WHITE PAPER

Soluzioni Fortinet per la sicurezza informatica nel settore manifatturiero

Come proteggere le risorse IT e OT dalle minacce avanzate nel settore manifatturiero attraverso un'unica piattaforma

Sintesi preliminare

Le organizzazioni del settore manifatturiero gestiscono attrezzature costose e sofisticate nei loro stabilimenti, e i sistemi che fanno funzionare i macchinari sono sempre più connessi a Internet. Le implicazioni di questa tendenza in termini di sicurezza sono significative, comprese le possibili minacce alla sicurezza fisica e, in alcuni casi, alla sicurezza nazionale. Le aziende si sforzano di proteggere i loro sistemi rispettando nel contempo imperativi di business come l'efficienza operativa, la continuità delle attività, l'integrità del prodotto e la compliance. Il Security Fabric di Fortinet fornisce un'architettura di sicurezza ampia, integrata e automatizzata che copre tutti gli aspetti dell'attività produttiva, dal back office all'impianto di produzione, dai sistemi isolati fisicamente dal mondo esterno a quelli connessi, dagli utenti interni ai partner esterni.

Gli exploit sono aumentati in volume e prevalenza nell'ultimo anno per quasi tutti i fornitori ICS/SCADA. [4]

La storia dell'odierno settore manifatturiero è una storia di convergenza. Le aziende che prima fabbricavano prodotti in maniera indipendente ora lavorano a stretto contatto con una rete di partner che eseguono diverse parti del processo.[1] E i sistemi elettronici che gestiscono le attività di fabbrica, storicamente a cielo aperto, sono sempre più connessi con i sistemi IT, e quindi con Internet. Di conseguenza, questi sistemi di tecnologia operativa (OT), compresi i sistemi di controllo industriale (ICS) e i sistemi di supervisione e acquisizione dati (SCADA), sono esposti a un panorama di minacce sempre più avanzate e sono obiettivi di hacker coinvolti nel terrorismo, nella guerra informatica e nello spionaggio.

Man mano che in tutto il mondo i sistemi OT sono stati connessi fisicamente alla rete, sono sempre più bersagliati sia da attacchi riciclati basati sull'IT che da exploit OT costruiti appositamente.[2] Un sondaggio rileva che il 74% dei tecnici OT ha subito una violazione negli ultimi 12 mesi.[3] Gli attacchi alle infrastrutture critiche del settore manifatturiero possono comportare perdite finanziarie, un rischio per la reputazione del marchio e, talvolta, anche la perdita di vite umane o minacce alla sicurezza nazionale.

Dal 2005 Fortinet protegge gli ambienti OT in settori con infrastrutture critiche come l'energia, la difesa, la produzione, l'alimentazione e i trasporti. Progettando la sicurezza informatica in queste infrastrutture complesse con l'uso del suo Security Fabric, le organizzazioni possono integrare la protezione della sicurezza informatica negli ambienti OT e IT, dal reparto di produzione al data center passando per i vari cloud.

Principali sfide della sicurezza informatica nel settore manifatturiero

Sicurezza degli impianti, dei lavoratori e della comunità

Gli impianti di produzione sono costituiti da macchinari che possono causare lesioni fisiche o morte se non funzionano correttamente. Nell'attuale panorama delle minacce, gli avversari che mirano a interrompere le attività con un attacco cyber-fisico possono creare un rischio per la sicurezza dei dipendenti in loco e persino dei residenti e dei passanti nelle vicinanze.[5] Gli attacchi possono inoltre colpire la sicurezza dei prodotti fabbricati in uno stabilimento, estendendo il rischio a una vasta area geografica.

Nella maggior parte delle organizzazioni, il problema è rappresentato dalla compartimentazione dei sistemi per la sicurezza IT, OT e fisica, che di certo non aiuta. Integrare solamente l'architettura di sicurezza IT tra il data center, i vari cloud e il perimetro è già alquanto difficile, ma comunque insufficiente considerato che viviamo in un'epoca in cui gli avversari possono sferrare contemporaneamente attacchi informatici e fisici. Integrare tutti gli elementi della sicurezza con una visibilità centralizzata è forse, dunque, l'unico modo possibile per proteggere la vita umana.

Produttività e operatività

Qualsiasi interruzione non pianificata delle attività può comportare costi significativi per un produttore, e l'interruzione può creare problemi a cascata lungo i canali di distribuzione e lungo la catena di approvvigionamento. Purtroppo, molti cyberattacchi ai produttori mirano a causare proprio un'interruzione. Altri cercano di muoversi lateralmente all'interno della rete una volta entrati, ma l'attacco può comunque avere un impatto sulle operazioni.

Dato che in passato i sistemi OT erano isolati fisicamente dal monto esterno e gli aggiornamenti di sistema sono meno frequenti, spesso la protezione a livello di sicurezza informatica è meno sofisticata rispetto ai sistemi IT. Di conseguenza, sono spesso presi di mira dai cybercriminali che li considerano relativamente facili da infiltrare.[6] Anche i sistemi OT isolati fisicamente possono essere infiltrati infettando gli aggiornamenti del software dei produttori prima dell'installazione.

Efficienza operativa
Le attività di sicurezza compartimentate, derivanti da una mancanza di integrazione tra diversi strumenti di sicurezza, aumentano inevitabilmente le inefficienze operative. Senza integrazione, compiti manuali come la correlazione dei report di registro da diversi sistemi e l'assemblaggio dei report di compliance fanno perdere tempo a tecnici della sicurezza informatica profumatamente pagati e ne sottraggono a un lavoro più strategico.

La compartimentazione a livello di architettura crea anche ridondanze nella gestione delle applicazioni. Una pletora di prodotti puntuali impone maggiori competenze specifiche in termini di prodotto all'interno di un team responsabile della sicurezza informatica già sovraccarico di lavoro. Possono inoltre comportare costi più elevati per le licenze software e hardware e il tempo del personale necessario per amministrare più licenze. Questi fattori possono aumentare notevolmente le spese di gestione complessive.

Esperienza del cliente
Che i prodotti siano per i consumatori o le imprese, oggigiorno i produttori assumono generalmente un impegno molto mirato con i clienti, usando i social media e altri strumenti di coinvolgimento, oltre alla presenza sul web. Ma questi sforzi legittimi possono essere contrastati dai cybercriminali che manipolano i social network a scopo di lucro. Uno studio ha scoperto che più della metà degli account dei social media nel mondo sono fraudolenti.[7]

Proteggere le proprietà del web e le interazioni con i social media è fondamentale per i produttori, poiché la perdita di dati dei potenziali clienti nelle prime fasi del ciclo di acquisto potrebbe essere devastante per la reputazione dell'azienda. Altri fattori come il tempo di inattività del sito web, l'indisponibilità temporanea del prodotto a causa di interruzioni nella produzione e simili possono avere un impatto negativo sull'esperienza del cliente.

Integrità del prodotto
Il deterioramento della qualità del prodotto, ancorché temporaneo, può essere disastroso per la reputazione di un marchio. Ad esempio, se un attacco informatico colpisce il sistema OT di un robot da cucina in modo tale che la temperatura viene leggermente modificata o il tempo di cottura viene leggermente alterato, si può verificare un deterioramento della qualità del prodotto. A seconda del prodotto, tale deterioramento può anche incidere sulla salute fisica e la sicurezza del cliente.

Compliance
I produttori sono soggetti a tutta una serie di regolamentazioni e standard, che variano in base al prodotto fabbricato. Le sanzioni per la mancata compliance sono a volte pesanti, ma un costo ancora più elevato spesso deriva dal danno subito dalla reputazione del marchio in caso di violazione.[8]

Le organizzazioni devono essere in grado di dimostrare il rispetto di più regolamentazioni e standard senza ridistribuire personale dalle iniziative strategiche alla preparazione dei report di verifica, il che fa perdere tempo prezioso al personale e può dar luogo a errori umani nella creazione dei report. La correlazione manuale dei dati per i report di verifica è quasi sempre necessaria con un'infrastruttura di sicurezza informatica disaggregata.

Casi di uso

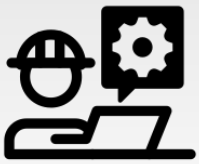
Di seguito sono riportati i principali casi di uso che le soluzioni Fortinet consentono ai produttori di risolvere:

"Da diversi anni si paventa teoricamente la possibilità di attacchi informatici descrivendoli come una grave minaccia. Ultimamente però questi attacchi sono diventati realtà."[9]

il 53% degli accessi ai siti di social media e il 25% delle richieste di nuovi account sono fraudolenti.[10]

Infrastrutture aziendali

Sebbene lo stabilimento sia il cuore della produzione, le aziende manifatturiere hanno esigenze IT aziendali simili alle organizzazioni di altri settori. La rete IT aziendale ospita dati importanti relativi a finanze, proprietà intellettuale, risorse umane, supporto prodotti, assistenza sul campo e altro ancora. Come per altri settori, le aziende manifatturiere si affidano sempre più ad applicazioni e infrastrutture basate sul cloud[11] e i dispositivi Internet-of-Things (IoT) sono sempre più numerosi lungo il perimetro della rete.[12]



Il 45% degli operatori SCADA/ ICS non utilizza il controllo degli accessi basato sui ruoli.[14]

Indipendentemente dai dati sensibili ospitati, l'infrastruttura aziendale ha bisogno di una soluzione di sicurezza informatica ampia, integrata e automatizzata con integrazione end-to-end. Il Security Fabric di Fortinet fornisce proprio una soluzione di questo tipo, costruita sulla base di firewall NGFW FortiGate e della threat intelligence nutrita dall'intelligenza artificiale di FortiGuard Labs, nella quale si integrano perfettamente vari strumenti di cybersecurity di Fortinet, insieme a decine di soluzioni di terze parti fornite dai Fabric Partner. Grazie poi all'ecosistema aperto e a un'estesa interfaccia di programmazione delle applicazioni (API), è possibile integrare anche altri strumenti di terze parti.

Sistemi di produzione isolati fisicamente dal mondo esterno

Benché ora, nella maggior dei casi, i sistemi OT siano collegati ai sistemi IT, una recente ricerca di Forrester rileva che il 40% dei sistemi OT è ancora "air gapped", ossia isolato fisicamente dal mondo esterno.[13] Si potrebbe dunque supporre siano al sicuro dai cyberattacchi. Tuttavia, tali sistemi utilizzano ancora meccanismi di controllo basati su IP e gli amministratori installano ancora aggiornamenti software forniti dal produttore, il che offre agli avversari la possibilità di penetrare nel sistema infettando gli aggiornamenti attraverso la rete del fornitore. E, per quanto i sistemi isolati fisicamente possano non contenere dati sensibili, le infiltrazioni possono causare costose interruzioni e problemi di sicurezza.

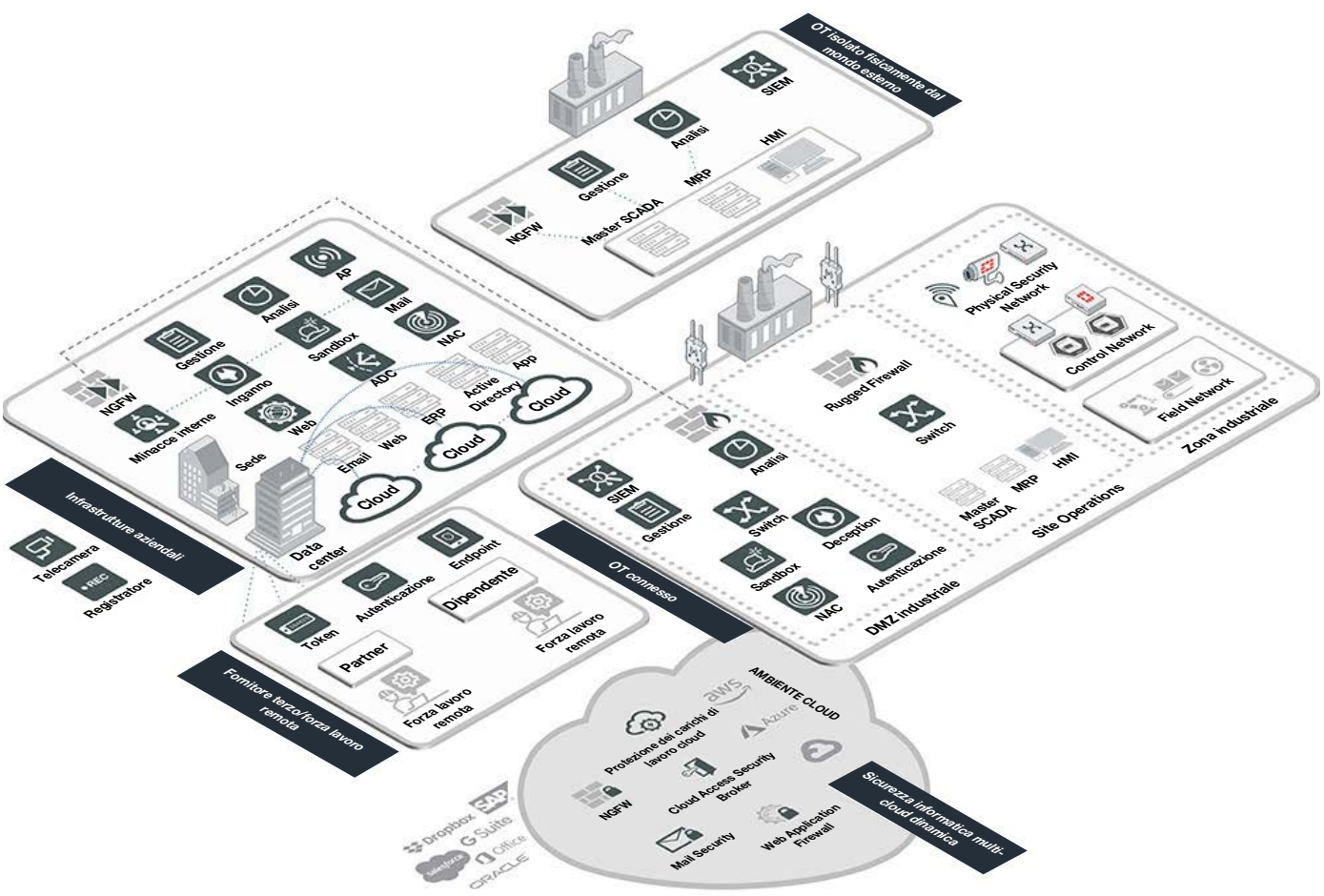
Di conseguenza, è necessario proteggere con firewall NGFW anche i sistemi isolati fisicamente, e la protezione deve essere accompagnata da un monitoraggio e un reporting completo sulla sicurezza informatica. I firewall FortiGate garantiscono una protezione robusta e prestazioni leader nel settore nell'ispezione del traffico crittografato e non crittografato, FortiManager consente di gestire il tutto attraverso un'unica interfaccia, grazie anche a vari strumenti di reporting, FortiAnalyzer permette di gestire log e sicurezza informatica sulla base di analisi per assicurare la massima visibilità e un miglior rilevamento delle violazioni e, infine, lo strumento di gestione delle informazioni e degli eventi di cybersecurity FortiSIEM consente una risposta coordinata e automatizzata agli attacchi.

Sistemi di produzione connessi

Come già affermato, la trasformazione digitale e il bisogno di agilità delle aziende stanno creando una crescente interdipendenza tra IT e OT. Dai sensori IoT industriali che monitorano le attività di produzione ai sistemi che estraggono da Internet dati pubblicamente disponibili per agevolare il processo decisionale, i sistemi OT sono sempre meno isolati. Dal punto di vista della sicurezza informatica, il principale risultato di questa convergenza è una superficie di attacco notevolmente ampliata. E poiché i sistemi OT spesso non sono sistematicamente aggiornati o migliorati, la protezione della cybersecurity ne risulta indebolita, e ciò a breve termine rappresenta un rischio per un'organizzazione.

Risolvendo però i problemi di cybersecurity, diventa effettivamente possibile combinare le reti IT e di automazione in un unico ambiente sicuro, gestibile e convergente, offrendo ai team responsabili della sicurezza informatica la visibilità centralizzata su tutti i sistemi, la capacità di segmentare la rete in base alle esigenze aziendali e il controllo centralizzato delle reti cablate e wireless di cui hanno bisogno.

Il Security Fabric di Fortinet copre l'intera superficie di attacco, dando un'ampia visibilità su chi è in rete e cosa sta facendo attraverso strumenti che permettono il controllo integrato di ogni sistema per garantire che faccia ciò che deve fare, oltre a consentire una segmentazione intelligente per garantire un maggiore controllo e una consapevolezza automatica delle minacce note e ignote. Costruito sulla base di firewall NGFW FortiGate e della threat intelligence nutrita dall'intelligenza artificiale di FortiGuard Labs, il Security Fabric offre una perfetta integrazione con decine di strumenti di sicurezza informatica proposti da Fortinet e dai suoi Fabric Partner.



Le soluzioni Fortinet per la sicurezza informatica nel settore manifatturiero permettono alle aziende di costruire un'architettura di sicurezza integrata end-to-end che abbraccia IT, OT e sicurezza fisica, estendendosi dalla sede centrale all'impianto di produzione e coprendo gli utenti interni e quelli di partner terzi.

Gestione di fornitori terzi

Man mano che il settore si dirige verso un modello Manufacturing-as-a-Service (MaaS),[15] i fornitori terzi hanno più accesso che mai alle reti aziendali e ai sistemi OT. Questo complica la nozione di utente affidabile e costringe le organizzazioni a valutare continuamente la loro protezione dalle minacce interne, anche da parte di terzi. È fondamentale tenere traccia della strategia di sicurezza informatica di ogni partner attraverso un controllo regolare. Le organizzazioni hanno inoltre bisogno di una solida protezione dalle minacce interne, siano esse accidentali o intenzionali, indipendentemente dal fatto che provengano dall'interno dell'azienda o da un elemento della rete di partner.

Le soluzioni integrate del Security Fabric di Fortinet creano una difesa multistrato contro tali minacce. Le capacità di segmentazione basate sull'intent dei firewall NGFW FortiGate permettono alle organizzazioni di segmentare la rete in modo intelligente in un mondo in cui ormai la fiducia è dinamica. La soluzione di gestione dell'identità e dell'accesso FortiAuthenticator e i token FortiToken sfruttano questa segmentazione nel concedere l'accesso agli utenti in base alla loro reale necessità di acquisire un'informazione. FortiInsight utilizza l'analisi del comportamento degli utenti e delle entità (UEBA) per identificare le anomalie nel comportamento atteso di utenti ed entità ritenuti affidabili, che potrebbero essere segnali di un account compromesso. Infine, FortiDeceptor utilizza la deception technology per ingannare, esporre e neutralizzare gli attacchi provenienti da fonti interne ed esterne.

Sicurezza informatica multi-cloud

I produttori stanno spostando rapidamente i servizi verso il cloud.[16] Molti ora dispongono di sistemi di pianificazione delle risorse produttive (MRP) e delle risorse aziendali (ERP) basati su cloud. Questi sistemi spesso estraggono dati sia da sistemi IT che da sistemi OT per un processo decisionale rapido ed efficace, basato sul cosiddetto "gemellaggio digitale". Le soluzioni basate su cloud sono anche utilizzate abitualmente per servizi che hanno un impatto sull'esperienza del cliente. Proteggere la sicurezza informatica per questi asset è fondamentale, il che significa che l'architettura di sicurezza informatica integrata di un'organizzazione deve estendersi dal data center ai sistemi OT e ai vari cloud.

Il Fortinet Security Fabric consente una protezione completa per l'ambiente multi-cloud, garantendo una gestione coerente delle policy, la gestione della configurazione, il rilevamento delle minacce e la risposta su tutta la superficie di attacco. FortiGate VM porta il firewall NGFW in una macchina virtuale che funziona bene in ambienti cloud, mentre il web application firewall (WAF) FortiWeb, disponibile in diversi fattori di forma, protegge il livello dell'applicazione con una threat intelligence nutrita costantemente dall'intelligenza artificiale in linea.

Il servizio CASB (Cloud Access Cybersecurity Broker) FortiCASB fornisce informazioni su risorse, utenti, comportamenti e dati memorizzati nel cloud con strumenti di reporting completi e consente di estendere i controlli avanzati delle policy alle risorse Infrastructure-as-a-Service (IaaS) e alle applicazioni Software-as-a-Service (SaaS). Lo strumento CWP (Cloud Workload Protection) FortiCWP consente ai team responsabili della sicurezza informatica e DevOps di valutare la loro strategia nella configurazione del cloud e identificare le potenziali minacce derivanti da configurazioni errate.

Elementi distintivi di Fortinet

Elementi distintivi di Fortinet per la sicurezza informatica nel settore manifatturiero

Le soluzioni Fortinet offrono ai produttori la possibilità di proteggere tutto attraverso le diverse reti OT e IT. I principali elementi distintivi sono:

- **Integrazione**
  La tecnologia Fortinet fornisce ai produttori un'architettura di cybersecurity integrata end-to-end che copre IT e OT, sicurezza informatica e fisica, stabilimento e sede centrale, data center e i vari cloud. Ciò permette una vera automazione della sicurezza e consente flussi di lavoro coordinati dalla protezione al rilevamento e, infine, alla risposta.
- **Monitoraggio e gestione**
  Fortinet permette ai produttori di consolidare le funzioni di rete, sicurezza informatica e sorveglianza in un unico sistema, con piena visibilità e controllo attraverso un'unica interfaccia. Ciò aiuta a prevenire gli attacchi fisici ed elimina la compartimentazione tra i diversi team.
- **Hardware robusto**
  L'hardware può essere sottoposto a frequenti sollecitazioni in un ambiente di produzione, e un danno fisico a un firewall può spesso comportare l'arresto delle attività di fabbrica. Fortinet offre un'ampia gamma di robuste appliance per soddisfare tutte le esigenze ambientali e supportare la continuità aziendale.
- **Protezione proattiva dalle minacce interne**
  La gestione del rischio derivante dalle minacce interne diventa più complessa man mano che più fornitori e partner terzi hanno accesso alla rete. Fortinet propone una soluzione completa per difendersi dalle minacce interne, compresa la segmentazione basata sull'intent, la deception technology e l'analisi del comportamento degli utenti e delle entità (UEBA).

Intrusioni subite dal settore manifatturiero[17] (negli ultimi 12 mesi)

- Malware, 61%
- Spyware, 45%
- DDoS, 28%
- Minacce interne, 26%
- Phishing, 24%
- Dispositivi mobili, 21%
- Ransomware, 21%
- Attacchi man-in-the-middle, 18%
- Attacchi zero-day, 17%
- Iniezione SQL, 8%

Impatto delle intrusioni subite dal settore manifatturiero[17] (negli ultimi 12 mesi)

- Il 45% ha subito un'interruzione operativa che ha inciso sulla produttività
- Il 40% ha subito un danno alla notorietà del marchio
- Il 35% ha subito un'Interruzione operativa che ha messo a repentaglio la sicurezza fisica
- Il 32% ha subito un'interruzione operativa che ha inciso sui proventi
- Il 26% ha perso dati fondamentali per l'azienda

- **Threat intelligence OT specifica**
  FortiGuard Labs mette a disposizione una ricca threat intelligence OT specifica, aiutando in tal modo i produttori a prendere decisioni strategiche migliori. Da 15 anni Fortinet collabora strettamente con i clienti del settore manifatturiero.
- **Ecosistema del Security Fabric**
  Oltre all'ampio portfolio di strumenti di sicurezza Fortinet, con il Security Fabric è possibile integrare facilmente soluzioni OT specializzate attraverso l'ecosistema di Fabric Partner di Fortinet per semplificare l'interpretazione dei dati riunendoli in un'unica vista in modo da giungere a un processo decisionale informato.

Conclusioni

In un mercato in rapida evoluzione che richiede una produzione just-in-time, i produttori non possono permettersi di essere rallentati da eventi legati alla sicurezza informatica o dagli sforzi per evitarli. Il Security Fabric di Fortinet fornisce una piattaforma unificata in grado di proteggere la sicurezza IT, OT e fisica, con ampia visibilità e controllo integrato attraverso un'unica interfaccia.

"Gli amministratori delegati e i team dirigenziali ai vertici aziendali... concordano unanimemente sul fatto che le strategie volte ad accelerare il time to market, migliorare la qualità dei prodotti e ascoltare i clienti stanno dando i loro frutti."[18]

"Nonostante le fluttuazioni stagionali e l'ampia varietà di obiettivi, su un aspetto i dati sono inequivocabili: gli attacchi IT ai sistemi OT sono in aumento."[19]

[1] Marco Annunziata, "Manufacturing-As-A-Service Platforms: The New Efficiency Revolution," Forbes, 13 maggio 2019.

[2] "Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems," Fortinet, 8 maggio 2019.

[3] "State of Operational Technology and Cybersecurity Report," Fortinet, accesso del 7 novembre 2019.

[4] "Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems," Fortinet, 8 maggio 2019.

[5] "Cyber Physical Systems Security," Department of Homeland Security, accesso del 7 novembre 2019.

[6] "Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems," Fortinet, 8 maggio 2019.

[7] "Q3 Fraud and Abuse Report," Arkose Labs, 18 settembre 2019.

[8] "Ninth Annual Cost of Cybercrime Study," Accenture and Pomenon Institute, 6 marzo 2019.

[9] Elizabeth Montalbano, "Six Cyber-Physical Attacks the World Could Live Without," The Security Ledger, 18 gennaio 2017.

[10] "Q3 Fraud and Abuse Report," Arkose Labs, 18 settembre 2019.

[11] Louis Columbus, "10 Ways Cloud Computing Will Drive Manufacturing Growth In 2018," Manufacturing Business Technology, 23 febbraio 2018.

[12] "Applications of IoT in Manufacturing Plants," The Manufacturer, 12 aprile 2018.

[13] "Independent Study Pinpoints Significant SCADA/ICS Security Risks," Fortinet, 16 aprile 2019.

[14] Ibid.

[15] Marco Annunziata, "Manufacturing-As-A-Service Platforms: The New Efficiency Revolution," Forbes, 13 maggio 2019.

[16] Louis Columbus, "10 Ways Cloud Computing Will Drive Manufacturing Growth In 2018," Manufacturing Business Technology, 23 febbraio 2018.

[17] Sulla base di una serie di sondaggi condotti presso diversi utenti tipo da Fortinet. Relazione di studio di prossima pubblicazione.

[18] Louis Columbus, "10 Ways Cloud Computing Will Drive Manufacturing Growth In 2018," Manufacturing Business Technology, 23 febbraio 2018.

[19] "Fortinet 2019 Operational Technology Security Trends Report: An Update on the Threat Landscape for ICS and SCADA Systems," Fortinet, 8 maggio 2019.

FORTINET

www.fortinet.com

10. giugno 2022, 11:09
517972-A-1-EN