FORTINET

REPORT

Report sullo stato dell'Operational Technology e della Cybersecurity

Sommario

Sintesi preliminare

La tecnologia operativa (OT) è vitale per la sicurezza pubblica e il benessere economico, poiché controlla apparecchiature in tutto il mondo che gestiscono gli impianti di produzione, le reti elettriche, i servizi idrici, il trasporto marittimo e altro ancora.

L'ascesa dell'OT è iniziata nei primi decenni del XX secolo, quando le macchine e i comandi elettrici hanno sostituito le macchine azionate a mano e a vapore. L'OT precede di molti decenni l'ascesa della tecnologia dell'informazione (IT) e, tradizionalmente, le reti OT e IT sono state separate. Recentemente, tuttavia, le tecnologie basate sull'IT come sensori, apprendimento automatico (ML, Machine Learning) e big data vengono integrati con le reti OT per creare nuove efficienze e vantaggi competitivi. Questo aumenta la superficie di attacco digitale e il rischio di intrusione.

Per esplorare lo stato della sicurezza informatica negli ambienti OT, Fortinet ha svolto un sondaggio sulle operazioni di stabilimento e i leader di produzione (leader delle operazioni di stabilimento) presso grandi aziende dei settori manifatturiero, dell'energia e dei servizi pubblici, sanitario e dei trasporti. Il sondaggio ha rivelato le informazioni strategiche seguenti:

1. **L'impatto degli attacchi informatici sugli ambienti OT è esteso e profondo.** Circa il 74% delle organizzazioni OT ha subito un'intrusione di malware negli ultimi 12 mesi, che ha compromesso produttività, ricavi, fiducia nel marchio, proprietà intellettuale e sicurezza fisica.

2. **Una carenza di sicurezza informatica contribuisce al rischio.** Il 78% ha una visibilità centralizzata solo parziale della sicurezza informatica dei propri ambienti OT. Il 65% non dispone di un controllo degli accessi basato sui ruoli e più della metà non utilizza l'autenticazione a più fattori o la segmentazione interna della rete.

3. **Il miglioramento della strategia di sicurezza dell'OT è limitato dalla necessità di tenere il passo con cambiamenti rapidi e dalla mancanza di risorse umane.** Quasi due terzi (64%) dei leader del settore OT affermano che tenere il passo con il cambiamento è la loro sfida più grande e quasi la metà (45%) è limitata dalla carenza di manodopera qualificata.

4. **Nelle organizzazioni OT è in aumento l'attenzione alla sicurezza informatica.** Il 70% prevede di introdurre la sicurezza informatica nei sistemi OT sotto la supervisione del CISO nel prossimo anno (solo il 9% dei CISO si occupano attualmente della sicurezza OT) e il 62% dei budget per la sicurezza informatica è in aumento.

Questo report esamina i risultati del sondaggio, tra cui:

- Sfide percepite dai responsabili operativi degli impianti per la protezione dei loro ambienti OT
- Il tipo e l'impatto delle intrusioni subite
- Come gestiscono la sicurezza informatica
- Quali lacune di sicurezza si trovano ad affrontare
- Come misurano il loro successo

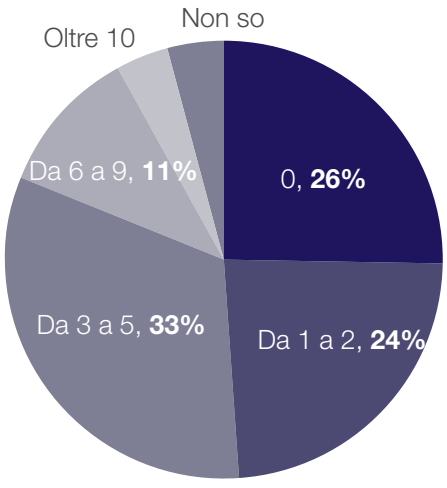
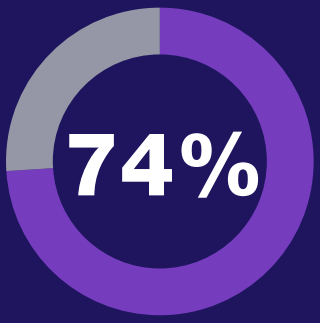
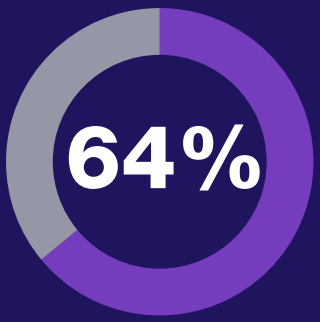


Figura 1. Numero di intrusioni negli ultimi 12 mesi

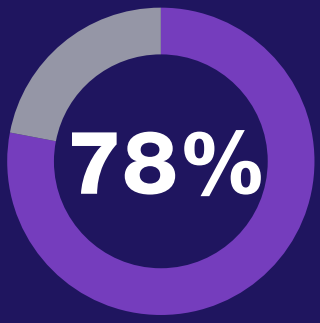
Infografica: risultati in evidenza sulla sicurezza OT



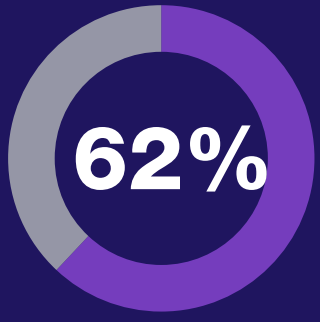
Percentuale delle organizzazioni OT intervistate che hanno subito violazioni negli ultimi 12 mesi, con conseguente perdita di dati, interruzioni operative e/o danno d'immagine.



Percentuale delle organizzazioni che hanno difficoltà a tenere il passo con i cambiamenti.



Percentuale delle organizzazioni che hanno una visibilità centralizzata limitata sulla sicurezza informatica.



Percentuale delle organizzazioni che stanno aumentando il budget dedicato alla sicurezza informatica.

Le violazioni hanno danneggiato

- Produttività (43%)
- Ricavi (36%)
- Reputazione del marchio (30%)
- Dati business-critical (28%)
- Sicurezza a rischio (23%)

Il 70% ha in mente di **affidare la sicurezza informatica al CISO** durante il prossimo anno.

Tuttavia, solo il 9% dei CISO supervisiona attualmente la sicurezza informatica in ambito OT.

Rispetto alle organizzazioni OT con risultati peggiori (6 o più intrusioni in 12 mesi), le organizzazioni OT con risultati migliori (zero intrusioni in 12 mesi) hanno:

100% maggiore probabilità di utilizzare l'autenticazione a più fattori

94% maggiore probabilità di utilizzare il controllo degli accessi basato sui ruoli

68% maggiore probabilità di gestire e monitorare gli eventi di sicurezza e di eseguire un'analisi degli eventi

51% maggiore probabilità di applicare la segmentazione di rete

46% maggiore probabilità di programmare controlli di conformità in materia di sicurezza

Metodologia di questo studio

Il Report sullo stato della tecnologia operativa e della sicurezza informatica si basa su un sondaggio del gennaio 2019 tra persone che:

- Lavorano in aziende con più di 2.500 dipendenti nei settori manifatturiero, dell'energia e dei servizi pubblici, sanitario e dei trasporti
- Hanno l'OT come responsabilità primaria
- Hanno responsabilità di reporting per le operazioni
- Sono coinvolti in decisioni di acquisto in materia di sicurezza informatica

Informazioni strategiche sulla sicurezza nelle operazioni OT

Informazione: l'impatto degli attacchi informatici sui sistemi OT è forte ed esteso

Quasi tre quarti (74%) delle organizzazioni OT hanno subito almeno un'intrusione di malware nell'ultimo anno e la metà (50%) ha subito da 3 a 10 o più intrusioni.

Come mostra la Figura 2, il malware è la principale forma di intrusione, seguito da phishing (45%), spyware (38%) e violazioni di dispositivi mobili (28%).

L'impatto delle violazioni sulle organizzazioni OT è stato notevole, come mostrato nella Figura 3.

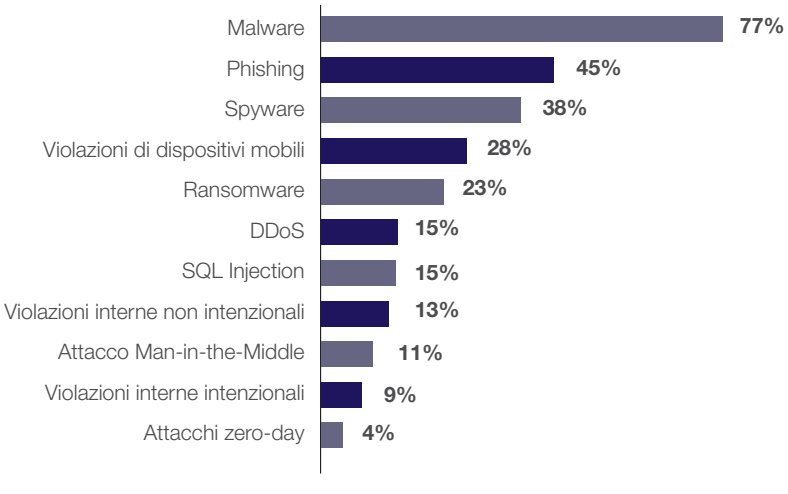


Figura 2. Tipi di intrusioni OT subite

Figura 3. Impatto delle violazioni nelle organizzazioni OT

Informazione: la mancanza di visibilità della sicurezza informatica contribuisce al rischio

Il 78% delle organizzazioni ha una visibilità centralizzata solo parziale della sicurezza informatica delle operazioni OT, come mostrato nella Figura 4.

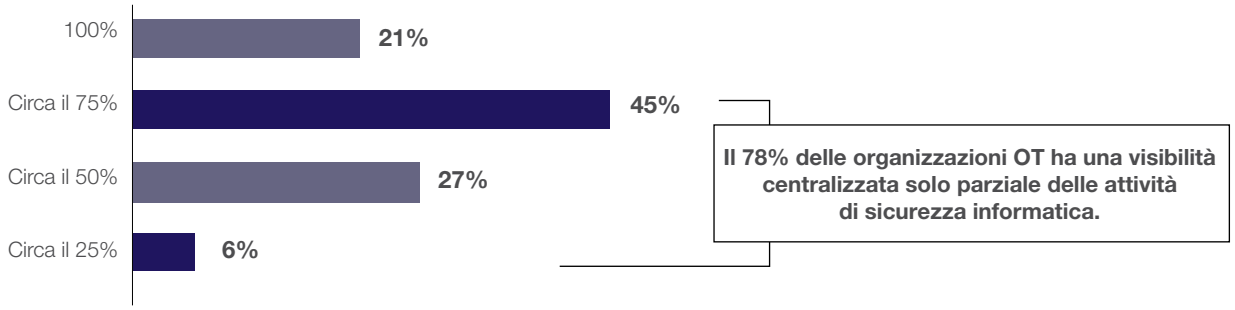


Figura 4. % di attività di sicurezza informatica OT visibili centralmente

Informazione: la carenza di manodopera qualificata è uno dei principali freni al miglioramento della sicurezza informatica

Quasi due terzi dei responsabili delle operazioni di stabilimento (64%) affermano che tenere il passo con il cambiamento è la loro sfida più grande, seguita da un'ampia serie di altre sfide, come ad esempio:

- Relazioni sindacali (45%)
- Carenza di manodopera qualificata (45%)
- Cambiamenti normativi (44%)
- Disponibilità e accessibilità di interventi formativi (42%)
- Vincoli di budget (42%)

Inoltre, la carenza di manodopera qualificata è un fattore che incide sulle quattro maggiori preoccupazioni che i responsabili delle operazioni di stabilimento hanno sull'aggiunta di soluzioni di sicurezza informatica:

- Crea maggiore complessità (53%)
- Richiede una difficile adozione di norme di sicurezza (45%)
- Richiede più personale operativo (45%)
- Ostacola la flessibilità operativa (44%)

Tuttavia, nonostante la carenza di risorse umane, le organizzazioni OT sono determinate a migliorare la loro strategia di sicurezza, secondo ulteriori dati. La Figura 5 mostra i concetti principali espressi dai responsabili operativi degli impianti quando viene chiesto loro quali sono le sfide che li spingono a migliorare la sicurezza informatica.

Figura 5. Sfide principali che spingono a migliorare la sicurezza informatica

La domanda alla base della Figura 5 era: "Quali sono le tre sfide principali che ti portano a migliorare o a cambiare la tua strategia di sicurezza informatica?" Quanto più frequentemente un concetto è apparso nelle risposte, tanto più grande appare sopra.

Le sfide di sicurezza più frequenti che i leader operativi degli impianti hanno espresso nella Figura 5 sono la capacità di contrastare gli hacker, proteggere una superficie di attacco crescente causata dalla trasformazione digitale, mantenere la sicurezza dei dati e mantenere gli ambienti sicuri, produttivi, convenienti e conformi, il tutto affrontando al contempo una carenza di competenze.

Informazione: l'attenzione alla sicurezza informatica è in aumento nelle organizzazioni OT

Il 70% delle organizzazioni intervistate prevede di introdurre la sicurezza informatica nei sistemi OT sotto la supervisione del CISO nel corso del prossimo anno. È interessante notare che solo il 9% dei CISO supervisiona attualmente la sicurezza informatica in ambito OT. Attualmente, il direttore/manager OT della sicurezza informatica è responsabile della sicurezza informatica nel 50% delle organizzazioni, con un altro 24% che indica che la sicurezza informatica è sotto la responsabilità del VP/direttore del reparto addetto alla gestione tecnica e operativa della rete.

L'assegnazione di una maggiore priorità alla sicurezza informatica è evidente non solo nella ristrutturazione organizzativa delle responsabilità. **Il 62% delle organizzazioni afferma che i budget per la sicurezza informatica stanno aumentando drasticamente** quest'anno, mentre il 38% mantiene i budget sulla sicurezza informatica attuali. Le organizzazioni OT stanno ponendo il rischio per la sicurezza al centro dell'attenzione: il 94% degli intervistati indica che la strategia di sicurezza OT è un fattore significativo o moderato nel più ampio punteggio di rischio che il CISO condivide con la direzione esecutiva e il consiglio di amministrazione.

Informazione: gli ambienti OT sono complessi da proteggere

Gli ambienti OT che gli intervistati lavorano per proteggere sono complessi. Sono costituiti da un numero variabile di dispositivi OT, da meno di 50 a più di 500, come mostrato nella Figura 6.

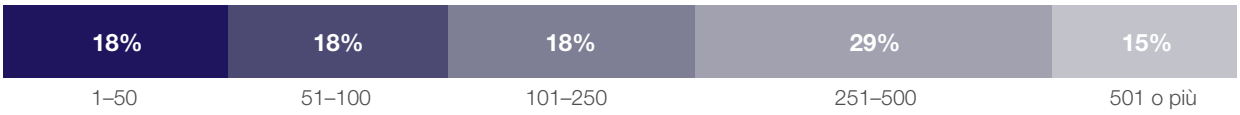


Figura 6. Numero di dispositivi OT in funzione

La maggior parte delle organizzazioni acquisisce i propri dispositivi da 2–4 fornitori, come mostrato nella Figura 7.

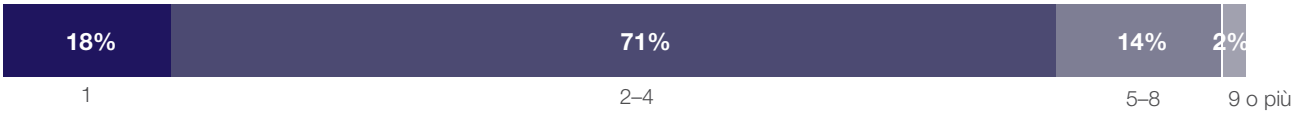


Figura 7. Numero di fornitori utilizzati per i dispositivi OT

I fornitori OT più utilizzati in questo sondaggio sono Honeywell, Siemens ed Emerson, come mostrato nella Figura 8.

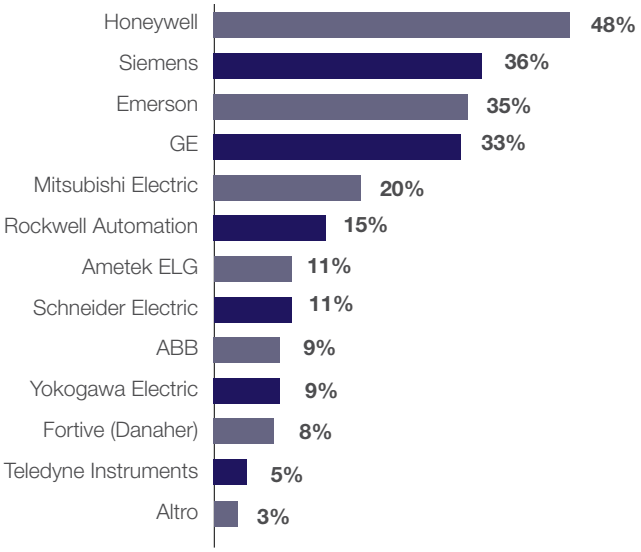


Figura 8. Fornitori utilizzati per i dispositivi OT

Informazione: i responsabili operativi dell'impianto hanno influenza per migliorare la sicurezza informatica

Mentre le organizzazioni OT rafforzano la sicurezza informatica dei loro ambienti, i responsabili operativi degli impianti sono attivamente coinvolti nelle scelte che vengono fatte. Più di tre quarti (76%) riferiscono di essere regolarmente inclusi nelle decisioni di sicurezza informatica e quasi la metà (45%) ha l'ultima parola nelle decisioni OT. Quasi tutti sono regolarmente (56%) o occasionalmente (39%) coinvolti nello sviluppo della strategia di sicurezza informatica della loro organizzazione.

È interessante notare che un ambiente sicuro e stabile è essenziale per le tre principali metriche di successo in base alle quali vengono giudicati i leader operativi dello stabilimento: massimizzare la produttività (55%), minimizzare i costi (53%) e ridurre i tempi di risposta alle vulnerabilità di sicurezza (44%).

Può sorprendere che "ridurre i tempi di risposta alle vulnerabilità di sicurezza" sia il terzo parametro di successo più importante. Ma si immagini quanto velocemente un attacco informatico può perturbare una struttura come una fabbrica, un'utilità o una ferrovia, danneggiando la produttività, le entrate e la sicurezza. Un ambiente stabile e resiliente è fondamentale anche per le tre principali responsabilità dirette dei responsabili operativi degli stabilimenti: gestione dell'efficienza produttiva (77%), supervisione del team operativo (77%) e gestione del controllo qualità e dei processi produttivi (76%).

> ***"La minaccia di un attacco informatico è un grande freno e stiamo investendo su come prevenirlo."***
>
> – Responsabile operazioni di stabilimento, produttore

Data la loro attenzione a stabilità e resilienza, è più evidente il motivo per cui il 76% dei responsabili operativi degli impianti è attivamente coinvolto nelle decisioni di sicurezza informatica OT. Questa attività richiederà più tempo poiché è previsto un aumento della spesa relativa alla sicurezza informatica OT del 50%, fino a 18,05 miliardi di dollari nel 2023, rispetto a 12,22 miliardi di dollari nel 2017.[1]

Vi è un certo numero di carenze in materia di sicurezza informatica che i team OT devono affrontare, come indicato nella sezione successiva.

Informazione: vi sono lacune della sicurezza OT nel controllo degli accessi, nell'autenticazione, nella segmentazione e in altre aree

La Figura 9 mostra la percentuale delle organizzazioni OT intervistate e che non hanno le capacità chiave elencate in materia di sicurezza informatica.

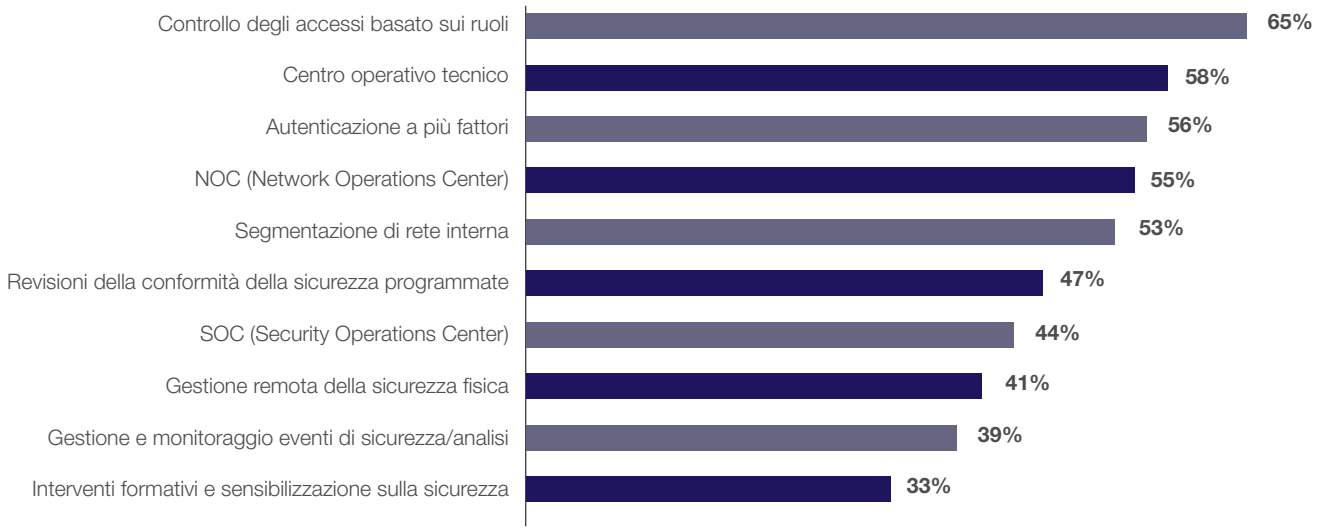


Figura 9. Percentuale di organizzazioni OT che non dispongono di misure chiave di sicurezza informatica e in generale di sicurezza.

Le capacità mancanti indicate nella Figura 9 causano una serie di lacune in materia di sicurezza:

- **Circa due terzi** (65%) delle aziende OT intervistate non applica un controllo degli accessi basato sui ruoli, dando agli aggressori una maggiore libertà di movimento all'interno dei loro ambienti OT.
- **Quasi 6 organizzazioni OT su 10** (56%) non utilizzano l'autenticazione a più fattori. Un recente report Verizon rileva che l'81% delle violazioni è iniziato con credenziali perse o sottratte.[2] Molte violazioni degli ambienti OT usano lo spear phishing per ottenere illecitamente credenziali. Secondo il *Wall Street Journal*, si stima che due dozzine di aziende della rete elettrica statunitensi siano state violate mediante spear phishing e credenziali sottratte negli ultimi due anni; inoltre gli aggressori hanno lasciato malware nei loro ambienti OT da utilizzare per futuri sabotaggi.[3] L'autenticazione a più fattori rende più difficile l'uso di credenziali sottratte.
- **Più della metà** delle organizzazioni (53%) non dispone di una segmentazione di rete interna. Le linee guida sulla sicurezza informatica del NIST (National Institute of Standards and Technology) hanno definito la segmentazione "uno dei concetti architetturali più efficaci che un'organizzazione possa implementare" per proteggere il proprio ambiente OT.[4] Gli esperti del settore sottolineano come molti recenti attacchi malware OT avrebbero potuto essere stati sventati dalla segmentazione, in quanto limita la libertà di movimento da una rete di produzione OT a un'altra, nonché all'interno della stessa rete.[5]
- **Quasi la metà** (44%) non ha un SOC (Security Operations Center) e più della metà (55%) non ha un NOC (Network Operations Center), il che porta a una visibilità ridotta e a un maggiore rischio. Un SOC è in grado di rilevare, contrastare o limitare una violazione più velocemente. Un NOC massimizza il throughput e la disponibilità della rete. SOC e NOC possono essere integrati per migliorare i risultati di entrambi.[6]
- **Quasi 4 organizzazioni su 10** (39%) non gestiscono, monitorano o analizzano gli eventi di sicurezza, rendendo le violazioni difficili da scoprire. Con la maggior parte delle organizzazioni che ora accettano l'inevitabilità di un'intrusione riuscita, la resilienza informatica, ossia la risposta agli incidenti e la gestione degli eventi, è fondamentale per ridurre al minimo l'impatto di una violazione.[7]
- Le pratiche di sicurezza di base rimangono una sfida per un numero significativo di organizzazioni, con **un terzo** (33%) di esse che ammette di non avere programmi di formazione interna di sensibilizzazione e di educazione alla sicurezza. Con le minacce interne che rappresentano il 30% di tutte le violazioni, questo è un requisito per qualsiasi organizzazione-IT o OT.[8]

Best practice delle organizzazioni OT più sicure

Il 26% dei nostri intervistati (le organizzazioni "di livello superiore") ha avuto **zero intrusioni** negli ultimi 12 mesi. D'altra parte, il 17% dei nostri intervistati (le organizzazioni "di livello inferiore") ha avuto **sei o più intrusioni** negli ultimi 12 mesi, mentre alcuni non sapevano neanche il numero di intrusioni avute. È interessante notare le disparità tra questi due gruppi, tra cui:

1. **Le organizzazioni di livello superiore hanno il 100% di probabilità in più delle organizzazioni di livello inferiore di utilizzare l'autenticazione a più fattori,** che rende più difficile l'accesso con credenziali sottratte.
2. **Le organizzazioni di livello superiore hanno il 94% di probabilità in più delle organizzazioni di livello inferiore di utilizzare il controllo degli accessi basato sui ruoli,** che limita i movimenti di un potenziale aggressore.
3. **Le organizzazioni di livello superiore hanno il 68% di probabilità in più delle organizzazioni di livello inferiore di gestire e monitorare gli eventi di sicurezza ed eseguire analisi degli eventi,** che limitano i rischi derivanti da una violazione riducendo al minimo il tempo di rilevamento.
4. **Le organizzazioni di livello superiore hanno il 51% di probabilità in più delle organizzazioni di livello inferiore di utilizzare la segmentazione di rete** per limitare i movimenti di un potenziale aggressore.
5. **Le organizzazioni di livello superiore hanno il 46% di probabilità in più delle organizzazioni di livello inferiore di programmare revisioni di conformità alla sicurezza** per rafforzare i livelli di sicurezza.

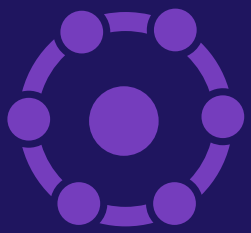
Conclusione: la sicurezza informatica è un requisito crescente per il successo OT

Il rischio in ambienti OT è elevato: quasi 8 su 10 sono stati violati nell'ultimo anno, con la metà che ha avuto da 3 a 10 o più violazioni. Sono stati segnalati danni da violazione che incidono su produttività, ricavi, fiducia nel marchio, proprietà intellettuale e sicurezza fisica. Questo studio identifica i fattori da affrontare per ridurre il rischio, come il fatto che il 78% delle organizzazioni non ha una visibilità completa e centralizzata della sicurezza informatica, il 56% non ha un'autenticazione a più fattori e il 53% non utilizza ancora la segmentazione di rete interna, una best practice OT altamente consigliata.[9]

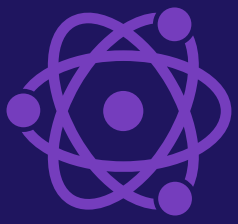
I responsabili delle operazioni degli impianti OT riferiscono di essere attivi e influenti nella valutazione delle soluzioni di sicurezza informatica. Sono alla ricerca di soluzioni che supportino i loro obiettivi principali di massimizzare la produttività riducendo al minimo i costi.

Per far fronte alla mancanza di visibilità centralizzata e alla carenza di personale, le organizzazioni OT dovrebbero seguire le seguenti raccomandazioni:

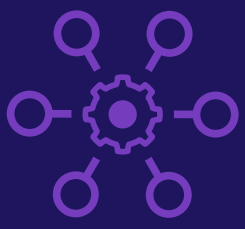
> ***"Le soluzioni di sicurezza devono agire in modo più intelligente ed essere più efficaci, spesso a fronte di budget ridotti".***
>
> – VP della produzione, grande produttore



Cercare soluzioni di sicurezza che assicurino interoperabilità per fornire un'ampia visibilità dell'intera superficie di attacco digitale, che si estende negli ambienti OT e IT.



Cercare un approccio basato sul Security Fabric che fornisca una protezione integrata in tutti i dispositivi, reti e applicazioni.



Cercare funzionalità di sicurezza automatizzate, con soluzioni che coordinano una risposta e utilizzano tecnologie come l'apprendimento automatico.

Ridurre al minimo i rischi con le best practice di sicurezza informatica OT come segmentazione della rete, autenticazione a più fattori e controllo degli accessi in base ai ruoli.

Questi approcci alla sicurezza informatica miglioreranno la strategia di sicurezza di un'organizzazione, aiutando nel contempo a compensare la carenza di manodopera qualificata.

Riferimenti

[1] Industrial Control Systems (ICS) Security Market worth $18.05 billion by 2023," MarketsandMarkets, consultato il 25 febbraio 2018.

[2] 2017 Data Breach Investigations Report, Verizon, consultato il 30 novembre 2018.

[3] Rebecca Smith e Rob Barry, "America's Electric Grid Has a Vulnerable Back Door—and Russia Walked Through It," The Wall Street Journal, 10 gennaio 2019.

[4] Keith Stouffer, et al., "Guide to Industrial Control Systems (ICS) Security," NIST, maggio 2015.

[5] Peter Newton, "Securing IIoT requires extra care. NAC and segmentation can help," TechTarget, 28 settembre 2018.

[6] "Bridging the NOC-SOC Divide," Fortinet, consultato il 5 marzo 2019.

[7] Patrick Spencer, "Cyber Resilience Rises to the Forefront in 2019, According to New Scalar Security Study," Scalar Security Blog, 20 febbraio 2019.

[8] "2018 Data Breach Investigations Report," Verizon, marzo 2018.

[9] Keith Stouffer, et al., "Guide to Industrial Control Systems (ICS) Security," NIST, maggio 2015.

www.fortinet.com

Copyright © 2019 Fortinet, Inc. Tutti i diritti riservati. Fortinet®, FortiGate®, FortiCare®, FortiGuard® e altri marchi sono marchi registrati di Fortinet, Inc. Anche altri nomi Fortinet qui citati possono essere marchi registrati e/o marchi di diritto comune di Fortinet. Tutti gli altri nomi di prodotti o società possono essere marchi registrati dei rispettivi proprietari. I dati riportati relativi a prestazioni e altre caratteristiche sono stati ottenuti con prove interne di laboratorio in condizioni ideali e, pertanto, le prestazioni effettive e altri risultati possono variare. Elementi variabili della rete, diversi ambienti di rete e altre condizioni possono influenzare i risultati delle prestazioni. Nulla di quanto qui contenuto rappresenta un impegno vincolante per Fortinet, e Fortinet esclude qualsiasi garanzia, esplicita o implicita, eccetto quelle previste da un contratto scritto, firmato da un rappresentante legale di Fortinet, che garantisca esplicitamente all'acquirente che le prestazioni del prodotto indicato saranno conformi a determinati dati esplicitamente indicati. In tal caso, solo gli specifici dati delle prestazioni esplicitamente identificati in tale contratto scritto saranno vincolanti per Fortinet. Per chiarezza, qualsiasi garanzia è limitata alle prestazioni ottenute nelle stesse condizioni ideali delle prove interne di laboratorio di Fortinet. Fortinet esclude in toto qualsiasi convenzione, rappresentanza e garanzia, esplicita o implicita, sulla base del presente documento. Fortinet si riserva il diritto di cambiare, modificare, trasferire o comunque revisionare questa pubblicazione senza alcun preavviso. La versione applicabile della presente pubblicazione è quella più recente.

luglio 10, 2019 10:42 AM

330327-0-1-IT

D:\ARGOS\2019\07_2019\Assignment A-344888-924146\Work\PAKIET\OT\Manufacturing-Plant Operations\report-state-of-operational-technology-A4_it_IT\report-state-of-operational-technology-A4_it_IT