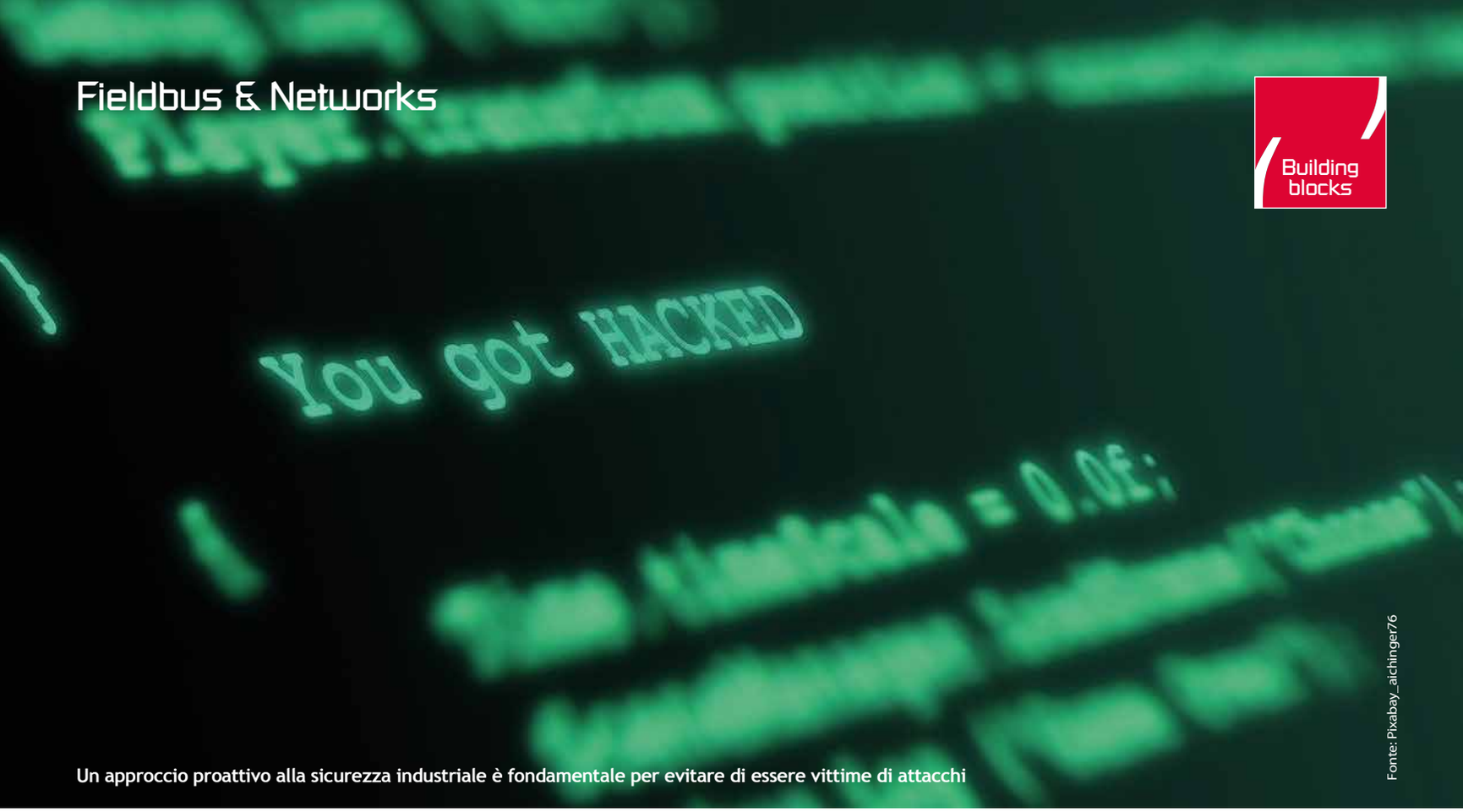


Un approccio proattivo alla sicurezza industriale è fondamentale per evitare di essere vittime di attacchi

Fonte: Pixabay_aichinger76

LE SFIDE DELLA SICUREZZA INDUSTRIALE

UNA RICERCA DI BARRACUDA RIVELA CHE LE ORGANIZZAZIONI HANNO DIFFICOLTÀ A PROTEGGERE LE TECNOLOGIE OPERATIVE E DI CONSEGUENZA SONO VITTIME DI ATTACCHI. IL 94% DI ESSE HA SUBITO UN INCIDENTE LEGATO ALLA SICUREZZA NEGLI ULTIMI 12 MESI. MANIFATTURIERO E SANITÀ I SETTORI PIÙ IN RITARDO

Stefano Pinato

Sono preoccupanti i risultati del report 'The State of Industrial Security in 2022', la ricerca globale commissionata da Barracuda Networks, che ha coinvolto 800 responsabili IT, responsabili della sicurezza e project manager da cui dipendono i progetti IIoT (Industrial Internet of Things) e OT (Operational Technology) delle rispettive organizzazioni. Il report ha inteso cogliere il loro punto di vista sul tema della sicurezza dei progetti IIoT/OT, i problemi di implementazione, gli incidenti legati alla sicurezza, gli investimenti tecnologici e altri aspetti relativi alla cybersecurity.

In generale, la ricerca dimostra come l'infrastruttura critica sia sotto attacco e, nonostante l'accordo unanime sul fatto che la sicurezza dell'IIoT e dell'OT siano fattori essenziali, le aziende stanno incontrando alcune sfide significative, legate anche alle tensioni geopolitiche. Le violazioni della sicurezza hanno impatti che vanno oltre il danno economico e i tempi di downtime da queste causati innescano conseguenze anche di lunga durata.

Nello specifico, la ricerca rivela che gli attacchi sono endemici. Il 94% delle organizzazioni ammette di avere avuto un incidente di sicurezza negli ultimi 12 mesi. La situazione geopolitica è poi preoccupante, tanto che l'89% degli intervistati è 'molto' o 'abbastanza' preoccupato per l'impatto che l'attuale scenario delle minacce e la situazione geopolitica potranno avere sulle aziende. Infine, le violazioni hanno generalmente un impatto significativo sulle organizzazioni. L'87% delle aziende vittime di un incidente ne ha subito le conseguenze per più di un giorno. "Nello scenario attuale, le infrastrutture critiche sono un obiettivo interessante per i cybercriminali, sfortunatamente però i progetti relativi alla sicurezza di IIoT e OT spesso finiscono in secondo piano rispetto ad altre iniziative per la sicurezza, o

falliscono a causa del costo e della complessità, mettendo a rischio l'intera organizzazione" sottolinea Tim Jefferson, SVP, engineering for data, networks and application security di Barracuda. "Aspetti come la mancanza di una segmentazione della rete e dell'autenticazione a più fattori lasciano la rete esposta ad attacchi e richiedono un intervento immediato".

Meno intenzioni e più fatti…

Le organizzazioni sono consapevoli dell'importanza di investire di più nella sicurezza IIoT e OT, come ammette il 96% degli intervistati. Il 72% delle aziende conferma di avere già implementato progetti di sicurezza IIoT/OT, o di essere sul punto di farlo, ma molte stanno incontrando difficoltà nell'implementazione, per esempio per quanto riguarda una 'cyber igiene' di base.

In particolare, i comparti del manifatturiero e della sanità sono indietro, mentre le realtà che detengono infrastrutture critiche sono le più avanti con l'implementazione. Nel comparto oil&gas, per esempio, il 50% delle aziende ha già completato i progetti di implementazione della sicurezza. Di contro, nel manifatturiero e nella sanità solo il 24% e 17% rispettivamente ha già completato i progetti.

Molte aziende falliscono, tanto che il 93% di queste non ha portato a termine con successo i progetti per la sicurezza IIoT/OT. Le implementazioni riuscite di sicurezza IIoT hanno però un impatto positivo e tra le organizzazioni che hanno completato progetti in questa direzione, il 75% non ha registrato alcuna conseguenza da tutti i maggiori incidenti subiti.

La ricerca 'The State of Industrial Security in 2022' ha colto il punto di vista delle organizzazioni sul tema della sicurezza dei progetti IIoT/OT

L'uso dell'autenticazione a più fattori (MFA) è ancora modesto, solo il 18% delle aziende intervistate limita l'accesso alla rete, o richiede l'autenticazione a più fattori per l'accesso remoto alle reti OT. L'uso di MFA è poco diffuso anche nei settori più critici, come quello dell'energia (47%), dove spesso viene concesso l'accesso completo da remoto a utenti esterni senza MFA. Un altro punto critico per le aziende è costituito dalla necessità di effettuare aggiornamenti manuali, anziché in automatico.

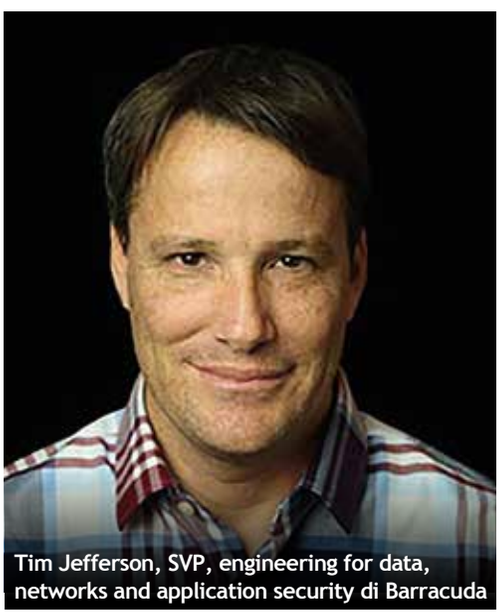
Meno della metà delle organizzazioni intervistate, inoltre, è in grado di applicare in autonomia gli aggiornamenti di sicurezza (49%), a dimostrazione della mancanza di competenze con cui questo ambito deve fare i conti.

Come evitare di essere la prossima vittima?

I dispositivi IIoT e OT continuano a essere un obiettivo importante per gli hacker, ma c'è speranza per le aziende che assumono un approccio proattivo. Le organizzazioni dovrebbero implementare strumenti di risposta idonei, per esempio con l'uso di dispositivi di connettività end point sicuri, o firewall rafforzati, tutti implementati centralmente e gestiti attraverso un servizio cloud sicuro, che possa consentire una segmentazione efficace della rete e una protezione avanzata dalle minacce, fornire l'autenticazione a più fattori e implementare l'accesso zero trust.

"Gli attacchi IIoT vanno oltre il mondo digitale e possono avere conseguenze anche nel mondo fisico" aggiunge Klaus Gheri, VP network security di Barracuda. "Nel momento in cui gli attacchi sono in crescita in tutti i settori, un approccio proattivo alla sicurezza industriale da parte delle aziende è fondamentale per evitare di essere le prossime vittime di un attacco".

Barracuda Networks - www.barracuda.com



Tim Jefferson, SVP, engineering for data, networks and application security di Barracuda

Klaus Gheri, VP network security di Barracuda