Nord America con il 26% e dall'Asia-Pacifico con il 23%. America Latina e Medio Oriente e Africa hanno rappresentato rispettivamente il 12% e il 7% degli incidenti.
In Europa, l'azione di attacco più frequente è stata il malware, che ha rappresentato il 44% degli incidenti. La regione ha anche visto il maggior numero di attacchi ransomware a livello globale, con un significativo 26%.

L'Europa sta vivendo una crescita esponenziale nell'utilizzo di piattaforme cloud. Questa diffusione potrebbe però contribuire a una maggiore superficie di attacco rispetto ad altre regioni. Infatti, il 30% degli attacchi ha utilizzato account validi (siano essi cloud, di dominio o locali) per compromettere le organizzazioni. Il phishing ha rappresentato anch'esso il 30% degli incidenti, mentre l'esploitazione di applicazioni pubblicamente esposte e l'uso di servizi remoti esterni hanno avuto entrambi una quota del 20%. Gli

impatti principali per le organizzazioni europee sono stati il furto di credenziali (28%), l'estorsione (24%) e la perdita di dati (16%).

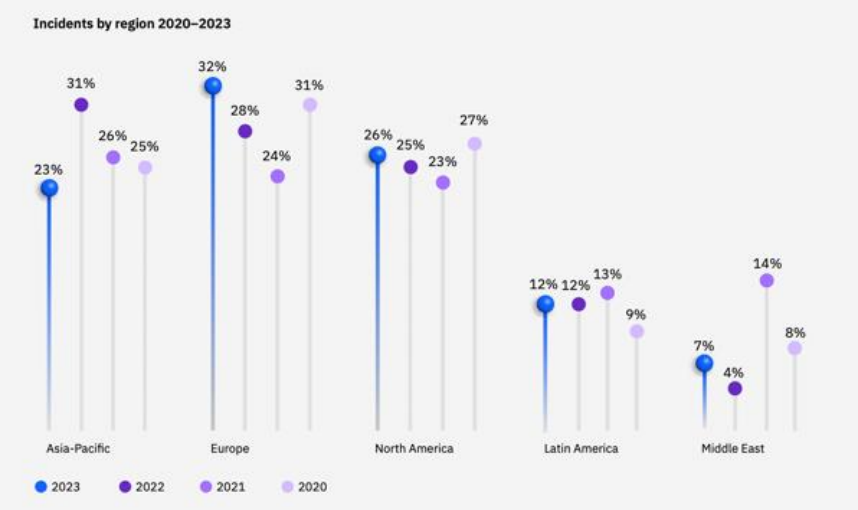

Figura 5 - Incidenti informatici per regione geografica

La Cybersecurity Industriale: Pilastro della Quarta Rivoluzione Industriale

Introduzione alla Cybersecurity Industriale

L'avvento dell'Industria 4.0 ha accelerato l'adozione di tecnologie avanzate portando a un livello senza precedenti di ottimizzazione e automazione. Questo progresso ha generato un'enorme quantità di dati, la cui gestione efficace è diventata cruciale per il successo delle aziende. Secondo Gartner, entro il 2025, oltre il 40% delle aziende manifatturiere integrerà soluzioni moderne per la qualità dei dati (DQ) per sostenere i propri obiettivi di trasformazione digitale e ottimizzare i processi decisionali (Aggarwal, 2023). Tuttavia, con l'afflusso massiccio di dati, è essenziale che le aziende mettano in atto strategie robuste per mitigare i rischi e garantire la sicurezza e l'integrità delle informazioni.

In questo contesto, la cybersecurity industriale si rivela un pilastro fondamentale sia nella Quarta che nella Quinta Rivoluzione Industriale. La convergenza tra tecnologie operative

(OT) e informatiche (IT) ha reso i sistemi industriali più interconnessi e, di conseguenza, più vulnerabili a minacce cibernetiche. Sebbene entrambi siano essenziali per il funzionamento delle imprese, presentano caratteristiche, obiettivi e vulnerabilità distinti:
La *Tecnologia Operativa (OT)* si riferisce a hardware e software utilizzati per monitorare e controllare dispositivi fisici, processi ed eventi in ambienti industriali. Include sistemi come i Sistemi di Controllo Industriale (ICS), i Sistemi di Controllo Distribuito (DCS), SCADA e l'Industrial Internet of Things (IIoT). Questi sistemi gestiscono e monitorano infrastrutture e processi industriali in tempo reale, garantendo efficienza operativa e sicurezza fisica in settori critici. Essi sono fondamentali per la produzione, la gestione delle risorse e la garanzia della sicurezza fisica nei settori industriali.
La *Tecnologia dell'Informazione (IT)* riguarda l'uso di computer, storage e altre infrastrutture per creare, elaborare, archiviare e scambiare dati elettronici. I sistemi IT tra cui server, reti, software applicativo e database, sono essenziali per gestire le informazioni aziendali e supportare le operazioni quotidiane. Questi sistemi sono vulnerabili a minacce informatiche quali il phishing, ransomware, e il furto di dati.
Storicamente, i sistemi OT e IT operavano in modo indipendente, con i sistemi OT spesso isolati ("air-gapped") per proteggere le operazioni fisiche da potenziali minacce esterne.
Tuttavia, l'evoluzione tecnologica ha comportato una crescente integrazione tra tecnologie operative (OT) e tecnologie dell'informazione (IT), guidata dalla necessità di migliorare l'efficienza operativa, la produttività e la visibilità dei dati in tempo reale.
I sistemi OT, inizialmente progettati senza robusti meccanismi di sicurezza informatica, sono ora vulnerabili agli stessi attacchi che colpiscono i sistemi IT. Per proteggere adeguatamente questi sistemi, è fondamentale comprendere le loro specifiche vulnerabilità e implementare strategie di sicurezza che includano monitoraggio continuo, aggiornamenti regolari e formazione del personale.

Gli attacchi informatici possono avere conseguenze devastanti per le aziende del settore industriale. La paralisi delle linee produttive, causata da malware o ransomware, può comportare ingenti perdite economiche e danni alla sicurezza dei lavoratori.
Inoltre, la sottrazione di informazioni strategiche e proprietà intellettuale può compromettere gravemente la competitività e la reputazione delle organizzazioni.

Tali incidenti cibernetici possono inoltre generare significativi impatti finanziari, tra cui costi di ripristino, penali contrattuali e sanzioni normative.
La coesistenza di infrastrutture OT, che possono essere obsolete e progettate senza considerare i rischi informatici, insieme a componenti IoT, caratterizzate da un elevato livello di connettività ma da capacità elaborativa limitata per la protezione dagli attacchi, rende questi ambiti potenzialmente molto vulnerabili.

Oltre alle sfide poste dalle minacce IT tradizionali e dalle vulnerabilità OT, i produttori devono anche affrontare i rischi associati al software personalizzato. Nel panorama industriale moderno, la necessità di una comunicazione efficiente e continua tra diversi sistemi è sempre più cruciale. Per raggiungere questo obiettivo, i produttori spesso personalizzano le loro apparecchiature e software per facilitare l'integrazione e lo scambio di dati. Tuttavia, questi sistemi potrebbero non funzionare con le attuali tecniche di cybersecurity o potrebbero introdurre involontariamente delle vulnerabilità.

Un altro problema chiave sta nel fatto che spesso il software, per timore di interruzioni del processo produttivo, non venga aggiornato o patchato regolarmente per affrontare nuove vulnerabilità. Questo lascia i sistemi esposti a falle di sicurezza note. Inoltre, se il software personalizzato non è progettato con la sicurezza come priorità e non riceve una manutenzione adeguata, può diventare un punto debole nell'intera architettura di sicurezza, consentendo accessi non autorizzati e rappresentando un rischio significativo per l'operatività aziendale.

Importante è quindi implementare procedure di protezione per difendere i sistemi industriali dagli attacchi informatici. Questo richiede misure di sicurezza avanzate, tra cui il monitoraggio del traffico di rete, la segmentazione delle reti, aggiornamenti regolari del software e autorizzazioni rigorose per l'accesso ai sistemi. Inoltre, è fondamentale la formazione continua dei dipendenti sulla sicurezza informatica e la preparazione di piani di emergenza per rispondere rapidamente a eventuali incidenti. Prevenire gli attacchi e gestire adeguatamente i rischi sono elementi essenziali per mantenere la stabilità e la sicurezza nel settore industriale.

Il report "State of Smart Manufacturing 2024" di Rockwell Automation offre un'analisi dettagliata del panorama attuale della manifattura intelligente. Il report evidenzia che, nel 2024, la cybersecurity si posiziona al terzo posto tra i rischi esterni per le aziende, evidenziando la crescente preoccupazione per le minacce legate alla digitalizzazione.
Parallelamente, la sicurezza informatica è emersa come la competenza numero uno richiesta dai datori di lavoro nel 2024, a testimonianza della necessità di professionisti capaci di affrontare sfide legate alla sicurezza dei sistemi informatici.
Guardando al futuro, le previsioni indicano che la cybersecurity sarà il secondo settore più influenzato dall'intelligenza artificiale nei prossimi tre anni, subito dopo la qualità. (Rockwell Automation, 2024)
Per affrontare efficacemente le sfide della cybersecurity nell'Industria 4.0, le aziende devono adottare un approccio olistico e integrato, che coinvolga tecnologia, processi e persone. L'implementazione di framework e standard di cybersecurity, come il NIST Cybersecurity Framework e la norma IEC 62443, consente di definire roadmap e linee guida per l'attuazione di misure di sicurezza adeguate. Queste includono la protezione dei sistemi industriali legacy, il monitoraggio dei dispositivi connessi e la formazione del personale.
A livello globale, i governi stanno prestando maggiore attenzione ai crimini informatici. In Europa, il Regolamento Generale sulla Protezione dei Dati (GDPR) ha rafforzato la responsabilità delle organizzazioni in caso di violazioni dei dati, obbligandole a comunicare tempestivamente le infrazioni, nominare un responsabile della protezione dei dati, ottenere il consenso degli utenti per l'elaborazione delle informazioni e anonimizzare i dati per garantire la privacy.

Analisi e Implicazioni della Crescita degli Incidenti Informatici

Se da un lato i vantaggi della connettività includono maggiori livelli di produttività, dall'altro possono moltiplicare le potenziali vulnerabilità della fabbrica intelligente. Infatti, la Cybersecurity and Infrastructure Security Agency (CISA) elenca oltre 1.200 problemi di sicurezza, vulnerabilità ed exploit noti relativi ai sistemi OT, provenienti da oltre 300 OEM e fornitori di sistemi. (Sean Peasley, 2020)

Secondo il rapporto X-Force di IBM del 2023, quando si tratta di attacchi informatici per settore, quello manifatturiero risulta il principale bersaglio. (IBM X-Force, 2024)

Di conseguenza, nel settore industriale globale, incluso il segmento manifatturiero, il costo medio di una violazione dei dati ha subito un incremento significativo, crescendo del 10% in un solo anno. Nel 2023, il costo medio globale di una violazione dei dati ha raggiunto i 4.88 milioni di dollari, rappresentando l'aumento più marcato dall'inizio della pandemia. Questo incremento è stato principalmente alimentato dalle spese legate alle interruzioni operative e alle attività di risposta post-violazione, che si sono dimostrate particolarmente onerose. (IBM, 2024)

Nello stesso settore, si è registrato l'aumento più significativo dei costi medi per violazione dei dati rispetto a tutti gli altri settori, con un incremento di 830.000 USD rispetto all'anno precedente. Questo aumento nei costi riflette non solo la complessità delle operazioni industriali e manifatturiere, ma anche la criticità delle interruzioni di produzione, che possono causare perdite finanziarie significative e richiedere interventi costosi per il ripristino delle normali attività.

Come mostrato in Figura 6, i costi legati alla perdita di affari e alle risposte post-violazione sono aumentati drasticamente, con un incremento di quasi l'11% rispetto all'anno precedente. I costi della perdita di affari comprendono la perdita di entrate dovuta ai tempi di inattività dei sistemi, i danni alla reputazione e la perdita di clienti. Le spese post-violazione includono i costi per l'istituzione di centri di assistenza e servizi di monitoraggio del credito per i clienti colpiti, oltre al pagamento di multe regolamentari.

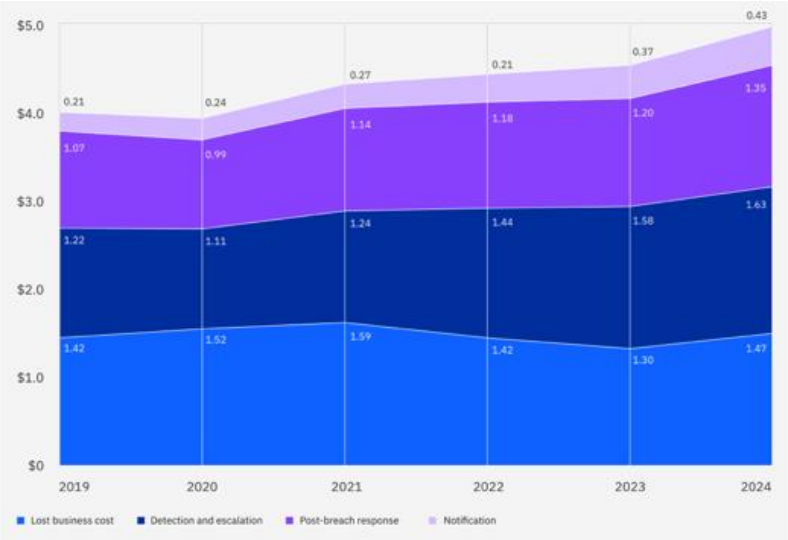

Figura 6 - Costo medio della violazione dei dati in USD

A livello globale, i team di sicurezza stanno migliorando nella capacità di rilevare e contenere le violazioni, nonostante la persistente carenza di competenze. Più della metà delle organizzazioni che subiscono violazioni sta affrontando una mancanza di personale qualificato in sicurezza, e i leader del settore stanno rispondendo a questa sfida adottando soluzioni basate su intelligenza artificiale e automazione per colmare il divario. Tuttavia, per salvaguardare le proprie aziende, una recente indagine IBM ha rilevato che il 51% dei leader ha dichiarato di voler aumentare gli investimenti in sicurezza (INCIT, 2024) .

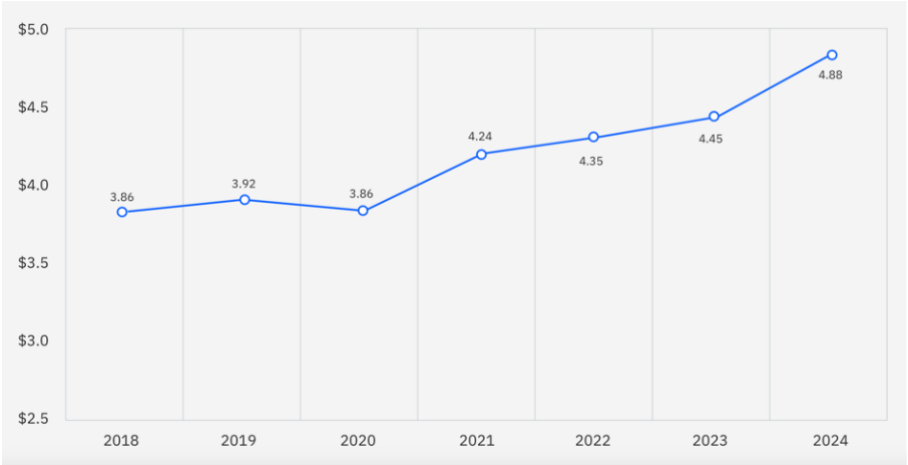

Figura 7 - Costo totale medio globale di una violazione dei dati

Secondo lo stesso report IBM, nel 2023, il settore manifatturiero è stato ancora una volta il più colpito dagli attacchi informatici, per il terzo anno consecutivo, rappresentando il 25,7% degli incidenti tra i primi 10 settori maggiormente attaccati. Tra le azioni malevoli più comuni, il malware si è confermato come il tipo di attacco più frequente, incidendo sul 45% dei casi. Il ransomware ha costituito il 17% degli incidenti, mantenendo lo stesso livello del 2022. Inoltre, è stato osservato che il 31% degli attacchi ha coinvolto l'uso di strumenti legittimi per scopi malevoli, con il furto di credenziali come la causa principale in ben il 17% dei casi. (IBM X-Force, 2024)

Industry	2023	2022	2021	2020	2019
Manufacturing	25.7%	24.8	23.2	17.7	8
Finance and insurance	18.2%	18.9	22.4	23	17
Professional, business and consumer services	15.4%	14.6	12.7	8.7	10
Energy	11.1%	10.7	8.2	11.1	6
Retail and wholesale	10.7%	8.7	7.3	10.2	16
Healthcare	6.3%	5.8	5.1	6.6	3
Government	4.3%	4.8	2.8	7.9	8
Transportation	4.3%	3.9	4	5.1	13
Education	2.8%	7.3	2.8	4	8
Media and telecommunications	1.2%	0.5	2.5	5.7	10

Figura 8 - Percentuale di attacchi per settore 2019 - 2023

Un altro dato rilevante è l'aumento degli incidenti legati all'accesso ai server, che hanno rappresentato il 21% dei casi, in crescita rispetto al 17% dell'anno precedente. Per quanto riguarda l'impatto sulle organizzazioni manifatturiere, il 36% degli incidenti ha riguardato la raccolta di credenziali e il furto o la perdita di dati. Altri incidenti hanno comportato distruzione dei dati ed estorsione, ciascuno dei quali ha impattato il 16% dei casi.
Nel contesto degli attacchi informatici, il phishing è stato il vettore di infezione iniziale più comune, colpendo il 39% delle aziende manifatturiere. Questo è seguito dallo sfruttamento delle applicazioni pubbliche, responsabile del 33% degli incidenti, e dall'abuso dei servizi remoti esterni, che ha rappresentato il 22% dei casi.
Geograficamente, la regione Asia-Pacifico ha visto il maggior numero di attacchi nel settore manifatturiero, con circa il 54% degli incidenti totali. L'Europa ha registrato il secondo maggior numero di attacchi, con il 26%, seguita dal Nord America con il 12% e dall'America Latina con il 5%. Questi dati sottolineano una crescente tendenza agli attacchi informatici nel settore manifatturiero, con un'evidente prevalenza di phishing come vettore iniziale e una concentrazione significativa di attacchi nella regione Asia-Pacifico. (IBM X-Force, 2024)

Un altro report, redatto da Dragos, un'azienda specializzata nella sicurezza informatica per le infrastrutture critiche e i sistemi di controllo industriale, ha osservato un aumento del 28% nel numero di gruppi di ransomware attivi rispetto all'anno precedente, con un totale di 50 gruppi e 905 incidenti di ransomware nel settore industriale, segnando un incremento del 49,5% rispetto al 2022. Tra i ransomware LockBit è stato quello più

utilizzato contro le organizzazioni industriali, responsabile del 25% degli incidenti, seguito da ALPHV e BlackBasta, ciascuno con il 9%. (Dragos, 2024)

Secondo lo stesso studio si è osservato che circa il 70% degli incidenti legati alle tecnologie operative (OT) è originato all'interno dell'ambiente IT, sottolineando l'importanza della segmentazione della rete e della creazione di domini separati come misure di mitigazione fondamentali. Questo problema è particolarmente rilevante per il settore industriale, che continua a lottare con la segmentazione, un componente essenziale di un'architettura difensiva efficace. Infatti, il report ha mostrato che numerosi settori, incluso il manifatturiero, continuano ad avere difficoltà con un'architettura difensiva adeguata. Le percentuali di difficoltà nella segmentazione variano tra i settori, ma il manifatturiero è il più colpito (51%), segnalando l'urgenza di adottare misure di sicurezza avanzate e proattive per proteggere le operazioni e i dati sensibili.

Dragos ha inoltre riscontrato problemi di segmentazione della rete o firewall configurati in modo errato nel 28% degli interventi. Questa situazione varia significativamente tra i diversi settori. Ad esempio, si sono osservati più frequentemente problemi di segmentazione della rete nel settore dei trasporti e della manifattura rispetto ad altri settori. (Dragos, 2024)

A conferma di quanto detto precedentemente, secondo il report *Security Navigator 2024* di Orange Cyberdefense, rispetto al 2022, gli attacchi nel settore manifatturiero sono aumentati del 42%, posizionandolo al primo posto tra i settori più colpiti, seguito dai servizi professionali, scientifici e tecnici. Di fatto, è stato un anno da record per le estorsioni informatiche - che includono il ransomware - con un aumento senza precedenti del 46% di questo tipo di attacchi. (Cyberdefense, 2024)
Tra le vittime di Cyber Extortion (Cy-X), il settore manifatturiero emerge come il più colpito. Negli ultimi 12 mesi, su un totale di 4.374 organizzazioni vittime, il 21% appartiene al settore manifatturiero, seguito dal 18% per i Servizi Professionali, Scientifici e Tecnici e dal 6% per il settore della Sanità e Assistenza Sociale. (Forbes, 2024)

Subindustry	% of victims
Machinery Manufacturing	12.04%
Fabricated Metal Product Manufacturing	10.41%
Transportation Equipment Manufacturing	9.22%
Computer and Electronic Product Manufacturing	9.00%
Chemical Manufacturing	8.68%

Figura 9 - Le sotto-industrie più colpite nel settore manifatturiero

Dallo stesso studio, viene evidenziato come la distribuzione delle vittime tra i principali settori industriali è sorprendentemente uniforme a livello globale, con il settore Manifatturiero che emerge come il più colpito nella maggior parte delle regioni. Tuttavia, si notano delle eccezioni nel Regno Unito e in Africa, dove il settore Manifatturiero non occupa la posizione di maggior impatto. Questa discrepanza è probabilmente dovuta alla minore prevalenza delle aziende manifatturiere in queste regioni. Nel Regno Unito e in Africa, altri settori potrebbero prevalere a causa delle diverse strutture industriali ed economiche. (Cyberdefense, 2024)

L'elevata frequenza di attacchi informatici nel settore manifatturiero è attribuita a diverse cause. In primo luogo, la crescente connettività dovuta all'integrazione di tecnologie online e all'espansione dell'Internet delle Cose (IoT) ha migliorato l'efficienza operativa, ma ha anche introdotto nuovi punti di accesso per i criminali informatici. Questi nuovi ingressi rappresentano vulnerabilità sfruttabili per compromettere i sistemi aziendali. Inoltre, la complessità delle catene di approvvigionamento crea ulteriori rischi, offrendo molteplici opportunità di infiltrazione per gli hacker. Ogni anello della catena diventa un potenziale punto di accesso, e le piccole e medie imprese (PMI), spesso coinvolte nella fornitura e manutenzione dei macchinari, sono particolarmente vulnerabili a causa delle loro risorse limitate e della scarsa preparazione in materia di cybersecurity. (Adel Alqudhaibi, 2024)

Un altro fattore cruciale è legato alle persone. Secondo un rapporto dell'University of Phoenix e ISC(2), l'inesperienza degli utenti finali e la mancanza di conoscenza delle nuove tattiche di crimine informatico sono tra i principali fattori che contribuiscono a gravi incidenti di cybersecurity. Il divario di conoscenze in materia di cybersecurity tra i dipendenti del settore manifatturiero è significativo, come evidenziato anche da uno studio congiunto tra (CS)²AI e KPMG, che ha rilevato come quasi la metà delle

organizzazioni in ambito OT e industriale manchi di personale adeguatamente formato e preparato. ((CS)AI - KPMG, 2022)

Sul fronte tecnologico, molte aziende utilizzano sistemi obsoleti che non dispongono delle necessarie funzionalità di sicurezza. L'uso di hardware e software non più supportati aumenta il rischio di attacchi, soprattutto se questi dispositivi critici sono connessi a reti insicure, compromettendo la cybersecurity complessiva.

A livello di attacchi mirati, non vi sono evidenze concrete che i criminali selezionino specificamente il settore manifatturiero come obiettivo privilegiato, sebbene le campagne di phishing possano talvolta sfruttare temi o eventi particolari per indirizzarsi verso di esso. È plausibile che gli operatori di Cyber Extortion (Cy-X) acquisiscano pacchetti di compromissione che includono aziende del settore manifatturiero, considerate più vulnerabili e propense a pagare riscatti elevati. Tuttavia, la pre-selezione di queste aziende come target non è confermata dai dati attualmente disponibili. (Cyberdefense, 2024)

Infine, sebbene il settore manifatturiero continui a essere uno dei più colpiti dagli attacchi informatici, questo non può essere spiegato esclusivamente dalla sua ampiezza come superficie di attacco. In realtà, il settore si colloca solo al dodicesimo posto per numero di entità aziendali colpite, suggerendo che la frequenza degli attacchi non può essere attribuita unicamente alla grandezza del settore. Pertanto, in assenza di prove concrete che dimostrino una selezione mirata da parte dei criminali, si conferma l'ipotesi che le aziende manifatturiere presentino livelli di sicurezza inferiori rispetto ad altri settori. Questa vulnerabilità superiore contribuisce a un numero maggiore di vittime di attacchi opportunistici, come evidenziato anche da un rapporto dell'Istituto Nazionale di Standard e Tecnologia (NIST).

A conferma di tale tesi, nel contesto delle fabbriche intelligenti, è emerso che molte organizzazioni presentano una preparazione insufficiente in termini di *consapevolezza*, *governance*, *protezione*, *rilevamento* e *resilienza*. Secondo il report "Cybersecurity in Smart Factories" di Capgemini, molte organizzazioni presentano una preparazione insufficiente in termini di consapevolezza, governance, protezione, rilevamento e resilienza. (Capgemini, 2022)

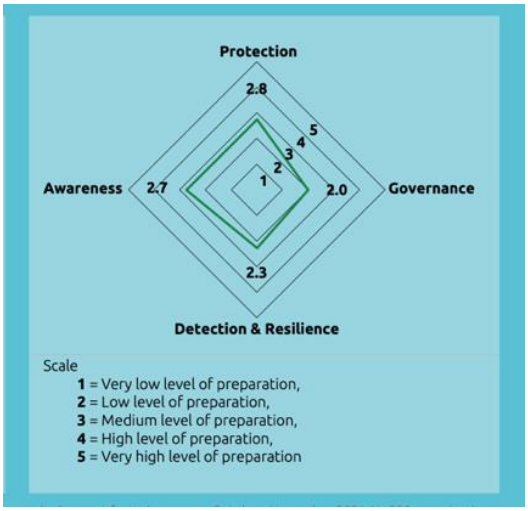

Figura 10 - Livelli di preparazione alla Cybersecurity nelle Smart Factories

La preparazione media delle organizzazioni si attesta su un basso punteggio di 2,8 su 5, indicando che, nonostante alcuni progressi in specifiche aree, la preparazione complessiva rimane insufficiente. Per quanto riguarda la governance della cybersecurity, molti sistemi OT/IIOT e IT non sono adeguatamente integrati. Il 47% dei produttori non considera la cybersecurity una priorità a livello dirigenziale, mentre il 44% ritiene che non sia necessario investire ulteriormente nella sicurezza dei processi produttivi. Questo ha portato a un punteggio medio di 2,0. Anche la consapevolezza e il rilevamento delle anomalie mostrano punteggi medi di 2,4 e 2,0 rispettivamente, indicando una significativa carenza nella preparazione e nella capacità di risposta alle minacce.

Per quanto riguarda l'importanza della formazione del personale in ambito cybersecurity, i dati riportati da IBM nel report "Data Breach Cost" evidenziano che falle informatiche ed errori umani sono responsabili di quasi la metà delle violazioni dei dati. Gli attacchi malevoli, perpetrati da esterni o da dipendenti con intenti criminali, rappresentano il 55% di tutte le violazioni. Tuttavia, è fondamentale riconoscere che il restante 45% delle violazioni è attribuibile a problemi interni di gestione. (IBM, 2024)
In dettaglio, il 23% delle violazioni è causato da guasti IT, che possono derivare da malfunzionamenti dei sistemi o da errori nella configurazione delle infrastrutture tecnologiche, mentre il 22% delle violazioni è il risultato di errori umani, come una cattiva gestione delle informazioni, la configurazione errata dei sistemi di sicurezza o una risposta inadeguata a minacce emergenti.

La formazione dei dipendenti si conferma come un elemento cruciale nelle strategie di difesa informatica, particolarmente efficace nella rilevazione e prevenzione degli attacchi di phishing. Quando le organizzazioni affrontano bassi livelli di formazione del personale, i costi medi delle violazioni dei dati ammontano a 5,10 milioni di dollari. Questo valore è significativamente più alto rispetto alle organizzazioni con elevati livelli di formazione, dove i costi medi delle violazioni si attestano a 4,15 milioni di dollari. Questa differenza sottolinea l'importanza cruciale della formazione dei dipendenti nella riduzione dei costi associati alle violazioni dei dati.

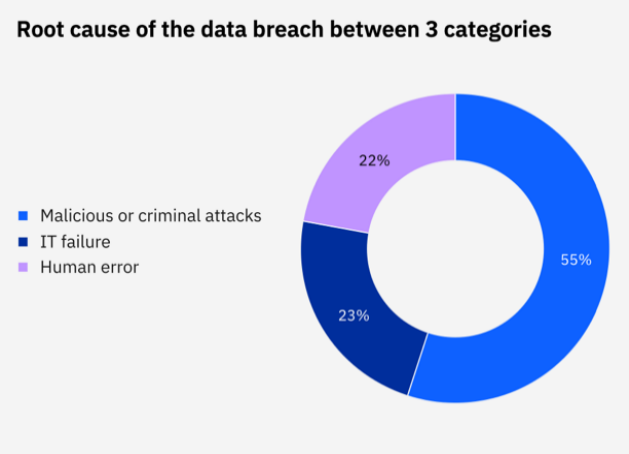

Figura 11 - Cause principali della violazione dei dati

Un'analisi condotta da Galinec et al. evidenzia l'importanza di affrontare le problematiche derivanti da una scarsa educazione o consapevolezza dei dipendenti. Anche un solo dipendente non informato può compromettere una strategia di cybersecurity altrimenti completa. L'Agenzia dell'Unione Europea per la Cybersecurity evidenzia che un coinvolgimento proattivo dei dipendenti è essenziale per una cybersecurity efficace, superando il mero rispetto delle normative e delle politiche, che potrebbero non essere sempre aggiornate rispetto alle minacce attuali. Questo approccio è supportato dal National Initiative for Cybersecurity Education framework, che riconosce la necessità di integrare la cybersecurity con il dipartimento IT e tutti i ruoli lavorativi all'interno dell'organizzazione

Le Sfide della Cybersecurity nelle Fabbriche Intelligenti

Le fabbriche intelligenti affrontano una serie di sfide significative nella protezione delle loro operazioni da attacchi informatici. Questi problemi emergono principalmente a causa di:

- *Mancanza di Collaborazione tra i Leader delle Fabbriche Intelligenti e il Chief Security Officer:* L'assenza di collaborazione tra i responsabili delle fabbriche e il Chief Security Officer ostacola una visione integrata delle esigenze di sicurezza e rallenta la risposta alle minacce emergenti.
- *Proporzione Inadeguata del Budget Annuale Destinata alla Cybersecurity*: La percentuale di budget annuale allocata alla cybersecurity è insufficiente rispetto all'aumento delle minacce e alla complessità degli attacchi informatici, rendendo le organizzazioni vulnerabili.
- *Mancata Rilevazione Precoce degli Attacchi Informatici*: La difficoltà nel rilevare tempestivamente gli attacchi porta a danni estesi e gravi alle operazioni, aumentando il rischio di interruzioni e perdite significative. Tuttavia, il Cost of a Data Breach Report di IBM 2023, ha mostrato un miglioramento del tempo medio necessario per rilevare e contenere un attacco informatico, pari a 258 giorni, il valore più basso degli ultimi sette anni, rispetto ai 277 giorni dell'anno precedente. (IBM X-Force, 2024)

Nel corso degli anni, gli attacchi informatici all'industria manifatturiera si sono evoluti in minacce altamente sofisticate e diffuse. Questi attacchi, che colpiscono vari aspetti delle operazioni industriali, possono causare gravi danni finanziari e reputazionali:

- *Attacchi ai Sistemi di Controllo Industriale (ICS):* I sistemi di controllo industriale (ICS) riducono la necessità di sorveglianza umana continua, ma la loro natura automatizzata crea opportunità per rischi significativi per la sicurezza informatica. Gli attaccanti non autorizzati possono manipolare o interrompere i processi produttivi, danneggiando attrezzature o compromettendo la qualità dei prodotti. Possono anche scoprire e sfruttare difetti non corretti (N-day) o vulnerabilità sconosciute (Zero-day).
- *Social Engineering e Phishing:* Gli attacchi di social engineering, come il compromesso delle e-mail aziendali (BEC), mirano spesso ai dipendenti per ottenere

accesso non autorizzato ai sistemi principali, segreti commerciali e dati dei clienti. Gli attacchi di phishing possono anche diffondere malware che interrompe le operazioni di produzione, causando tempi di inattività prolungati e perdite finanziarie sia a breve che a lungo termine.

- *Furto di Proprietà Intellettuale (IP):* La proprietà intellettuale (IP) di un produttore è uno degli asset più preziosi e la sua compromissione può avere gravi conseguenze. Il furto di IP è uno dei rischi informatici più onerosi finanziariamente e può essere perpetrato sia da attaccanti esterni in cerca di segreti commerciali, sia da insider malevoli che mirano a vendere informazioni riservate.
- *Estorsione e Ransomware:* Le aziende manifatturiere affrontano rischi crescenti, da estorsioni come ransomware e furto di dati, dove il tempo perso si traduce direttamente in perdite finanziarie. Anche se il pagamento di un riscatto può sembrare una soluzione per evitare ritardi nella produzione, tuttavia non garantisce che i dati rubati non vengano diffusi o venduti, né che la vittima eviti danni finanziari o reputazionali a lungo termine. Inoltre, pagare può comportare sanzioni federali e costi legali significativi, nonché spese elevate per l'indagine, il recupero e il rafforzamento della sicurezza.
- *Attacchi alla Catena di Fornitura:* Gli attacchi alla catena di fornitura mirano ai partner o fornitori di un'azienda attraverso phishing o compromissione delle loro reti. Gli attaccanti, una volta ottenuto l'accesso, possono infiltrarsi nella rete del produttore per rubare dati, distribuire malware o interrompere la produzione. Il settore manifatturiero è particolarmente vulnerabile a causa della vasta rete di fornitori interconnessi, dove un attacco a un singolo fornitore può rapidamente influenzare tutta la catena
- *Attacchi da Parte di Stati-Nazione:* Le minacce informatiche contro le aziende manifatturiere non sono solo opera di criminali informatici motivati finanziariamente, ma possono anche derivare da concorrenti stranieri e attori informatici sponsorizzati da stati-nazione. I dati recenti indicano che il 17,7% degli attacchi da parte di stati-nazione è stato diretto al settore manifatturiero. Questi attori, che spesso dispongono di risorse significative, utilizzano strumenti avanzati per eseguire attacchi difficili da individuare e contrastare. (IBM, 2024)

- *Attacchi IoT:* Con l'adozione di tecnologie come l'Industria 4.0 e i dispositivi IoT, i produttori sono sempre più a rischio di attacchi. Gli attaccanti possono sfruttare questi dispositivi connessi per infiltrarsi nelle reti, compromettendo dati sensibili e mettendo a rischio sia informazioni proprietarie che dati dei clienti. Molti dispositivi IoT mancano di robuste misure di sicurezza, rendendoli facili bersagli per i criminali informatici. Una volta compromessi, i dispositivi smart possono servire da punti di ingresso alla rete manifatturiera più ampia.

Architettura e Funzionamento dei Sistemi di Tecnologia Operativa

I Sistemi di Tecnologia Operativa (OT) comprendono una gamma di tecnologie utilizzate per controllare e monitorare processi industriali e infrastrutture critiche. Questi sistemi, noti anche come Sistemi di Controllo e Automazione Industriale (ICS), integrano componenti elettrici, meccanici, idraulici e pneumatici per raggiungere obiettivi specifici, come la produzione, il trasporto di materiale o energia. All'interno degli ICS, rientrano diverse tecnologie, tra cui i sistemi SCADA, DCS e PLC.

Un sistema di Tecnologia Operativa (OT) tipico, è un'infrastruttura complessa che include numerosi cicli di controllo, interfacce uomo-macchina (HMI) e strumenti per la diagnostica e la manutenzione remota.
Un ciclo di controllo è essenziale per la gestione e il monitoraggio di un processo controllato e si compone di tre elementi principali:

- *Sensori:* Questi dispositivi misurano una proprietà fisica specifica, come la temperatura o la pressione, e inviano i dati raccolti come variabili controllate al controllore.
- *Controllore:* Il controllore riceve e interpreta le informazioni dai sensori utilizzando un algoritmo di controllo. Basandosi su questi dati e sui punti di settaggio predefiniti, il controllore genera variabili manipolate e le invia agli attuatori. L'obiettivo del controllore è mantenere il processo vicino ai valori desiderati.
- *Attuatori*: Gli attuatori, come valvole di controllo, interruttori di circuito e motori, ricevono i comandi dal controllore e agiscono direttamente sul processo controllato sulla base dei comandi del controllore.

In un sistema di monitoraggio tipico, generalmente non ci sono connessioni dirette tra i sensori e gli attuatori. Gli operatori e gli ingegneri utilizzano le interfacce uomo-macchina (HMI) per monitorare e configurare i punti di settaggio, gli algoritmi di controllo e per regolare e stabilire parametri nel controllore. L'HMI visualizza anche informazioni sullo stato del processo e informazioni storiche.

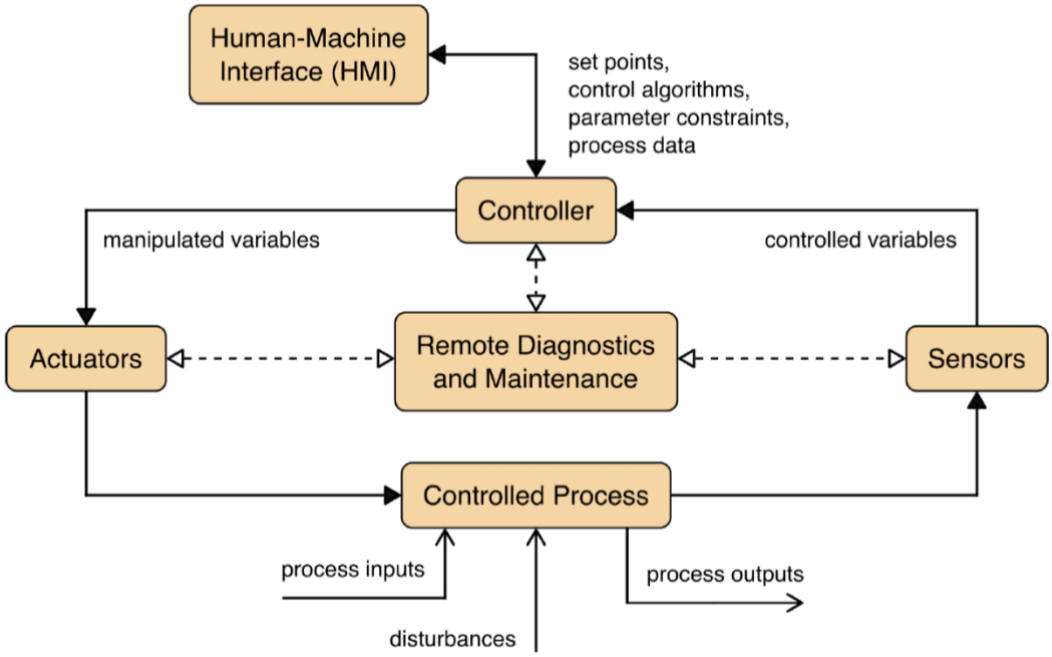

Figura 12 - Funzionamento di base di un sistema OT

SCADA

Tra i sistemi OT, gli SCADA (Supervisory Control And Data Acquisition) sono progettati per gestire risorse distribuite, dove l'acquisizione centralizzata dei dati è tanto cruciale quanto il controllo stesso. Questi sistemi sono utilizzati in vari settori, inclusi gli oleodotti e gasdotti, i sistemi elettrici e i trasporti pubblici come le ferrovie.

I sistemi SCADA combinano sistemi di acquisizione dati con tecnologie di trasmissione e software HMI (Interfaccia Uomo-Macchina) per offrire un monitoraggio e controllo centralizzati. Questi sistemi raccolgono dati dai punti di campo, li trasferiscono a un centro di controllo e li visualizzano in modo grafico o testuale, permettendo all'operatore di controllare e monitorare il sistema da una posizione centrale quasi in tempo reale. In base alla complessità e configurazione del sistema, il controllo può essere automatico o gestito manualmente dall'operatore.

L'hardware di un sistema SCADA comprende un server di controllo situato nel centro di controllo, apparecchiature di comunicazione come radio, linee telefoniche, cavi o satelliti, e siti remoti distribuiti geograficamente con unità terminali remote (RTU) o PLC. Questi RTU o PLC controllano gli attuatori e monitorano i sensori, mentre il server di controllo memorizza e gestisce le informazioni provenienti dagli RTU e dai PLC. Il software del sistema è programmato per determinare cosa e quando monitorare, quali parametri sono accettabili e quali azioni intraprendere quando le variabili di processo si discostano dai valori predefiniti.

Inoltre, dispositivi elettronici intelligenti (IED) (un controllore integrato capace di impartire comandi di controllo), possono comunicare direttamente con il server di controllo, oppure un RTU locale può interrogare gli IED per raccogliere i dati e passarli al server. Gli IED offrono un'interfaccia diretta per il controllo e la supervisione di apparecchiature e sensori e spesso possono operare autonomamente grazie alla loro programmazione locale.

I sistemi SCADA sono generalmente progettati per essere resistenti ai guasti, con misure di ridondanza significative integrate, anche se tali misure potrebbero non essere sufficienti a proteggere contro attacchi malevoli.

Nel diagramma illustrativo, il centro di controllo è mostrato in cima e ospita il server di controllo, i router di comunicazione, l'HMI, le stazioni di lavoro per l'ingegneria e il data historian, tutti collegati tramite una rete locale (LAN). Il centro di controllo gestisce la raccolta e registrazione dei dati dai siti remoti, visualizza le informazioni attraverso l'HMI e può eseguire azioni basate sugli eventi rilevati. È anche responsabile dell'allerta centralizzata, dell'analisi delle tendenze e della generazione di rapporti.

I siti remoti, situati nella parte inferiore del diagramma, gestiscono localmente gli attuatori e monitorano i sensori. Questi siti dispongono di capacità di accesso remoto che consente diagnosi e manutenzione a distanza, spesso tramite modem dial-up[1] o connessioni a rete geografica (WAN). Le informazioni tra il centro di controllo e i siti remoti sono trasmesse utilizzando protocolli di comunicazione standard e proprietari, che possono operare su linee telefoniche, cavi, fibre ottiche e frequenze radio (ad esempio, broadcast, microonde, satellite).

[1] Terminale Dial-up: Tipo di connessione alla rete Internet che si stabilisce tramite una chiamata telefonica, utilizzando le linee telefoniche tradizionali.

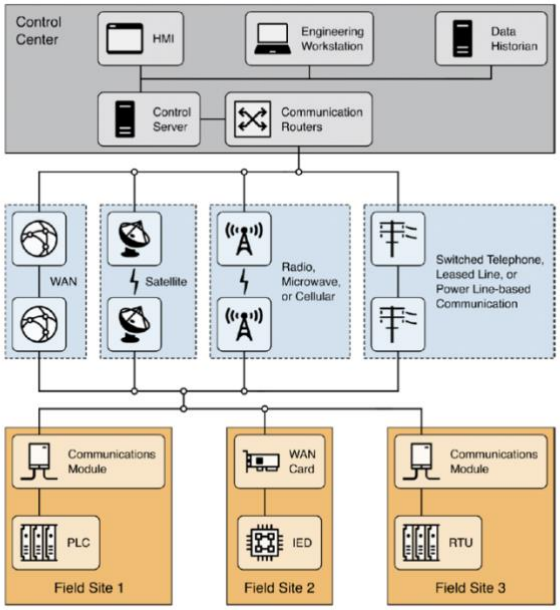

Figura 13 - Layout generale di un sistema SCADA

La Figura 14 mostra un sistema SCADA con un centro di controllo principale, un centro di controllo regionale e tre siti sul campo. È previsto un centro di controllo di backup per garantire ridondanza. Le comunicazioni tra il centro di controllo e i siti avvengono tramite connessioni punto-punto (che garantisce un collegamento diretto tra due dispositivi), con telemetria radio per due siti e WAN per il terzo. Sopra il centro di controllo principale si trova un centro di controllo regionale che fornisce un ulteriore livello di supervisione. La rete aziendale corporativa collega tutti i centri di controllo tramite la WAN, permettendo l'accesso remoto ai siti sul campo per attività di troubleshooting e manutenzione.

Il centro di controllo principale effettua interrogazioni periodiche dei dispositivi sul campo a intervalli specificati (ad esempio, ogni 5 o 60 secondi) e può inviare nuovi set point ai dispositivi quando necessario.

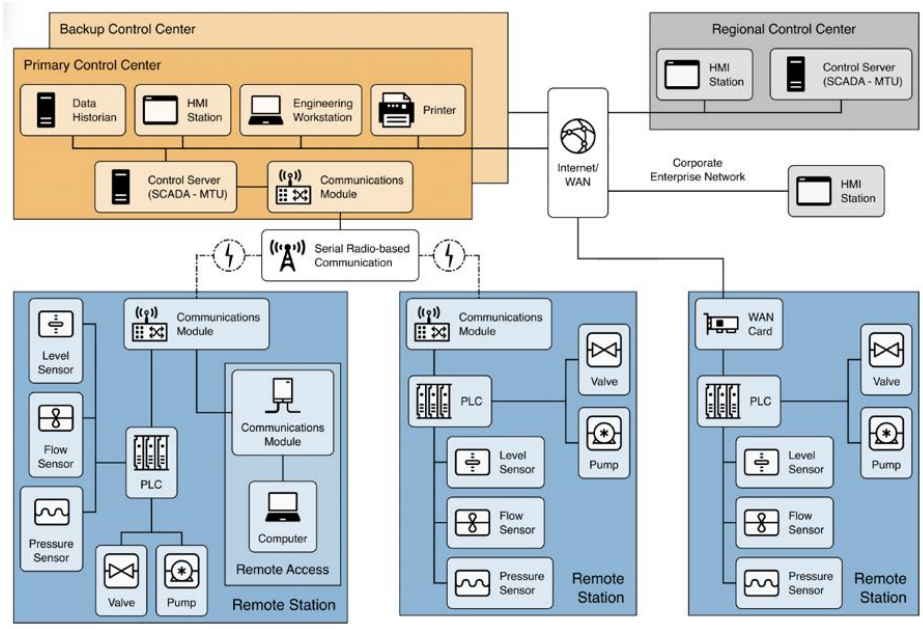

Figura 14 - Esempio di implementazione di un sistema SCADA

Sistema di Controllo Distribuito (DCS)

Un Sistema di Controllo Distribuito (DCS) viene utilizzato per controllare i sistemi di produzione situati nella stessa area geografica, come quelli nelle raffinerie di petrolio, negli impianti di trattamento dell'acqua e delle acque reflue. Questi sistemi possono essere dedicati al controllo dei processi o delle parti discrete.
Il DCS è progettato come un'architettura di controllo che integra un livello di supervisione centrale. Questo livello supervisiona diversi sottosistemi, ognuno dei quali è responsabile della gestione di un particolare processo locale. In sostanza, il DCS si occupa di suddividere l'intero processo produttivo in diverse sezioni gestite in modo autonomo, ma coordinate da un sistema centrale. Infatti, Il DCS utilizza un ciclo di controllo supervisionale centralizzato per coordinare un gruppo di controller localizzati, che condividono i compiti complessivi di esecuzione dell'intero processo produttivo. Questi controller locali, che possono essere specifici controller di processo o PLC (Programmable Logic Controllers), eseguono i comandi e monitorano il processo produttivo in tempo reale.
Per mantenere il processo produttivo entro parametri specifici, il DCS utilizza cicli di controllo a feedback o feedforward, che mantengono automaticamente le condizioni chiave del prodotto e/o del processo attorno a un punto di riferimento desiderato. Questi cicli aiutano a regolare automaticamente le condizioni chiave del processo (come temperatura, pressione, flusso, ecc.) mantenendole vicino ai valori desiderati, noti

come *set point*. Se il processo si discosta da questi valori, i controller locali effettuano correzioni per riportarlo in linea.

La Figura 15 mostra un esempio di implementazione dei componenti e della configurazione generale di un DCS. Questo DCS copre un'intera struttura, dai processi produttivi di base fino al livello aziendale. In questo esempio, un controller di supervisione (server di controllo) comunica con i suoi subordinati tramite una rete di controllo. Il supervisore invia set point e richiede dati ai controller distribuiti sul campo, i quali gestiscono i loro attuatori di processo basandosi sui comandi del server di controllo e sui feedback provenienti dai sensori di processo.

I dispositivi di controllo sul campo mostrati includono un controller di macchina, un PLC e un controller di processo. Il controller di macchina si interfaccia con sensori e attuatori tramite cablaggio punto-punto, mentre gli altri tre dispositivi sul campo utilizzano reti fieldbus[2] per collegarsi ai sensori e agli attuatori di processo. Le reti fieldbus eliminano la necessità di cablaggio punto-punto tra un controller e i singoli sensori e attuatori sul campo, poiché utilizzano un unico canale di comunicazione condiviso, attraverso il quale più dispositivi possono trasmettere e ricevere dati simultaneamente. Inoltre, un fieldbus consente una maggiore funzionalità oltre al controllo, come la diagnostica dei dispositivi sul campo, e può eseguire algoritmi di controllo all'interno del fieldbus stesso, evitando il percorso del segnale fino al PLC per ogni operazione di controllo.

[2] Reti Fieldbus: sistemi di comunicazione digitali che permettono lo scambio di dati tra dispositivi di campo (come sensori e attuatori) e sistemi di controllo.

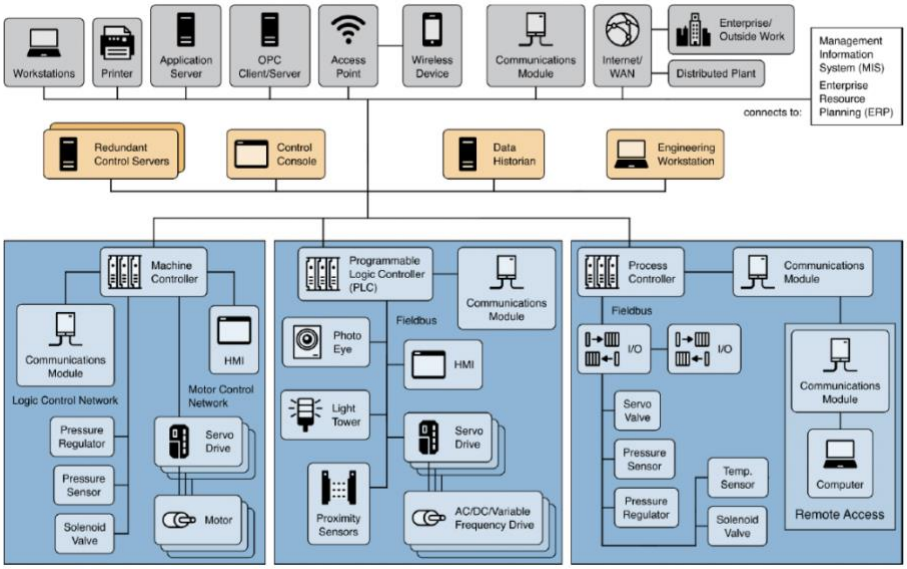

Figura 15 - Esempio di implementazione di un sistema DCS

Programmable Logic Controllers (PLC)

I PLC (Programmable Logic Controllers) sono componenti di controllo versatili utilizzati sia nei sistemi SCADA che DCS come parte di un framework di controllo gerarchico per gestire processi locali attraverso meccanismi di feedback. Nei sistemi SCADA, i PLC possono svolgere funzioni simili agli RTU (Remote Terminal Units), gestendo compiti di controllo locale e interfacciandosi con il sistema di supervisione più ampio. Quando integrati nei DCS (Distributed Control Systems), i PLC operano come controllori locali sotto la direzione di un controllo di supervisione centrale, gestendo segmenti specifici dell'intero processo.

I PLC possono anche fungere da unità di controllo principali in configurazioni di sistemi OT (Operational Technology) più piccoli, dove gestiscono compiti di controllo di processi discreti, come quelli che si trovano in linee di assemblaggio automobilistiche o controllori di processo specializzati. A differenza delle configurazioni SCADA e DCS, questi sistemi più piccoli tipicamente non includono un server di controllo centrale o un'interfaccia HMI (Human-Machine Interface), risultando in un'operazione di controllo prevalentemente ad anello chiuso con un intervento umano minimo.

Una caratteristica chiave dei PLC è la loro memoria programmabile dall'utente, che memorizza istruzioni per eseguire varie funzioni di controllo, tra cui il controllo I/O, l'elaborazione logica, il timing, il conteggio, le comunicazioni, le operazioni aritmetiche e l'elaborazione dei dati.

Come illustrato nella Figura 8, un PLC può controllare un processo di produzione su una rete fieldbus, con la possibilità di essere accessibile e programmato tramite una workstation di ingegneria. Inoltre, i dati di processo vengono raccolti e memorizzati in uno storico dei dati, con tutti i componenti interconnessi attraverso una rete locale (LAN).

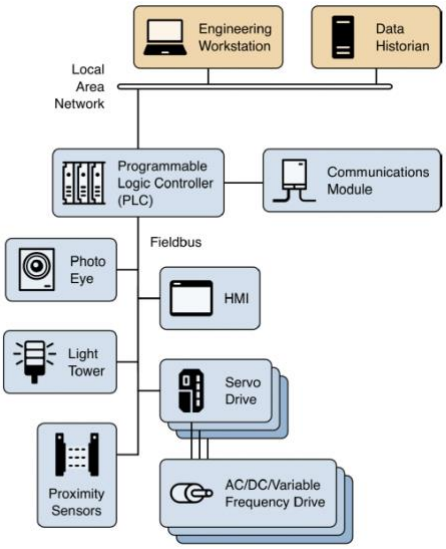

Figura 16 - Esempio di implementazione di un sistema PLC

Industrial internet of things (IIoT)

Industrial Internet of Things (IIoT) si basa su un modello architettonico a tre livelli, definito dal Consorzio Industrial IoT, per gestire i flussi di dati e di controllo nelle operazioni industriali. Questi tre livelli sono: *edge* (periferico), *platform* (piattaforma) ed *enterprise* (aziendale). Ogni livello ha un ruolo specifico nella gestione delle attività operative e sono interconnessi da tre reti: la rete di prossimità, la rete di accesso e la rete di servizi.

- *Il livello enterprise* implementa applicazioni specifiche per il dominio e sistemi di supporto alle decisioni, fornisce interfacce agli utenti finali, riceve flussi di dati dagli altri livelli e invia comandi di controllo agli altri livelli.
- *Il livello platform* riceve, elabora e inoltra i comandi di controllo dal livello enterprise al livello edge. Consolida e analizza i flussi di dati provenienti dagli altri livelli, fornisce funzioni di gestione per dispositivi e asset e offre servizi non specifici per il dominio, come interrogazioni e analisi dei dati. A seconda dell'implementazione, queste funzioni possono essere realizzate su una piattaforma IIoT distribuita in un data center in loco, fuori sede o nel cloud.

- *Il livello edge* raccoglie dati dai nodi periferici utilizzando la rete di prossimità. Le caratteristiche architettoniche di questo livello variano a seconda dell'implementazione specifica (ad esempio, distribuzione geografica, posizione fisica, ambito di governance). Esso rappresenta uno strato logico piuttosto che una vera e propria divisione fisica. Dal punto di vista aziendale, la posizione dell'edge dipende dagli obiettivi dell'azienda. L'edge computing è un'infrastruttura di calcolo decentralizzata in cui risorse di calcolo e servizi applicativi possono essere distribuiti lungo il percorso di comunicazione tra la sorgente di dati e il cloud. Esso esiste verticalmente nell'intero stack (cioè dal dispositivo al cloud) e orizzontalmente tra i sottosistemi IIoT. L'edge non è solo un modo per trasmettere al data center o al cloud, ma agisce sui dati raccolti localmente.

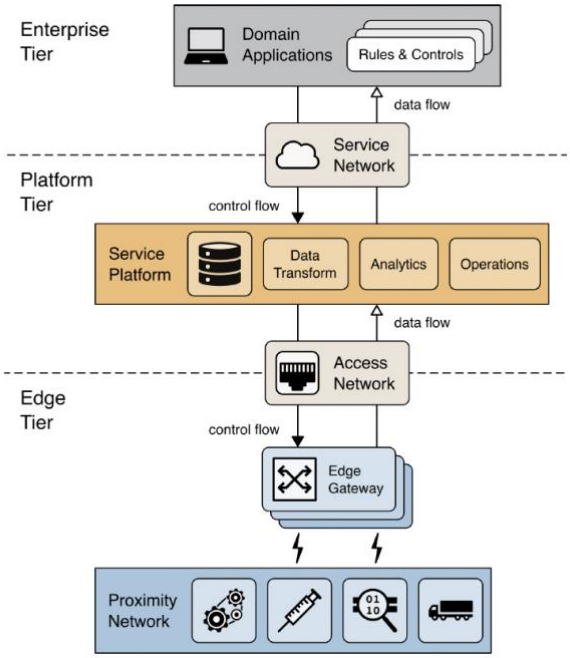

Figura 17 - Architettura di sistema IIoT a tre livelli

Vulnerabilità e Minacce dei sistemi ICS

L'importanza dei sistemi ICS/OT nelle infrastrutture critiche non può essere sopravvalutata. Qualsiasi interruzione di questi sistemi può avere gravi conseguenze, tra cui la perdita di vite umane, danni ambientali e perdite economiche.
Infatti, i Sistemi di Controllo Industriale (ICS) utilizzati nelle infrastrutture critiche e nelle industrie manifatturiere sono obiettivi di attacchi informatici sofisticati.

Le violazioni industriali sono diventate più frequenti, con gli aggressori che mirano tanto ai sistemi IT all'interno delle reti OT quanto ai dispositivi specifici dell'OT.
Un esempio significativo è il cyberattacco del 2015 contro la rete elettrica dell'Ucraina, che causò un blackout esteso che colpì oltre 230.000 persone. Gli aggressori utilizzarono malware per accedere ai sistemi ICS/OT e poi manipolarono i sistemi per interrompere l'erogazione di energia a diverse città. Questo attacco ha dimostrato il potenziale impatto degli attacchi informatici sulle infrastrutture critiche, sottolineando l'importanza di proteggere adeguatamente i sistemi ICS/OT. (Rebultan, 2023) (Micheal M. Amiri, 2024)

Il *2024 State of Operational Technology and Cybersecurity Report* di Fortinet, basato su un'indagine globale che ha coinvolto oltre 550 professionisti del settore OT, mette in luce un aumento significativo delle intrusioni nelle infrastrutture operative. La tendenza delle intrusioni che colpiscono i sistemi OT è in costante crescita. Nel 2023, il 49% delle organizzazioni intervistate ha subito attacchi che hanno compromesso i sistemi OT o entrambi i sistemi IT e OT. Quest'anno, la situazione è peggiorata ulteriormente, con quasi il 73% delle organizzazioni che ha riportato intrusioni. Di particolare rilievo è l'aumento delle intrusioni che hanno interessato esclusivamente i sistemi OT, salito dal 17% al 24% rispetto all'anno precedente. (Fortinet, 2024)

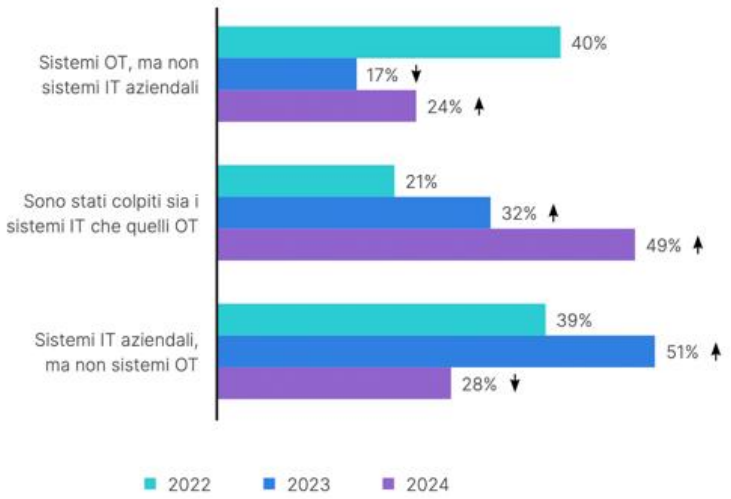

Figura 18 - Intrusioni IT e OT

Secondo Gartner, entro il 2025, i cybercriminali avranno sfruttato gli ambienti di tecnologia operativa (OT) per causare danni fisici o addirittura provocare vittime. Le motivazioni principali dietro gli incidenti di sicurezza che coinvolgono l'OT e altri sistemi

ciber-fisici (CPS) sono tre: causare danni fisici reali, effettuare vandalismo commerciale attraverso la riduzione della produzione, e compiere vandalismo reputazionale, rendendo un produttore inaffidabile o non attendibile. Questi attacchi rappresentano una minaccia crescente, richiedendo alle organizzazioni di rafforzare le misure di sicurezza per proteggere le loro infrastrutture critiche e prevenire conseguenze potenzialmente devastanti. (Moore, 2021)

Uno delle problematiche più comuni nei sistemi OT è l'uso di *software obsoleti* o *legacy* che, pur essendo stati affidabili nel tempo, presentano limiti significativi dal punto di vista della sicurezza. Questi software, spesso privi di aggiornamenti recenti, non dispongono delle funzionalità di sicurezza avanzate come autenticazione forte, crittografia e controllo dell'integrità. Di conseguenza risultano vulnerabili ad attacchi informatici, soprattutto quando esposti a reti esterne.

Un altro aspetto cruciale è rappresentato dalle *configurazioni predefinite* non sicure. Molti sistemi OT vengono forniti con impostazioni standard, quali password predefinite e configurazioni di base non sicure, che raramente vengono modificate dopo l'installazione. Questo facilita il compito degli aggressori, che possono utilizzare credenziali note o facili da individuare per ottenere accesso non autorizzato.

Le *politiche di accesso remoto insufficienti* rappresentano un altro potenziale punto debole. Molti sistemi SCADA e altri dispositivi OT, una volta connessi alle reti aziendali, risultano accessibili online senza adeguati controlli. Questo espone i sistemi a una vasta gamma di potenziali attacchi, come il "man-in-the-middle" o accessi non autorizzati.

Un'altra vulnerabilità comune riguarda la *mancanza di segmentazione della rete.* Molti ambienti industriali mantengono architetture di rete piatte, dove i sistemi IT e OT sono interconnessi senza adeguate misure di segmentazione. Questa mancanza di separazione permette agli aggressori, una volta entrati nella rete, di muoversi lateralmente e compromettere una vasta gamma di dispositivi.

L'adozione di *dispositivi IoT* in contesti industriali introduce nuovi vettori di attacco. Molti di questi dispositivi presentano scarse misure di sicurezza e possono essere compromessi e trasformati in botnet[3] per lanciare attacchi DDoS, che possono causare interruzioni operative significative.

[3] Botnet: rete di computer o altri dispositivi connessi a Internet infettati da software dannoso e utilizzati per svolgere attività dannose.

Man mano che le linee di distinzione tra IT e OT si affievoliscono, la superficie di attacco per i sistemi interconnessi IT/OT si espande notevolmente. Uno dei vettori di attacco più comuni utilizzati dagli hacker per infiltrarsi in queste infrastrutture è Internet. I sensori dei sistemi di controllo industriale (ICS), gli strumenti e i dispositivi OT, che sono accessibili tramite una rete OT, diventano sempre più vulnerabili e possono essere "armati" dagli attaccanti. Un altro punto di debolezza significativo è rappresentato dalle interfacce uomo-macchina (HMI), che collegano gli operatori umani ai sistemi di controllo industriale. Queste interfacce sono spesso connesse alle infrastrutture IT, creando un ponte diretto tra le reti OT e le reti aziendali esposte a Internet.

Normative e Regolamenti

Normative e Regolamenti che Guidano la Sicurezza Informatica nell'Ambito Industriale

La sicurezza informatica nell'ambito industriale è regolata da una serie di normative e regolamenti che mirano a proteggere le infrastrutture critiche e garantire la resilienza dei sistemi operativi. Queste normative sono fondamentali per stabilire standard di sicurezza, promuovere la conformità e mitigare i rischi associati agli attacchi informatici. Di seguito sono riportati alcuni dei principali regolamenti e normative che influenzano la sicurezza informatica nell'ambito industriale.

Il *NIST Cybersecurity Framework* (CSF) è un insieme ampiamente utilizzato di best practice, standard e linee guida per migliorare la cybersecurity a livello organizzativo. Sebbene sia stato progettato principalmente per i sistemi IT, può essere adattato agli ambienti OT. Il CSF è costruito attorno a cinque funzioni chiave:

- *Identificare***:** Comprendere i sistemi, le risorse, i dati e le capacità dell'organizzazione per gestire i rischi di cybersecurity;
- *Proteggere*: Implementare salvaguardie per garantire la fornitura dei servizi di infrastruttura critica;
- *Rilevare*: Sviluppare meccanismi per identificare eventi di cybersecurity mentre accadono;
- *Rispondere*: Stabilire processi per agire quando si verifica un incidente di cybersecurity;

- *Recuperare*: Implementare piani per la resilienza e il ripristino tempestivo delle capacità o dei servizi compromessi a causa di un evento di cybersecurity.

La struttura flessibile del framework consente di adattarlo alle esigenze uniche dei sistemi OT. Il CSF aiuta le organizzazioni a allineare le loro strategie di cybersecurity con le sfide specifiche dell'OT, sottolineando l'importanza di proteggere sia le risorse IT che quelle OT. (NIST, 2024)

La *NIST Special Publication 800-82* fornisce una guida completa per la sicurezza degli ambienti OT, che includono sistemi di controllo industriale (ICS), sistemi SCADA (Supervisory Control and Data Acquisition) e altre infrastrutture critiche. La pubblicazione copre:

- Topologie di sistema: Architetture tipiche dei sistemi OT e come interagiscono con le reti IT;
- Minacce e vulnerabilità: Identificazione delle minacce comuni come malware, accessi non autorizzati e minacce interne, nonché le vulnerabilità intrinseche nei sistemi OT;
- Misure di sicurezza: Raccomandazioni per la protezione dei sistemi OT, come l'implementazione della segmentazione della rete, l'uso di protocolli di comunicazione sicuri e la garanzia della sicurezza fisica. (NIST, 2023)

La NIST SP 800-82 è particolarmente utile per coloro che sono responsabili della sicurezza dei sistemi OT, offrendo indicazioni specifiche che affrontano le peculiarità degli ambienti industriali in cui la sicurezza e l'affidabilità sono fondamentali.

La serie *ISA/IEC 62443* è un insieme di standard sviluppati dalla International Society of Automation (ISA) e dalla International Electrotechnical Commission (IEC) per la sicurezza degli ambienti OT. Lo standard è organizzato in quattro gruppi principali:

- Generale (ISA/IEC 62443-1-x): Copre terminologia, concetti e modelli per la cybersecurity nell'OT;
- Politiche e Procedure (ISA/IEC 62443-2-x): Fornisce indicazioni sulla creazione e gestione di un programma di cybersecurity, inclusa la valutazione e gestione dei rischi;

- Sistema (ISA/IEC 62443-3-x): Offre indicazioni sulla progettazione sicura del sistema, inclusi requisiti dettagliati per la segmentazione della rete, controlli di sicurezza e l'architettura di sistemi sicuri;
- Componente (ISA/IEC 62443-4-x): Si concentra sullo sviluppo sicuro dei prodotti e sull'assicurare che i singoli componenti soddisfino gli standard di sicurezza.

Gli Standard di *Protezione delle Infrastrutture Critiche (CIP) del North American Electric Reliability Corporation (NERC*) sono progettati specificamente per il settore delle utility elettriche in Nord America. Gli standard si concentrano sulla sicurezza dei sistemi di produzione e trasmissione di energia elettrica (Bulk Electric Systems, BES) e sulla garanzia dell'affidabilità della rete elettrica. Le aree chiave includono la gestione della Cybersecurity, segnalazione degli Incidenti, sicurezza fisica e formazione del Personale.

La Direttiva sulla *Sicurezza delle Reti e dell'Informazione (NIS)*, e il suo successore, *NIS2*, sono quadri legislativi dell'Unione Europea mirati a migliorare la cybersecurity dei servizi essenziali e dei fornitori di servizi digitali in tutta l'UE. Le direttive impongono:

- Gestione dei Rischi e Segnalazione: Le organizzazioni devono implementare misure di gestione dei rischi e segnalare gli incidenti significativi all'autorità nazionale competente;
- Requisiti di Sicurezza: Stabilisce requisiti minimi di sicurezza per gli operatori di servizi essenziali e i fornitori di servizi digitali;
- Supervisione e Applicazione: Le autorità nazionali hanno il potere di supervisionare e applicare i requisiti della direttiva, con la possibilità di imporre sanzioni in caso di non conformità.

Analisi degli Standard di Sicurezza Specifici per l'Industria e delle Loro Implicazioni Pratiche

L'adozione degli standard di sicurezza specifici per l'industria ha implicazioni profonde e concrete per la protezione delle infrastrutture critiche e dei sistemi industriali. L'analisi di tali standard rivela come le organizzazioni possano applicare pratiche di sicurezza efficaci e affrontare le sfide emergenti in modo sistematico.

Gli standard come l'IEC 62443 enfatizzano l'importanza della progettazione di architetture sicure per i sistemi industriali. L'uso di segmentazioni di rete e zone di sicurezza aiuta a contenere e isolare eventuali minacce, riducendo il rischio di propagazione degli attacchi e facilitando la gestione delle vulnerabilità. Questa segmentazione è cruciale per garantire che i sistemi critici siano protetti da accessi non autorizzati e che le comunicazioni tra i vari componenti siano sicure.
Gli standard richiedono l'implementazione di controlli di accesso rigorosi per proteggere le risorse critiche. Questo include l'adozione di tecniche di autenticazione forte, come l'autenticazione multifattore (MFA), l'implementazione di autorizzazioni basate sui ruoli, e la registrazione e monitoraggio delle attività per rilevare e rispondere a eventuali anomalie o accessi non autorizzati.
Per quanto riguarda la gestione dei rischi e conformità, gli standard come il NIST SP 800-82 offrono metodologie per la valutazione e la gestione dei rischi associati ai sistemi ICS. Le organizzazioni devono identificare le minacce e le vulnerabilità specifiche dei loro ambienti industriali e implementare controlli adeguati a mitigare questi rischi. Questo processo di analisi aiuta a garantire che le misure di sicurezza siano proporzionate ai rischi identificati e che le risorse siano protette in modo efficace.

Molti ambienti industriali continuano a utilizzare tecnologie legacy che possono non essere progettate per soddisfare gli standard di sicurezza moderni. Integrare queste tecnologie con soluzioni più recenti può comportare sfide significative, richiedendo soluzioni creative per garantire la sicurezza senza compromettere le operazioni. L'adozione di gateway e soluzioni di middleware sicuri può aiutare a mitigare i rischi associati alle tecnologie legacy.
Mantenere la conformità agli standard di sicurezza richiede un impegno continuo nella gestione delle patch, nella formazione del personale e nella revisione delle politiche di sicurezza. Le organizzazioni devono adottare pratiche di sicurezza automatizzate, implementare processi di aggiornamento regolari e assicurarsi che le loro pratiche di sicurezza siano adattate alle nuove minacce emergenti.

OT Security e Best Practices

Per ridurre i rischi informatici nei sistemi OT, le organizzazioni devono creare e attuare un programma di cybersecurity OT capace di integrarsi con i programmi di cybersecurity IT esistenti ed adattarsi alle specificità degli ambienti OT.
Un programma efficace deve considerare la sicurezza durante tutto il ciclo di vita del sistema, dalla progettazione all'installazione e alla manutenzione, evitando di fare affidamento sulla sicurezza post-distribuzione.

Sviluppare e implementare una strategia di cybersicurezza ha un impatto diretto sulle decisioni architetturali, aumentando la probabilità di raggiungere efficacemente gli obiettivi di sicurezza a livello di sistema. Un approccio chiave in questo contesto è la *difesa in profondità*, che si basa su molteplici livelli di protezione per garantire una sicurezza olistica. Questa strategia integra persone, tecnologia e capacità operative, creando barriere a più livelli e su diverse aree dell'organizzazione.
La difesa in profondità è ampiamente considerata una best practice ed è inclusa in numerosi standard e regolamenti di sicurezza. Si fonda su due principi fondamentali: evitare punti unici di vulnerabilità e riconoscere che le minacce possono provenire da diverse fonti. I controlli di sicurezza sono strutturati per fornire livelli successivi di protezione intorno ai sistemi e ai componenti critici. Questo approccio è particolarmente efficace negli ambienti OT, dove consente di concentrare le difese su funzioni vitali.
Le strategie di difesa in profondità si basano su diversi strati, ognuno dei quali contribuisce a creare una protezione robusta e multilivello.
Il primo strato*,* la *gestione della sicurezza*, stabilisce il programma di cybersecurity complessivo che supporta l'ambiente OT, fornendo le basi per le decisioni relative agli altri strati.
Il secondo strato*, la sicurezza fisica***,** mira a ridurre il rischio di danni accidentali o intenzionali agli asset e all'ambiente circostante. Gli asset protetti possono includere sistemi di controllo, strumenti, attrezzature, l'ambiente, la comunità circostante e proprietà intellettuali come i dati riservati (ad es. impostazioni dei processi e informazioni sui clienti). Un approccio completo alla sicurezza fisica in una strategia di difesa in profondità dovrebbe comprendere diversi attributi:

- *Protezione delle sedi fisiche*: Implementare barriere di sicurezza come recinzioni, muri, e serrature per proteggere edifici, attrezzature e altri asset.
- *Controllo degli accessi fisici*: Assicurare che i cabinet e le apparecchiature siano bloccati quando non necessari, mantenere le chiavi degli asset OT nella posizione "Run" se non in fase di programmazione.
- *Sistemi di monitoraggio degli accessi*: Utilizzare telecamere, sensori e sistemi di identificazione per registrare la presenza o l'assenza di persone e oggetti e per rilevare accessi non autorizzati.
- *Tracciamento di persone e veicoli*: Monitorare i movimenti per garantire la sicurezza, identificare chi necessita assistenza e supportare la risposta alle emergenze.

Il terzo strato, la *sicurezza della rete*, garantisce che le comunicazioni tra i diversi componenti del sistema siano protette da attacchi esterni e vulnerabilità.

Partendo dalla sicurezza fisica, le organizzazioni devono estendere il loro focus alle comunicazioni di rete per proteggere i dati e i dispositivi che supportano i loro ambienti di Tecnologia Operativa (OT). Una pianificazione e un'implementazione efficaci della sicurezza di rete comprendono diversi aspetti chiave, tra cui:

- *Segmentazione e Isolamento:* La segmentazione comporta la suddivisione e l'isolamento della rete in zone distinte basate su vari criteri come autorità di gestione, livello di fiducia, criticità, flusso di dati o posizione. Le organizzazioni possono impiegare modelli riconosciuti a livello industriale, come il modello Purdue, i livelli ISA-95 o l'architettura a tre livelli dell'IIoT, per strutturare efficacemente la segmentazione della rete OT. L'inclusione di una Demilitarized Zone (DMZ) come confine di enforcement tra i segmenti di rete migliora ulteriormente la sicurezza.
- *Registrazione Centralizzata:* I dispositivi come router, switch, firewall, server e workstation devono essere configurati per registrare eventi rilevanti per supportare il monitoraggio, l'allerta e la risposta agli incidenti. Una piattaforma centralizzata di gestione dei log aiuta nella conservazione, monitoraggio e analisi dei log.
- *Monitoraggio della Rete:* Il monitoraggio della rete comporta l'analisi di avvisi e log per rilevare potenziali incidenti di cybersecurity. Strumenti che supportano il rilevamento di anomalie comportamentali (BAD), la gestione delle informazioni e degli eventi di sicurezza (SIEM), i sistemi di rilevamento delle intrusioni (IDS) e i sistemi di prevenzione delle intrusioni (IPS) sono essenziali per un monitoraggio

efficace, aiutando le organizzazioni a monitorare il traffico in tutta la rete e a generare avvisi quando identificano traffico anomalo o sospetto.

- *Architettura Zero Trust (ZTA):* Questa architettura è un modello di cybersecurity che enfatizza la verifica continua delle richieste di accesso piuttosto che assumere fiducia basata sulla posizione di rete. A differenza dei modelli tradizionali che si basano sulla difesa perimetrale, la ZTA richiede decisioni di autorizzazione più vicine alla risorsa e valuta continuamente l'accesso. Una volta all'interno del perimetro di rete, gli utenti sono tipicamente considerati "fidati" e spesso ricevono un ampio accesso alle risorse accessibili. Di conseguenza, i dispositivi di protezione dei confini tra le zone non mitigano i rischi di movimento laterale all'interno di una zona. In questo contesto, l'adozione dei principi Zero Trust offre maggiore sicurezza, eliminando la fiducia implicita e applicando controlli di accesso rigorosi in ogni fase dell'interazione con le risorse aziendali.

Il quarto strato, la *sicurezza dell'hardware*, si concentra sulla protezione dei dispositivi fisici utilizzati nei sistemi OT. La sicurezza hardware fornisce una base fondamentale per garantire la sicurezza e la fiducia nei dispositivi all'interno di un ambiente OT. Una volta stabilita la fiducia nei dispositivi, è essenziale mantenere e monitorare questo stato in conformità con il modello di sistema e le politiche aziendali. In generale, le capacità di sicurezza hardware potenziano i dispositivi per soddisfare requisiti specifici di funzionalità e sicurezza, tra cui: monitoraggio e analisi, configurazione e gestione sicura, protezione degli endpoint, protezione dell'integrità e controllo degli accessi.

Infine, il quinto strato, la *sicurezza del software*, protegge i programmi e le applicazioni da minacce ed exploit. In generale, le capacità di sicurezza del software possono potenziare la sicurezza degli endpoint quando le organizzazioni integrano le seguenti pratiche:

- *Application allowlisting***:** Consente solo l'esecuzione di applicazioni autorizzate, prevenendo l'esecuzione di software non approvato che potrebbe contenere vulnerabilità o malware.
- *Patching:* Implica l'applicazione regolare di aggiornamenti e correzioni al software per risolvere vulnerabilità note e migliorare la sicurezza complessiva. Gli

aggiornamenti (patch) servono a risolvere vulnerabilità e migliorare le funzionalità. Alcuni strumenti, come i firewall per applicazioni web (WAF) e gli IPS, possono essere configurati in modo da fornire una protezione aggiuntiva per rilevare o prevenire gli attacchi contro le vulnerabilità non patchate.

- *Secure code development:* Include l'adozione di pratiche di codifica sicura per ridurre le vulnerabilità nel software durante la fase di sviluppo, garantendo che le applicazioni siano progettate e implementate in modo sicuro.
- *Configuration management, inclusa la messa in sicurezza delle applicazioni***:** Comporta l'applicazione di misure di sicurezza alle configurazioni delle applicazioni e dei sistemi, per garantire che siano impostate correttamente per ridurre i rischi e migliorare la protezione contro gli attacchi. Questo include la configurazione di controlli di accesso, l'abilitazione della crittografia per i dati e il blocco di porte di rete non necessarie.

Implementare questi strati di sicurezza in modo coordinato aiuta a costruire un'architettura difensiva che non solo protegge gli ambienti OT, ma rende anche le difese più resilienti e adattabili alle minacce emergenti, contribuendo a mantenere una sicurezza integrata e continua.

Inoltre, le organizzazioni dovrebbero valutare attentamente i casi d'uso del flusso di dati IIoT (Industrial Internet of Things), compresi quelli che comportano la condivisione di dati esternamente, per determinare se siano necessari ulteriori meccanismi di controllo degli accessi. È essenziale considerare che i vettori di attacco per i dispositivi IIoT possono differire da quelli gestiti negli ambienti OT (Operational Technology), a causa di requisiti di comunicazione più complessi o dell'uso di servizi aggiuntivi, come i sistemi cloud, necessari per supportare le esigenze operative.

Il modello Purdue

Per localizzare i dispositivi all'interno del contesto aziendale, è utile fare riferimento all'Architettura di Riferimento Purdue. Sviluppata negli anni '90 dalla Purdue University, questa architettura suddivide gli Industrial Control Systems (ICS) in zone o livelli distinti, ognuno con specifiche considerazioni di sicurezza. Il Modello Purdue fornisce una struttura chiara per comprendere le interconnessioni tra i vari elementi di un'architettura

ICS, facilitando la progettazione della rete, migliorando la comunicazione tra i team IT e OT, e potenziando la sicurezza e la resilienza operativa.
Nei livelli inferiori si trovano i sistemi OT, responsabili del controllo dei processi industriali, mentre i livelli superiori ospitano i sistemi IT, che gestiscono le informazioni aziendali. Tra questi due mondi si inserisce una zona demilitarizzata (DMZ), un'area di convergenza che consente un controllo centralizzato e sicuro dei punti di connessione, riducendo il rischio di attacchi informatici e garantendo una segregazione efficace tra IT e OT. Di seguito è riportata una panoramica dei livelli del modello, comprensiva delle zone aggiuntive e delle loro funzioni principali:

Livello 0: (Processo Fisico) Questo livello fondativo include i processi fisici e le attrezzature, come sensori, attuatori e dispositivi di campo, che interagiscono direttamente con il mondo fisico. Questi dispositivi eseguono compiti cruciali come l'assemblaggio e la lubrificazione e comunicano spesso direttamente con il software di monitoraggio tramite reti cellulari.
Livello 1: (Controllo Base) In questo livello si trovano i controllori e i Programmable Logic Controllers (PLC). Questi dispositivi sono responsabili dell'automazione dei singoli processi, traducendo i dati dei sensori in comandi eseguibili per gestire le operazioni industriali, inviando i comandi ai dispositivi del livello 0.
Livello 2: (Controllo di Supervisione) Questa zona contiene sistemi che supervisionano, monitorano e controllano i processi fisici, aggregando i dati provenienti dai controllori. Questo livello comprende i sistemi SCADA, DCS e e le Interfacce Uomo-Macchina (HMI).
Livello 3: (Operazioni di Manifattura) Questa zona contiene dispositivi OT personalizzati che gestiscono i flussi di lavoro di produzione in officina come i Sistemi di *Manufacturing execution systems (MES*), utilizzato per raccogliere dati in tempo reale per ottimizzare la produzione*, Manufacturing operations management (MOM)*, per la gestione delle operazioni di produzione, e i registratori storici, i quali memorizzano i dati di processo e, nelle soluzioni moderne, eseguono analisi contestuali.
Livello 3.5: (Zona Demilitarizzata (DMZ)) La DMZ funge da buffer sicuro tra la rete ICS e le reti esterne. In questa zona si trovano i dispositivi di sicurezza, come firewall, proxy e Sistemi di Prevenzione delle Intrusioni (IPS), che aiutano a prevenire il movimento

laterale delle minacce tra IT e OT. Questa configurazione garantisce che i sistemi dei livelli inferiori rimangano al riparo da potenziali attacchi o compromissioni. In caso di violazione della DMZ, questa può essere prontamente disattivata, isolando così i sistemi compromessi e consentendo il proseguimento della produzione senza interruzioni.
Livello 4/5: (Rete Aziendale) Il livello della rete aziendale comprende l'infrastruttura IT più ampia, inclusi le applicazioni aziendali e la connettività a Internet. Qui si trovano i sistemi di pianificazione delle risorse aziendali che gestiscono i programmi di produzione dello stabilimento, l'utilizzo dei materiali, le spedizioni e i livelli di inventario.
Nello specifico, il livello 4 comprende sistemi come il software ERP (Enterprise Resource Planning), i database, i server di posta elettronica e altri sistemi logistici che supportano la gestione e il coordinamento delle operazioni di produzione, garantendo la comunicazione e l'archiviazione sicura dei dati. Il livello 5, invece, rappresenta la rete aziendale vera e propria. Pur non essendo direttamente parte dell'ICS (Industrial Control Systems), questo livello svolge un ruolo cruciale nel raccogliere e analizzare i dati provenienti dagli ICS, permettendo alle decisioni aziendali di essere informate dai dati operativi.

L'Architettura di Riferimento Purdue offre una serie di vantaggi significativi per la sicurezza degli Industrial Control Systems (ICS), grazie alla sua struttura a più livelli.
Questo approccio implementa la difesa in profondità, creando numerosi punti di controllo di sicurezza che rendono più complessa l'infiltrazione di minacce nei sistemi critici. Segmentando la rete in zone distinte, il Modello Purdue consente inoltre di isolare i sistemi legacy, riducendo così l'esposizione a potenziali vulnerabilità e limitando l'impatto di eventuali falle di sicurezza.
Un altro beneficio importante è la mitigazione dei rischi. L'isolamento dei componenti critici assicura una maggiore protezione contro accessi non autorizzati e minimizza i danni accidentali, salvaguardando l'integrità operativa dell'intero impianto. Grazie all'approccio a più livelli, viene favorita l'implementazione di sistemi di monitoraggio e logging in ciascuna zona, il che aumenta la visibilità sulle attività di rete e facilita la rilevazione tempestiva di minacce.
La chiara segmentazione offerta dal Modello Purdue contribuisce a una visibilità migliorata. Questa struttura facilita un monitoraggio più accurato e completo della rete,

permettendo una risposta proattiva agli incidenti e migliorando la capacità di prevenzione degli attacchi

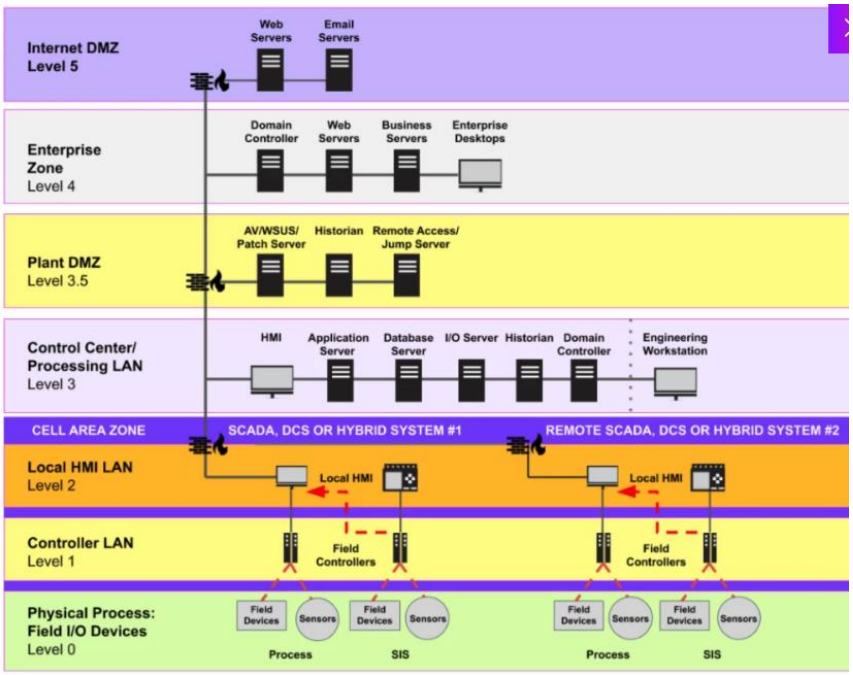

Figura 19 - Framework modello Purdue

Applicazione di un'Architettura di Difesa a Strati

Nel Sistema SCADA

La Figura 20 mostra un esempio di architettura di sicurezza per un sistema SCADA. L'architettura di difesa a strati per questi sistemi prevede la separazione della rete in zone distinte per isolare i componenti critici. Oltre alla segmentazione logica, possono essere integrate misure di sicurezza fisiche, come il monitoraggio e i controlli di accesso (ad esempio telecamere, lettori di carte).

I firewall industriali, che offrono supporto per protocolli specifici dell'OT e una protezione avanzata per dispositivi come PLC e controllori, devono essere posizionati tra le regioni della rete per monitorare e filtrare il traffico, garantendo che solo le comunicazioni autorizzate possano passare tra le regioni.

Per garantire la sicurezza delle connessioni tra segmenti distanti della rete, come tra centri regionali e stazioni remote, è fondamentale utilizzare tecnologie come VPN, canali criptati o connessioni punto-punto. In caso di connessioni tramite internet o WAN, queste devono essere rigorosamente limitate e protette per impedire accessi non autorizzati.

Una VPN (Virtual Private Network) consente di creare una rete privata virtuale tra i dispositivi, che crittografa i dati in transito per proteggerli dagli intrusi e dalla sorveglianza.

Un ulteriore livello di protezione è rappresentato dalla DMZ, che separa la rete aziendale dall'ambiente OT. Ogni comunicazione tra la rete aziendale e i centri di controllo deve passare attraverso questa zona cuscinetto, garantendo un monitoraggio continuo per prevenire potenziali compromissioni. Poiché la DMZ è collegata ad ambienti esterni, è vitale monitorare e proteggere i servizi all'interno della DMZ per evitare che gli attaccanti possano accedere all'ambiente OT inosservati.

Per i Livelli 4 e 5, le organizzazioni dovrebbero applicare il principio di funzionalità minima a tutti i componenti delle stazioni remote, ai componenti dei centri di controllo e ai dispositivi nella DMZ. Questo significa identificare e disabilitare qualsiasi funzionalità, software o porta non essenziale sui dispositivi. Ad esempio, se web servers non sono necessari su alcuni PLC o HMI più recenti, questi servizi dovrebbero essere disabilitati e le relative porte TCP/UDP chiuse. Le funzionalità devono essere abilitate solo quando strettamente necessario.

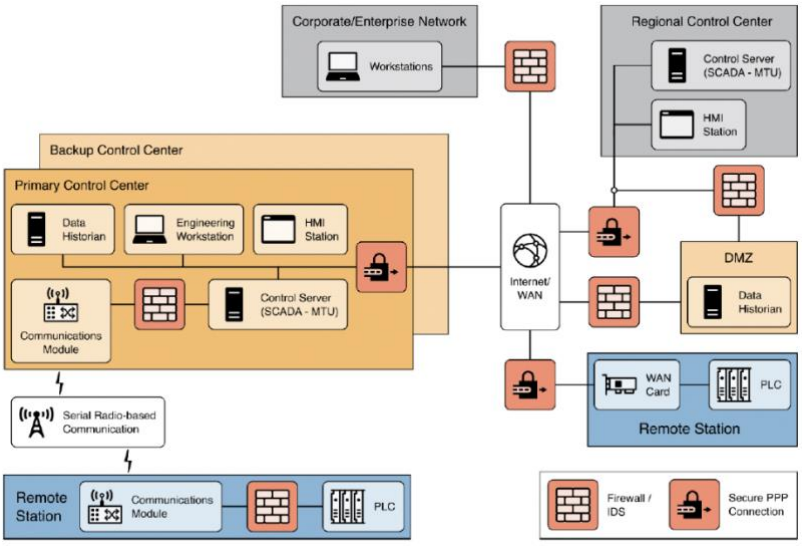

Figura 20 - Esempio di architettura di sicurezza per sistemi SCADA

Nel Sistema DCS

Similmente al SCADA, anche nel sistema DCS l'architettura di sicurezza si basa su una segmentazione della rete. Nel Livello 3, i dispositivi di campo che operano direttamente sui processi fisici sono separati da quelli del livello di gestione delle operazioni,

responsabili del monitoraggio e della gestione dei dispositivi di campo. Anche qui, la DMZ funge da zona di protezione tra l'ambiente OT e la rete aziendale.

I firewall industriali, posizionati tra il livello di campo e il livello di gestione, sono essenziali per filtrare e proteggere il traffico. Le regole di comunicazione devono essere definite con precisione, consentendo solo al traffico autorizzato di passare tra i livelli, per prevenire movimenti laterali indesiderati all'interno della rete.

Anche nel caso del DCS, la DMZ protegge l'infrastruttura OT dai rischi provenienti dall'ambiente aziendale, e le comunicazioni tra i due devono avvenire esclusivamente attraverso i servizi monitorati all'interno della DMZ. La gestione rigorosa degli accessi è garantita da server di autenticazione separati per l'IT e l'OT, che controllano l'accesso a seconda del contesto operativo.

Infine, anche nel DCS, per i livelli 4 e 5, si applica il principio della funzionalità minima. Disabilitare servizi non essenziali, come i web servers su PLC o HMI, riduce drasticamente le vulnerabilità e migliora la sicurezza complessiva del sistema, proteggendo l'intera infrastruttura industriale.

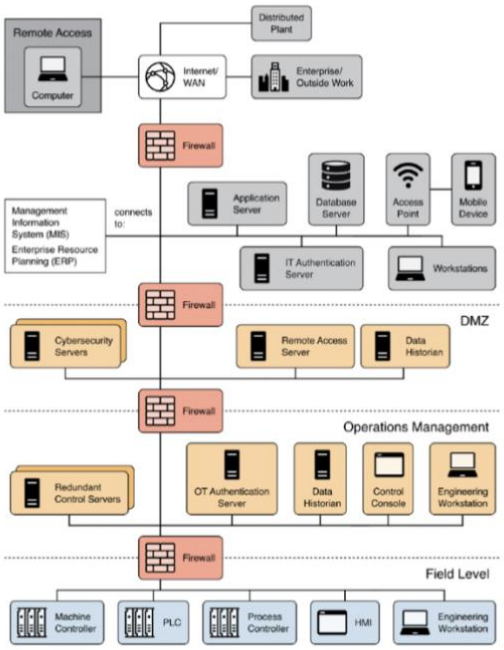

Figura 21 - Esempio di architettura di sicurezza per sistemi DCS

Architettura di Sicurezza per Sistemi DCS e PLC con IIoT

La Figura 22 illustra un esempio semplificato di architettura di sicurezza per un sistema DCS integrato con dispositivi IIoT (Industrial Internet of Things), basata sulle linee guida

per ambienti OT con DCS e PLC. Nell'implementazione di soluzioni IIoT, è fondamentale creare segmenti di rete separati per gestire i nuovi componenti IIoT e le loro specifiche esigenze di comunicazione. Questi segmenti sono progettati per interfacciarsi con la piattaforma IIoT e collegarsi in modo sicuro al sistema DCS.

L'architettura illustra come la comunicazione tra il livello della piattaforma IIoT e il sistema DCS avvenga attraverso un firewall al confine della DMZ (zona demilitarizzata). Questa configurazione consente di indirizzare i dati verso i server situati nella DMZ o verso la rete aziendale/internet, a seconda delle necessità operative dell'IIoT. Esistono diversi modi per archiviare i dati generati dai dispositivi IoT, anche ai fini della loro analisi: on premises (in loco), in cloud o ibridando le due opzioni.
La scelta fra le varie possibilità dipende dal volume dei dati, ma anche dal tipo di connettività, oltre che da altri fattori

La trasmissione dei dati attraverso la DMZ è un elemento chiave per soddisfare i requisiti operativi e di sicurezza del IIoT. Questo approccio non solo agevola il trasferimento dei dati verso i server DMZ, ma consente anche ai servizi di cybersecurity presenti nella DMZ di monitorare e gestire in tempo reale le comunicazioni della piattaforma IIoT. Implementare questa architettura assicura che i dati siano protetti e che le comunicazioni siano costantemente sotto controllo, riducendo così il rischio di compromissioni della sicurezza.

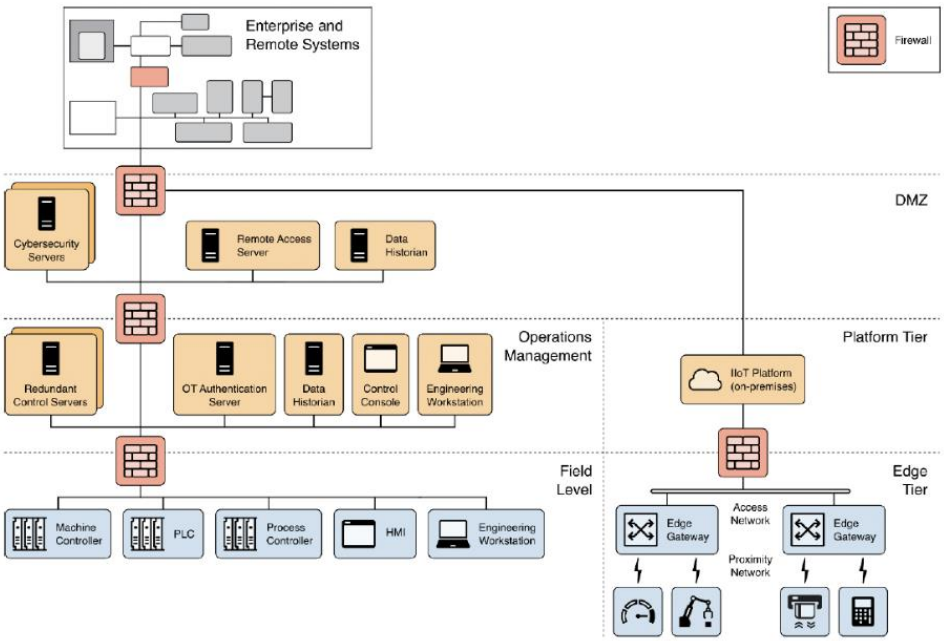

Figura 22 - Esempio di architettura di sicurezza per sistemi DCS e IoT

La Sicurezza degli Ambienti Complessi e Ibridi

Con l'accelerazione della digitalizzazione molte organizzazioni stanno dando priorità a iniziative di trasformazione come la migrazione al cloud, l'automazione e l'Industrial IoT. Secondo l'Illumio Cloud Security Index, il 92% dei produttori esegue già applicazioni di grande valore nel cloud, e il 97% ritiene che una violazione del cloud avrebbe un impatto significativo sulla propria organizzazione, con il 43% che sostiene che le operazioni normali diventerebbero impossibili. (Ilumio, 2023)
Nonostante la possibilità teorica di spostare i Sistemi di Controllo Industriale (ICS) al cloud esista da oltre un decennio, l'adozione è stata lenta a causa dei rischi associati.
In pratica, le applicazioni e i servizi ICS, inclusi i database come l'Historian, verrebbero ospitati nel cloud, con i PLC (Programmable Logic Controllers) che inviano i dati direttamente al cloud. Questo permetterebbe alle postazioni di lavoro di accedere ai dati ICS in remoto. Di conseguenza, l'attacco di superficie del SaaS[4] per ICS – noto come 'ICSaaS' – sarà più simile a quello delle reti SaaS comuni piuttosto che a quello delle reti SCADA/ICS tradizionali.

La migrazione al cloud non si limita a cambiare il luogo in cui vengono ospitati i sistemi, ma introduce cambiamenti significativi nella gestione della sicurezza, nella connettività e nei controlli di accesso. I sistemi OT, tradizionalmente progettati per operare in ambienti locali e isolati, seguendo il modello Purdue (ISA-95), si basavano su architetture centralizzate che minimizzavano il rischio di attacchi esterni. Il cloud computing ha ribaltato questo paradigma, offrendo alle aziende una piattaforma flessibile, scalabile e accessibile da remoto per gestire ed elaborare i dati su larga scala. Questo ha migliorato la collaborazione, l'efficienza operativa e la capacità di prendere decisioni informate in tempo reale.

Questa trasformazione è supportata dall'Industrial Internet of Things (IIoT), che utilizza il cloud per integrare sensori, dispositivi e applicazioni in una piattaforma unificata. L'integrazione dei dati raccolti da sensori avanzati e dispositivi di campo consente

[4] Il Software as a Service (SaaS) è un modello di distribuzione del software basato su cloud in cui il provider di servizi cloud sviluppa e mantiene il software applicativo, fornisce aggiornamenti automatici e mette il software a disposizione dei propri clienti via Internet.

un'analisi più approfondita e tempestiva, contribuendo a ottimizzare le operazioni e a prendere decisioni basate su dati reali.

Una delle principali innovazioni introdotte dal cloud computing è l'adozione dell'*Edge computing*, che sposta l'elaborazione dei dati più vicino alla fonte di origine. Questo approccio riduce la latenza e il traffico di dati verso i data center centrali, migliorando la velocità e la resilienza operativa. I dispositivi edge elaborano i dati localmente, inviando solo le informazioni rilevanti al cloud per ulteriori analisi, il che è particolarmente utile per applicazioni di diagnostica remota, manutenzione predittiva e monitoraggio della sicurezza.

Oltre a migliorare la velocità e l'efficienza operativa, il cloud ha ampliato l'integrazione dei sistemi aziendali. In passato, l'integrazione riguardava principalmente i livelli superiori della piramide ISA-95, come i sistemi ERP. Oggi, con la diffusione della Trasformazione Digitale (DX), l'integrazione si estende a tutte le aree aziendali, dalla supply chain ai sistemi finanziari e alle risorse umane. Questo livello di interconnessione consente alle aziende di automatizzare processi critici, migliorando la trasparenza e la capacità di rispondere rapidamente alle dinamiche del mercato. Tuttavia, la transizione verso il cloud comporta anche nuove sfide.

La sicurezza dei dati nel cloud è fondamentale e richiede l'uso di crittografia durante il transito e a riposo, ma molti sistemi OT legacy non supportano nativamente la crittografia, rendendo complessa l'implementazione di soluzioni di sicurezza end-to-end. Inoltre, le organizzazioni devono assicurarsi che le soluzioni cloud siano conformi alle normative di settore e locali, integrando la conformità nella loro strategia di sicurezza.

Un'altra sfida è la gestione della responsabilità condivisa tra fornitori di servizi cloud e organizzazioni, che richiede una chiara definizione dei ruoli per la sicurezza e la gestione delle vulnerabilità. L'integrazione di sistemi legacy con il cloud può introdurre vulnerabilità, e quindi è necessario un approccio attento che includa aggiornamenti o sostituzioni per garantire la compatibilità e la sicurezza.

Infine, il cloud può influenzare la latenza e le prestazioni dei sistemi OT, compromettendo la capacità di rispondere in tempo reale. È cruciale bilanciare la sicurezza con la necessità di mantenere bassa la latenza per garantire un funzionamento efficiente.

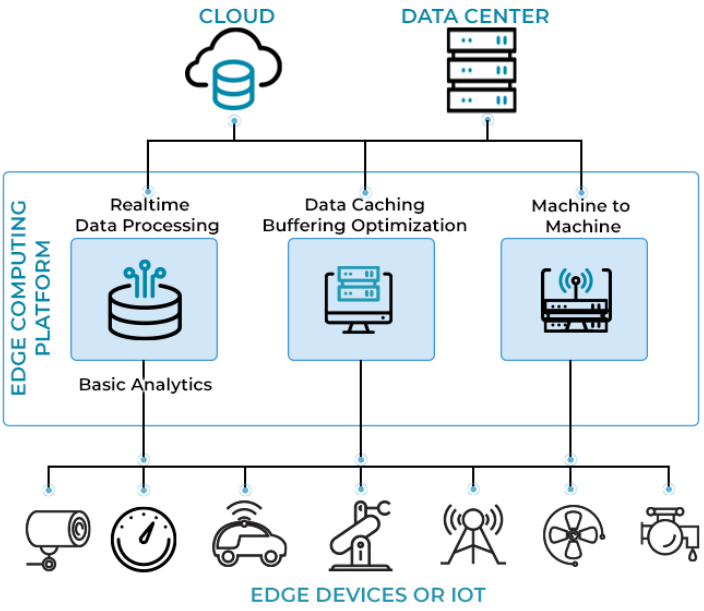

Figura 23 - Edge Computing

Soluzioni per Superare le Problematiche degli Ambienti IoT

Non è possibile fare affidamento completo sui provider cloud e sulle infrastrutture IoT per garantire la sicurezza del proprio ecosistema. È quindi fondamentale adottare una serie di pratiche per proteggere i dati e rafforzare la sicurezza dell'organizzazione. Un passo iniziale cruciale è l'implementazione di misure di autenticazione e controllo degli accessi solide. Questo include l'adozione di metodi come l'autenticazione a due fattori (2FA) e il controllo degli accessi basato sui ruoli (RBAC). Inoltre, è necessario sviluppare politiche che incoraggino audit di sicurezza regolari e l'aggiornamento continuo degli standard di sicurezza.

La crittografia rappresenta un elemento essenziale per garantire la riservatezza dei dati, sia quando sono in fase di archiviazione sia durante il loro trasferimento. La crittografia dei dati in transito protegge le informazioni mentre vengono trasmesse attraverso le reti, prevenendo intercettazioni e accessi non autorizzati. La crittografia dei dati a riposo garantisce che le informazioni memorizzate nel cloud siano protette da accessi non autorizzati anche in caso di compromissione fisica del supporto di memorizzazione. È importante implementare protocolli di rete sicuri, come il Transport Layer Security (TLS), per proteggere i dati IoT durante il transito, soprattutto quando vengono trasferiti nel cloud. Il TLS è un protocollo crittografico progettato per garantire che i dati scambiati

tra dispositivi, applicazioni o server siano trasmessi in modo sicuro. Occorre prestare particolare attenzione alla conservazione sicura delle chiavi di crittografia, in modo che solo i soggetti autorizzati possano accedere ai dati.

Un'altra misura cruciale è l'aggiornamento regolare e la patching dei dispositivi IoT e dell'infrastruttura cloud. Il firmware e il software dei componenti IoT devono essere aggiornati frequentemente per garantire che eventuali vulnerabilità di sicurezza siano risolte. È fondamentale anche monitorare attentamente gli aggiornamenti di sicurezza rilasciati dal provider cloud e applicare tempestivamente le patch necessarie.

Infine, la conduzione di audit e valutazioni di sicurezza è indispensabile per proteggere l'infrastruttura IoT. Secondo un report di IBM del 2021, due violazioni della sicurezza su tre avrebbero potuto essere evitate tramite la patching dei sistemi e l'applicazione di politiche di sicurezza appropriate. Gli audit regolari consentono di identificare e risolvere eventuali punti deboli, garantendo un livello di protezione elevato e aggiornato rispetto alle minacce emergenti.

Studio di Caso: Vulnerabilità e Incidenti di Sicurezza nell'Industria

Questo capitolo si propone di analizzare alcuni casi reali di incidenti di sicurezza informatica che hanno colpito il settore industriale. Attraverso un'analisi approfondita di questi eventi, sarà possibile comprendere l'impatto delle minacce informatiche sulla continuità operativa e sui danni finanziari che possono derivarne. L'obiettivo è fornire una panoramica chiara delle conseguenze che tali attacchi possono avere, evidenziando l'importanza di strategie di sicurezza adaguate.

Colonial Pipeline Attack

Nel maggio 2021, il Colonial Pipeline, uno degli oleodotti più grandi e vitali degli Stati Uniti, è stato vittima di un attacco ransomware. Tale attacco ha causato gravi conseguenze sull'approvvigionamento di carburante lungo tutta la costa orientale del paese. L'oleodotto, attivo dal 1962, si estende per oltre 5.500 miglia dal Texas al New Jersey e sostiene il 45% delle forniture di carburante della costa orientale, trasportando 2,5 milioni di barili al giorno, inclusi benzina, jet fuel e olio per riscaldamento domestico. (Kerner, 2022)

L'attacco, considerato il più grande contro infrastrutture critiche degli Stati Uniti, è stato orchestrato dal gruppo di hacker noto come DarkSide. Gli aggressori hanno ottenuto l'accesso alla rete del Colonial Pipeline grazie a una password esposta utilizzata da un account VPN. Probabilmente il dipendente dell'azienda ha utilizzato la stessa password, utilizzata per collegarsi alla VPN, anche in altri contesti, facilitando l'individuazione di questa e conseguentemente permettendo l'ingresso nei sistemi dell'azienda da parte di attaccanti.

Una volta all'interno, DarkSide ha rubato 100 gigabyte di dati in sole due ore e ha infettato la rete con un ransomware, paralizzando diversi sistemi cruciali, tra cui quelli di fatturazione e contabilità. Sebbene i sistemi operativi dell'oleodotto, che gestiscono effettivamente il trasferimento del petrolio, non siano stati compromessi, l'azienda ha deciso di chiudere l'intera conduttura per prevenire ulteriori danni.

Il 7 maggio 2021, Colonial Pipeline ha scoperto l'intrusione e ha immediatamente contattato società di sicurezza per investigare e le autorità federali. Per accelerare il recupero dei sistemi, l'azienda ha pagato un riscatto di 75 bitcoin, pari a circa 4,4 milioni di dollari all'epoca, ottenendo così la chiave di decrittazione necessaria per riprendere il controllo dei propri sistemi. Il 12 maggio 2021, il Colonial Pipeline è tornato operativo.

Gli attacchi ransomware, come quello subito dal Colonial Pipeline, criptano i dati di un'organizzazione e li tengono in ostaggio fino al pagamento di un riscatto.

DarkSide operava con un modello di ransomware-as-a-service (RaaS), fornendo le sue capacità ransomware ad altri attori delle minacce, che potevano utilizzare questo servizio per colpire ulteriori vittime.

L'attacco ha avuto un impatto immediato e significativo, colpendo il settore aereo con carenze di carburante per molti vettori e causando interruzioni in aeroporti come Atlanta e Nashville, portando ad un aumento del carburante, che ha superato i 3 dollari al gallone.

Fortunatamente, il Dipartimento di Giustizia degli Stati Uniti è riuscito a recuperare parte del riscatto pagato. Il 7 giugno 2021, grazie a un'ordinanza del tribunale, gli agenti dell'FBI hanno sequestrato 63,7 bitcoin, pari a circa 2,3 milioni di dollari, tracciando il pagamento fino all'indirizzo del portafoglio digitale utilizzato dagli hacker.

In risposta all'attacco, sia il governo degli Stati Uniti che l'industria hanno intensificato gli sforzi per prevenire futuri incidenti simili, concentrandosi sulla sicurezza della catena di approvvigionamento. Poiché le grandi organizzazioni gestiscono un'ampia varietà di

applicazioni e dipendenze software, diventa difficile monitorare e proteggere ogni componente da potenziali minacce.
Per affrontare queste sfide, l'amministrazione Biden ha emesso un ordine esecutivo nel maggio 2021, che impone alle agenzie governative di adottare misure proattive per rafforzare la sicurezza informatica, tra cui l'uso della distinta base del software (SBOM). La SBOM permette ai produttori di mantenere aggiornati i componenti software e di rispondere rapidamente a eventuali vulnerabilità. Gli acquirenti possono usare la SBOM per analizzare le vulnerabilità o le licenze dei componenti software, valutando così i rischi associati.
L'ordine esecutivo ha inoltre incaricato la National Telecommunications and Information Administration (NTIA) di sviluppare una guida sui requisiti minimi per l'implementazione della SBOM, pubblicata nel luglio 2021. Questa guida fornisce indicazioni su come adottare efficacemente la SBOM, migliorando la resilienza delle infrastrutture digitali contro attacchi futuri.

Tale episodio evidenzia l'importanza di strategie quali la protezione degli endpoint e il rafforzamento dell'accesso remoto, nonché la necessità di formazione dei dipendenti sulle tematiche della cybersecurity.
La protezione degli endpoint è essenziale e si basa sull'implementazione del principio del minimo privilegio. Questo principio limita l'accesso ai sistemi e ai dati sensibili solo agli utenti che ne hanno realmente bisogno per svolgere le loro mansioni. Se applicato rigorosamente, questo principio avrebbe impedito agli hacker di sfruttare le credenziali rubate per ottenere privilegi elevati e accedere a risorse critiche.
La gestione degli accessi privilegiati e l'autenticazione a più fattori (MFA) sono altrettanto cruciali per proteggere l'accesso remoto. È fondamentale gestire rigorosamente gli utenti con privilegi elevati e garantire che le connessioni remote siano protette da sistemi di gestione degli accessi privilegiati. Questi sistemi devono assicurare che solo gli utenti autorizzati possano accedere ai sistemi e solo alle risorse strettamente necessarie.
Inoltre, l'adozione di soluzioni di Endpoint Privilege Management (EPM) rappresenta un ulteriore passo per prevenire attacchi, come il ransomware. Le soluzioni EPM bloccano qualsiasi processo o applicazione che tenti operazioni non autorizzate, come la

crittografia dei file, rendendo inefficace il ransomware indipendentemente dal livello di privilegio dell'utente**.**

In aggiunta, un piano di risposta agli incidenti ben strutturato è essenziale per gestire e mitigare i danni durante un attacco informatico. Questo piano deve prevedere scenari di attacco, metodi per mantenere le operazioni critiche e procedure di comunicazione con le parti interessate. Esercitazioni regolari e revisioni del piano aiutano a garantire preparazione e a identificare vulnerabilità.

Infine, l'attacco al Colonial Pipeline ha sottolineato la necessità di una copertura assicurativa adeguata per i rischi informatici. Le organizzazioni dovrebbero considerare una polizza di assicurazione specifica per i rischi cyber per proteggersi contro le perdite potenziali e consultare esperti per determinare la copertura più adatta.

Triton Attack

Nel panorama della sicurezza informatica, l'attacco malware Triton del 2017 rappresenta una svolta inquietante. Per la prima volta, un cyberattacco ha mirato direttamente ai sistemi di sicurezza di un impianto industriale, mettendo a rischio la vita umana.

Durante l'estate del 2017, un impianto petrolchimico in Arabia Saudita fu vittima di un sofisticato attacco informatico. Gli aggressori sono stati in grado di installare un malware, conosciuto come Triton (o Trisis), con lo scopo di compromettere i Safety Instrumented Systems (SIS) dell'impianto. Questi sistemi sono cruciali per prevenire disastri industriali, intervenendo automaticamente in caso di condizioni pericolose, come il rilascio di gas tossici o esplosioni, tramite l'attivazione di valvole di chiusura e meccanismi di rilascio della pressione.

I SIS utilizzano una tipologia speciale di PLC (Controllori Logici Programmabili) progettati per essere altamente affidabili e prevedibili. Per garantire la sicurezza, i SIS sono spesso collocati su reti isolate e l'accesso è rigorosamente controllato. Se i parametri operativi superano limiti predefiniti, i SIS attivano meccanismi di spegnimento sicuro per evitare danni. Sebbene i sistemi di sicurezza siano autonomi, sono spesso collegati a stazioni di ingegneria per gli aggiornamenti e la manutenzione.

Durante questo attacco, gli hacker sono riusciti ad ottenere l’accesso alla rete IT dell'impianto industriale usando strumenti informatici comuni. Una volta all'interno, gli

attaccanti hanno condotto attività di riconoscimento per mappare l'infrastruttura IT e OT, identificando i dispositivi e i sistemi presenti, comprese le interfacce HMI e i controllori di processo.
Nello specifico, gli aggressori hanno preso di mira una stazione di lavoro usata per gestire i sistemi di sicurezza dell'impianto. Probabilmente l'infezione è avvenuta tramite una tecnica di social engineering, in cui l'ingegnere ha scaricato un file con un nome apparentemente legittimo, "trilog.exe".
Questo file, creato inizialmente come uno script Python e poi compilato in un eseguibile, ha iniettato file dannosi nella memoria del PLC, dando così agli attaccanti il controllo totale del sistema. Gli attaccanti avevano intenzione di usare il loro accesso per manipolare i dispositivi di sicurezza dell'impianto e causare danni fisici. Tuttavia, a causa di un errore nel loro codice, il sistema di sicurezza dell'impianto si è attivato automaticamente. Questo ha portato l'impianto a entrare in modalità di emergenza e fermare la produzione. L'arresto dell'impianto ha rivelato l'attacco e impedito ulteriori danni. (Lab, 2021)

L'attacco Triton rappresenta un significativo passo avanti nella minaccia informatica, poiché per la prima volta i cybercriminali hanno mirato direttamente a sistemi progettati per garantire la sicurezza fisica. La scoperta del malware rivelò che gli hacker erano riusciti a infiltrarsi nella rete aziendale dell'impianto già nel 2014, attraverso una falla in un firewall mal configurato o sfruttando una vulnerabilità nel codice di Windows. Una volta penetrati nella rete dell'impianto, avevano ottenuto informazioni sui controllori SIS e sul loro firmware[5]. Questo attacco ha sollevato preoccupazioni globali sulla sicurezza delle infrastrutture critiche, dimostrando che le minacce informatiche possono andare oltre il furto di dati e l'interruzione dei servizi, e possono mettere a rischio direttamente la vita umana e la sicurezza industriale.
L'attacco malware Triton del 2017 ha sottolineato l'urgenza di migliorare la sicurezza dei sistemi industriali. Le lezioni principali emerse dall'incidente includono la necessità di aggiornamenti regolari del software, configurazioni di rete sicure e un monitoraggio costante delle reti industriali. Per difendersi efficacemente, è fondamentale implementare

[5] Il firmware è un tipo di software che fornisce istruzioni operative ai componenti hardware di un dispositivo, consentendone il funzionamento di base.

tecnologie avanzate come la segmentazione delle reti e sistemi di rilevamento delle intrusioni (IDS) progettati specificamente per ambienti industriali.

Un'altra priorità è la formazione continua del personale per affrontare i rischi di social engineering, assicurandosi che il personale sia in grado di riconoscere e gestire file sospetti e tentativi di phishing. Le organizzazioni devono anche sviluppare e testare piani di risposta agli incidenti che prevedano scenari di attacco e procedure di comunicazione per minimizzare i danni durante una crisi.

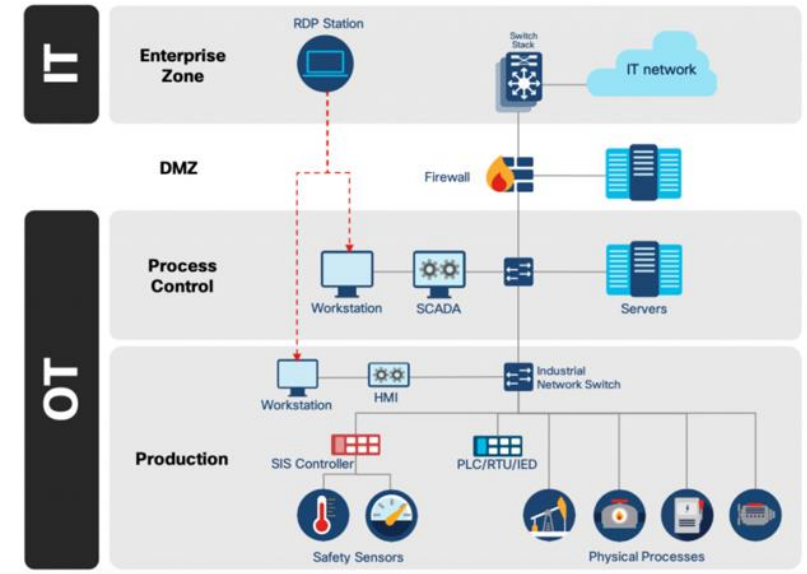

Figura 24 - Infrastruttura OT con sistemi SIS

Norsk HYDRO Attack

Nel marzo 2019, Norsk Hydro, uno dei principali fornitori mondiali di alluminio, ha subito un attacco informatico di grande portata, perpetrato tramite il ransomware LockerGoga. Questo tipo di ransomware non si limita a criptare i file, ma adotta anche tecniche aggiuntive per complicare ulteriormente il recupero del sistema. Dopo aver criptato i dati, LockerGoga disconnette tutti gli utenti, disabilita gli adattatori di rete e cambia le password locali e di amministratore, paralizzando sia i sistemi informatici aziendali sia le reti di controllo dell'impresa.

Norsk Hydro possiede e gestisce centinaia di impianti in 40 paesi e impiega oltre 36.000 persone. La loro base industriale comprende tutti i processi necessari per produrre prodotti in alluminio, inclusi l'estrazione delle materie prime e la gestione di centrali idroelettriche.

L'attacco ha colpito principalmente il dipartimento delle Soluzioni Estruse, responsabile della produzione di prodotti in alluminio pressati attraverso uno stampo.
Nonostante le minacce, Norsk Hydro ha scelto di non pagare il riscatto richiesto dagli aggressori e ha assunto consulenti di cybersecurity per ridisegnare e recuperare le loro reti. Durante questo processo, l'azienda è stata costretta ad operare manualmente, mantenendo la trasparenza durante il recupero, il che ha avuto un impatto positivo sulla loro reputazione. Sebbene l'attacco non abbia direttamente compromesso i sistemi di controllo, l'incidente serve come importante studio di caso per comprendere l'impatto che un attacco ransomware può avere sulle operazioni industriali, data la loro dipendenza dai sistemi IT.
Le tecniche utilizzate dagli attaccanti hanno incluso l'accesso iniziale tramite un'e-mail contenente un allegato malevolo, noto come spear phishing. Dopo aver ottenuto l'accesso, gli aggressori hanno catturato le credenziali di amministratore per ottenere privilegi elevati fino a diventare amministratori di dominio. Con tali privilegi, hanno potuto distribuire e attivare il ransomware attraverso l'Active Directory di Microsoft. Questo attacco ha messo in evidenza le vulnerabilità delle reti aziendali e l'importanza di avere misure di sicurezza robuste e una risposta ben strutturata per affrontare tali emergenze. L'attacco ha compromesso 160 siti aziendali con oltre 20.000 sistemi infetti. I sistemi compromessi sono stati resi completamente inutilizzabili. Norsk Hydro è riuscita a continuare la produzione, ma in modo limitato subito dopo l'attacco. L'azienda ha riportato una perdita stimata di 67-84 milioni di dollari (USD) e ci sono voluti diversi mesi per ripristinare completamente la capacità operativa. (BLAINE JEFFRIES, 2022)

L'incidente di ransomware a Norsk Hydro dimostra l'impatto ampio che un attacco ransomware può avere, data la dipendenza di un'organizzazione dai sistemi IT. La decisione di Norsk Hydro di non pagare il riscatto offre una visione realistica del tempo di recupero nel caso in cui sistemi critici di governo subiscano un attacco simile. Sebbene gli aggressori non abbiano ottenuto un guadagno finanziario diretto, hanno dimostrato che il malware IT di consumo può avere un impatto duraturo sulle operazioni.

Sviluppo di un Framework di Sicurezza Personalizzato

In un contesto industriale sempre più connesso e interdipendente, la protezione delle infrastrutture critiche e dei sistemi di automazione richiede soluzioni di sicurezza avanzate e personalizzate. L'obiettivo è creare un sistema di sicurezza su misura, capace di offrire una protezione completa e scalabile per ambienti eterogenei, rispettando al contempo le necessità di continuità operativa e resilienza. Il framework di seguito riportato suddivide le reti in diverse zone di sicurezza, ognuna con controlli specifici e adattati in base alla sensibilità delle risorse, seguendo i principi di difesa in profondità. Le raccomandazioni basate sui livelli di difesa in profondità suggeriscono misure fondamentali per affrontare questi rischi. In primo luogo, dissuadere gli incidenti implica ridurre la superficie di attacco attraverso la scansione delle vulnerabilità, l'aggiornamento regolare del software, la prevenzione delle intrusioni in rete e la formazione continua degli utenti. Questo approccio aiuta a rinforzare l'infrastruttura IT e a ridurre l'efficacia degli attacchi di spearphishing e ingegneria sociale.
Un altro aspetto fondamentale riguarda i rimedi, come il backup regolare dei dati e la creazione di ridondanze per i servizi critici. I backup devono essere conservati in ambienti isolati, preferibilmente offline, per prevenire la compromissione da parte degli aggressori. La scelta tra backup caldi e freddi[6] dipenderà dalle esigenze specifiche del sistema. Allo stesso tempo, le mitigazioni del ripristino richiedono il mantenimento e l'esercizio regolare dei piani di recupero. Questo assicura che i backup siano disponibili, verificabili e aggiornati, e che la formazione e gli esercizi sul ripristino delle risorse critiche garantiscano un rapido recupero con il minimo impatto operativo.
Comprendere l'impatto della compromissione dei sistemi IT/OT sulle infrastrutture critiche è fondamentale per informare accuratamente le operazioni e garantire che, anche in caso di attacco, le operazioni possano continuare con il minimo impatto.

[6] backup a freddo: la copia dei dati viene effettuata quando il database non è accessibile da chi, normalmente, lo utilizza per lavorarci.
backup a caldo: la copia dei dati viene effettuata anche quando il database è accessibile per modifiche.

Nel capitolo verranno presentati i concetti chiave alla base di questa visione, insieme alle tecnologie e alle strategie utilizzate per l'implementazione un una architettura di sicurezza personalizzata, con particolare attenzione all'isolamento delle reti critiche e alla protezione dei processi produttivi. Attraverso questo framework, si intende fornire una soluzione flessibile per le diverse realtà industriali, garantendo un elevato livello di sicurezza senza compromettere le prestazioni operative. Il framework presentato segue la segmentazione a livelli del modello Purdue.

In questo caso, la segmentazione vede come primo livello, a partire dall'alto, l'*Internet DMZ* (Demilitarized Zone). Esso rappresenta una zona di rete intermedia che funge da barriera protettiva tra Internet e la rete interna di un'organizzazione. La DMZ è progettata per ospitare risorse e servizi accessibili al pubblico, garantendo al contempo un isolamento sufficiente per proteggere la rete aziendale da potenziali attacchi esterni. Questa architettura è cruciale per migliorare la sicurezza della rete, limitando l'esposizione dei sistemi critici a minacce provenienti dall'esterno e consentendo l'erogazione di servizi pubblici senza compromettere la sicurezza dei dati sensibili dell'organizzazione.

Come nella maggior parte degli altri livelli, uno switch di rete gestisce il traffico all'interno della DMZ, facilitando la comunicazione tra i vari server e ottimizzando le prestazioni della rete. Grazie alla sua capacità di gestire una vasta gamma di protocolli e applicazioni, lo switch assicura una gestione efficiente delle connessioni, migliorando la fluidità e la velocità delle comunicazioni.

All'interno della DMZ vengono collocati diversi tipi di server. I *web server* gestiscono le richieste HTTP degli utenti esterni, consentendo l'accesso ai contenuti online e fungendo spesso da prima interfaccia tra l'utente e l'organizzazione, rendendo la loro sicurezza fondamentale. Gli *e-mail server* sono responsabili della gestione delle comunicazioni via e-mail, permettendo agli utenti di inviare e ricevere messaggi e fungendo da canale principale di comunicazione aziendale. Inoltre, nella DMZ possono essere presenti server di servizi aggiuntivi che supportano applicazioni specifiche, come sistemi di gestione delle identità, servizi di archiviazione dati o altre applicazioni che richiedono accesso pubblico.

Per sostenere la protezione dei server pubblici, vengono proposte una serie di soluzioni di sicurezza avanzate, tra cui sistemi *EDR, NDR, SOAR, SIEM* e *tecnologie di Deception,*
I sistemi EDR (Endpoint Detection and Response), piattaforme dedicate alla rilevazione e risposta agli attacchi informatici, sono in grado di proteggere i terminali monitorando e rispondendo a minacce in tempo reale, difendendo i server da malware e altre minacce.

Il SOAR (Security Orchestration, Automation, and Response) è un workbench olistico per l'orchestrazione, l'automazione e la risposta della sicurezza, progettato per i team di sicurezza operativa (SOC). Questo sistema permette di rispondere in modo efficiente al crescente afflusso di avvisi, automatizzare processi manuali ripetitivi e affrontare la carenza di risorse. Fornisce playbook automatizzati e triaging degli incidenti, oltre a rimedi in tempo reale per identificare, difendere e contrastare i cyberattacchi.

La Network Detection and Response (NDR) è una soluzione per la rilevazione delle minacce sulla rete, capace di identificare attività anomale e potenzialmente dannose, fornendo risposte tempestive e mirate per mitigare i rischi. Questa soluzione monitora il traffico di rete per rilevare attività sospette e rispondere a potenziali minacce, utilizzando analisi comportamentale e rilevamento delle anomalie per identificare attacchi avanzati o compromissioni.
Inoltre, la gestione centralizzata delle politiche di sicurezza consente la configurazione e il monitoraggio delle politiche di sicurezza su tutta la rete da un'unica interfaccia utente semplificata, permettendo l'applicazione coerente dei criteri di sicurezza e l'aggiornamento del software su tutte le appliance.

Le tecnologie di Deception sono sistemi di inganno progettati per attirare potenziali attaccanti e rilevare minacce prima che possano compromettere la rete, raccogliendo informazioni sulle tattiche degli aggressori e migliorando le difese.
Per quanto riguarda l'analisi delle minacce vengono utilizzati strumenti per l'analisi dei file sospetti in ambienti controllati, come sandbox, che identificano comportamenti malevoli e consentono una risposta adeguata alle minacce, aiutando a identificare malware e altre minacce prima che possano causare danni.

Un sistema di gestione delle informazioni e degli eventi di sicurezza (SIEM) offre la capacità di ingerire e analizzare i dati di log provenienti da ambienti IT e OT, in

particolare da strumenti di sicurezza (IDS/IPS, sistemi antivirus e antimalware, VPN e web filters), dispositivi di rete (router, switch, DNS server, WAN), apparati (dispositivi di rete, server di autenticazione, database) e applicazioni (applicazioni internet e web). È una soluzione software che, in tempo reale, provvede al monitoraggio e alla gestione degli eventi che accadono all'interno della rete e sui vari sistemi di sicurezza, fornendo una correlazione e aggregazione tra essi. L'interfaccia è una console centralizzata, preposta ad attività di monitoraggio, segnalazione e risposta automatica a determinati eventi.

Il Livello 5 è direttamente connesso a Internet, permettendo ai server nella DMZ di ricevere richieste esterne. È fondamentale sottolineare che, in un'implementazione pratica, un firewall di rete è sempre presente per filtrare il traffico in ingresso e in uscita. Questo firewall filtra le connessioni da e verso i server nella DMZ, consentendo solo le comunicazioni autorizzate e riducendo il rischio di attacchi informatici. Inoltre, impedisce agli attaccanti di sfruttare vulnerabilità nei server pubblici per accedere alla rete interna.

Tra il Livello 5 e il Livello 4 viene posto un ulteriore firewall, il quale gioca un ruolo cruciale nella sicurezza complessiva della rete, gestendo il traffico tra la DMZ e la rete aziendale. Le sue funzioni principali includono il controllo delle comunicazioni tra i server della DMZ e i server interni, garantendo che solo il traffico autorizzato possa passare. Inoltre, assicura che le politiche di sicurezza definite dall'organizzazione siano applicate, garantendo che il traffico che entra nella rete interna sia conforme agli standard di sicurezza, riducendo al minimo il rischio di compromissioni.

Il Livello 4, noto come *Enterprise LAN*, rappresenta la rete locale aziendale che ospita risorse critiche e dati sensibili. Questa rete è progettata per garantire un accesso sicuro e controllato ai servizi interni dell'organizzazione, consentendo la comunicazione tra vari dispositivi, applicazioni e sistemi operativi.
All'interno di questo livello è presente uno switch di rete in grado di gestire il traffico all'interno dell'Enterprise LAN, collegando vari server e dispositivi di rete. Grazie a funzionalità avanzate come il VLAN tagging e la gestione del traffico, lo switch ottimizza le prestazioni della rete e garantisce una comunicazione fluida tra i componenti.

I server critici presenti in questo livello includono: i server di autenticazione, responsabili della gestione degli accessi degli utenti (assicurando che solo il personale autorizzato

possa accedere alle risorse aziendali), i server aziendali possono comprendere applicazioni ERP, CRM e altri sistemi gestiscono la logistica delle operazioni di produzione e forniscono comunicazioni e archiviazione dei dati.

Questo livello include quindi i desktop e le workstation degli utenti, solitamente impiegati per attività di pianificazione, gestione e amministrazione aziendale. L'accesso sicuro per dipendenti e fornitori on-site è garantito tramite autenticazione a più fattori (MFA), assicurando che solo utenti autorizzati possano accedere alla rete aziendale. Questa soluzione può includere soluzioni di password, token hardware, biometria e one-time password (OTP) con notifiche push o un token OTP hardware a tempo.
È inoltre utile implementare controllo degli Accessi Basato sui Ruoli (RBAC). Ogni utente deve essere assegnato a un ruolo specifico con privilegi limitati, che garantisca l'accesso solo alle risorse di cui ha effettivamente bisogno.
Inoltre, la Gestione delle Identità e degli Accessi (IAM) viene utilizzata per centralizzare e automatizzare la gestione delle identità e delle autorizzazioni, assicurando che gli utenti abbiamo accesso solo alle risorse rilevanti in base al ruolo e che gli accessi siano revocati rapidamente in caso di modifiche. Questo sistema viene utilizzato sia per controllare l'accesso a risorse IT (livello 4 e 5) che OT (Livello 3 e inferiori), assicurando che solo utenti autorizzati possano interagire con i sistemi di controllo (SCADA, HMI). L'IAM potrebbe essere integrato con i servizi di autenticazione remota, ad esempio per la gestione sicura degli accessi VPN o applicazioni basate su cloud.

Ogni desktop deve essere protetto con software antivirus e antimalware che siano aggiornati e configurati per rilevare le minacce più recenti, inclusi attacchi zero-day. È inoltre necessario implementare una politica di whitelisting che consenta solo l'esecuzione di applicazioni autorizzate sui desktop aziendali. Inoltre, tutti i dati sensibili memorizzati su di essi devono essere criptati utilizzando standard di crittografia avanzati, per garantire la protezione anche in caso di perdita o furto di un dispositivo.
I desktop aziendali devono essere inclusi in un piano di backup e ripristino completo per evitare perdite di dati critici in caso di incidenti di sicurezza o guasti. Implementare soluzioni di backup centralizzate, garantisce che i dati importanti siano copiati regolarmente e archiviati in modo sicuro, sia on-premise che su cloud. Un piano di

disaster recovery deve quindi includere il ripristino rapido dei backup in caso di compromissioni.

Per evitare che eventuali compromissioni ai desktop aziendali si diffondano ad altri segmenti della rete, è importante implementare VLAN separate per i desktop aziendali rispetto ai sistemi OT e ai server critici, limitando la capacità degli attaccanti di spostarsi lateralmente all'interno della rete.
Utilizzare soluzioni di Network Access Controll (NAC), garantisce il controllo degli accessi alla rete IT aziendale e verifica le conformità dei dispositivi prima di permettere di connettersi. Questo include desktop, laptop e server che appartengono all'infrastruttura IT. I dispositivi che non soddisfano le politiche di sicurezza, come la presenza di patch o antivirus aggiornati, devono essere isolati. È infatti necessario implementare un sistema di gestione delle patch automatizzato per garantire che tutte le workstation ricevano aggiornamenti di sicurezza critici non appena rilasciati dai fornitori.

Il Livello 4 comunica con il Livello 3.5 tramite un firewall. Questo firewall è essenziale per gestire il traffico tra l'Enterprise LAN e l'Operation DMZ, contribuendo a proteggere la rete interna da possibili minacce provenienti dall'operatività esterna. Le sue funzioni principali includono il controllo del traffico, che gestisce e monitora il flusso di dati tra i due livelli, impedendo accessi non autorizzati e filtrando le comunicazioni in base a regole di sicurezza predefinite. Inoltre, garantisce l'isolamento delle risorse, consentendo di isolare i server e le risorse dell'Enterprise LAN da quelle esposte nell'Operation DMZ, riducendo così il rischio di attacchi laterali.

Il Livello 3.5, denominato *Operation DMZ*, è una zona intermedia progettata per facilitare la comunicazione tra l'Enterprise LAN e le operazioni industriali. Originariamente non fa parte della struttura del modello Purdue, ma viene comunemente utilizzata in architetture moderne per migliorare la sicurezza e separare ulteriormente i sistemi IT e OT. Questa zona è particolarmente utile per facilitare la comunicazione tra i sistemi aziendali e quelli operativi, senza esporre direttamente i sistemi critici OT ai rischi proveniente dalla rete. Questo livello garantisce che i dati e le informazioni provenienti dai sistemi di controllo industriale possano essere gestiti e monitorati senza compromettere la sicurezza della rete aziendale.

Il livello 3.5 agisce come barriera tra il livello 4 (Enterprise) ed il livello 3 (Operations/Control Systems). Ha lo scopo di proteggere i sistemi operativi OT dagli attacchi provenienti dalla rete aziendale, limitando il traffico e consentendo solo le comunicazioni autorizzate attraverso un set di regole di sicurezza rigorose.

A questo livello, i server che raccolgono dati dai sistemi operativi (es. PLC, SCADA) e li rendono disponibili ai sistemi IT senza esporre direttamente questi ultimi alle reti OT. Questi server richiedono l'utilizzo di protocolli rigidi per garantire una comunicazione sicura e monitorata.

La DMZ è definita da due rigidi confini segmentati: uno tra la DMZ e la rete esterna non attendibile (cioè Internet) e uno tra la DMZ e la rete interna attendibile. Questi confini tra la DMZ e le altre reti sono rigorosamente applicati e protetti da firewall (come Next Generation Firewall) che ispezionano tutto il traffico che attraversa il confine della rete e hanno la capacità di rilevare e bloccare i contenuti dannosi prima che attraversino il confine da Internet alla DMZ o dalla DMZ alla rete interna protetta. Questi sistemi fanno in modo che attacchi provenienti dal mondo IT non possano compromettere i sistemi OT.
Questo significa che l'autore di un attacco così sofisticato da superare il primo firewall, deve anche accedere ai servizi rinforzati nella DMZ prima di poter danneggiare un'azienda. Se l'autore di un attacco riesce a penetrare il firewall esterno ed a compromettere un sistema nella DMZ, deve anche superare un firewall interno prima di avere accesso ai dati aziendali sensibili.

Essi sono configurati per applicare regole di sicurezza rigorose che garantiscono la protezione delle comunicazioni industriali, impedendo l'accesso non autorizzato e bloccando potenziali minacce.
È inoltre consigliato implementare un Web Application Firewall (WAF), una soluzione di scansione e-mail o altri controlli di sicurezza per fornire una protezione mirata ai servizi implementati.
Le organizzazioni in genere archiviano nella DMZ servizi e risorse rivolti all'esterno, nonché server per il sistema dei nomi di dominio (DNS), FTP (File Transfer Protocol), posta, proxy, Voce tramite protocollo Internet (VoIP) e server Web. Questi server e

risorse sono isolati e dispongono di un accesso limitato alla rete LAN, per garantire che sia possibile accedervi tramite Internet, ma la LAN interna non può farlo. Di conseguenza, un approccio con la DMZ rende più difficile per un hacker ottenere l'accesso diretto ai dati e ai server interni di un'organizzazione tramite Internet.

Il livello 3, denominato Operations and Control Systems o Operation Management si concentra sulla gestione delle operazioni industriali e dei processi produttivi. Contiene dispositivi che gestiscono i flussi di lavoro di produzione in officina come i Sistemi di Manufacturing execution systems (MES), utilizzato per raccogliere dati in tempo reale per ottimizzare la produzione, Manufacturing operations management (MOM), per la gestione delle operazioni di produzione, e i registratori storici, i quali memorizzano i dati di processo e, nelle soluzioni moderne, eseguono analisi contestuali.

All'interno dell'Operations and Control Systems possono essere presenti diversi server per applicazioni specifiche, tra cui:
I Domain Controller gestiscono l'autenticazione e l'autorizzazione degli utenti all'interno della rete operativa, assicurando che solo utenti legittimi possano accedere alle risorse.
Gli Application Server eseguono applicazioni utilizzate per gestire le operazioni industriali, come i sistemi SCADA (Supervisory Control and Data Acquisition).
Il Data Historian archivia i dati storici delle operazioni industriali, consentendo l'analisi e il monitoraggio delle performance nel tempo.

La protezione di questo livello è garantita da una serie di sistemi di sicurezza avanzati. Il Network Access Control (NAC) gestisce l'accesso alla rete operativa e ai sistemi di controllo (Scada, HMI, DCS). In questo contesto, in NAC viene utilizzato per monitorare e limitare l'accesso alle reti OT, assicurandosi che solo dispositivi e utenti autorizzati possano interagire con i sistemi operativi critici. Questo sistema offre visibilità, controllo e risposta automatica per tutto ciò che si connette alla rete, prevenendo accessi non autorizzati e limitando i rischi di compromissione.

Un altro componente fondamentale è il Centralized Reporting System che fornisce monitoraggio, registrazione e reporting centralizzati per le appliance di sicurezza

distribuite in ambito IT e OT. Questo strumento consente una visibilità completa sugli eventi di sicurezza, facilitando l'identificazione e la risposta tempestiva alle minacce. Raccoglie e analizza i dati di sicurezza da tutte le fonti per fornire report completi e dettagliati, facilitando la visibilità e la gestione delle minacce.

Il Centralized Policy Management permette la configurazione e il monitoraggio delle politiche di sicurezza su tutta la rete da un'unica interfaccia utente semplificata. Questo assicura l'applicazione coerente dei criteri di sicurezza e l'aggiornamento del software su tutte le appliance, migliorando l'efficienza operativa e riducendo il rischio di errori umani.

Il Privileged Access Management (PAM) offre funzionalità di gestione delle identità e degli accessi privilegiati, consentendo l'implementazione di una strategia di sicurezza zero-trust per le risorse critiche. PAM offre un controllo granulare sugli accessi degli utenti alle applicazioni e ai sistemi critici. Questo sistema registra tutte le attività degli utenti privilegiati, consentendo il monitoraggio delle azioni in tempo reale e la creazione di report dettagliati per analisi future.

È fondamentale monitorare continuamente il traffico e le attività a livello 3 per identificare eventuali comportamenti sospetti. I log dei sistemi devono essere raccolti e analizzati tramite una piattaforma SIEM, così da poter rilevare tempestivamente tentativi di intrusione o anomalie.

Infine, per limitare l'accesso alle workstations di ingegneria e ai sistemi critici, è necessario implementare un controllo degli accessi tramite autenticazione a più fattori (MFA) o RBAC, assicurando che solo utenti autorizzati possano accedere a determinati strumenti e informazioni.

Il Livello 3 è connesso al Livello 2 tramite firewall, che proteggono la comunicazione tra i sistemi di supervisione e i sistemi operativi. Questi firewall svolgono funzioni essenziali come il filtraggio avanzato, impedendo che traffico non autorizzato o dannoso possa raggiungere i sistemi di controllo industriali, e il monitoraggio e logging, che registrano tutte le attività di rete per permettere l'identificazione di potenziali minacce e attacchi in tempo reale.

Nel *Livello 2*, conosciuto come Supervisory HMI LAN o Local Supervisory, si trovano i dispositivi che supervisionano, monitorano e controllano i processi fisici, come le interfacce uomo-macchina (HMI), il software SCADA e DCS. Questo livello è dedicato alla supervisione locale e al controllo dei processi industriali, specificiamente per un singolo processo, cella linea o sistema di controllo distribuito.
Il software di controllo di supervisione e acquisizione dati (SCADA) supervisiona e controlla i processi fisici, localmente o in remoto, e aggrega i dati da inviare agli storici. I sistemi di controllo distribuiti (DCS) svolgono funzioni SCADA, ma di solito sono distribuiti localmente. Le interfacce uomo-macchina (HMI) si collegano ai DCS e ai PLC per consentire i controlli e il monitoraggio di base. Questi sistemi consentono agli operatori di monitorare e interagire con i processi in tempo reale, offrendo una visualizzazione grafica delle operazioni e un controllo diretto ai sistemi.

A questo livello si trovano anche gli Alarm Servers (gestiscono e inoltrano gli allarmi degli impianti), sistemi analitici di processo, Historians (per la raccolta dei dati di processo) e sale di controllo (centro operativo per il monitoraggio e la gestione dei processi).

I firewall di sicurezza sono utilizzati per proteggere i sistemi HMI (Human-Machine Interface) e garantire la sicurezza delle comunicazioni tra i dispositivi di controllo e i sistemi di supervisione. Questi firewall assicurano che solo il traffico autorizzato possa attraversare la rete, impedendo accessi indesiderati e proteggendo i dati sensibili.

In questo caso, vengono utilizzati switch robusti per resistere a condizioni ambientali difficili e garantire una connettività affidabile all'interno dell'ambiente industriale. Questi switch offrono una connettività stabile e sicura, essenziale per il funzionamento continuo dei sistemi di supervisione.

È fondamentale implementare confini di applicazione minori per proteggere le diverse aree delle reti industriali. In particolare, i dispositivi all'interno delle celle, linee e processi diversi devono essere isolati gli uni dagli altri per evitare un problema in un'area possa propagarsi ad altre. Ciò può essere realizzato mediante segmentazione della rete e firewall dedicati. Ai dispositivi presenti a livello 2 e inferiori deve essere garantito che l'accesso fisico sia strettamente controllato e monitorato.

Il Livello 2 comunica con il Livello 1 attraverso forti controlli di accesso e sistemi di sicurezza avanzati. Questo collegamento è cruciale per garantire che solo le comunicazioni autorizzate possano raggiungere i controllori di processo. Le principali funzionalità di sicurezza includono il controllo degli accessi e la sicurezza delle comunicazioni.

Il *Livello 1*, noto come Controller LAN, è la rete dedicata ai controllori di processo, come i PLC (Programmable Logic Controllers), processori di controllo, relè programmabili e le RTU (Remote Terminal Units). Tutti strumenti che inviano comandi ai dispostivi del livello 0. Questo livello è cruciale per la gestione operativa dei processi industriali e la raccolta dei dati dai sensori.
I PLC monitorano gli input automatizzati o umani nei processi industriali e regolano di conseguenze le uscite, mentre le RTU collegano l'hardware del livello 0 ai sistemi del livello 2.

Per garantire la sicurezza di questo livello, gli elementi di controllo locale devono essere isolati fisicamente e logicamente dagli altri livelli per prevenire attacchi che possano propagarsi attraverso la rete. Inoltre, l'utilizzo di sistemi di logging e monitoraggio per tenere traccia delle attività sui dispositivi di controllo garantisce un questi operino in modo affidabile e sicuro all'interno dell'ambiente industriale.

Il Livello 1 è collegato al Livello 0, che rappresenta la rete di strumentazione utilizzata per raccogliere dati da sensori e attuatori. Esso garantisce il funzionamento dei processi industriali e per garantire che le informazioni siano trasmesse in tempo reale ai controllori.

Il Livello 0 è la zona dei processi fisici e rappresenta il fondamento dell'architettura di automazione. I componenti di questo livello includono sensori (dispositivi che rilevano variabili fisiche, come temperatura, pressione e umidità), attuatori (dispositivi che eseguono azioni fisiche basate sui comandi ricevuti dai controllori e dispositivi di misurazione (strumenti utilizzati per monitorare e registrare dati operativi in tempo reale).

Le principali funzioni di sicurezza in questo livello includono la sicurezza fisica, per proteggere l'hardware e i cavi di rete da danni fisici e accessi non autorizzati e l'integrità

dei dati, garantendo che i dati raccolti dai sensori siano accurati e non alterati durante il loro trasferimento ai livelli superiori.

Ad oggi, molti sensori moderni comunicano direttamente con il software di monitoraggio nel cloud tramite reti cellulari. In questo caso i Secure WiFi Access Point sono essenziali per garantire un accesso wireless sicuro alla rete industriale. Questi dispositivi permettono ai vari elementi della rete, come i PLC e le RTU, di comunicare senza la necessità di cavi fisici, aumentando la flessibilità e la facilità di installazione.
I Secure WiFi Access Point sono dotati di misure di sicurezza avanzate, come crittografia dei dati e autenticazione robusta, che impediscono accessi non autorizzati alla rete. Questi sistemi proteggono le connessioni wireless, prevenendo accessi non autorizzati e garantendo la sicurezza delle comunicazioni.

L'architettura di sicurezza multilivello proposta rappresenta una risposta robusta alle sfide crescenti dell'automazione industriale moderna, grazie a una stratificazione ben definita tra i sistemi IT e OT. La segmentazione dei diversi livelli di rete, che va dalla DMZ fino al network di strumentazione, consente un isolamento efficace dei sistemi critici, contribuendo così a ridurre la superficie di attacco e a migliorare la sicurezza complessiva dell'infrastruttura.

Per rendere la sicurezza ancora più efficace, è fondamentale implementare test di simulazione, come quelli condotti dai team Red e Blue. Questi esercizi ricreano scenari di attacco in ambienti reali, permettendo al team di sicurezza di prepararsi adeguatamente e di affinare le proprie capacità di risposta in caso di emergenze.

Tutte le comunicazioni tra i Livelli 3 e superiori devono essere criptate utilizzando standard robusti, come TLS 1.3 o VPN IPsec, per garantire la protezione dei dati in transito. L'adozione della crittografia end-to-end assicura che le informazioni siano al riparo da intercettazioni o alterazioni, specialmente per le connessioni remote. Nel caso in cui vengano utilizzati punti di accesso Wi-Fi, come nel caso di PLC/RTU collegati in modalità wireless, è cruciale adottare protocolli di sicurezza avanzati, come WPA3 e crittografia AES-256, oltre a segmentare il traffico wireless mediante l'uso di VPN.

Inoltre, ogni livello del modello deve disporre di un piano di risposta dedicato, contenente procedure specifiche per la gestione delle violazioni di sicurezza sia nei sistemi OT che in quelli IT. Tali piani devono affrontare scenari specifici, come attacchi ransomware a SCADA, compromissioni di PLC e tentativi di movimenti laterali tra le reti IT e OT. È altrettanto importante mantenere aggiornati e testati i dati critici relativi ai processi operativi e i backup dei dispositivi industriali. L'implementazione di sistemi di failover e strategie di ripristino rapido è fondamentale per minimizzare i tempi di inattività e garantire la continuità operativa.

Questo approccio assicura che ogni livello della rete abbia un ruolo specifico nella difesa dell'infrastruttura industriale, migliorando sia la sicurezza che la resilienza operativa. Il valore di un sistema di sicurezza personalizzato risiede nella sua capacità di adattarsi alle esigenze particolari di ciascun ambiente industriale, senza compromettere l'efficienza dei processi e la continuità operativa. Così, l'architettura di sicurezza proposta non solo protegge, ma sostiene anche la funzionalità e l'affidabilità delle operazioni industriali a lungo termine, contribuendo a un ambiente operativo più sicuro e resiliente.

Best practices

In un contesto in cui le minacce informatiche sono in continua evoluzione, adottare un approccio strutturato e affidabile diventa essenziale per garantire la continuità operativa delle infrastrutture critiche e industriali. La protezione di sistemi OT (Operational Technology) e CPS (Cyber-Physical Systems) richiede una strategia che non solo prevenga gli attacchi informatici, ma che riduca anche il rischio di gravi ripercussioni nel mondo fisico. Per rafforzare la postura di sicurezza all'interno delle organizzazioni e mitigare i potenziali impatti di un incidente digitale sui processi operativi, è fondamentale seguire un insieme di linee guida che contribuiscano a una difesa multilivello. Queste pratiche sono pensate per migliorare la protezione delle infrastrutture critiche, garantendo che i sistemi OT e CPS siano adeguatamente protetti contro le minacce e i rischi associati.

Definire ruoli e responsabilità
Per garantire un'efficace gestione della sicurezza, è cruciale avere una chiara definizione dei ruoli. Ogni struttura organizzativa deve designare un responsabile della sicurezza OT, il quale avrà il compito di attribuire e documentare i ruoli e le responsabilità di sicurezza per tutti i dipendenti, i dirigenti e le terze parti coinvolte.

Assicurare formazione e consapevolezza appropriate
È fondamentale che tutto il personale OT sia adeguatamente formato e consapevole dei rischi legati alla sicurezza. Ogni membro del team deve essere preparato a riconoscere i pericoli di sicurezza, le modalità di attacco più frequenti e le azioni da intraprendere in caso di incidenti. In particolare, è essenziale che i dipendenti imparino a identificare tentativi di phishing e altre forme di ingegneria sociale, che sono spesso utilizzati per penetrare i sistemi OT.

Implementare e testare la risposta agli incidenti
Ogni unità deve avere un piano di gestione degli incidenti di sicurezza OT che comprenda quattro fasi principali: preparazione, rilevamento e analisi, contenimento e recupero, e follow-up post-incidente. È consigliabile effettuare test di penetrazione regolari e coinvolgere team Red e Blue per simulare attacchi reali e testare la resilienza dei sistemi OT.

Backup, ripristino e recupero di emergenza
Devono essere messe in atto procedure dettagliate per il backup e il ripristino in caso di emergenze. È essenziale disporre di un sistema di backup con diversi livelli (locale, impianto e disaster recovery) e testare regolarmente le capacità di ripristino per assicurare la disponibilità dei dati e dei file critici. Ad esempio, devono essere previste fonti di energia alternative per gestire interruzioni prolungate e proteggere i sistemi di monitoraggio e controllo dell'energia da minacce informatiche.
Per evitare che eventi fisici come incendi compromettano i backup, è importante conservare i supporti di backup in luoghi separati dai sistemi di produzione. Inoltre, i backup devono essere protetti da accessi non autorizzati e, in caso di grave incidente, deve essere possibile ripristinare i dati su nuovi sistemi o ambienti virtuali.

Gestione dei supporti portatili
È necessario stabilire regole chiare per la gestione dei dispositivi di archiviazione portatili, come chiavette USB e laptop. Questi dispositivi devono essere scansionati per verificare la presenza di malware, sia che appartengano a dipendenti interni che a terze parti, come subappaltatori o fornitori. Solo i dispositivi verificati come privi di minacce possono essere collegati ai sistemi OT.

Mantenere un inventario aggiornato degli asset
Per garantire una solida sicurezza delle Tecnologie Operative (OT), è fondamentale mantenere un inventario dettagliato e aggiornato di tutti gli asset OT, comprendente dispositivi, software e sistemi collegati alla rete. Una valutazione completa delle vulnerabilità deve essere condotta per identificare debolezze e potenziali punti di accesso per attaccanti, analizzando hardware, software e configurazioni di rete. Parallelamente, è essenziale effettuare un'analisi dei rischi per valutare le minacce e le conseguenze di una possibile violazione della sicurezza, considerando l'impatto sulle operazioni e le potenziali ripercussioni

Segmentazione di rete
Le reti OT devono essere isolate da altre reti, sia interne che esterne, mediante misure fisiche o logiche. È essenziale segmentare la rete per creare zone distinte, isolando i sistemi critici da quelli meno critici e prevenendo il movimento laterale degli attaccanti

Il traffico tra i sistemi OT e le altre reti deve passare attraverso un gateway sicuro, come una zona demilitarizzata (DMZ), e le interazioni con i sistemi OT devono essere protette da autenticazione multi-fattore. È fondamentale controllare l'accesso ai sistemi OT implementando meccanismi di autenticazione robusti e controlli di accesso basati sui ruoli, per limitare i privilegi degli utenti in base alle loro responsabilità.

Raccolta dei log e rilevamento in tempo reale
È fondamentale implementare procedure per la registrazione automatica e la revisione degli eventi di sicurezza, con chiari tempi di conservazione per i log e misure per prevenire manipolazioni non autorizzate. Il monitoraggio continuo deve includere l'uso di sistemi di rilevamento delle intrusioni (IDS) per identificare attività sospette in tempo reale, algoritmi di rilevamento delle anomalie per individuare deviazioni dal comportamento normale e un sistema di gestione delle informazioni e degli eventi di sicurezza (SIEM) per aggregare e analizzare i dati da diverse fonti.

Implementare un processo di configurazione sicura
È essenziale sviluppare e applicare configurazioni sicure per tutti i sistemi pertinenti, inclusi endpoint, server e dispositivi di rete. Il software di sicurezza, come antivirus e antimalware, deve essere installato e operativo su tutti i componenti dell'ambiente OT che lo richiedono.

Processo formale di patching
Deve essere implementato un processo sistematico per validare le patch fornite dai produttori prima della loro applicazione. Questo processo dovrebbe includere una fase preliminare di valutazione, durante la quale ogni patch fornita dai produttori viene attentamente esaminata e testata in ambienti controllati per verificarne la compatibilità e l'impatto sui sistemi operativi. Una volta qualificate, le patch devono essere distribuite in modo sistematico, seguendo una cadenza regolare pianificata in base alle esigenze operative dell'organizzazione. È importante che l'applicazione delle patch avvenga in finestre di manutenzione specifiche.

Considerazioni Aggiuntive per l'Architettura di Sicurezza

Nella progettazione e implementazione dell'architettura di sicurezza per ambienti OTle organizzazioni devono considerare anche altri aspetti cruciali, tra cui la disponibilità, la distribuzione geografica dei sistemi, le considerazioni ambientali e i requisiti normativi:

Sistemi Distribuiti Geograficamente: le infrastrutture critiche sono spesso distribuite su più siti, e quindi è fondamentale proteggere i siti remoti e garantire che possano comunicare informazioni di sicurezza in modo sicuro. Le comunicazioni tra siti devono essere criptate e autenticate end-to-end, indipendentemente dalla connessione utilizzata (link punto a punto, satellite, internet). È essenziale assicurare una banda adeguata al trasferimento dei dati di monitoraggio della sicurezza.

*Requisiti Normativi: l*e organizzazioni che operano in settori regolamentati devono rispettare requisiti normativi specifici nella progettazione della loro architettura di sicurezza. Ad esempio, gli standard NERC CIP per i sistemi elettrici forniscono linee guida dettagliate per garantire la conformità e proteggere le operazioni.
Considerazioni Ambientali: è importante effettuare un'analisi dei rischi ambientali per identificare potenziali pericoli legati ai processi e alle attrezzature. Qualora si rilevino rischi ambientali dovuti a fallimenti informatici, devono essere adottate misure architetturali per prevenirli e mitigarli.
Sicurezza del Field I/O (Livello 0 del Purdue): i dispositivi e i protocolli al livello Field I/O spesso non offrono meccanismi di autenticazione, esponendoli a rischi di inserimento o modifica non autorizzata dei dati. È necessario implementare controlli di sicurezza, come reti di monitoraggio separate o "digital twins", per rilevare e correggere dati errati o compromessi.
Considerazioni Aggiuntive per IIoT: l'integrazione dell'IIoT negli ambienti OT aumenta la connettività e le interazioni con i sistemi aziendali e basati su cloud, richiedendo adattamenti nell'architettura di sicurezza. È fondamentale valutare i flussi di dati dell'IIoT e le comunicazioni esterne per determinare se siano necessari ulteriori meccanismi di controllo accessi e considerare i vettori di attacco specifici per questi dispositivi.

Conclusioni e Prospettive Future

Principali Conclusioni

Nel 2023, il panorama della cybersecurity ha subito sviluppi significativi che hanno influenzato diverse industrie a livello globale, evidenziando la costante evoluzione e complessità delle minacce e delle soluzioni nel campo della sicurezza informatica.

Un elemento chiave dell'evoluzione del 2023 è stato l'aumento dell'adozione delle architetture Zero Trust, che sostituiscono il tradizionale approccio del "fidati ma verifica" con il principio "non fidarti mai, verifica sempre". Modelli di sicurezza Zero Trust, supportati da enti come il NIST, la CISA e il Dipartimento della Difesa statunitense, richiedono la verifica rigorosa dell'identità di ogni utente o dispositivo che tenta di accedere alle risorse di rete. Questo approccio, che enfatizza la micro-segmentazione e l'autenticazione robusta, ha guadagnato popolarità grazie alla sua capacità di mitigare minacce interne e violazioni dei dati. L'adozione di Zero Trust è particolarmente importante per proteggere asset critici, inclusi gli endpoint, con una verifica continua della loro sicurezza.

Parallelamente, nel 2023 l'Intelligenza Artificiale e l'automazione sono diventate componenti essenziali per la difesa informatica. Sistemi basati su AI e machine learning sono stati adottati per identificare, prevedere e rispondere alle minacce in tempo reale, migliorando notevolmente l'efficienza operativa e riducendo i tempi di risposta agli incidenti. L'automazione ha permesso di colmare il divario di competenze nel settore della cybersecurity, riducendo il carico di lavoro manuale associato alla gestione delle minacce e abbattendo i costi legati alla sicurezza. La capacità di risposta automatizzata agli attacchi e l'uso di analisi predittive hanno rafforzato le difese informatiche, rendendo le organizzazioni più resilienti.

L'espansione del lavoro remoto ha continuato a rappresentare una sfida significativa per la sicurezza nel 2023. La fusione tra gli ambienti personali e professionali ha incrementato il rischio di violazioni, spingendo le organizzazioni a rafforzare la sicurezza degli accessi remoti, delle VPN e delle soluzioni basate sul cloud. I team di cybersecurity hanno inoltre intensificato l'educazione dei dipendenti per contrastare le minacce derivanti dalle

configurazioni domestiche, come gli attacchi di forza bruta sui router WiFi, che sono diventati vettori comuni per ransomware.
Il ransomware stesso è diventato più sofisticato nel 2023, con attacchi mirati a grandi organizzazioni e infrastrutture critiche attraverso tecniche come la doppia estorsione, che comporta sia la criptazione dei dati che la minaccia di rendere pubblici i dati sottratti. In risposta, le aziende hanno adottato soluzioni di backup più avanzate e protocolli di sicurezza migliorati, collaborando sempre di più con le autorità governative per contrastare questa crescente minaccia. La rapida remediation delle vulnerabilità si è dimostrata essenziale per prevenire movimenti laterali all'interno delle reti e scongiurare attacchi devastanti.
Un ulteriore trend del 2023 è stata la crescente enfasi sulla conformità regolamentare e la protezione della privacy. Con l'entrata in vigore di nuove leggi sulla protezione dei dati, come il GDPR e il CCPA, le organizzazioni hanno investito significativamente per garantire la conformità a queste normative. Le strategie di sicurezza ora includono l'adozione di framework "privacy-by-design" e un miglioramento delle pratiche di governance dei dati. Le aziende si sono concentrate sulla protezione delle informazioni di identificazione personale (PII) e sulla creazione di report personalizzati per soddisfare i requisiti degli auditor, rafforzando la loro capacità di scoprire e mitigare le minacce alla privacy.

Prospettive Future

Guardando avanti, il panorama della cybersecurity è destinato a evolvere ulteriormente con l'introduzione di nuove tecnologie e strategie di sicurezza informatica.
Piu di tutti, l'Intelligenza Artificiale continuerà a rivoluzionare la cybersecurity attraverso modelli predittivi più avanzati e meccanismi di risposta automatizzati. Algoritmi AI sofisticati saranno capaci di prevedere e neutralizzare le minacce prima che si materializzino, rendendo i sistemi più proattivi piuttosto che reattivi. L'affidamento crescente su modelli di machine learning migliorerà la capacità di rilevare pattern anomali e comportamenti sospetti, consentendo interventi tempestivi e mirati.

Tradizionalmente, i leader della sicurezza si sono concentrati sul superare gli attaccanti. Tuttavia, con la digitalizzazione massiccia delle operazioni aziendali, è necessario un

cambio di paradigma verso la riduzione del rischio aziendale come mezzo per superare la concorrenza. Ciò implica adottare un approccio ponderato in cui le azioni intraprese per migliorare la sicurezza devono essere bilanciate con gli obiettivi di business e l'impatto operativo, garantendo che le misure di sicurezza supportino e non ostacolino le attività aziendali critiche.

Con l'evoluzione delle minacce informatiche, le regolamentazioni diventeranno sempre più stringenti e complesse. La privacy dei dati e la conformità assumeranno un ruolo centrale, con requisiti regolatori più severi attraverso diverse regioni e industrie. Le organizzazioni dovranno intensificare il focus sulla conformità come aspetto fondamentale delle loro strategie di cybersecurity, implementando sistemi e processi che garantiscano l'aderenza alle norme e la protezione efficace delle informazioni sensibili.

La proliferazione dei dispositivi Internet of Things (IoT) introdurrà nuove vulnerabilità ed espanderà la superficie di attacco disponibile per i criminali informatici. Si prevede un aumento degli attacchi iniziati attraverso dispositivi connessi, richiedendo protocolli di sicurezza più robusti e specifici per l'IoT. Le organizzazioni dovranno implementare strategie di sicurezza che considerino l'intero ecosistema IoT, inclusi monitoraggio continuo, autenticazione forte e aggiornamenti regolari dei dispositivi.

La mitigazione proattiva del debito tecnologico riguarda la gestione dei rischi associati all'uso di hardware, software e sistemi operativi che hanno raggiunto la fine del loro ciclo di vita (End-of-Life, EoL) o non ricevono più supporto (End-of-Support, EoS). Questi sistemi, quando non più aggiornati o supportati dai produttori, diventano vulnerabili a minacce di sicurezza poiché non ricevono più patch di sicurezza o aggiornamenti critici, aumentando il rischio di attacchi informatici. Tuttavia, eliminare completamente l'uso di tecnologie EoL o EoS è spesso irrealistico, soprattutto per organizzazioni con infrastrutture complesse. Per affrontare questa sfida, i responsabili della sicurezza, come i CISO (Chief Information Security Officer), devono avere una visione chiara e unificata del debito tecnologico imminente, cioè una mappa dei sistemi che stanno raggiungendo o hanno già raggiunto lo stato di EoL o EoS. Questa visione dovrebbe essere priorizzata

in base al rischio che ogni elemento obsoleto rappresenta per l'azienda, valutando l'impatto che una potenziale vulnerabilità potrebbe avere sulle operazioni.

La sicurezza del cloud rimarrà una linea di difesa vitale, data la crescente adozione di servizi cloud e l'aumento delle violazioni in questi ambienti. Nel 2023, oltre l'80% delle violazioni analizzate nel Cost of a Data Breach Report di IBM ha coinvolto dati memorizzati in ambienti cloud pubblici o privati, con quasi il 40% degli attacchi che hanno interessato più ambienti contemporaneamente, comportando costi medi per violazione di 4,75 milioni di dollari. Secondo le previsioni di Gartner, la spesa per la sicurezza del cloud e la privacy dei dati registrerà tassi di crescita superiori al 24% nel 2024. (IBM, 2024)
Per affrontare efficacemente le sfide della sicurezza in questi ambienti, sarà essenziale investire nella formazione specifica sul Cloud, garantendo che i team di sicurezza siano adeguatamente formati sulle tecnologie cloud per prevenire errori di configurazione, una delle principali cause di violazioni dei dati nel cloud.

Altrettanto importante, è l'integrazione della sicurezza nel ciclo di vita dello sviluppo del software (SDLC), che vede la necessità di coinvolgere sviluppatori e ingegneri per affrontare proattivamente le vulnerabilità e ridurre la necessità di rielaborazioni costose. Allo stesso modo, Modelli Zero Trust Data-Centric, ovvero architetture di sicurezza che utilizzano la micro-segmentazione e monitorino continuamente attività anomale, sono necessarie per contenere potenziali violazioni.

Il 2024 rappresenta un punto di svolta per la cybersecurity, con sfide e opportunità che richiedono un approccio strategico e integrato alla sicurezza informatica. L'evoluzione delle minacce, l'adozione di nuove tecnologie come l'AI generativa, la diffusione dell'IoT e la crescente complessità del panorama normativo impongono alle organizzazioni di essere proattive, resilienti e adattabili.
Investire nelle migliori pratiche di sicurezza, adottare tecnologie avanzate, promuovere una cultura della sicurezza attraverso formazione continua e collaborare efficacemente tra diverse funzioni aziendali saranno elementi chiave per costruire difese solide contro le minacce informatiche in continua evoluzione. Solo attraverso un impegno costante e

una vigilanza attiva le organizzazioni potranno navigare con successo il complesso e dinamico panorama della cybersecurity, garantendo la protezione dei propri asset digitali e sostenendo la continuità operativa in un mondo sempre più interconnesso.

Bibliografia

(CS)AI - KPMG. (2022). *https://assets.kpmg.com/content/dam/kpmgsites/ch/pdf/cs2ai-kpmg-cscs-report-2024.pdf.* From KPMG: https://assets.kpmg.com/content/dam/kpmgsites/ch/pdf/cs2ai-kpmg-cscs-report-2024.pdf

ABS Group. (n.d.). *Infographic: Managing the Risks of Integrating IT and OT Systems.* From ABS Group: https://www.abs-group.com/Knowledge-Center/Insights/Infographic-Managing-the-Risks-of-Integrating-IT-and-OT-Systems/

Adel Alqudhaibi, M. A. (2024). *Securing industry 4.0: Assessing cybersecurity challenges and proposing strategies for manufacturing management.* From https://www.sciencedirect.com/science/article/pii/S277291842400033X?ref=pdf_download&fr=RR-2&rr=8ba4a9b85c754c4c

Agbeleye, O. (2023). *What Is Cybersecurity? A Complete Overview Guide*. From Springboard: https://www.springboard.com/blog/cybersecurity/what-is-cybersecurity/

Aggarwal, S. (2023, Agosto). *3 Levers That Manufacturing CIOs Must Pull to Improve and Sustain Data Quality.* From Gartner: https://emt.gartnerweb.com/ngw/globalassets/en/doc/documents/789057-3-levers-that-manufacturing-cios-must-pull-to-improve-and-sustain-data-quality.pdf

Baker, K. (2024). *Most Common Types of Cyberattacks*. From Crowd Strike: https://www.crowdstrike.com/en-us/cybersecurity-101/cyberattacks/common-cyberattacks/

BCG. (2023). *Industry 4.0.* From BCG: https://www.bcg.com/capabilities/manufacturing/industry-4.0#collapsible-00000175-659a-d2c0-ad7d-e79eb10d0002-0

Bisht, R. (2024, Febbraio). *Top OT Security Threats*. From Infosectrain: https://www.infosectrain.com/blog/top-ot-security-threats/

Capgemini. (2022). *SMART & SECURE: WHY SMART FACTORIES NEED* . From Capgemini: https://prod.ucwe.capgemini.com/wp-content/uploads/2022/06/Cybersecurity-in-Smart-Factories_Web-2.pdf

Clim, A. (2022). *The Need for Cybersecurity in Industrial Revolution and Smart Cities.* From MDPI: https://www.mdpi.com/1424-8220/23/1/120

Cybel Angel. (2024). *Biggest Cyber Attacks*. From Cybel Angel : https://cybelangel.com/the-biggest-cyber-attacks-in-the-manufacturing-industry/

Cyberdefense. (2024). *Security Navigator.* From Cyberdefense.

Dragos. (2024, Febbraio). *OT CYBERSECURITY.* From Dragos: https://hub.dragos.com/hubfs/312-Year-in-Review/2023/Dragos-2023-Year-in-Review-Full-Report.pdf?hsLang=en

Forbes. (2024, Giugno). *Why Your Organization Should Focus More On OT Cybersecurity*. From Forbes: https://www.forbes.com/councils/forbestechcouncil/2024/06/06/why-your-organization-should-focus-more-on-ot-cybersecurity/

Fortinet. (2024). *2024 State of Operational Technology and Cybersecurity.* From Fortinet: https://www.fortinet.com/resources/reports/state-of-ot-cybersecurity

Gartner. (2024). *Cyberthreats*. From Gartner: https://www.ibm.com/think/topics/cyberthreats-types

Gartner. (n.d.). *3 Levers That Manufacturing CIOs Must Pull to Improve and Sustain Data Quality.* From Gartner: 3 Levers That Manufacturing CIOs Must Pull to Improve and Sustain Data Quality

IBM. (2024). *Cost of Data Breach.* From IBM: https://www.ibm.com/downloads/cas/1KZ3XE9D

IBM. (2024). *Cyberthreats*. From IBM: https://www.ibm.com/think/topics/cyberthreats-types

IBM X-Force. (2024). *IBM X-Force Threat Intelligence Index 2024.* From IBM: https://www.ibm.com/downloads/cas/L0GKXDWJ

IDC. (2024). *Global Digital Transformation Market.* From Data Bridge : https://www.databridgemarketresearch.com/reports/global-digital-transformation-market#:~:text=Digital%20Transformation%20Market%20Analysis%20and%20Size&text=The%20global%20digital%20transformation%20market,period%20of%202024%20to%202031

IDC. (n.d.). *Guida all'IoT Security: sfide e soluzioni.* From IDC: https://www.checkpoint.com/it/solutions/iot-security/

INCIT. (2024, Aprile). *Safeguarding data in the age of smart manufacturing.* From International Centre for Industrial Transformation: https://incit.org/en/thought-leadership/safeguarding-data-in-the-age-of-smart-manufacturing/

Industry 4.0 Market Size, Share & Industry Growth Analysis Report. (2021). From MarketsandMarkets: https://www.marketsandmarkets.com/Market-Reports/industry-4-market-102536746.html

Janusz Pochmara, A. S. (2024). *Cybersecurity of Industrial Systems Report.* From MDPI: https://www.mdpi.com/2079-9292/13/7/1191

Lareina Yee, M. C. (2024, Luglio). *McKinsey Technology Trends Outlook 2024*. From McKinsey Digital: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech#new-and-notable

Lawson, D. (2023, Ottobre). *The Growing Accessibility Of Smart Manufacturing For SMEs.* From Forbes: https://www.forbes.com/councils/forbestechcouncil/2023/10/12/the-growing-accessibility-of-smart-manufacturing-for-smes/

Market.us. (2024). *Global Smart Manufacturing Market By Component.* From Market.us: Straits Research

McKinsey Technology Trends Outlook 2024. (2024). From McKinsey: https://www.mckinsey.com/capabilities/mckinsey-digital/our-insights/the-top-trends-in-tech#tech-trends-2024

Micheal M. Amiri, M. M. (2024). *THE STATE OF OT SECURITY:.* From PaloAlto: https://www.paloaltonetworks.com/content/dam/pan/en_US/assets/pdf/reports/state-of-ot-security-report-2024.pdf

Moore, S. (2021). *Gartner Predictions*. From Gartner: https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we

NIST. (2023, Settembre). *Guide to Industrial Control* . From NIST: https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.800-82r2.pdf

NIST. (2024, Febbraio). *The NIST Cybersecurity* . From NIST: https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.29.pdf

OT Security. (2023). From PaloAlto: https://www.paloaltonetworks.in/cyberpedia/what-is-ot-security

Pochmara, J. (2023). *Cybersecurity of Industrial Systems*. From MDPI: https://www.mdpi.com/2079-9292/13/7/1191

Rebultan, M. A. (2023, Aprile). *Introduction to ICS/OT Systems and their Role in Critical Infrastructure.* From ISACA: https://www.isaca.org/resources/news-and-trends/isaca-now-blog/2023/introduction-to-ics-ot-systems-and-their-role-in-critical-infrastructure

Rockwell Automation. (2024). *State of Smart Manufacturing Report 2024.* From Rockwell Automation: https://www.rockwellautomation.com/content/dam/rockwell-automation/documents/pdf/campaigns/state-of-smart-2024/9th-annual-state-of-smart-manufacturing-report-en.pdf

Sean Peasley, R. H. (2020). *Cybersecurity for smart factories - Tools for managing cyber threats to manufacturing.* From Deloitte: https://www2.deloitte.com/us/en/pages/energy-and-resources/articles/smart-factory-cybersecurity-manufacturing-industry.html

SentinelOne. (2023, Settembre). *Risks Within The Factory Lines.* From SentinelOne: https://www.sentinelone.com/blog/risks-within-the-factory-lines-examining-top-threats-facing-the-manufacturing-industry/

Smart Manufacturing Market Size, Share & Industry Analysis, By Component Source: https://www.fortunebusinessinsights.com/smart-manufacturing-market-103594. (2023). From Fortune Business Insight: https://www.fortunebusinessinsights.com/smart-manufacturing-market-103594

SNS Insider. (2024, Giugno). *Smart Manufacturing Market Size.* From GlobNewswire: https://www.globenewswire.com/news-release/2024/07/24/2918283/0/en/Smart-Manufacturing-Market-Size-to-Reach-US-880-42-Billion-by-2032-Rising-Demand-for-Automation-to-Minimize-Human-Error-Optimize-Resource-Fuels-Growth-Research-by-SNS-Insider.html

Straits Research. (2023, Maggio). *Smart Manufacturing Market Size, Share & Trends Analysis.* From Straits Research: https://straitsresearch.com/report/smart-manufacturing-market

Toth, P. (2022). *A Critical Component of Industry 4.0 Implementation*. From NIST: Cybersecurity – A Critical Component of Industry 4.0 Implementation

Toth, P. (2022). *Cybersecurity – A Critical Component of Industry 4.0 Implementation*. From NIST: https://www.nist.gov/blogs/manufacturing-innovation-blog/cybersecurity-critical-component-industry-40-implementation

Types of cybersecurity. (2023). From SailPoint: https://www.sailpoint.com/identity-library/five-types-of-cybersecurity