MEET IT

PROTEZIONE PER
LE RETI INDUSTRIALI

FIREWALL OT OPERATIONAL TECHNOLOGY

Datasheet

Le aziende del Gruppo MEET IT

3CiME TECHNOLOGY ICT & INNOVATION

Via di Corticella, 89/2
40128 Bologna BO

+39 05 14070383
www.3cime.com | info@3cime.com

ntnuovetecnologie 25

Viale Alcide De Gasperi, 37
33100 Udine UD

+39 0432 524001
info@ntonline.it | www.ntonline.it

PROTEGGI LE RETI E LE MACCHINE DI PRODUZIONE

Spesso le reti Internet di produzione sono le più dimenticate, perché non avendo dati, si pensa che siano meno soggette ad attacchi. Ma non è così, i cybercriminali hanno compreso la criticità delle infrastrutture OT e sviluppato nuovi tipi di attacco per danneggiare la catena produttiva.
Un data breach in tale ambito può mettere in ginocchio tutta l'azienda.

PREMESSA

Il servizio **Firewall OT** del Gruppo MEET IT ha lo scopo di coprire queste lacune e comprendere nel perimetro di sicurezza aziendale la parte OT (Operational Technology), come le **reti delle macchine di produzione**, l'**Internet of Things (IoT)** ed i **PLC**.

Con l'introduzione della quarta rivoluzione industriale e dei concetti di **produzione intelligente**, la necessità di **dispositivi industriali connessi** è aumentata in modo massiccio nel corso degli anni. Tuttavia, la tipica **rete di tecnologia operativa (OT)** ha alcuni requisiti chiave che la differenziano in modo significativo da una normale rete IT. Allo stesso tempo molti PLC sono ancora comandati da PC Windows XP o Windows7, mettendo a rischio la sicurezza dell'intera rete.

Per sua natura, una tipica rete OT deve garantire che il **reparto di produzione sia sempre attivo**. Non c'è spazio per i tempi di inattività e i tecnici devono essere in grado di eseguire operazioni di manutenzione o sostituzione con breve preavviso.

Dovendo gestire un **impianto di produzione 24 ore su 24, 7 giorni su 7**, con centinaia di celle di produzione che devono essere tutte protette, segmentate e collegate, è necessario che il dispositivo di gestione mantenga centralmente i file di configurazione e le licenze e le assegni in base alle esigenze.

CARATTERISTICHE

Il servizio prende in considerazione gli **ambienti network**, abitualmente **LAN di produzione**, che sono normalmente gestiti, protetti e separati attraverso semplici **VLAN**.

Il servizio Firewall OT consiste nell'inserimento di appliance industriali in grado di difendere specifici bracci di rete da attacchi hacker di diverso tipo. **I firewall sono di tipo industriale**, in grado quindi di essere **installati anche in ambienti ostili, polverosi e tipici degli ambienti di fabbrica**.

Il servizio viene erogato dal firewall configurato in ambiente cloud, anche se installato on premise, verso i bracci di rete oggetto di protezione.

FUNZIONALITÀ

Micro-segmentazione trasparente, segmentazione e isolamento

La micro-segmentazione di uno stabilimento è un must dal punto di vista della sicurezza. Questo assicura che quando una cella di prodotto è soggetta a manutenzione, o nel peggiore dei casi è compromessa, tutte le altre celle di prodotto possono rimanere attive. In altre parole, **la possibile superficie di attacco è più piccola** con la micro-segmentazione fatta bene.

Accesso remoto e sicuro su richiesta

Per motivi di sicurezza è obbligatorio che l'accesso a questi dispositivi non sia sempre possibile, ma debba essere **abilitato su richiesta** dal tecnico della cella di produzione. Ogni Firewall OT offre l'opzione di abilitare l'**accesso remoto temporaneo** (con scadenza automatica) su richiesta tramite un'applicazione di semplice utilizzo o un'interfaccia utente basata sul web. L'applicazione può essere facilitata montando un dispositivo tablet presso la cella di produzione.

VISITA IL SITO *MEETIT.CLOUD*

Visibilità e applicazione dei permessi

A seconda dei requisiti specifici di un ambiente di produzione, potrebbe essere obbligatorio **mantenere l'ambiente strettamente bloccato e sottoposto a controlli approfonditi**.

Per garantire che tali ambienti non siano compromessi, Firewall OT applica **vari metodi di autenticazione e registra automaticamente gli accessi** degli utenti. Questa visibilità e applicazione dei permessi consente di avere **più gruppi di utenti con diritti di accesso diversi**. Ad esempio, un gruppo può impartire comandi di lettura, mentre un altro gruppo può impartire comandi di scrittura

Connessione sicura tra IT e OT

Il Firewall OT viene implementato **tra la rete IT e la rete OT** e **tra la rete OT e Internet**. La piattaforma del firewall monitora la comunicazione di rete interna e fornisce informazioni dettagliate sugli asset industriali, avvisi su comportamenti anomali della rete e segnalazioni di rischi e vulnerabilità. Una volta che il sistema rileva un'anomalia, Firewall OT blocca automaticamente la fonte dannosa nel punto di ingresso della rete OT.

Patching virtuale e sicurezza specifica per i dispositivi OT

L'aggiunta di unità firewall per la protezione di specifici dispositivi OT consente agli amministratori di applicare **criteri di sicurezza specifici per i dispositiv**i sensibili o vulnerabili. Questo è particolarmente efficace quando ci sono dispositivi che sono più critici per il processo e, quindi, richiedono un maggiore controllo della sicurezza. Inoltre, se ci sono dispositivi legacy con vulnerabilità note che non sono patchabili, la combinazione di servizio e firewall consente di identificare i dispositivi più critici o vulnerabili in base alle loro attività di rete e alle loro vulnerabilità. Una volta identificati questi dispositivi, **i firewall possono essere configurati correttamente in base al loro ruolo effettivo nell'ambiente**.

Secondo il Fortinet State of Operational Technology Report, **quasi il 74% delle aziende OT ha riferito di aver subito un attacco malware nell'ultimo anno**, con conseguenti danni economici, produttivi, di affidabilità e integrità dei dati.