Zero trust negli ambienti OT: perché l’air gap non basta più

Dalla fine dell’air gap alla necessità, problematica dello Zero Trust OT.

Con questo articolo si apre una serie in otto parti dedicata al paper «**Zero Trust selettivo negli ambienti OT: modello MATRIX**» di **Vincenzo Calabrò**, *Funzionario alla Sicurezza CIS del Ministero dell’Interno*. Il paper propone MATRIX, un metodo per decidere quali controlli zero trust applicare a ciascun dispositivo di un impianto industriale e con quale priorità.

In questa prima parte l’autore presenta il problema. La convergenza tra IT e OT ha cancellato l’isolamento su cui si reggeva la sicurezza degli impianti. Lo zero trust, nato per le reti aziendali, è la risposta naturale, ma non si può trasferire così com’è dove contano disponibilità, tempo reale e sicurezza delle persone.

Zero Trust OT: il ruolo del framework MATRIX

La trasformazione digitale delle infrastrutture critiche ha eroso la tradizionale separazione tra le reti informatiche aziendali (Enterprise Information Technology, EIT) e i sistemi di automazione industriale (Operational Technology, OT), esponendo gli impianti progettati per operare in isolamento a minacce sempre più sofisticate. Il paradigma zero trust, basato sul principio “never trust, always verify”, è diventato un punto di riferimento per la sicurezza dell’EIT, ma la sua applicazione diretta agli ambienti OT è ostacolata da differenze sostanziali in termini di architettura, vincoli di

tempo reale e requisiti di sicurezza, nonché dalla presenza diffusa di tecnologie legacy. Questo studio propone MATRIX, un framework metodologico per l'adozione selettiva e mission-driven dei controlli zero trust in ambienti OT eterogenei.

Il framework, suddiviso in sei fasi (caratterizzazione del contesto di missione, profilazione dell'idoneità degli asset, modellazione delle minacce, analisi dei compromessi, implementazione tramite matrice di allocazione delle capacità ed esecuzione con evoluzione incrementale della maturità), collega in modo esplicito la comprensione dell'ambiente operativo alla selezione dei controlli tecnicamente sostenibili per ciascuna classe di asset. La metodologia integra i principi normativi consolidati (NIST SP 800-207, NIST SP 800-82r3, ISA/IEC 62443) e la letteratura scientifica più recente e viene illustrata mediante uno scenario applicativo relativo alle sottostazioni elettriche digitali. I risultati attesi includono la riduzione della superficie d'attacco, il contenimento del movimento laterale e la gestione esplicita del rischio residuo associato ai componenti non aggiornabili.

Convergenza IT/OT e fine dell'air gap

Per decenni, la sicurezza dei sistemi di controllo industriale si è basata su un presupposto rassicurante, ma fragile: l'isolamento fisico. Le reti che governano impianti energetici, sistemi idrici, processi manifatturieri e infrastrutture di trasporto erano concepite come enclavi separate, protette da un air gap rispetto al mondo esterno e alle reti aziendali.

Tale separazione, già imperfetta in passato, si è progressivamente dissolta sotto la spinta della trasformazione digitale e della convergenza tra Information Technology (IT) e Operational Technology (OT). L'esigenza di analisi dei dati in

tempo reale, di manutenzione predittiva, di accesso remoto dei fornitori e di integrazione con i servizi cloud ha moltiplicato i punti di contatto tra i due domini, trasformando i sistemi, che un tempo erano opachi per l'attaccante, in bersagli raggiungibili.[1]

Perché il modello perimetrale non protegge più gli ambienti OT

Le conseguenze di questa esposizione non sono solo ipotesi accademiche. La scoperta di Stuxnet nel 2010 ha dimostrato che un'arma informatica può oltrepassare l'isolamento di un impianto e manipolare i controllori logici programmabili responsabili di un processo fisico, con conseguenze distruttive sul macchinario.[2]

Pochi anni dopo, l'attacco alla rete elettrica ucraina del dicembre 2015 provocò un'interruzione di corrente che coinvolse centinaia di migliaia di utenti, confermando la capacità degli avversari di colpire deliberatamente la distribuzione dell'energia.[3] La successiva ondata di campagne di ransomware contro le infrastrutture critiche, culminata con episodi che hanno paralizzato la logistica di approvvigionamento del carburante, ha messo in luce come le motivazioni economiche e geopolitiche possano convergere sullo stesso obiettivo.

Perché lo Zero Trust è diventato necessario negli ambienti OT

In risposta all'inadeguatezza delle difese perimetrali, è emerso così il paradigma zero trust, introdotto da Kindervag nel 2010 come superamento del modello "castello e fossato"[4] e successivamente formalizzato dal National Institute of Standards and Technology nella Special Publication 800-207.[5]

Lo Zero Trust sposta il baricentro della sicurezza dal confine

di rete alle risorse, alle identità e ai singoli flussi di accesso. Il suo principio fondamentale è che nessuna entità, che si tratti di un utente, di un dispositivo o di un servizio, debba godere di fiducia implicita solo in virtù della sua collocazione di rete; ogni richiesta di accesso deve essere autenticata, autorizzata e valutata dinamicamente prima e durante l'interazione con una risorsa.[6]

Zero Trust OT: disponibilità, integrità e safety cambiano le regole

Il modello si è dimostrato efficace nei contesti EIT, in cui la mobilità degli utenti, l'adozione del cloud e la diffusione di dispositivi personali avevano già reso obsoleto il concetto di perimetro. La sua applicazione agli ambienti OT, tuttavia, non è affatto immediata. I sistemi OT, infatti, ribaltano la gerarchia delle priorità in materia di sicurezza tipica dell'IT: se nell'IT prevale la riservatezza, nell'OT la gerarchia si capovolge a favore della disponibilità e dell'integrità, perché un'interruzione del processo fisico può tradursi in danni materiali, rischi per l'incolumità delle persone e interruzione di servizi essenziali.[7]

A ciò si aggiungono vincoli stringenti in termini di latenza, la necessità di un funzionamento continuo, l'uso di protocolli proprietari privi di autenticazione e la pervasiva presenza di dispositivi legacy progettati quando la connettività era un'eccezione e non la regola. Meccanismi che nell'IT si danno per scontati, come gli agenti software sugli endpoint, le scansioni antimalware e le frequenti riconfigurazioni delle policy, possono risultare semplicemente impraticabili su un relè di protezione che ha ancora decenni di servizio davanti a sé.

Solo di recente la comunità tecnica e normativa ha colmato questo vuoto. La revisione 3 della NIST SP 800-82 ha ampliato il proprio ambito di applicazione, estendendolo dall'insieme

ristretto dei sistemi di controllo industriale all'intera categoria dell'OT (Operational Technology) e aggiornando l'analisi delle minacce, delle vulnerabilità e delle contromisure.[8] Nel mese di ottobre 2024, la Cloud Security Alliance ha pubblicato una guida dedicata all'applicazione dei principi Zero Trust alle infrastrutture critiche, organizzata attorno a un processo in cinque fasi.[9]

A livello europeo, l'Agenzia dell'Unione europea per la cibersicurezza (ENISA) ha elaborato una guida tecnica per l'attuazione delle misure di gestione del rischio previste dalla direttiva NIS2,[10] mentre la ricerca del Software Engineering Institute sui sistemi OT ad alta criticità, nata per i sistemi di difesa con OT embedded ma di valenza generale, ha contribuito a tradurre i principi in pratica.[11] [12] Sul piano normativo, parallelamente, l'entrata in vigore della direttiva NIS2 e del suo recepimento nazionale ha trasformato l'adozione di adeguate misure di sicurezza per l'OT da una buona pratica ingegneristica a un obbligo giuridico per gli operatori dei settori essenziali, tra cui il settore energetico.[13] [14]

MATRIX: un approccio selettivo allo Zero Trust OT

Questi contributi forniscono principi solidi e, in alcuni casi, architetture di riferimento puntuali. Ciò che ancora manca è una metodologia strutturata e ripetibile che colleghi sistematicamente la comprensione dell'ambiente operativo alla selezione e all'allocazione granulare dei controlli Zero Trust, riconoscendo che in un impianto reale tali controlli non possono essere applicati in modo uniforme. La domanda fondamentale non è quale architettura Zero Trust adottare, ma quali capacità Zero Trust sono tecnicamente sostenibili per ciascuna classe di asset e con quale priorità rispetto alla missione.

Questo lavoro affronta questa lacuna proponendo MATRIX, un framework metodologico per l'adozione selettiva e orientata alla missione dello Zero Trust negli ambienti OT. L'acronimo riassume le sei fasi del processo: "Mission context", "Asset suitability", "Threat surface", "Risk tradeoff", "Implementation" ed "Execution". Il framework si basa su una matrice che associa le capacità Zero Trust alle classi di asset, ponderata in base alla criticità della missione e vincolata dal profilo di idoneità tecnica.

Il testo è organizzato come segue. La Sezione 2 ricostruisce i fondamenti dello zero trust e le specificità degli ambienti OT, proponendo una rassegna critica della letteratura che motiva la necessità di un framework. La Sezione 3 presenta MATRIX, descrivendone le sei fasi. La Sezione 4 ne illustra l'applicazione a uno scenario di sottostazioni elettriche digitali e ne conduce la validazione su standard, confronto e caso reale. La Sezione 5 ne illustra i pregi, i limiti e la generalizzabilità, la Sezione 6 lo colloca nel quadro normativo europeo e nazionale e ne illustra il contributo alla conformità, mentre la Sezione 7 ne trae le conclusioni e indica gli sviluppi futuri.

> ***PRINCIPIO GUIDA:*** *La domanda non è quale architettura Zero Trust adottare, ma quali capacità sono tecnicamente sostenibili per ciascuna classe di asset, e con quale priorità rispetto alla missione.*

Nella prossima parte

Chiarito il problema, resta da capire perché i controlli pensati per l'IT si scontrano con la realtà degli impianti. Nella seconda parte della serie l'autore ricostruisce i fondamenti dello zero trust e l'organizzazione degli ambienti OT secondo il modello Purdue, e introduce i cinque attributi che misurano quanto un dispositivo può accogliere i controlli. Il paper integrale «**Zero Trust selettivo negli ambienti OT**»,

con figure, tabelle e bibliografia completa, è disponibile per il download.

Fonti:

[1] Cloud Security Alliance, Zero Trust Guidance for Critical Infrastructure. Seattle, WA, USA: CSA Zero Trust Working Group, ott. 2024.

[2] R. Langner, “Stuxnet: Dissecting a cyberwarfare weapon,” IEEE Security & Privacy, vol. 9, n. 3, pp. 49–51, 2011.

[3] R. M. Lee, M. J. Assante e T. Conway, Analysis of the Cyber Attack on the Ukrainian Power Grid. Washington, DC, USA: E-ISAC e SANS Industrial Control Systems, 2016.

[4] J. Kindervag, Build Security Into Your Network’s DNA: The Zero Trust Network Architecture. Cambridge, MA, USA: Forrester Research, 2010.

[5] S. Rose, O. Borchert, S. Mitchell e S. Connelly, Zero Trust Architecture, NIST Special Publication 800-207. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2020, doi: 10.6028/NIST.SP.800-207.

[6] S. Rose, O. Borchert, S. Mitchell e S. Connelly, Zero Trust Architecture, NIST Special Publication 800-207. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2020, doi: 10.6028/NIST.SP.800-207.

[7] K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V. Pillitteri, S. Lightman, A. Hahn, S. Saravia, A. Sherule e M. Thompson, Guide to Operational Technology (OT) Security, NIST Special Publication 800-82r3. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2023, doi: 10.6028/NIST.SP.800-82r3.

[8] K. Stouffer, M. Pease, C. Tang, T. Zimmerman, V.

Pillitteri, S. Lightman, A. Hahn, S. Saravia, A. Sherule e M. Thompson, Guide to Operational Technology (OT) Security, NIST Special Publication 800-82r3. Gaithersburg, MD, USA: National Institute of Standards and Technology, 2023, doi: 10.6028/NIST.SP.800-82r3.

[9] Cloud Security Alliance, Zero Trust Guidance for Critical Infrastructure. Seattle, WA, USA: CSA Zero Trust Working Group, ott. 2024.

[10] Agenzia dell'Unione europea per la cibersicurezza (ENISA), Technical Implementation Guidance on Cybersecurity Risk Management Measures, v1.0. Atene, Grecia: ENISA, giugno 2025.

[11] C. J. Alberts, T. Morrow, R. Brown e C. M. Wallen, Tailoring Security and Zero Trust Principles to Weapon System Environments, Special Report. Pittsburgh, PA, USA: Software Engineering Institute, Carnegie Mellon University, 2025.

[12] R. Brown, "Implementing Zero Trust in Operational Technology: A Practical Case Study," SEI Insights (blog), Software Engineering Institute, Carnegie Mellon University, 16 giugno 2026.

[13] Parlamento europeo e Consiglio, Direttiva (UE) 2022/2555 (NIS2), relativa a misure per un livello comune elevato di cibersicurezza nell'Unione, 14 dicembre 2022. GU UE L 333.

[14] Decreto Legislativo 4 settembre 2024, n. 138, recepimento della direttiva (UE) 2022/2555 (NIS2). Gazzetta Ufficiale della Repubblica Italiana, n. 230, 1° ottobre 2024.

https://www.ictsecuritymagazine.com/articoli/zero-trust-ot-air-gap/