SAFE NETWORK

Sicurezza Informatica nel Mondo OT/IoT

Strategie e Tecnologie di sicurezza informatica nel settore Marittimo-Portuale-Logistico

Introduzione

Trasformazione Digitale

Il settore dei trasporti e della logistica sta vivendo una trasformazione aziendale per migliorare i processi tramite l'implementazione di tecnologie come l'Internet of Things (IoT), la tecnologia operativa (OT), i big data, il 5G e l'intelligenza artificiale (IA). Questo sta portando a una modernizzazione delle infrastrutture e dei sistemi per affrontare la crescente domanda di trasporti globali.

Rischi nei Sistemi OT/IoT

L'obiettivo principale della modernizzazione e della trasformazione digitale è migliorare l'operatività, l'utilizzo delle risorse e la produttività dei dipendenti. Tuttavia, l'implementazione di queste tecnologie richiede soluzioni di sicurezza informatica efficaci per proteggere le reti e ridurre il rischio di violazioni dei dati.

Obiettivi della Modernizzazione

L'aumento dell'interconnessione tra persone e sistemi di bordo con il cloud sta aumentando il rischio per la sicurezza informatica, evidenziando la necessità di affrontare le vulnerabilità e proteggere l'ambiente OT/IoT dalle minacce esistenti.

Quali sono le cause dell’aumento dei rischi di attacco nell’ambito OT?

Questi sforzi di digitalizzazione collegano persone e sistemi di bordo al cloud, aumentando il rischio per la sicurezza informatica.

Questo è sicuramente uno dei temi più caldi in questo momento. Infatti, negli ultimi anni, abbiamo assistito ad un aumento significativo di attacchi nei sistemi di produzione, nell'ambito dell'Operational Technology (OT).

Questo fenomeno è stato alimentato dalla progressiva eliminazione della separazione fisica tra strumenti di produzione e sistemi informatici tradizionali (IT). Oggi, infatti, i dispositivi OT sono sempre più connessi e integrati con le reti IT principali.

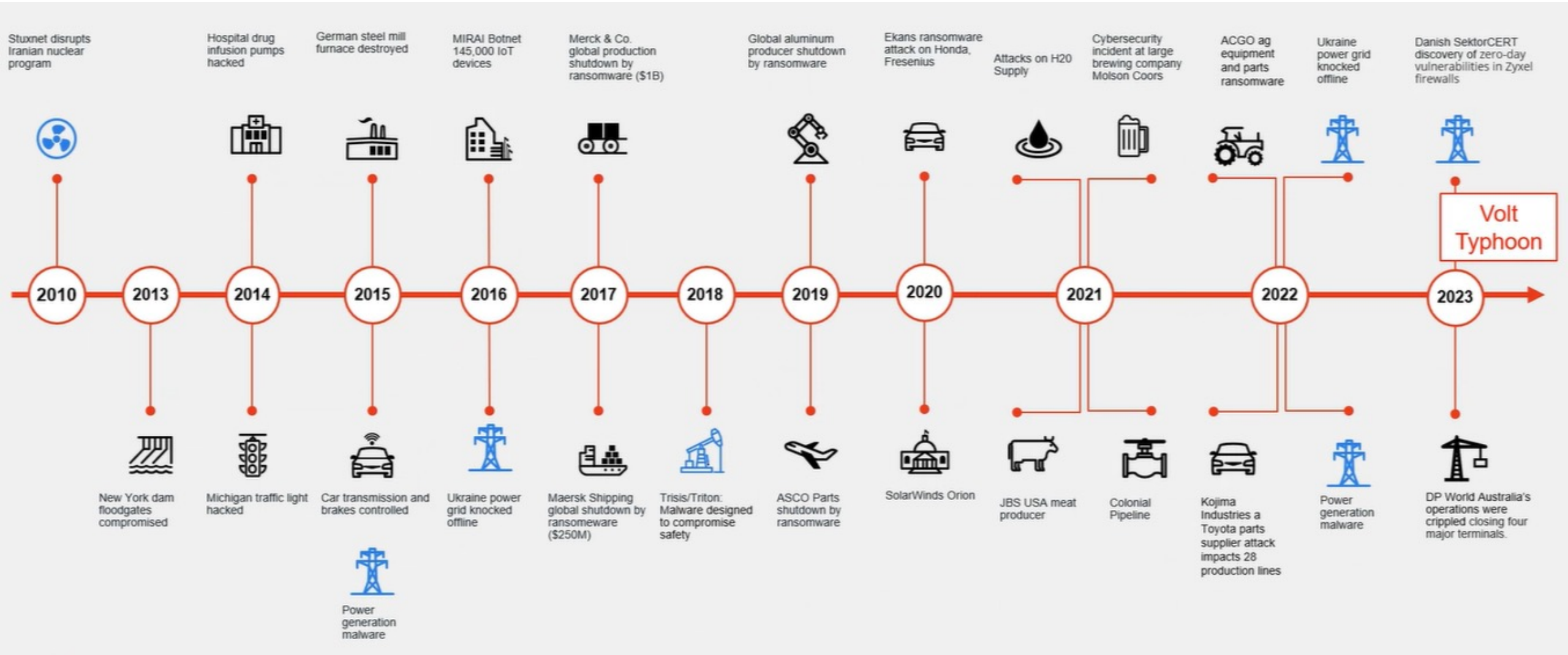
Da qui nasce il bisogno di rendere più sicura questa tecnologia all’interno della rete.

Questo aumeto delle superfici di attacco ha creato vulnerabilità e ha messo a rischio la continuità operativa e la sicurezza dei dati sensibili

Pertanto, è fondamentale esplorare strategie e tecnologie efficaci per affrontare questa crescente minaccia e proteggere l'ambiente OT dalle potenziali vulnerabilità.

Rischi e Impatti nelle Infrastrutture OT

Gli attacchi alle infrastrutture OT



SAFE NETWORK

NEXT

Il caso MAERSK SHIPPING

Le intrusioni nei sistemi di produzione rappresentano una delle principali minacce per le aziende che operano nell'ambito OT. Questi attacchi possono causare interruzioni della produzione, danni agli impianti e perdite finanziarie significative.

Maersk Shipping

L'attacco informatico alla compagnia Maersk Shipping ha causato **danni economici stimati in oltre 250 milioni di dollari.** Tale attacco ha provocato enormi interruzioni e blocchi dei terminal portuali di tutto il mondo, influendo sulla catena di fornitura a livello globale.

Ovviamente oltre all'enorme perdita finanziaria, **l'attacco ha creato enormi interruzioni e blocchi dei terminal portuali di tutto il mondo**, bloccando i sistemi di gestione dei container, che coordinavano funzioni vitali per il corretto svolgimento operativo. Ha interrotto la catena di fornitura interrompendo il flusso delle merci e causando ritardi e interruzioni a livello mondiale.

Persino alcuni **sistemi di navigazione e gestione delle navi sono stati colpiti**, causando ritardi, interruzioni di supporto e compromettendo la capacità della compagnia di coordinare le rotte sulle navi.

Rischi per la Sicurezza Vitale

Un attacco ai sistemi OT, può rivelarsi pericoloso anche per la sicurezza umana. La compromissione di sistemi critici a bordo e non che gestiscono operazioni fisiche, logistiche e di sicurezza possono creare incidenti che potrebbero diventare catastrofici.

Incidenti di Gru e Carrelli Elevatori

Il compromettere i sistemi che controllano gru e carrelli elevatori può causare incidenti che coinvolgono il sollevamento e trasporto di container pesanti, mettendo a rischio la vita degli operatori.

Controllo sostanze pericolose

Gli attacchi ai sistemi di controllo delle sostanze pericolose possono causare rilasci accidentali di sostanze chimiche o biologiche pericolose, mettendo a rischio la salute e la sicurezza del personale e della popolazione circostante.

Principali Criticità

Il ciclo di vita dei componenti tecnologici installati nel mondo OT

è molto più lungo rispetto ai rispettivi dispositivi presenti nei sistemi IT, per diverse motivazioni. La sostituzione di questi componenti comporta tempistiche, costi e processi differenti, basti pensare ad un fermo nave. Ovviamente diverso da un aggiornamento tecnologico o sostituzione di un apparato all'interno di un datacenter aziendale.

Le nuove tecnologie che vengono installate nel mondo OT,

spesso vengono poste accanto a sistemi che per loro natura sono obsoleti, oppure non cyber resilienti. perchè molto probabilmente al tempo in cui sono state installati, non sono stati progettati per questo scopo. anche se a livello funzionale svolgono quello che devono fare

Inoltre, con l'avvento di Internet, i sistemi che erano precedentemente isolati, adesso possono essere esposti alle reti Globali.

Nell'industria 4.0, tutte le risorse comunicano continuamente dati a un datacenter centrale, creando uno scambio costante di informazioni che, sebbene ottimizzi il processo centrale, comporta anche un incremento significativo della superficie di attacco.

Tutto ciò comporta un aumento di rischio alle minacce cyber.

Elementi Chiave per la Riduzione del Rischio

A questo proposito esistono processi ed elementi chiave per la riduzione del rischio. **Il lavoro svolto in precedenza in termini di sicurezza informatica, non va gettato via, ma adattato facendo tesoro delle analisi effettuate per valutare i rischi cyber e le vulnerabilità presenti.**

L'ottica e l'obiettivo devono essere quelli del miglioramento continuo. Un continuo aggiornamento delle strategie e dei sistemi.

È risaputo che le minacce informatiche evolvono e cambiano **molto più velocemente** di quelle che possono essere le mitigazioni e i remediation, Per tanto questo squilibrio pone sfide importanti per le compagnie di questo settore.

Quali sono i principali elementi sui quali agire per ridurre il rischio?

Per affrontare efficacemente i rischi di sicurezza nell'ambito OT, è essenziale agire su tre fronti principali: **le persone, i processi e le tecnologie.**

1

Formazione delle Persone

La formazione delle persone è fondamentale per aumentare la consapevolezza del rischio informatico e promuovere una cultura della sicurezza all'interno dell'organizzazione. Gli operatori OT devono essere informati sui potenziali rischi e sulle migliori pratiche per proteggere i sistemi di produzione da intrusioni e violazioni della sicurezza.

2

Processi

È importante implementare processi chiari e ben definiti per gestire le minacce alla sicurezza nell'ambito OT. Questi processi devono coinvolgere l'intera catena OT e IT e fornire linee guida dettagliate su come rilevare, rispondere e mitigare le intrusioni nei sistemi di produzione.

3

Tecnologie

L'adozione di tecnologie avanzate è essenziale per proteggere l'ambiente OT da potenziali minacce. Ciò include strumenti per l'analisi del traffico che attraversa la rete OT, la protezione dei dispositivi e la gestione delle vulnerabilità.

5 Pilastri Fondamentali

Connettività sicura	Proteggere la condivisione dei dati nel mondo OT con protocolli sicuri e crittografia.
Zero trust	Verificare ogni accesso e comunicazione, garantendo l'accesso remoto solo con autenticazione sicura.
Convergenza e sistemi SOC	Integrare IT e OT per monitoraggio e gestione centralizzata da un unico Security Operations Center.
Analisi del traffico di rete	Monitorare tutte le comunicazioni che avvengo in rete in modo da rilevare tempestivamente le connessioni malevole.
AI nei servizi di sicurezza	Utilizzare l'intelligenza artificiale per migliorare la sicurezza OT, rilevando minacce e anomalie rapidamente.

Strategie e Tecnologie

Uno degli obiettivi principali di protezione è quello di proteggere il **punto di convergenza,** ovvero il punto in cui i due ambienti si incontrano e si integrano, luogo in cui si introducono nuovi punti di vulnerabilità.

La strategia per mettere in sicurezza il mondo OT e ridurre il rischio di attacco, adotta una serie di strategie e tecnologie avanzate tra cui alcuni punti fondamentali:

- **VISIBILITY**
- **CONTROL**
- **PROTECTION**

VISIBILITY

Con Visibility, si intende, la visibilità completa dei dispositivi connessi alla rete.
Questo è fondamentale per comprendere appieno il panorama della sicurezza nell'ambito OT.

Utilizzando strumenti come **FortiNAC, FortiSwitch e FortiAP, è possibile identificare in modo preciso e granulare tutti i dispositivi connessi alla rete OT e applicare controlli e protezione mirati.**

Il punto di partenza, quindi, è la visibility.

Che segue di conseguenza questo principio:
"SE NON SO COSA DEVO PROTEGGERE NON RIUSCIRO' A PROTEGGERLO NEL MODO CORRETTO"

FortiSwitch e FortiAP sono la nostra soluzione di networking per interconnettere dispositivi, che ci permettono di andare ad implementare una micro-segmentazione , ovvero la possibilità di isolare in una bolla ogni singolo oggetto che è collegato alla rete OT.

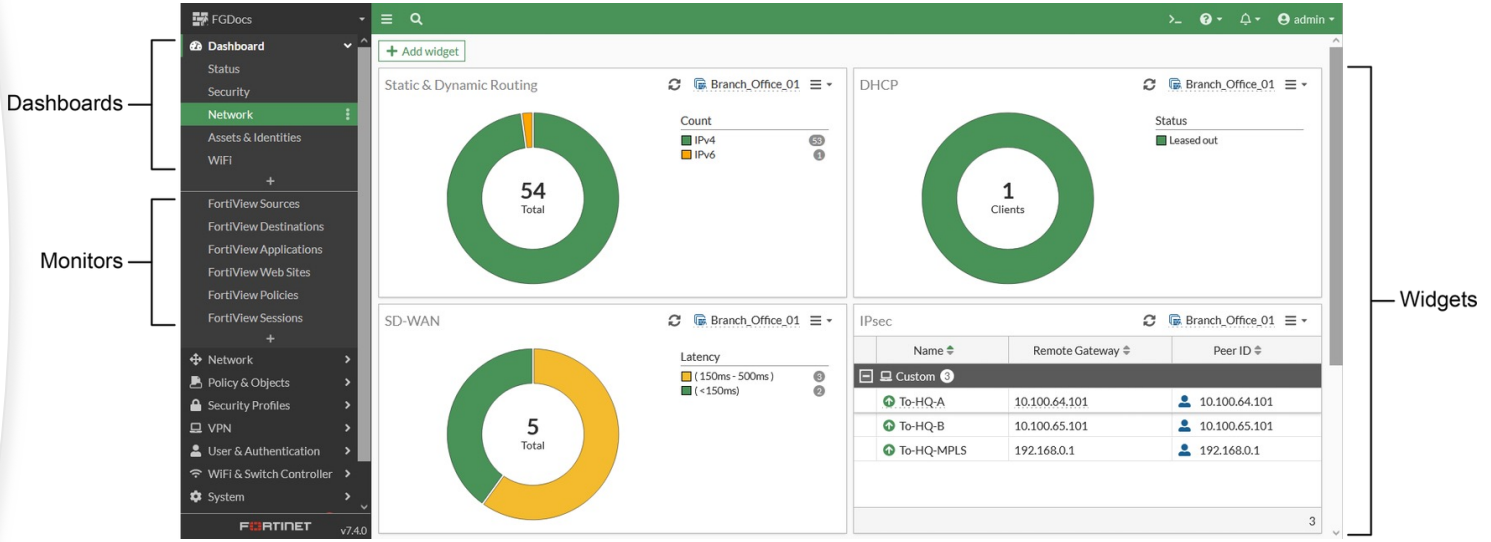
CONTROL

Dopo aver aumentato la visibility e implementato la micro-segmentazione, il passo successivo è implementare il cuore della soluzione, il **FortiGate**.

Il controllo del traffico è essenziale per garantire la sicurezza delle reti OT.

Attraverso l'utilizzo di soluzioni come FortiGate, è possibile analizzare e **controllare il traffico tra dispositivi OT e IT, bloccando potenziali minacce e proteggendo l'ambiente OT da intrusioni esterne.**

All'interno del NGFW (*Next-Generation FireWall*) del FORTIGATE, ci sono tutta una serie di funzionalità avanzate specifiche per il mondo industrial, che riconoscono tutti i protocolli che vengono utilizzati all'interno del mondo OT e **che permettono conoscendo i protocolli di poter analizzare dal punto di vista applicativo quali sono le funzionalità che vengono utilizzare da ogni singolo device andando ad applicare, la vulnerability patch,** la possibilità di eliminare rischi legati ad oggetti che nel mondo OT molte volte sono difficilmente aggiornabili per una serie di problematica di gestione.



PROTECTION

La piattaforma principale Security Fabbric, permette di far dialogare tra di loro tutti gli strumenti e le tecnologie citate, ma anche la possibilità di estendere l'ecosistema di tu56tti gli strumenti verticali che lavorano nel mondo OT per poter integrare questi strumenti nella nostra soluzione di Security.

La protezione avanzata è fondamentale per mitigare i rischi di attacco nell'ambito OT. Integrazione con strumenti come **FortiDECEPTOR e FortiSANDBOX consentono di identificare e neutralizzare le minacce in tempo reale**, proteggendo l'ambiente OT da vulnerabilità e intrusioni.
L'uso di honeypot può effettivamente aiutare a rilevare e analizzare le tecniche degli attaccanti senza compromettere i sistemi di produzione, agendo come esca per attirare gli attaccanti

4. Integrazione e Automazione
L'integrazione e l'automazione sono cruciali per massimizzare l'efficacia delle difese nell'ambito OT. Attraverso strumenti come FortiSIEM e FortiORCHESTRATOR, è possibile raccogliere e correlare gli eventi di sicurezza, nonché automatizzare le risposte agli attacchi per garantire una protezione continua e reattiva.


SAFE
NETWORK

Conclusioni

La sicurezza informatica nell'ambito OT rappresenta una sfida sempre più critica per le aziende di produzione. **Tuttavia, con l'adozione di strategie e tecnologie avanzate, è possibile ridurre significativamente il rischio di attacco e proteggere l'ambiente OT da potenziali minacce.** Investire nella formazione delle persone, implementare processi chiari e utilizzare tecnologie all'avanguardia sono fondamentali per garantire la sicurezza e la continuità operativa nell'ambito OT.

SAFE NETWORK

NEXT