Sistemi di controllo industriale: il primo rischio sono le persone

Author : Enzo Maria Tieghi

Date : 9 Luglio 2019

Le persone rappresentano il maggior rischio per la compromissione di sistemi OT/ICS: l'elemento umano è quasi sempre al centro di incidenti e violazioni di cybersecurity.

Nella nuova edizione del *SANS 2019 State of OT/ICS Cybersecurity Survey*, pubblicato a giugno 2019 e curato da Barbara Filkins, si possono trovare interessanti spunti sulla percezione del rischio OT/ ICS Cyber nelle aziende, su come vengono fissati i confini tra sistemi OT, IT e sistemi esterni, su come sono adottate le contromisure di Sicurezza OT/ICS e su dove si posiziona la Cybersecurity per la convergenza OT/IT.

Aziende più mature, ma il rischio resta alto

Tra i 338 intervistati a livello globale, oltre il 50% ha valutato il livello di rischio cyber OT/ICS della propria azienda come critico o alto. È un dato in calo rispetto al 69% dell'ultimo sondaggio, condotto nel 2017: questo potrebbe sembrare un po' sorprendente, visto l'aumento di attacchi informatici e violazioni dei dati (come anche segnalato dalle analisi di Clusit).

Questi numeri indicano che le aziende sono più coinvolte; che, sul tema della cybersecurity in ambito OT/ICS, stanno diventando più mature e che il livello di rischio è valutato come inferiore rispetto al passato.

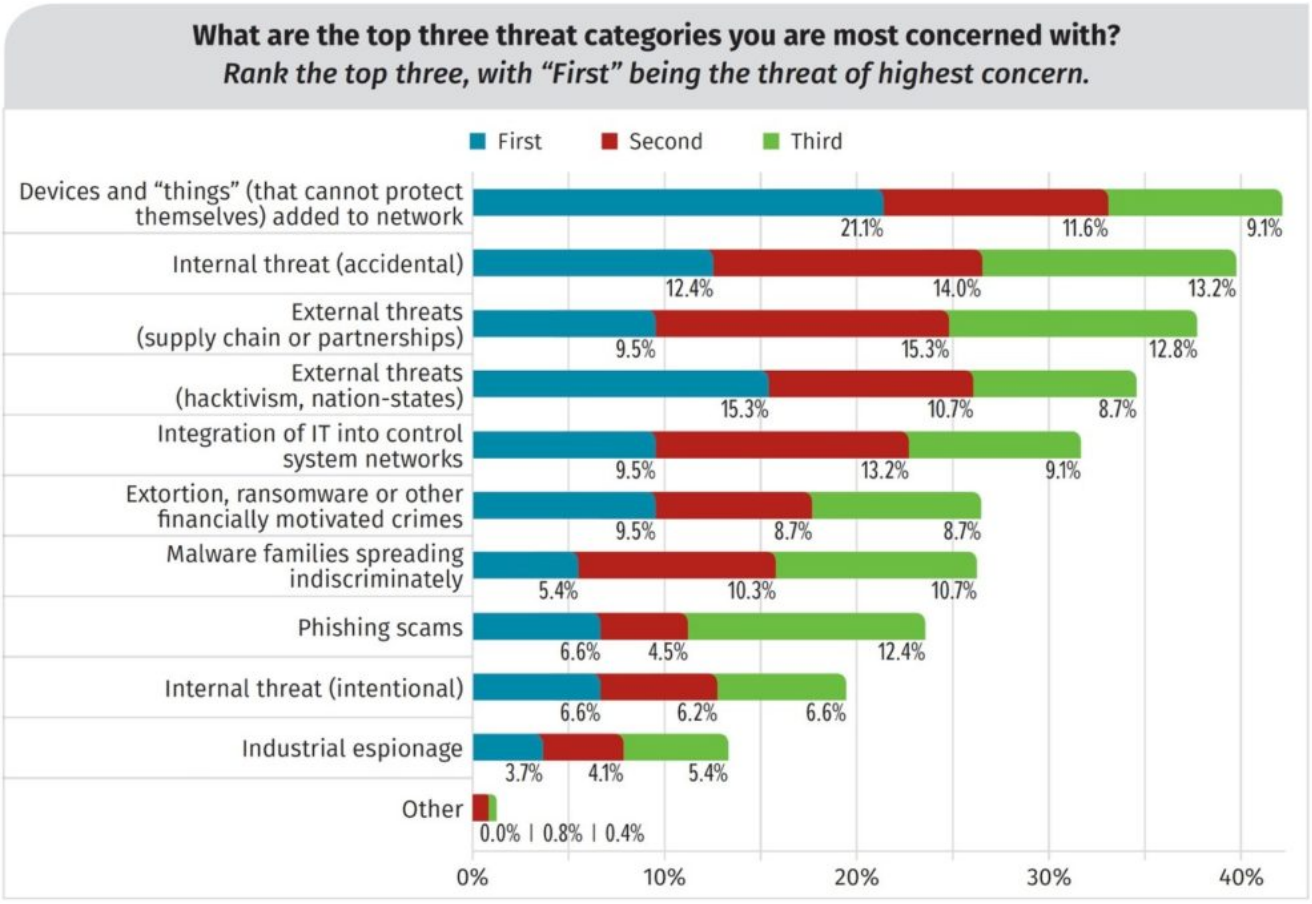
Allo stesso tempo, tuttavia, la sfida per proteggere i sistemi OT/ICS si sta allargando quanto le dimensioni della superficie di attacco: i confini di reti e sistemi OT/ICS sono sempre più ampi in quanto *"…connessi e interdipendenti, e si scambiano anche dati e informazioni con una miriade di altri sistemi e processi".*

Il rapporto sottolinea che alcune applicazioni mobili stanno sostituendo le applicazioni di *workstation* di ingegneria, quindi la relativa gestione del rischio dovrebbe essere trattata a un livello più alto.

Inoltre, l’uso di dispositivi mobili e del wireless è sempre più diffuso per trasferire i dati dai sensori a reti e operatori di impianto: ciò aumenta ulteriormente la superficie di attacco ed espone a gravi conseguenze se compromessa.

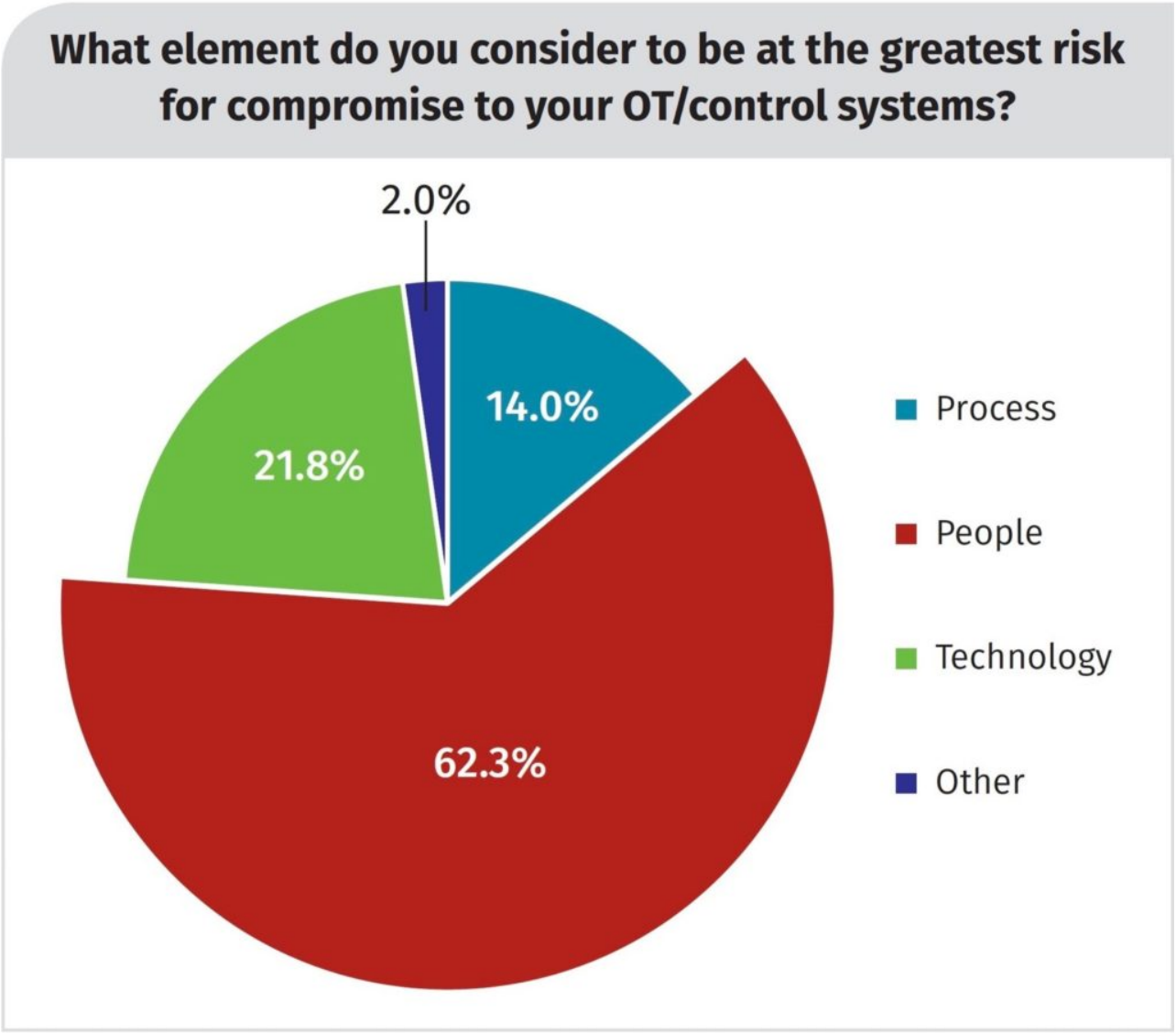
Il rischio più grosso? Sempre le persone!

Il rischio, ovviamente, guida l’approccio delle organizzazioni alla sicurezza dei sistemi OT/ICS: circa il 50% degli intervistati giudica il livello del rischio cyber OT/ICS come alto/critico se riferito al profilo di rischio complessivo della propria azienda.



Le persone rappresentano il maggior rischio (62%) per la compromissione di sistemi OT/ICS; questo non sorprende, perché l’elemento umano è quasi sempre al centro di incidenti e delle violazioni alla cybersecurity. Troviamo poi, a una certa distanza, la tecnologia (22%) e il processo (14%).

Il report solleva **un’interessante domanda** sul perché il processo come categoria di rischio non sia superiore, possibilmente superiore alla tecnologia. La progettazione e l’implementazione del processo industriale rappresentano elementi chiave nelle scelte e implementazioni delle architetture OT/ICS e delle tecnologie da utilizzare.



Le persone rappresentano un’ampia categoria di rischio, che comprende esterni e attori interni, con azioni intenzionali (danneggiamenti e sabotaggi) e non intenzionali (incidenti, errori e incuria).

OT/ICS Security by Visibility

Avere una chiara visibilità di ciò che avviene nella rete di fabbrica e sui dispositivi OT/ICS è un elemento fondamentale in un robusto programma di cybersecurity. Inoltre, la necessità di definire e proteggere il confine tra IT e OT include la necessità di visualizzare e monitorare le risorse di sistema all’interno del perimetro.

Il report *SANS 2019 State of OT/ICS Cybersecurity Survey* indica una crescente richiesta per una **maggiore visibilità di asset cyber dei sistemi di controllo**: questa è una tendenza per i prossimi 12-18 mesi.

In effetti, la necessità di identificare le risorse all'interno di una rete di controllo industriale è un fattore chiave per molte aziende industriali e *utility*.

Per esperienza abbiamo visto che non è insolito, per il team, chiedere ed effettuare un *Proof of Concept* (PoC) per fare "Asset Discovery" e "Vulnerability Assessment": al primo incontro i responsabili indicano che sulla propria rete di fabbrica hanno connesso - diciamo - 200/300 dispositivi.

Poi, quando il *tool* di individuazione degli asset viene installato, si identificano rapidamente oltre 5-600 dispositivi (a volte anche molti di più!).

E dopo diverse installazioni, è quindi normale scoprire una grande discrepanza tra il numero di dispositivi connessi percepiti rispetto al numero reale.

Sfida delle persone e convergenza IT/OT

Il report citato mette in luce le sfide per le persone coinvolte e il miglioramento della cybersecurity OT/ICS: è interessante notare che le organizzazioni stanno aumentando lo staff di personale interno per i loro programmi di cybersecurity. È un altro indicatore della maturazione dei processi che circondano la cybersecurity industriale.

La cybersecurity interna OT richiede che IT e OT lavorino insieme, anche se allineare le priorità e assicurare la cooperazione e la comunicazione tra i team non è, tuttavia, semplice.

Secondo i risultati del sondaggio SANS, l'IT assume un ruolo guida nella gestione della politica di sicurezza aziendale e nell'attuazione dei controlli necessari, anche nel dominio dell'OT, mentre OT spesso controlla il budget per la salvaguardia dei sistemi OT/ICS stessi.

Gli obiettivi di questi due domini non sono ben allineati: la *governance* IT e la gestione dei rischi si concentrano sulla continuità, sulla protezione delle informazioni e della reputazione (privacy e GDPR), mentre l'OT si concentra sulla Safety e affidabilità dei processi cyber-fisici in produzione.

Per garantire la collaborazione e ridurre i rischi per l'organizzazione, è necessaria una comprensione comune di questi concetti chiave.

I budget di spesa per la cyber security IT e OT/ICS

Dal 2017, i budget per la sicurezza di OT/ICS sono cambiati dall'essere principalmente condivisi tra IT e OT, ad oggi dove:

- Il 48,7% degli intervistati ha dichiarato che il proprio budget è controllato da OT, con un aumento del 18% dal 2017;
- Il 31,6% degli intervistati ha dichiarato che il budget è controllato dall'IT, con un aumento del 14,5% rispetto al 2017;

- Il 29,4% degli intervistati ha dichiarato che il controllo del budget è ancora condiviso tra IT / OT, ??in calo del 9,1% dal 2017.

Table 9. Organization Controlling OT/Control System Budget 2017 vs. 2019

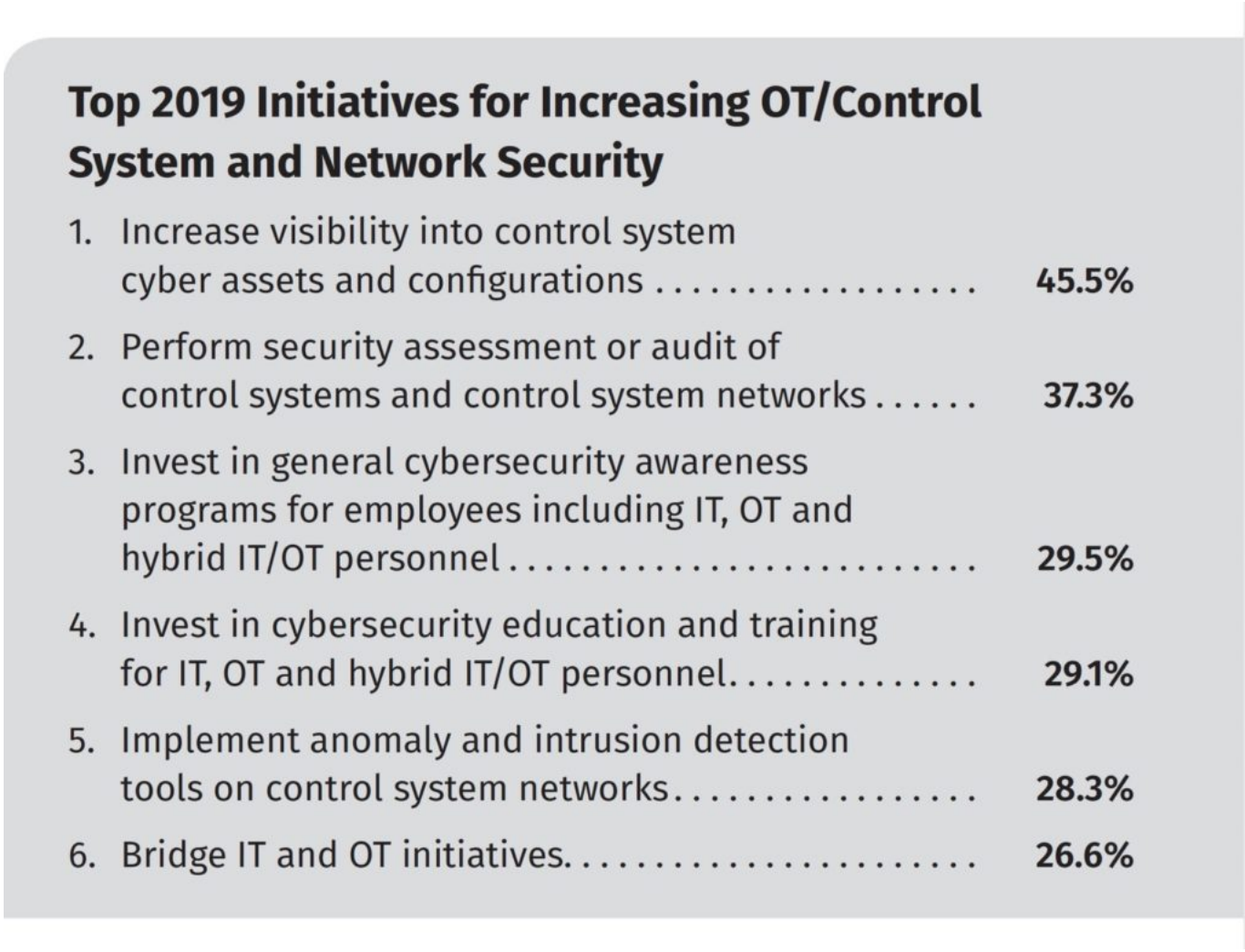
Organization Controlling Budget	2017	2019	% Change
Operations	30.8%	48.7%	+17.9%
Enterprise IT	17.1%	31.6%	+14.5%
Shared budget between IT/OT	38.5%	29.4%	-9.1%

Quando il budget è detenuto da uno o dall'altro, è essenziale che i gruppi lavorino insieme per dare priorità alle persone, ai processi e alle misure tecnologiche che saranno al centro di un piano annuale di miglioramento della cybersecurity.

Quali le prime scelte per la protezione di reti e sistemi OT/ICS?

Ecco alcune indicazioni sui trend (dal campione della Survey) per le scelte fatte e da fare per il 2019 per migliorare la sicurezza dei sistemi OT/ICS:

- al primo posto, i *tool* per aumentare la visibilità su asset e configurazioni di sistemi OT/ICS (45,5%);
- fare *security assessment* e/o audit su sistemi e reti OT/ICS (37,3%);
- investire in programmi di cybersecurity awareness/training che includano OT/ICS (29,5% e 29,1%);
- installare tool per anomaly/intrusion detection su reti e sistemi OT/ICS (28,3%).



Come si vede, un mix di attività da fare e *tool* da implementare per rafforzare in modo consistente la protezione dal rischio cyber di reti e sistemi di fabbrica e impianto, sia nell'industria che nelle *utility*.

Quali gli standard e le *best practices* più utilizzati per proteggere OT/ICS?

Riguardo a framework e regolamentazioni di riferimento per la OT/ICS cyber security abbiamo la conferma, come **prima scelta**, del NIST CSF (Cyber Security Framework) menzionato dal 38,1% degli intervistati.

Abbiamo poi menzionati tra i più utilizzati le ISO2700x, NIST SP800-53, NIST SP800-82m ed ISA/IEC62443. Interessante il "debutto nell'elenco della Direttiva NIS europea con un 8,3%.

Table 8. Top 10 Regulations, Standards, Best Practices Used

Rank	Regulation	% Response
1	NIST CSF (Cyber Security Framework)	38.1%
2	ISO 27000 series	32.0%
3	NIST 800-53	31.4%
4	NIST 800-82	30.9%
5	ISA/IEC 62443	30.4%
6	CIS Critical Security Controls	29.9%
7	NERC CIP	23.7%
8	GDPR	15.5%
9	C2M2 (Cybersecurity Capability Maturity Model)	10.3%
10	NIS Directive (EU)	8.3%

IT e OT/ICS, come lavorare insieme

Il report *SANS 2019 State of OT/ICS Cybersecurity Survey* è un documento prezioso per tutti quelli che si occupano di sicurezza OT/ICS e, probabilmente, può aiutare a chiedere e ottenere impegno e budget più forti da parte del management delle aziende: con le sue analisi, infatti, ci indica dove si trovano le difficoltà, ricordandoci che la nostra azienda non è l'unica organizzazione alle prese con la sfida di migliorare la resilienza informatica operativa e la cybersecurity OT/ICS.

Articolo a cura di **Enzo Maria Tieghi**