FORTINET

REPORT

Studi indipendenti individuano notevoli rischi per la sicurezza dei sistemi SCADA/ICS

Sommario

Sintesi preliminare

Negli ultimi anni molte aziende ed enti pubblici hanno adottato sistemi SCADA (Supervisory Control And Data Acquisition) o ICS (Industrial Control System), ma queste tecnologie devono confrontarsi con importanti sfide di sicurezza. In uno studio commissionato da Fortinet a Forrester Consulting e rivolto a organizzazioni che utilizzano SCADA o ICS, **quasi 6 su 10** riferiscono di avere **subito una violazione** di questi sistemi nell'ultimo anno. Molte di queste organizzazioni aggravano i loro rischi concedendo ai partner tecnologici e commerciali un alto livello di accesso ai propri sistemi. La maggior parte delle organizzazioni indica anche la presenza di **collegamenti tra i sistemi IT tradizionali e i sistemi SCADA/ICS**, che aprono ad hacker esterni la possibilità di penetrare questi sistemi di controllo.

Nonostante questi rischi, molti operatori non sfruttano molti degli strumenti di sicurezza disponibili per proteggere i sistemi SCADA/ICS. Circa **la metà** degli intervistati **non ha implementato la crittografia del traffico SSH (Secure SHell) o TLS (Transport Layer Security)** per i propri sistemi SCADA/ICS e molti non utilizzano il controllo degli accessi basato sui ruoli per i dipendenti.

Allo stesso tempo, molte organizzazioni che utilizzano SCADA/ICS aprono vie d'attacco consentendo la connessione alle loro reti di una serie di altre tecnologie, tra cui dispositivi GPS (Global Positioning System), RFID (Radio-Frequency IDentification) attivi e Wi-Fi. Ciò nonostante, il 97% degli intervistati ha confermato le sfide in materia di sicurezza portate dalla convergenza tra tecnologia dell'informazione tradizionale (IT) e tecnologia operativa (OT).

Mentre, dal lato negativo, gli ambienti SCADA/ICS devono affrontare diverse minacce, dal lato positivo gli operatori possono prendere provvedimenti per proteggere i propri sistemi introducendo altri strumenti di sicurezza.

Definizione di SCADA e ICS

I sistemi ICS sono spesso gestiti da un'interfaccia grafica SCADA, che consente agli operatori di osservare lo stato di un sistema, ricevere avvisi o inserire rettifiche per gestire i processi.

Il mercato ICS è previsto in rapida crescita, verso la cifra di **81 miliardi di dollari** nel 2021.

La superficie d'attacco si espande ogni anno.

Per il mercato SCADA è prevista una crescita del **6,6%** l'anno, fino a **13,43 miliardi di dollari** nel 2022.

Introduzione: SCADA/ICS sono obiettivi attraenti

Negli ultimi anni, molte aziende oltre a quelle elettriche e idriche hanno implementato sistemi SCADA/ICS con l'obiettivo di automatizzare le loro operazioni di raccolta dati e le loro apparecchiature. Queste tecnologie sono diventate bersagli di alto valore per gli hacker che puntano a compromettere la continuità delle operazioni aziendali, ottenere riscatti o attaccare le infrastrutture critiche delle nazioni rivali.[1] Secondo lo studio Forrester, il **56%** delle organizzazioni che utilizzano SCADA/ICS **ha segnalato una violazione** nell'ultimo anno e solo l'11% riferisce di non avere mai subito violazioni.

Gli aggressori possono causare danni reali. Nel dicembre 2015, diverse aree dell'Ucraina occidentale hanno subito interruzioni di corrente a causa di un attacco a sistemi di controllo elettrico industriali.[2] Episodi simili non sono limitati a entità esterne agli Stati Uniti. Ad esempio, nel marzo 2016 degli hacker hanno violato la rete di un'anonima azienda idrica statunitense e, per un breve periodo di tempo, hanno preso il controllo di diversi controllori logici programmabili che regolano il flusso di sostanze chimiche tossiche utilizzate per il trattamento delle acque.[3]

Una parte importante del problema è rappresentata dall'accesso ai sistemi SCADA/ICS da parte di soggetti esterni. Molte organizzazioni ripongono molta fiducia nella sicurezza dei loro fornitori di tecnologia e di altre organizzazioni esterne, concedendo loro un ampio accesso ai propri sistemi interni. Circa **6 organizzazioni su 10** intervistate da Forrester hanno accordato un **accesso completo o di alto livello** a organizzazioni partner o governative. In breve, gli operatori SCADA/ICS sono esposti a gravi rischi e devono affrontare diversi ostacoli sulla strada per migliorare la sicurezza.

SCADA/ICS in rapida diffusione e penetrazione

I mercati SCADA/ICS sono in rapida crescita. Transparency Market Research prevede che il solo mercato ICS globale passerà da 58 miliardi di dollari nel 2014 a 81 miliardi di dollari nel 2021, con un tasso di crescita annuo del 4,9% tra il 2015 e il 2021.[4] I sistemi ICS si sono ampiamente diffusi nelle industrie produttive, nei porti marittimi, negli impianti di trattamento delle acque, negli oleodotti, nelle società energetiche e nei sistemi di controllo ambientale degli edifici.[5] Allo stesso tempo i sistemi SCADA, che fungono da interfaccia grafica per ICS, crescono a un tasso annuo del 6,6%.[6]

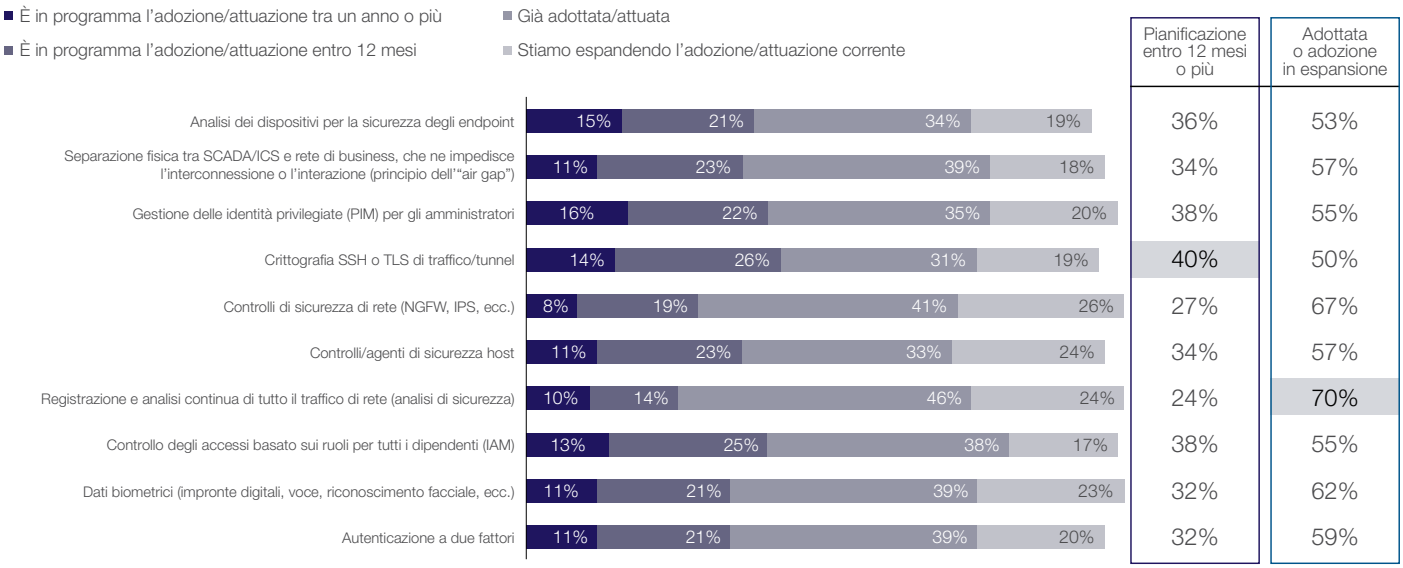
L'aspetto positivo è che le organizzazioni che gestiscono i sistemi SCADA/ICS sembrano essere consapevoli dei rischi che devono affrontare. Molte utilizzano diverse tecnologie e metodi di sicurezza per proteggere i sistemi. Ad esempio, lo studio di Forrester ha rilevato che il **70%** delle organizzazioni intervistate **registra e analizza continuamente tutto il traffico di rete** e il 24% di queste sta espandendo i propri sistemi di analisi di sicurezza. Circa **due terzi** utilizzano qualche tipo di **controllo della sicurezza di rete** e il **62%** adotta **controlli di sicurezza basati su dati biometrici**, come le impronte digitali o il riconoscimento facciale.

Nonostante questi numeri, molte organizzazioni non hanno distribuito diverse altre tecnologie di sicurezza che potrebbero contribuire a proteggere i loro sistemi SCADA/ICS. La metà degli intervistati non ha implementato la crittografia SSH o TLS del traffico, anche se più della metà di questi prevede di adottare una di queste tecnologie entro un anno.

Inoltre, il **45%** degli intervistati non utilizza la gestione delle identità privilegiate (PIM, Privileged Identity Management) per gli amministratori, che consente alle organizzazioni di monitorare gli account di alto livello nei propri ambienti IT. Un altro **45%** non utilizza il controllo degli accessi basato sui ruoli per i dipendenti. Tuttavia, solo una piccola percentuale dichiara di non avere in programma l'adozione di queste tecnologie.

La maggior parte delle organizzazioni adotta attualmente diverse misure per proteggere i loro sistemi SCADA/ICS

D1: quali sono i piani della tua organizzazione per adottare o attuare le misure seguenti per proteggere i sistemi SCADA/ICS aziendali?



					Pianificazione entro 12 mesi o più	Adottata o adozione in espansione
Analisi dei dispositivi per la sicurezza degli endpoint	15%	21%	34%	19%	36%	53%
Separazione fisica tra SCADA/ICS e rete di business, che ne impedisce l'interconnessione o l'interazione (principio dell'"air gap")	11%	23%	39%	18%	34%	57%
Gestione delle identità privilegiate (PIM) per gli amministratori	16%	22%	35%	20%	38%	55%
Crittografia SSH o TLS di traffico/tunnel	14%	26%	31%	19%	40%	50%
Controlli di sicurezza di rete (NGFW, IPS, ecc.)	8%	19%	41%	26%	27%	67%
Controlli/agenti di sicurezza host	11%	23%	33%	24%	34%	57%
Registrazione e analisi continua di tutto il traffico di rete (analisi di sicurezza)	10%	14%	46%	24%	24%	70%
Controllo degli accessi basato sui ruoli per tutti i dipendenti (IAM)	13%	25%	38%	17%	38%	55%
Dati biometrici (impronte digitali, voce, riconoscimento facciale, ecc.)	11%	21%	39%	23%	32%	62%
Autenticazione a due fattori	11%	21%	39%	20%	32%	59%

Base: 429 decisori globali responsabili della sicurezza di infrastrutture critiche, della protezione a livello IP, di tecnologie IoT e/o SCADA
Fonte: studio commissionato da Fortinet a Forrester Consulting, gennaio 2018

Figura 1: la maggior parte degli operatori SCADA/ICS registra e analizza continuamente il traffico di rete, mentre poco più della metà utilizza l'analisi dei dispositivi per la sicurezza degli endpoint.

Molti operatori SCADA/ICS ignorano gli strumenti di sicurezza di base.

Il 45% non utilizza il controllo degli accessi basato sui ruoli.

In questo modo si lasciano varchi aperti per le minacce interne.

Sfide per la sicurezza SCADA/ICS

Le organizzazioni che si affidano a tecnologie SCADA/ICS sembrano avere dubbi sull'uso del cloud da parte dei fornitori di tali sistemi. In particolare, le organizzazioni sono preoccupate per l'uso da parte dei dipendenti di tecnologie personali e cloud che possono connettersi ai loro sistemi SCADA/ICS.

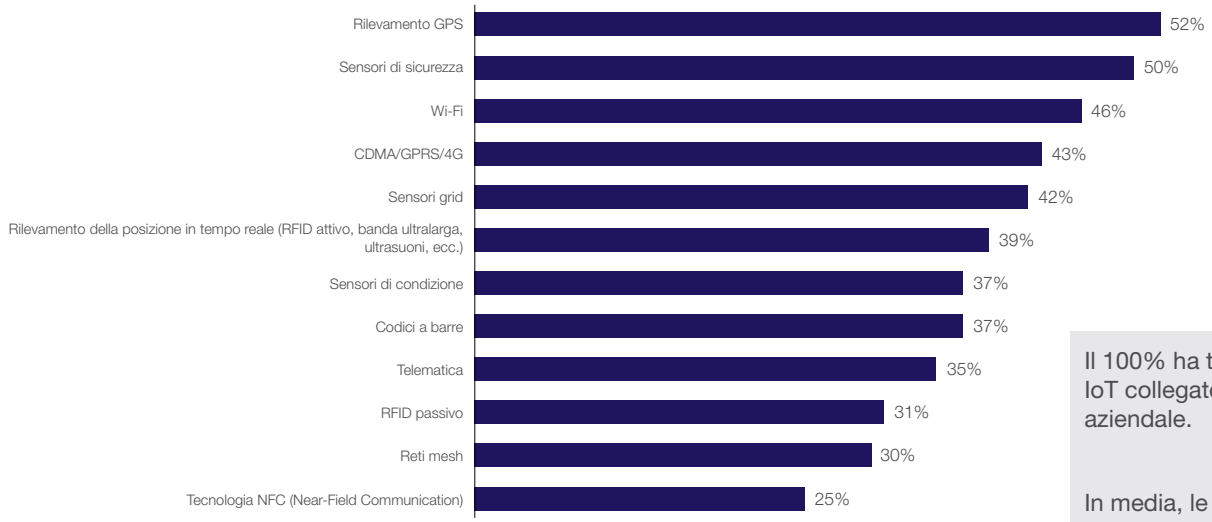
Nonostante le organizzazioni vedano diversi rischi potenziali per la sicurezza, alcune delle loro azioni possono introdurre ulteriori problemi. In particolare, molte organizzazioni consentono a un numero considerevole di **tecnologie wireless e IoT di connettersi alle loro reti**, creando vulnerabilità aggiuntive. Ogni azienda intervistata nello studio Forrester riferisce di avere alcune tecnologie IoT o wireless collegate alla propria rete, che possono includere connessioni ai sistemi SCADA/ICS. Il rischio è certo, con una media di 4,7 tecnologie IoT collegate.

Il Wi-Fi è un problema altrettanto importante. Oltre il **40%** delle organizzazioni ha dispositivi Wi-Fi, dispositivi mobili e sensori grid collegati. Molte di queste connessioni portano a complicazioni per le organizzazioni che cercano di gestire la convergenza delle loro infrastrutture IT e OT, l'hardware e il software su cui si basano i sistemi SCADA e ICS. Inoltre, quasi **tre quarti** delle organizzazioni hanno almeno connessioni di base tra IT e OT, un possibile campanello di allarme per quanto riguarda la loro protezione dalle minacce.

Le preoccupazioni sulla convergenza tra IT e OT variano. Circa **4 organizzazioni su 10** temono di non avere, o che i loro partner per la sicurezza non abbiano, le competenze necessarie per proteggere i sistemi IT e OT. Un altro **39%** si preoccupa per le fughe di dati sensibili e **un terzo** è preoccupato di possibili exploit di backdoor nei dispositivi collegati. Un altro potenziale problema per le organizzazioni che gestiscono SCADA/ICS è il livello di accesso fornito ai partner tecnologici e commerciali. Questo accesso offre agli hacker un'altra via d'attacco.

Tecnologie IoT attualmente connesse alla rete

D13: Quali delle seguenti tecnologie IoT sono attualmente connesse alla tua rete aziendale? (Seleziona tutte le risposte applicabili)



Il 100% ha tecnologie IoT collegate alla rete aziendale.

In media, le aziende hanno 4,7 tecnologie collegate alla loro rete.

Base: 429 decisori globali responsabili della sicurezza di infrastrutture critiche, della protezione a livello IP, di tecnologie IoT e/o SCADA
Fonte: studio commissionato da Fortinet a Forrester Consulting, gennaio 2018

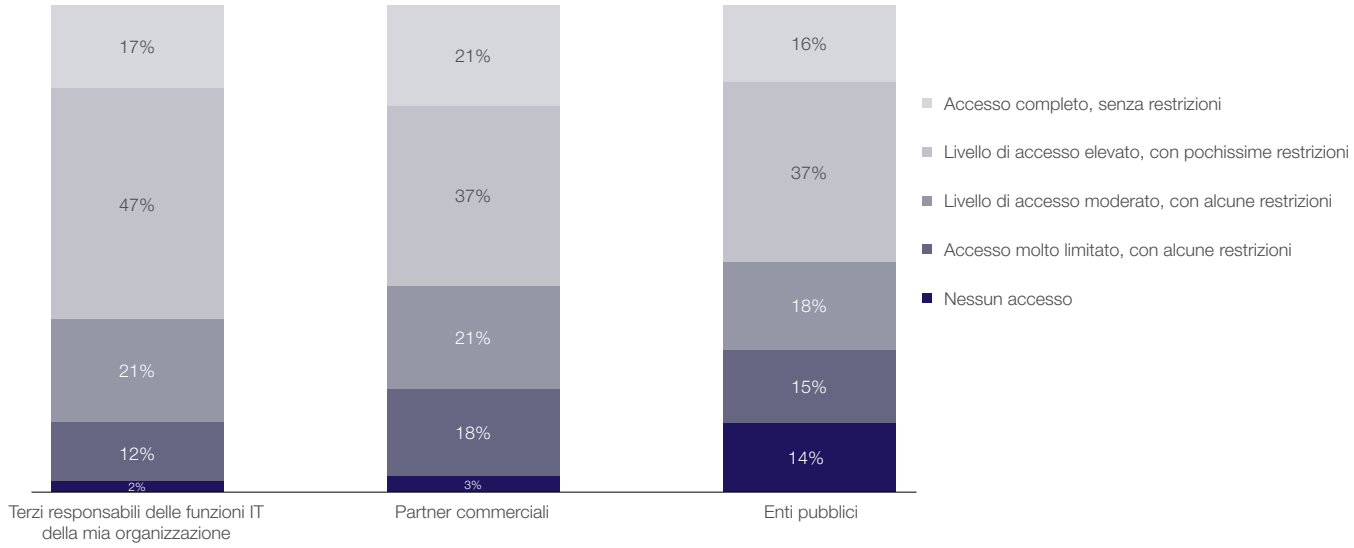
Figura 2: la maggior parte degli utenti SCADA/ICS ha un gran numero di altre tecnologie collegate alle loro reti.

Ad esempio, il **64%** delle organizzazioni concede ai fornitori IT esterni un accesso completo o di alto livello ai propri sistemi SCADA/ICS. Ma il problema non inizia con il primo livello delle relazioni: quasi il 60% concede ad altri partner commerciali un accesso completo o di alto livello e più del **50%** accorda lo stesso livello di accesso agli enti pubblici. Nella suddivisione per settori, le industrie manifatturiere sono le più inclini a fornire un accesso completo a organizzazioni esterne.

A questo rischio potenziale si somma il fatto che molte organizzazioni esternalizzano parte della gestione della sicurezza SCADA/ICS. Le principali funzioni SCADA/ICS esternalizzate a fornitori IT sono la sicurezza wireless, il rilevamento delle intrusioni, il controllo degli accessi alla rete e la sicurezza dell'IoT. E l'outsourcing è un fenomeno tutt'altro che isolato: il **56%** delle organizzazioni intervistate affida la sicurezza SCADA a più fornitori esterni. In alcuni casi, l'uso di più fornitori crea un **coacervo di difese che non funzionano bene insieme.**

La maggior parte delle organizzazioni concede a soggetti esterni un accesso completo o di alto livello

D3: Cosa descrive meglio il livello di accesso ai sistemi SCADA/ICS concessi dalla tua organizzazione alle entità seguenti?



Base: 429 decisori globali responsabili della sicurezza di infrastrutture critiche, della protezione a livello IP, di tecnologie IoT e/o SCADA
Fonte: studio commissionato da Fortinet a Forrester Consulting, gennaio 2018

Figura 3: molti utenti SCADA/ICS concedono ai fornitori di tecnologia e ad altri partner commerciali un accesso di alto livello ai loro sistemi.

Le organizzazioni che gestiscono SCADA/ICS aprono i loro sistemi ai loro partner.

Il 64% concede ai fornitori IT esterni un accesso completo o di alto livello.

Le vulnerabilità del vostro fornitore IT possono diventare le vostre.

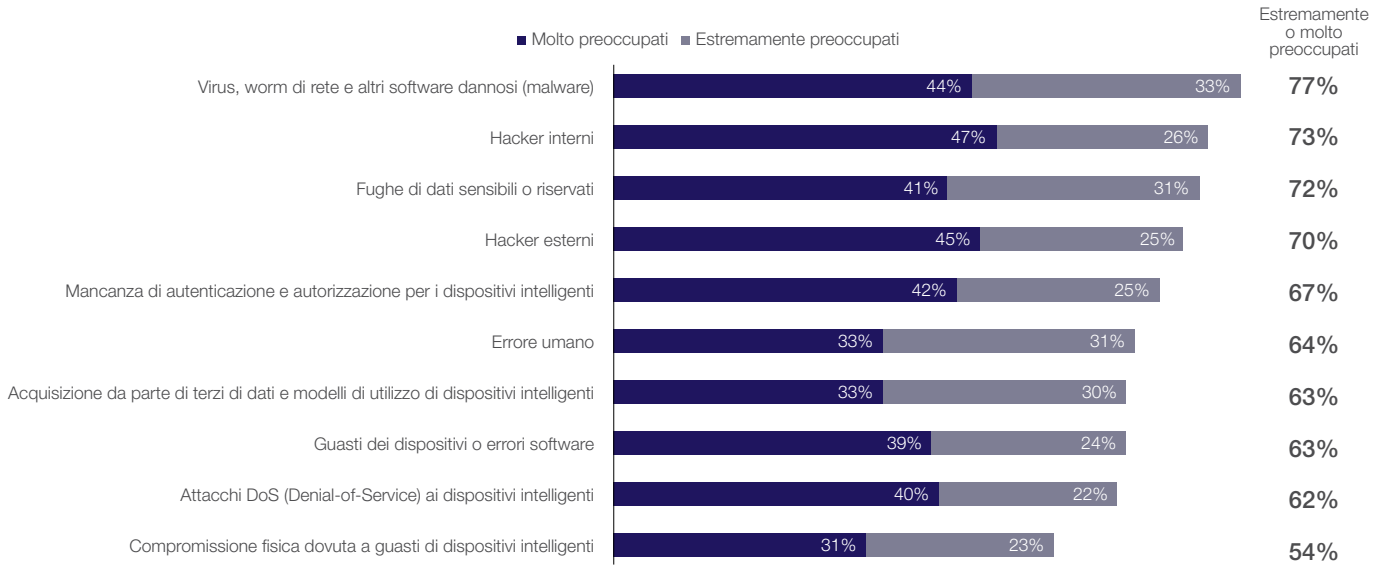
Minacce alle reti SCADA e ICS

Oltre alle domande sulle policy interne, lo studio di Forrester ha posto alle organizzazioni che gestiscono reti SCADA/ICS domande sulle minacce più gravi alla sicurezza. Gli operatori vedono più minacce provenienti da diverse fonti, con il malware e le fughe interne di dati in cima alle preoccupazioni sulla sicurezza. Più di **tre quarti** delle organizzazioni riconoscono di essere molto o estremamente preoccupate per il malware esterno. Più di **7 su 10** sono molto o estremamente preoccupate per gli hacker interni, la fuga di dati sensibili e gli hacker esterni. Più di **due terzi** sono preoccupate per la mancanza di autenticazione o autorizzazione per i dispositivi intelligenti e quasi due terzi per gli errori umani e per l'acquisizione di dati e modelli di utilizzo dei dispositivi da parte di terzi.

Le preoccupazioni per il malware e gli hacker interni sono cresciute rispetto a uno studio simile condotto nel 2016. E mentre da allora il panorama delle minacce si è notevolmente evoluto e il livello di rischio per i sistemi SCADA/ICS è aumentato, gli operatori di tali sistemi percepiscono in realtà una diminuzione dei rischi. Attribuiscono ad esempio minore importanza agli errori umani, all'acquisizione di informazioni da parte di terzi, ai guasti dei dispositivi e agli errori software, anche se ciò può essere dovuto all'aumentata percezione dei rischi per la sicurezza provenienti da altre fonti.

Le preoccupazioni di sicurezza vanno da virus e hacker a fughe di dati e mancanza di autenticazione

D7: Valuta il tuo livello di preoccupazione sugli aspetti seguenti della sicurezza della rete SCADA/ICS aziendale.



Base: 429 decisori globali responsabili della sicurezza di infrastrutture critiche, della protezione a livello IP, di tecnologie IoT e/o SCADA
Fonte: studio commissionato da Fortinet a Forrester Consulting, gennaio 2018

Figura 4: gli operatori SCADA/ICS sono preoccupati per il malware, gli hacker interni e diverse altre minacce.

Oltre il
70% delle organizzazioni OT
è estremamente preoccupato per gli hacker interni, la fuga di dati sensibili e gli hacker esterni.

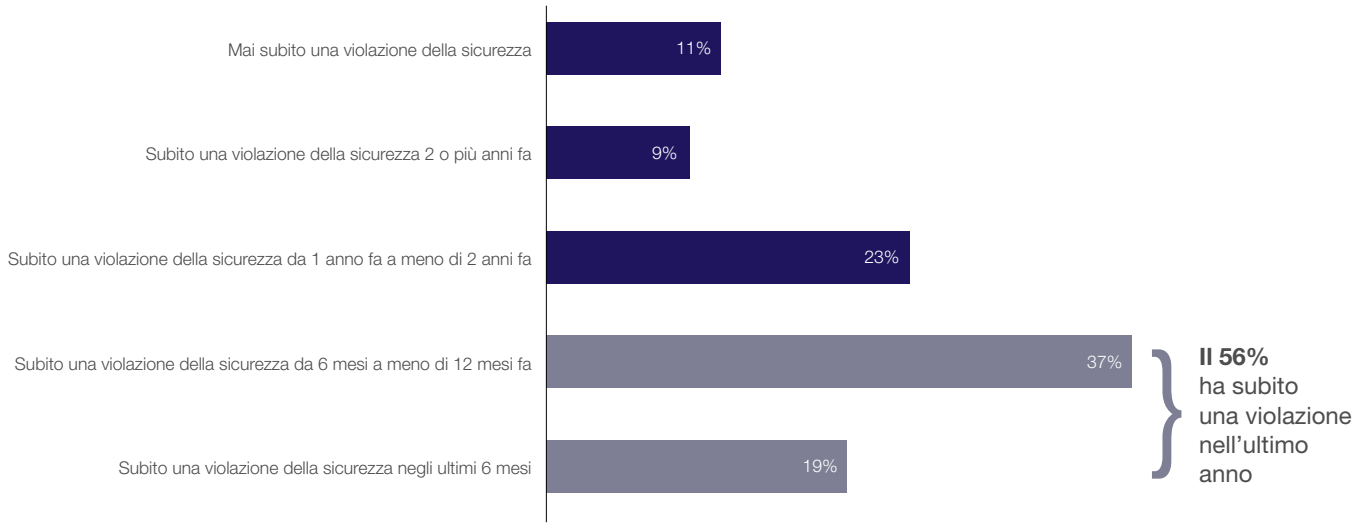
L'impatto delle minacce

Anche se molte organizzazioni attuano più pratiche di sicurezza, le violazioni delle reti SCADA/ICS sono comuni. Ad esempio, il **56%** degli intervistati ha segnalato una violazione SCADA/ICS **nell'ultimo anno e un altro** 32% ha subito una violazione in precedenza. Rimane quindi solo una piccola percentuale che afferma di non aver mai subito una violazione.

Le violazioni dei sistemi SCADA/ICS hanno conseguenze gravi. Il **63%** delle organizzazioni afferma che una violazione della sicurezza SCADA/ICS ha avuto un impatto elevato o critico sulla sicurezza dei propri dipendenti. Un altro **58%** riferisce conseguenze serie sulla stabilità finanziaria della propria organizzazione e il **63%** rileva un serio freno alla propria capacità di operare a un livello accettabile.

Il 56% delle organizzazioni ha subito una violazione della sicurezza dei sistemi SCADA/ICS negli ultimi 12 mesi

D8: Per quanto a tua conoscenza, i sistemi SCADA/ICS della tua organizzazione hanno subito una violazione della sicurezza?



Base: 429 decisori globali responsabili della sicurezza di infrastrutture critiche, della protezione a livello IP, di tecnologie IoT e/o SCADA
Fonte: studio commissionato da Fortinet a Forrester Consulting, gennaio 2018

Figura 5: la maggior parte degli utenti SCADA/ICS ha subito una violazione dei sistemi nell'ultimo anno.

Le violazioni dei sistemi SCADA/ICS sono comuni.

Il 56% degli operatori SCADA/ICS ha segnalato una violazione nell'ultimo anno.

Le violazioni compromettono la sicurezza dei dipendenti e la stabilità finanziaria delle organizzazioni.

Raccomandazioni sull'attenuazione dei rischi

Molte organizzazioni vedono diverse opzioni per attenuare i problemi di sicurezza dei sistemi SCADA/ICS. Quasi la metà ritiene che una valutazione completa del rischio aziendale o operativo sia il modo ottimale per migliorare la propria strategia di gestione del rischio nel contesto della convergenza dei sistemi OT e IT. Altri approcci comuni per l'attenuazione del rischio sono l'applicazione di standard comuni, una maggiore centralizzazione della gestione dei dispositivi e la richiesta di consulenza a enti governativi come l'Industrial Control Systems Cyber Emergency Response Team (ICS-CERT).

Alla domanda sulla scelta di un fornitore di sicurezza per i sistemi SCADA/ICS, poco più della metà delle organizzazioni ritiene che i consulenti tecnologici forniscano informazioni affidabili. Ad esempio, i fornitori e i partner SCADA/ICS ottengono un punteggio di poco superiore al **50%** per quanto riguarda la fiducia ottenuta.

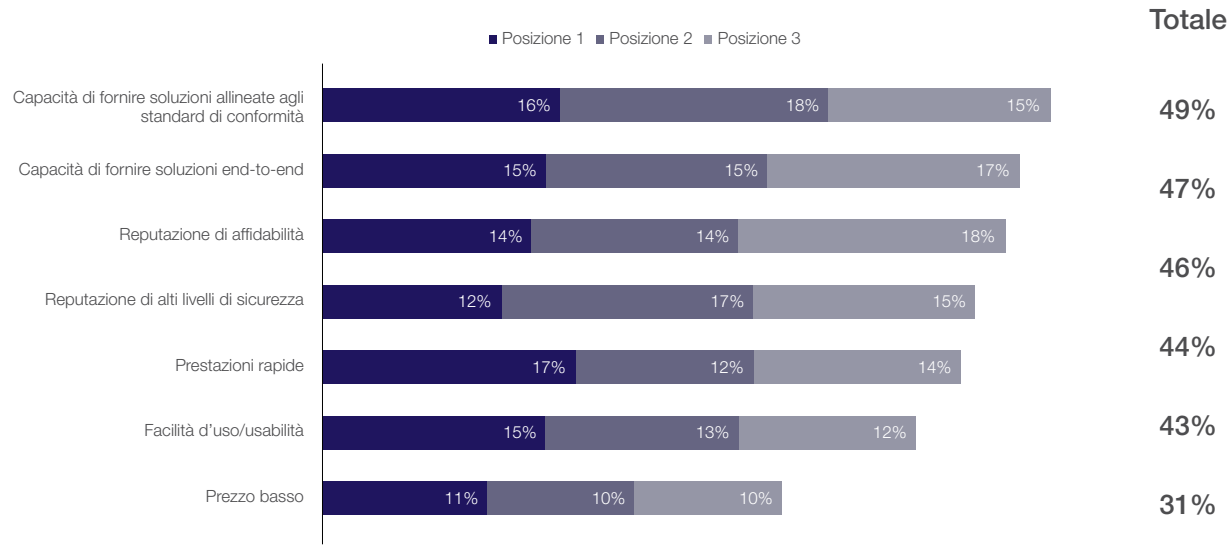
Per la valutazione dei fornitori e delle tecnologie di sicurezza, le organizzazioni devono considerare la loro capacità di fornire:

- Prestazioni rapide
- Capacità di rispettare gli standard di conformità
- Soluzioni complete end-to-end

Una reputazione di affidabilità e di alti livelli di sicurezza ha ottenuto un punteggio elevato tra le organizzazioni. La conformità agli standard di settore e di sicurezza è una delle principali preoccupazioni: quasi la metà delle organizzazioni intervistate ha indicato nella capacità di rispettare gli standard di conformità il fattore principale nella scelta delle soluzioni di sicurezza. La capacità di fornire soluzioni end-to-end è al secondo posto nell'elenco dei fattori discriminanti. È interessante notare che solo **3 su 10** hanno citato il basso costo come fattore principale.

Il rispetto degli standard di conformità, la fornitura di soluzioni end-to-end e l'affidabilità sono gli aspetti più importanti nella selezione di un fornitore

D20: Nella valutazione dei fornitori di sicurezza per i sistemi SCADA/ICS della tua organizzazione, quali dei seguenti fattori, se presenti, hanno il maggior peso? (Classifica i primi tre)



Base: 429 decisori globali responsabili della sicurezza di infrastrutture critiche, della protezione a livello IP, di tecnologie IoT e/o SCADA
Fonte: studio commissionato da Fortinet a Forrester Consulting, gennaio 2018

Figura 6: gli utenti SCADA/ICS hanno diverse priorità per i fornitori di sicurezza, tra cui la capacità di rispettare gli standard di conformità e di fornire soluzioni end-to-end.

La strada da seguire

Molte organizzazioni che impiegano sistemi SCADA/ICS prevedono quest'anno di aumentare la spesa per le relative tecnologie di sicurezza. Chi non ha intenzione di aumentare il proprio budget rischia di rimanere indietro. Quasi tre quarti delle organizzazioni prevedono di aumentare la spesa per la sicurezza dell'IoT e il 36% delle organizzazioni l'aumenterà del 5% o più. Oltre 7 su 10 prevedono di spendere di più per la sicurezza OT e quasi **4 su 10** prevedono di aumentare la spesa di almeno il 5%. Altre **7 su 10** spenderanno quest'anno di più per le infrastrutture OT, con il 37% che prevede un aumento del 5% e oltre. Questi investimenti sono indice di un impegno costante e crescente nella tecnologia OT e negli standard e controlli di sicurezza necessari per proteggerla.

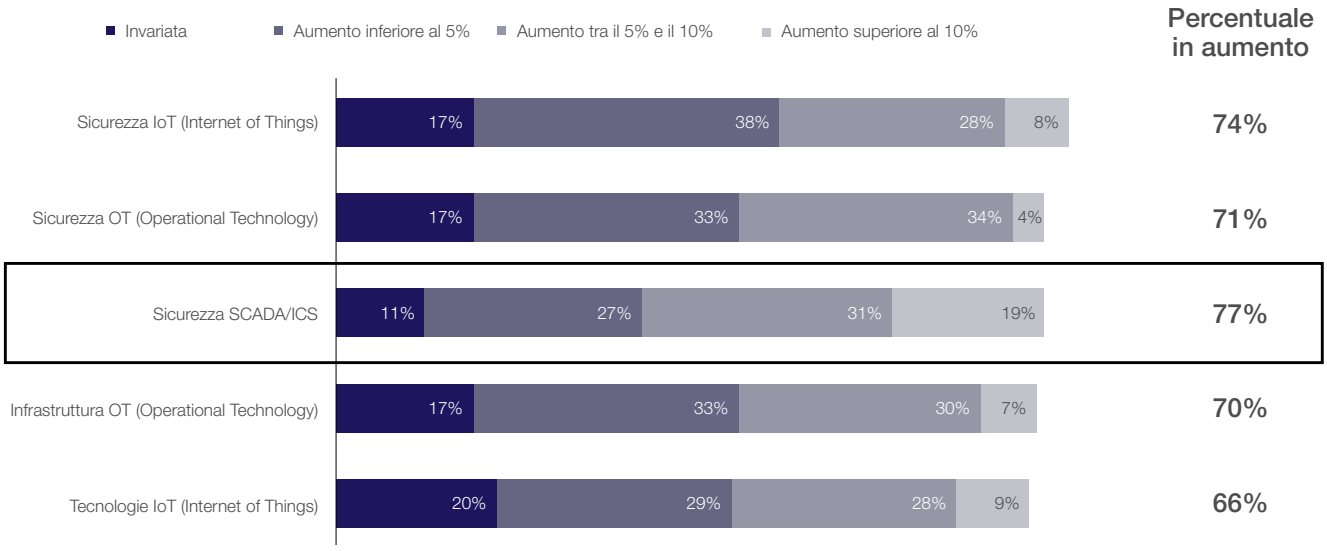
Nel considerare le misure di sicurezza in cui investire, gli operatori SCADA/ICS possono prendere diverse iniziative per proteggere le loro risorse, fra cui:

- Segmentare le reti separando le tecnologie wireless e IoT collegate dai sistemi SCADA/ICS
- Proteggere l'infrastruttura di rete, compresi switch, router e reti wireless, attraverso firewall e altri strumenti di protezione progettati per tali risorse
- Applicare policy di gestione di identità e accessi per tenere gli estranei fuori dalla rete e per impedire ai dipendenti di accedere a parti della rete non necessarie per il loro lavoro
- Utilizzare un Web Application Firewall (WAF) per eseguire scansioni e patch di applicazioni Web non protette
- Distribuire protezione degli endpoint per fornire in tempo reale funzionalità utili all'azione di intelligence e visibilità sulle minacce

Tenuto conto del potenziale impatto sulla sicurezza fisica di dipendenti o clienti, le considerazioni di sicurezza per SCADA/ICS devono essere diverse da quelle dei sistemi IT tradizionali. L'aspetto positivo è che, adottando un approccio multilivello alla sicurezza SCADA/ICS, le organizzazioni possono migliorare significativamente i loro livelli di sicurezza e quindi ridurre i rischi.

La spesa per la sicurezza SCADA/ICS sta aumentando più che in altre aree

D20: Nella valutazione dei fornitori di sicurezza per i sistemi SCADA/ICS della tua organizzazione, quali dei seguenti fattori, se presenti, hanno il maggior peso? (Classifica i primi tre)



Base: 429 decisori globali responsabili della sicurezza di infrastrutture critiche, della protezione a livello IP, di tecnologie IoT e/o SCADA
Fonte: studio commissionato da Fortinet a Forrester Consulting, gennaio 2018

Figura 7: molti operatori SCADA/ICS prevedono di aumentare la spesa per la sicurezza in diverse aree nel 2018.

Riferimenti

[1] Joe Weiss, "Industrial control systems: The holy grail of cyberwar," The Christian Science Monitor, 24 marzo 2017.

[2] Kim Zetter, "Inside the Cunning, Unprecedented Hack of Ukraine's Power Grid," WIRED, 3 marzo 2016.

[3] John Leyden, "Water treatment plant hacked, chemical mix changed for tap supplies," The Register, 24 marzo 2016.

[4] "Global Industrial Controls System Market to Grow at CAGR of 4.9% from 2015 to 2021," Transparency Market Research, settembre 2015.

[5] Mark Fabro, "Industrial Control Systems Cyber Security," Presentazione al Dipartimento della difesa statunitense, 7 giugno 2017.

[6] "SCADA Market Worth 13.43 Billion USD by 2022," MarketsandMarkets, consultato il 12 aprile 2019.

www.fortinet.com

luglio 10, 2019 11:26 AM

373566-A-1-IT

D:\ARGOS\2019\07_2019\Assignment A-344888-924146\Work\PAKIET\OT\CISO\Report-OT-Forrester_Updated\report-operational-technology-forrester_A4_it_IT\report-operational-technology-forrester_A4_it_IT