UN NUOVO MODO DI SEGMENTARE E PROTEGGERE LA RETE DI FABBRICA/IMPIANTO

(con riferimento a IEC62443)

Un nuovo modo di segmentare e proteggere la rete di fabbrica/impianto (con riferimento a IEC62443)

Da molto tempo parliamo della necessità di sementare la rete di fabbrica secondo quanto contenuto nello standard IEC62443 e come consigliato dai maggiori esperti per evitare eventuali propagazioni di problemi e contaminazioni da una zona della rete all'altra.

Poi quando ci viene presentato il caso concreto da parte di un Cliente, ecco che dobbiamo spesso scendere a compromessi: il Cliente vuole proteggere solo "quella parte della rete", in quanto un intervento su "tutta la rete" potrebbe risultare troppo intrusivo e spesso anche troppo costoso, in definitiva, poco praticabile se la segmentazione fosse estesa a tutto la rete di fabbrica.

Non si tratta di non capire l'obiettivo della necessità di proteggere adeguatamente i sistemi di controllo ed automazione o di non apprezzarne i benefici, il problema è colmare il divario tra dove sono oggi e ciò che è necessario per implementare una rete segmentata completa e sostenibile in futuro.

È, come dice il detto, una strada lunga da percorrere e spesso le risorse sono scarse. Ne abbiamo parlato spesso anche in altri altri white paper sull'argomento.

La maggior parte delle soluzioni utilizza un approccio esteso all'intera rete per pianificare una soluzione.

Anche GE Digital ha pubblicato una guida parlando dell'importanza delle strategie e delle zone di segmentazione virtuale per uno SCADA con iFix e/o Cimpicity: si tratta di un documento molto valido, con una bella grafica che mette in evidenza molti punti importanti. (la trovate qui https://www.ge.com/digital/sites/default/files/download_assets/ifix-secure-deployment-guide.pdf)

Questi alcuni punti che troviamo come ostacoli:

- Gli impianti e gli apparati elettro strumentali dei macchinari industriali si trovano spesso dentro cabinet (armadi) elettrici in posizioni fisse, in prossimità di macchinari ed impianti, talvolta distanti tra di loro e difficilmente raggiungibili, e quasi certamente non possono essere spostati

-La vera segmentazione della rete, quella fisica, risulta quindi ancora più complessa di quanto si pensi, e spesso risulta difficile connettere in zone congrue tutti quegli endpoint fisicamente distanti e separati

-Le tecniche di rete aziendali tradizionali, come VLAN e regole di routing, sono a volte difficili da implementare e gestire con il personale limitato che si occupa di sistemi e reti ICS/OT

La segmentazione della rete ICS/OT

La soluzione - segmenti e zone virtuali – viene proposta da molti fornitori di rete e sicurezza.

L'idea è semplice: definire le risorse in gruppi logici (zone), indipendentemente dalla loro posizione reale, e applicare le regole di autorizzazione al traffico e applicazione dei contenuti per gruppo/zona.

Se si desidera definire un elenco di dispositivi e assicurarsi che comunichino solo tramite EtherNet / IP, si può realizzare fintanto che tutti i punti di controllo rispondono alle politiche della zona.

Tuttavia, tali approcci dipendono ancora da una visibilità completa sulla rete.

Da qualche parte deve esserci un dispositivo centralizzato dove confluisca tutto il traffico e lo ispezioni fisicamente determinando l'accesso e l'esecuzione.

Gestire le eccezioni o le anomalie dipende quindi unicamente dal sistema di controllo centrale, che risulta essere sovraccaricato di oneri di elaborazione e di configurazione mettendo potenzialmente a rischio il lavoro complessivo in caso anche di piccoli errori sempre possibili all'aumentare delle istruzioni configurate.

In ServiTecno, grazie agli spunti ed ai prodotti messi oggi a disposizione da Bayshore Networks, abbiamo deciso di adottare un approccio più semplice:

- Perché obbligare il Cliente o il S.I. a segmentare l'intera rete contemporaneamente?
- Perché anche in caso di reti di produzione / ICS / OT essenzialmente ancora piatte e non segmentate, non provare a ritagliare singoli segmenti a piacimento e quindi applicare controlli molto rigorosi contro attacchi e malware che in qualche modo potrebbero portare ad interruzioni della produzione?

Questo white paper esplorerà queste domande effettuando il confronto tra la segmentazione virtuale dell'intera rete rispetto ad una *microsegmentazione* di reti PLC/SCADA con alcune valutazioni di carattere economico, di efficacia dei controlli di sicurezza e facilità complessiva di implementazione.

Approcci alla segmentazione dell'intera rete

I dipartimenti IT nelle aziende di grandi dimensioni spesso eseguono strategie di segmentazione globali sulle reti corporate aziendali e governano quali tipi di traffico possono spostarsi all'interno e tra le zone e sono in genere organizzati per funzione aziendale.

Un segmento potrebbe ospitare server delle applicazioni, un altro potrebbe avere database back-end, un terzo potrebbe gestire desktop utenti all'interno di una particolare struttura.

Le opzioni sono infinite. Il più delle volte, è necessaria una certa quantità di interazione tra i segmenti e c'è sempre spazio per discutere su quanto siano efficaci queste configurazioni se intrusi o malware riuscissero a trovare il modo per penetrarle e propagarsi internamente.

Pensate al numero di storie di ransomware che iniziano con qualcuno che da un PC in rete visita la pagina Web errata (tramite l'accesso a Internet consentito) o scarica l'allegato email errato. Il danno è raramente limitato alle sole stazioni di lavoro personali adiacenti.

Tuttavia, nella nostra discussione sulla rete OT/ICS assumeremo che molte Aziende non abbiano né capitale umano, né skill, né i budget sufficienti per implementare e mantenere un tale sistema.

Di conseguenza, le loro opzioni saranno maggiormente orientate verso strategie di segmentazione più sostenibili.

Queste strategie le vediamo definite maggiormente con un approccio di livello 3, mediante sottoreti, più spesso delle vere VLAN di livello 2, semplicemente perché le sottoreti sono più facili da gestire.

Non sono efficaci quanto le VLAN nel limitare il traffico, soprattutto perché le VLAN creano domini di trasmissione separati a livello di data link. Ciò significa però che un dispositivo su una VLAN non può trovare un dispositivo su un'altra VLAN a meno che non sia presente un router di livello 3 e lo switch che gestisce le VLAN stesse.

Al contrario, una sottorete di livello 3 ha caratteristiche migliori per la crescita pianificata della rete. Creando più ID host all'interno dell'ID di rete principale si ha più spazio per espandersi quando si aggiungono dispositivi alla rete.

Ciò è positivo in ambienti in rapida evoluzione, consideriamo però che molte infrastrutture ICS/OT tendono a non variare/crescere così rapidamente. La maggior parte dei Clienti finisce per utilizzare le sottoreti solo allo scopo di una facile identificazione visiva delle funzioni all'interno del proprio impianto, ad esempio

associando un ID host per edificio, per impianto o per sito fisico. In questo modo un piccolo team che gestisce la rete ICS/OT apprende molto rapidamente che qualsiasi cosa sulla rete 10.x è relativo al building 1, 20.x è il building 2 e così via.

In ultimo quindi, tutto questo risulta solo una scorciatoia per risparmiare lavoro piuttosto che un significativo vantaggio di rete sicura. In breve, le VLAN possono funzionare bene se il cliente ha le attrezzature di switching e routing necessarie e metodo e disciplina per studiare tutte le loro risorse e il traffico di rete per costruire una segmentazione che abbia significato. Molti Clienti con impianti più piccoli potrebbero non ritenere che i vantaggi valgano lo sforzo e, di conseguenza, tendono a passare automaticamente alle sottoreti per un flusso di lavoro semplificato, evitando al contempo significativi vantaggi in termini di security.

Approccio alla "segmentazione selettiva"

Ora torniamo alla domanda posta in precedenza: cosa significa *segmentare* una singola zona?

Per i nostri scopi stiamo assumendo che la definizione di zona stessa sia significativa, ovvero che consenta un qualche vantaggio in termini di sicurezza.

Il nostro obiettivo è quello di dare al gestore della rete ICS/OT un ulteriore controllo sul traffico all'interno di quel segmento, senza dover effettuare una valutazione completa e riprogettare la rete con le conseguenze che ne derivano in termini di gestione e di manutenzione.

Per i nostri scopi esploreremo due tipi di "segmentazione selettiva", a cui faremo riferimento

- Endpoint Segment
- Trusted Domain Segment

Cos'è un Endpoint Segment

Un segmento endpoint è un piccolo numero (in genere 10 o meno) di dispositivi, probabilmente tutti all'interno di un singolo cabinet, impianto o almeno un singolo edificio, che svolgono collettivamente una funzione di base all'interno della rete ICS/OT. Potrebbe essere formato da uno o più PLC e/o HMI che gestiscono collettivamente una pompa di sollevamento in un impianto idrico, ad esempio, o uno skid o un macchinario in un ambiente di produzione. In generale, la maggior parte dei gestori di rete concorderà sul fatto che l'ambito di lavoro che il segmento Endpoint dovrebbe svolgere è allo stesso tempo molto ben definito e cambia di rado, o addirittura mai.

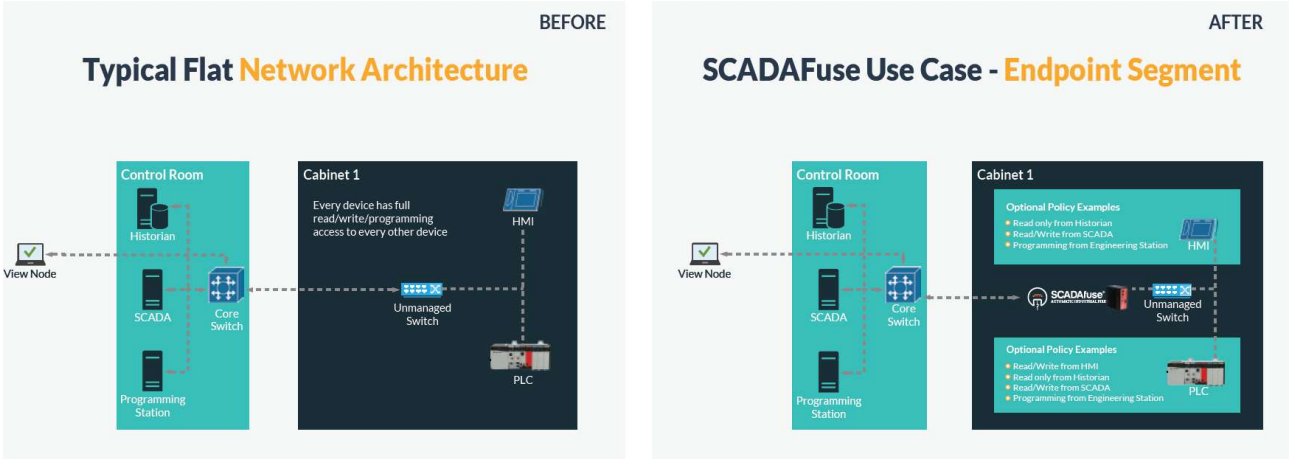
È quindi possibile applicare degli specifici parametri relativamente al traffico di rete che entra o esce da quel segmento di endpoint (il conduit secondo la terminologia IEC62443).

La maggior parte, o tutte, le seguenti affermazioni saranno generalmente vere, riferite a questa zona:

- Le connessioni esterne al segmento endpoint che devono interagire con le risorse al suo interno sono tutte note
- I modelli di traffico tra tali asset e gli asset del segmento endpoint sono facilmente osservabili e non variano
- Le eccezioni sono rare e di solito possono essere riconosciute in anticipo, in modo che le modifiche possano essere impostate e programmate con preavviso

A questo punto possiamo stabilire rinforzi agendo su questi parametri in quanto questo ci consente di estendere la protezione della sicurezza fino alle risorse in quel segmento di endpoint.

Con gli strumenti giusti, possiamo costruire automaticamente le regole necessarie e c'è un basso rischio di falsi positivi a causa della natura relativamente statica dei dispositivi e delle comunicazioni di rete in un ambiente ICS/OT.



Bayshore offre una famiglia di dispositivi di sicurezza automatizzati - SCADAfuse® - che fanno esattamente questo.

Funzionano come uno switch di livello 2 (o, più precisamente, un bridge trasparente) che si pone di fronte al cabinet, prelevando il traffico di rete che va e viene dai dispositivi all'interno, direttamente da uno switch di rete.

Apprende tutti gli indirizzi IP e le porte di origine e destinazione per tutti i flussi di rete, in entrambe le direzioni, e classifica il traffico in base alla porta e al protocollo industriale utilizzato. Analizza ulteriormente tutte le attività del protocollo usando un approccio di Deep Content Inspection, per costruire regole che sono organizzate in tre classi di tipi di attività:

- Read only
- Read & write
- Programming update / full access

All'inizio il Cliente deve solo attivare SCADAfuse in modalità di apprendimento, lasciarlo costruire le sue regole per poi rivedere e convalidare le policy suggerite. Tutte le modifiche necessarie possono essere apportate manualmente e testate in produzione impostando il dispositivo in modalità "Monitoraggio". In questa configurazione, le violazioni delle policy verranno registrate, ma non verrà intrapresa alcuna azione per limitare o filtrare il traffico. I Clienti possono poi aggiungere, con pochi clic, le ulteriori anomalie che in realtà vogliono impostare nelle policy per il futuro (whitelisting), mentre tutte le altre rimarranno escluse.

Una volta passato alla modalità "Protection", SCADAfuse applicherà la sua policy personalizzata ai dispositivi del segmento endpoint direttamente e in tempo reale, avvisando il Cliente, tramite il sistema SCADA esistente, di eventuali eventi bloccati.

I Clienti possono interagire con il singolo SCADAfuse direttamente dalla loro sala di controllo o utilizzare una console di gestione centralizzata basata su Web per la revisione di policy ed eventi da un gran numero di singole appliance SCADAfuse.

Bayshore offre anche varianti di SCADAfuse progettate per creare un segmento endpoint attorno ai server di applicazioni SCADA critiche.

Il primo di questi, SCADAfuse per iFix, è realizzato per la famiglia di soluzioni SCADA iFIX 6.x di GE Digital e funziona nativamente con i protocolli proprietari che iFIX utilizza per comunicare tra i server SCADA, i vari tipi di nodi client di visualizzazione e tutti i dispositivi, collettori e driver connessi con i dispositivi di automazione distribuiti nell'impianto.

In definitiva, SCADAfuse permette di definire e mettere in pratica i segmenti di endpoint per un un'implementazione più rapida, a un costo inferiore e permette un controllo più flessibile, il tutto rispettando le regole adottate dall'IT dell'Azienda riferite all'utilizzo di firewall, switch e router.

Anche se la rete di controllo rimane completamente invariata ad eccezione di questo segmento di endpoint controllato da uno SCADAfuse per l'asset più critico, il Cliente vedrà sicuramente un aumento significativo della protezione attorno a quel dispositivo. Tutto questo può essere installato in un pomeriggio e il costo è una piccola parte di qualsiasi altro tipo di attività di riprogettazione parziale o dell'intera rete.

Cos'è un Trusted Domain Segment?

La distinzione cruciale tra un "Trusted Domain Segment" e un "Endpoint Segment" in una rete ICS/OT riguarda il tipo di traffico rilevato.

In un “endpoint segment”, il traffico su più porte e protocolli dovrebbe avere pattern riferiti a collegamenti in ingresso e uscita dal segmento, in quanto le connessioni vengono avviate dall'interno del segmento endpoint verso l’esterno o da fuori di esso verso l’interno.

In un "Trusted Domain Segment", in genere, si considera che il traffico attraversi il punto di confine solo quando viene esplicitamente avviato da dispositivi all'interno del trusted domain.

In altre parole, prevediamo una preponderanza di attività unidirezionale dal dominio trusted verso un dominio esterno.

In alcune circostanze, potremo anche consentire risposte, ma solo se in primo luogo sono staticamente correlate a una richiesta innescata dall’interno del “trusted domani" e poi provengono da fonti e tipi di contenuto predefiniti.

Un "Trusted Domain Segment", se utilizzato in sistemi di controllo e reti ICS/OT di impianti critici, dovrebbe pertanto essere protetto con sistemi più rigidi di Security, indipendentemente dagli standard o dalle tecnologie in uso sulle reti IT dell’Azienda.

Il metodo più efficace per proteggere un simile segmento dagli attacchi di rete e dal malware è in primo luogo, logicamente, quello di impedire che ci si possa connettere al “Trusted Domain”.

In passato, su molte reti industriali di usava il cosiddetto “air gap" dal resto del mondo. Un cuscino d’aria è proprio questo - una rottura fisica nello spazio senza alcun tipo di connessione di rete: nel tempo però la maggior parte di questi sistemi di “air gap” in rete sono state erosi o compromessi dalla richiesta di un utilizzo più flessibile e la necessità di estrarre maggiori dati dall’impianto, informazioni utili al management.

Le esigenze di interoperabilità tra le reti ICS/OT e gli stakeholder a monte, insieme alla necessità, anche occasionale, di connettività Internet, rendono molto difficile isolare un'intera rete di grandi dimensioni tramite “air gap”.

La maggior parte degli assessment di tali reti trova spesso una sorta di canali di backdoor o soluzioni alternative tramite connessioni (a volte complesse e non censite), il che rende inutili gli “air gap”.

Come già visto per gli “endpoin segment”, ServiTecno con Bayshore Networks offre una soluzione per creare e proteggere un "Trusted Domain Segment"

Questa soluzione si chiama SCADAwall ™ e ha lo scopo di consentire flussi unidirezionali da un trusted domain a un dominio esterno, comunicazione che avviene solo in condizioni esplicitamente definite.

Il principio di funzionamento è basato sull’utilizzo di due server separati. Ognuno ha un'interfaccia Ethernet standard. In pratica si può parlare di un “diodo logico”.

Uno è connesso esclusivamente al trusted domain, l'altro è connesso esclusivamente al dominio esterno.

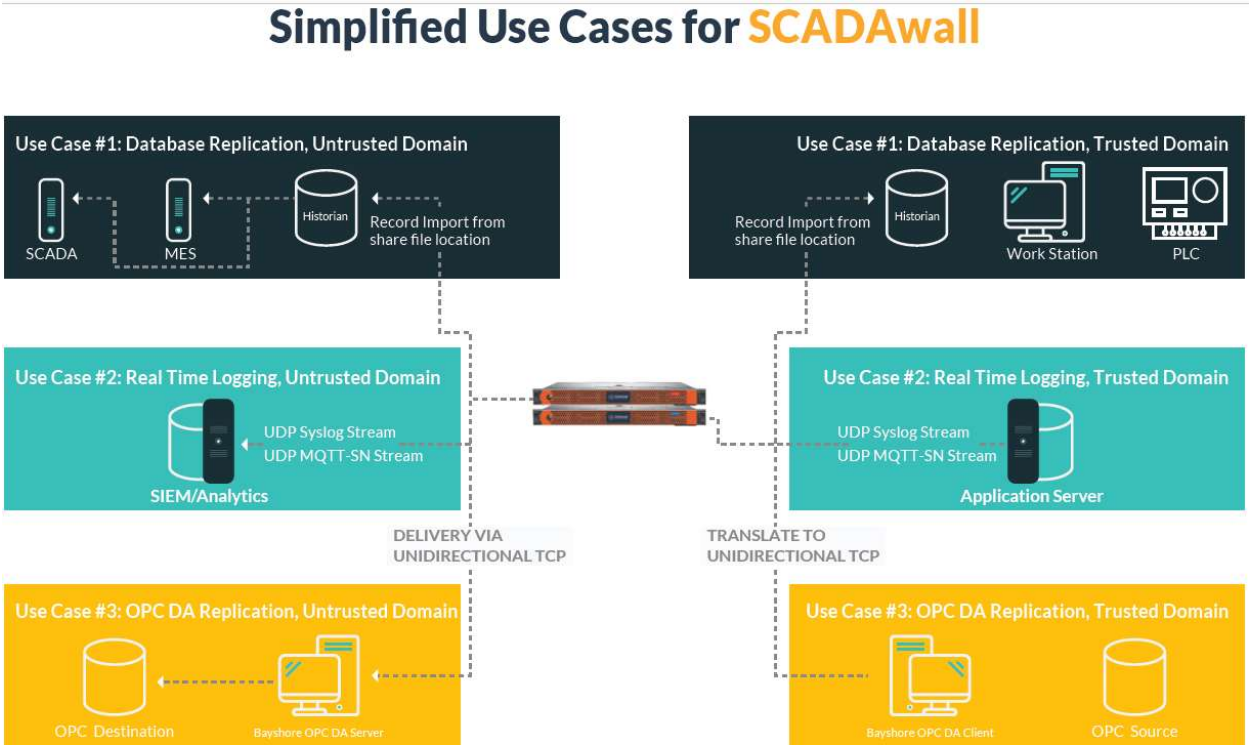
Tra i due server è presente un cavo di interfaccia PCI Express.

La parte trusted è in grado di fornire dati alla parte non trusted in conformità con le regole stabilite dall'amministratore.

Queste regole dovrebbero essere le seguenti:

- Indirizzo IP di origine consentito e porta su dominio trusted
- Indirizzo IP e porta di destinazione previsti su dominio non trusted
- Un tipo di regola, che può essere TCP, UDP, File Transfer, OPC o Modbus / TCP: per File Transfer, OPC e Modbus/TCP, sono richiesti vari dettagliati parametri per configurare la connessione corretta

Una volta configurato lo SCADAwall per funzionalità diverse dal file trasfert, il server del trusted domain ascolterà tramite le porte gestite con filtro sulla sua interfaccia di rete locale le connessioni in entrata dalle porte autorizzate.



Man mano che il traffico viene ricevuto, viene disassemblato, i metadati del payload e della connessione vengono recapitati al secondo server sul lato non trusted che, a sua volta, riassembla i dati in una nuova connessione di rete e consegnata solo alla destinazione autorizzata. Il server del trusted domani può garantire che i messaggi siano stati recapitati correttamente al dominio esterno poiché, prima della trasmissione, calcola un checksum verificabile sul messaggio che sta per trasmettere.

La larghezza di banda interna tra questi server è molto alta - fino a 40 gigabit al secondo - quindi c'è ampio margine per sessioni di consegna simultanee multiple.

SCADAwall è disponibile in vari livelli prestazionali fino alla velocità gigabit inclusa, e in futuro sono previste versioni multi-gigabit.

SOMMARIO

I vantaggi dell'utilizzo di SCADAfuse e di SCADAwall per le esigenze di segmentazione della rete ICS/OT per i Endpoint Segment e Trusted Domain Segment affidabili sono molto semplici:

- Isolare il segmento di dominio trusted con un perimetro di sicurezza elettronica verificabile
- Garantire che malware, connessioni non autorizzate e intrusioni non abbiano possibilità di entrare nel segmento definito
- Disponibilità di banda completa per replicare i dati nel dominio esterno
- Consegna garantita dei dati
- Piattaforma che cresca nel tempo da 50 Megabit/sec a 10 Gigabit/sec semplicemente aggiornando la licenza software