ServiTecno

Quattro preoccupazioni

per chi gestisce la Security

di reti e sistemi ICS

(Industrial Contro System)

ServiTecno s.r.l.
Via F. Koristka, 10 - 20154 Milano (MI) – Italy
Tel. 02 486141 - Fax 02 48614441 – info@servitecno.it - www.servitecno.it

Vers.1.0 – Gennaio 2015

Indice

1	**INTRO**	**4**
2	**No.1: neccesità di integrare la rete aziendale**	**6**
3	**No.2: configurazione di VLAN per la rete Process Network**	Errore. Il segnalibro non è definito.
4	**No.3: accessi remoti mal gestiti**	Errore. Il segnalibro non è definito.
5	**No.4: change management nella rete di impianto**	Errore. Il segnalibro non è definito.
6	**conclusioni**	Errore. Il segnalibro non è definito.

intro

Gli attacchi ai sistemi di controllo industriale e telecontrollo nelle utility stanno diventando sempre più attuali. Qui elenchiamo quattro situazioni comuni che creano vulnerabilità alla Security di reti e sistemi ICS (e come sia possibile evitarle).

Anche in recenti film di successo abbiamo visto dannosi attacchi informatici che devastano infrastrutture critiche. Mentre i “cattivi” cercano di caricare i virus in 'rete' nel tentativo di conquistare il mondo, gli “eroi” sono a digitare furiosamente sulla tastiera per riprendere il controllo dei 'mainframe'. Questi “incidenti” sembrano essere solo mero intrattenimento immaginario e altamente improbabile che si verifichi, ma una volta che il film finisce ci lasciano il dubbio: "Che cosa potrebbe realmente accadere?"

Purtroppo, non solo è potuto accadere, ma sta accadendo sempre più spesso: gli attacchi di cyberSecurity ampiamente pubblicizzati come Stuxnet e Flame lo hanno dimostrato.

Ricordate aa copertura mediatica di Stuxnet, un worm che sfuggì al controllo nell’estate 2012 ed è stato utilizzato per attaccare gli impianti nucleari iraniani, proprio come in una trama di un film?

Ancora: Flame, una forma di cyber-spionaggio scoperto nel 2012, ha attaccato i computer con Microsoft Windows che potevano registrare l'audio, le immagini, e l'attività sulla tastiera e del traffico di rete. Flame è considerato uno dei "malware più complessi mai trovati". Ed ancora un altro attacco, quello con “Duqu” , ha letteralmente spazzato via 30.000 computer della società petrolifera Saudi Aramco.

Nonostante questi attacchi siano stati molto pubblicizzati, la minaccia ancora sembra un evento raro e qualcosa che accade solo ad Agenzie governative in lontane terre straniere.

Tuttavia, la triste realtà è che questo attualmente accade negli Stati Uniti ed in Europa (sì, anche in Italia) e più spesso di quanto si potrebbe immaginare.

Secondo l'Industrial Control Systems Cyber Emergency Response Team (ICS-CERT), una divisione del Department of Homeland Security USA, ci sono stati più di 200 gli incidenti con intrusioni in tutti i settori delle infrastrutture critiche nella prima metà del 2013. Di questi incidenti, 111 è avvenuto nel settore dell'energia e 32 in alcuni settori di produzioni critiche.

Questo aumento di attività di attacchi alla Security ICS hanno spinto Kyle Wilhoit , Threat Researcher di Trend Micro a esaminare se gli hacker sarebbero stati interessati anche ai sistemi SCADA. Le sue scoperte, pubblicate in un Libro bianco intitolato “Your SCADA Devices are Being Attacked” sono riassunti in questa citazione da parte dell'autore:

"Tutto ciò che è connesso in rete è più che probabile che prima o poi venga attaccato", ha detto Wilhoit.

Per misurare l'esistenza di attacchi effettivi a sistemi SCADA, Wilhoit ha con figurato due sistemi con architetture “honeypot” per attirare hacker e monitorare le loro abilità d'attacco. Uno dei sistemi era un duplicato/Mirror di un vero impianto di trattamento delle acque, dotato di attrezzature SCADA e pannelli HMI, tutti collegati a falsi "controllori/trappole" che hanno permesso agli aggressori di avere le

stesse risposte come se stessero attaccando un vero impianto di gestione dell'acqua di una utility comunale.

Wilhoit ha rilevato un numero sorprendente di attacchi. Il più evidente è avvenuto col tentativo di aggirare l'autenticazione dello SCADA/HMI - evidenziato anche da un attacco di phishing di 'alto livello', in quanto hanno tentato di hackerare il sistema inviando e-mail all'amministratore del sistema per ottenerne in modo subdolo e fraudolento le credenziali di accesso.

Alla fine, i risultati di Wilhoit suggeriscono che, "ben 17 tentativi sarebbero da considerare 'catastrofici' per il sistema di pompaggio in pressione dell'acqua."

Incidenti e ricerche come questa indicano chiaramente come questi attacchi sono e saranno sempre più numerosi, sofisticati , e distruttivi nel futuro a breve termine. E l'unico modo per evitare che è quello di giocare in difesa, prepararsi e prendere opportune contromisure

In altre parole, se finora non si è affrontato direttamente il tema della protezione e della sicurezza "Cyber", è necessario farlo subito, in quanto la minaccia è in continuo aumento. E poiché la connettività e la "banda" crescono, così aumenta anche il numero di passaggi da fare e mettere in cantiere per proteggere la vostra infrastruttura di ICS.

In questa White Paper ci sono quattro situazioni reali che stanno creando problemi di Security ICS in architetture di rete attuali e abbastanza comuni.

No. 1: Necessità di Integrare la rete di Controllo con la rete aziendale

L'infrastruttura IT di un'organizzazione cresce in proporzione al suo personale: alle persone esistenti si aggiungono i nuovi assunti, PC e computer portatili vengono acquistati e collegati, account di posta elettronica vengono creati e gli utenti hanno accesso alla rete aziendale e Internet.

E' un processo naturale, infatti è pratica commerciale comune, ma le cose si complicano quando si arriva al punto di doversi integrare nello stesso ambiente ove sono presenti reti di automazione e controllo, PLC e SCADA. A questo punto, i reparti produttivi o di manutenzione/ ingegneria molto probabilmente sosterranno che l'aggiunta di server esposti a Internet sulla stessa rete, aprono il sistema fino al web, e quindi aumenta la possibilità di intrusioni.

È evidente l'idea che una volta che si aprano le porte verso l'esterno, è quasi implicito l'invito per le "cose a venire dentro".

In altre parole: i server Web e di posta elettronica sulla stessa rete dei server SCADA sono l'inizio di un sistema che facilmente possa essere preso di mira perché, come gli hacker dicono, se è possibile eseguire un ping, si può facilmente "possederlo".

Un recente studio condotto da Positive Technologies, ha scoperto che più del "40% dei sistemi SCADA "visibili" in Internet è vulnerabile e può essere violato da anche persone con poche capacità di intrusione, anche solo attraverso semplici malware ".

Ciò ha indotto il Dipartimento dell'Energia degli Stati Uniti a suggerire nelle sue '21 misure per migliorare la Cyber Security di reti SCADA ' (21 Steps to Improve Cyber Security of SCADA Networks'), che le imprese industriali chiudano sulle loro reti SCADA tutti i collegamenti assolutamente non indispensabili, al fine di garantire il massimo livello di sicurezza possibile.

Il Dipartimento di Energia invita specificamente ad eliminare dalla rete SCADA, eventuali collegamenti con server e sistemi di posta elettronica e di Internet, suggerendo che l'hardening ed i rafforzamento della security dei sistemi SCADA comporta l'interruzione di collegamenti a server per la manutenzione a distanza, servizi di fatturazione (billing) a distanza, la lettura automatica dei contatori (metering), servizi di posta elettronica e accesso a Internet.

Qualcuno potrebbe sostenere che questo 'blocco delle porte' comporta anche il blocco all'uso di tecnologie emergenti che consentono una maggiore efficienza operativa.

Ad esempio, gli operatori idrici possono oggi accedere alle informazioni critiche del sistema SCADA per gestire meglio le attività o seguire le procedure operative standard per rispondere agli allarmi direttamente sui loro dispositivi intelligenti (Tablet o smartphone), tutti basati anche su geo-localizzazione. E gli operatori sull'impianto possono visualizzare schermate sul loro iPad e accedere a KPI del macchinario al quale sono fisicamente accanto.

Mentre queste funzioni possono essere estremamente utili in molte situazioni, è chiaro che si introducono alcuni incubi di Security ICS. Poiché il numero di dispositivi collegati a Internet aumenterà drasticamente nel prossimo futuro, il giusto equilibrio di connettività nel rispetto della Security deve

essere una priorità assoluta per coloro che possiedono e governano infrastrutture ICS, reti e sistemi di controllo e telecontrollo.

No. 2: configurazione di VLAN per la rete Process Network

Le Virtual Local Area Network, o VLAN, hanno protetto e proteggono con successo l'infrastruttura IT da molti, molti anni.

Insieme ad una infrastruttura IT configurata correttamente e con la protezione antivirus specifico per i dispositivi, le VLAN sono ottime per proteggere qualsiasi "Smart Devices" come i Server , PC, laptop e dispositivi mobili. E proprio a causa del loro uso molto diffuso in ambienti IT, le VLAN si stanno facendo strada anche nelle infrastrutture ICS, cioè la rete "Process Network".

E qui sta l'incubo: VLAN sono state progettate per proteggere adeguatamente l'infrastruttura IT, che non è l'infrastruttura "industriale".

Una VLAN è quasi sempre una rete "piatta", una rete "trusted" con baluardi di security a livello perimetrale e Security interna pari a zero (in quanto, per definizione, tutti i partecipanti sono "trusted"): il che è sufficiente in ambienti IT tradizionali, in cui i dispositivi sono 'intelligenti' e abbastanza carrozzati di antimalware per proteggere se stessi. E cerchiamo di essere onesti, se è un PC o un portatile ad infettarsi, è possibile accorgersene subito, isolarlo e rimuoverlo rapidamente dalla rete senza interrompere l'operatività dell'azienda nel suo complesso.

D'altra parte, se un "Vanilla malware" - che è considerata una grande minaccia per ICS – riesce ad oltrepassare il perimetro di Security su una rete di processo , questa VLAN permetterà in breve al malware di paralizzare tutti i dispositivi (PC, PLC, ecc.) e le apparecchiature sulla VLAN e, in definitiva, portare ad una fermata dell'impianto (come avvenuto anche recentemente in un grande impianto siderurgico in Germania, con colossali danni economici e rischi per l'incolumità di persone ed ambiente).

Il tempo necessario per il recovery da un attacco informatico "importante", insieme con i relativi costi, aumenta esponenzialmente con il numero di dispositivi infetti. Quindi, più attrezzature si hanno sulla VLAN, più è alto il rischio e più tempo ci vorrà per recuperare la normalità.

Questo spiega perché sono così tanti quelli che predicano la "Segmentazione e Segregazione" (anche per seguire i dettami dello standard industriale ISA99/IEC62443) e stanno cercando di isolare ulteriormente i propri dispositivi, perché le soluzioni VLAN tradizionali semplicemente non forniscono la Security necessaria a resti e sistemi ICS.

Questo isolamento mediante "Segmentazione e Segregazione", porta però con sé una serie di sfide ed un serio cambiamento di mentalità e gestione, e spesso riduce di molto i benefici normalmente associati con una maggiore connettività.

Così, mentre una sola VLAN contenente tutte le apparecchiature può lasciare l'infrastruttura ICS esposta e vulnerabile, diverse VLAN isolate possono una soluzione. Però possono anche essere più fragili e costose da gestire e mantenere. E spesso nemmeno sono veramente in grado di garantire la Security dell'infrastruttura ICS.

No. 3: Accessi remoti mal gestiti

I fornitori di sistemi ed apparecchiature in fabbrica spesso richiedono l'accesso alle loro attrezzature per una serie di buone ragioni: consente al fornitore di monitorare e mantenere la stabilità della salute a lungo termine di quanto hanno fornito, di cui devono dare garanzia e fornire la manutenzione, cosa che è fondamentale per la resa dell'impianto e la stabilità dell'ambiente operativo nel suo complesso.

Ogni dispositivo è essenzialmente un anello della catena, e ogni collegamento richiede attenzione per garantire che non diventi il temuto 'anello debole'.

Dal punto di vista operativo e per l'efficienza, l'accesso remoto è un plus, in quanto consente di monitorare e mantenere efficienti le attrezzature da una postazione remota, senza realmente visitare la fabbrica.

Questo accesso remoto viene normalmente concesso tramite VPN: spesso è configurato attraverso la rete e quindi la porta d'ingresso all'azienda, e spesso richiede i giorni, o in base alla disponibilità delle risorse IT, settimane per essere definito.

Una volta configurato, il fornitore è quindi in grado di utilizzare la VPN per l'accesso 24 ore al giorno, sette giorni alla settimana e spesso può avere accesso ad altri dispositivi in rete anche senza che voi lo sappiate.

Così, mentre una VPN è considerata la forma più sicura di accesso remoto, può essere difficile da configurare, monitorare, limitare e revocare.

Secondo il Progetto SHINE, un gruppo di ricerca ha studiato come i sistemi SCADA/ICS possono essere trovati in Internet dai motori di ricerca come ad esempio SHODAN: circa da 2.000 a 8.000 nuovi dispositivi esposti vengono scoperti ogni giorno.

"Direi un quarto o un terzo di loro sono dispositivi che potrebbero essere vulnerabili agli attacchi di malware ... e buffer overflow, cross-site scripting, ed altre cose del genere", ha detto Bob Radvanovsky, ricercatore del Project SHINE. "Abbiamo la sensazione che la maggior parte sia o "non configurato per la security" o "non correttamente configurato"."

In realtà, il RISI, un database/repository a livello di settore per la raccolta, l'analisi e la condivisione delle informazioni in materia di incidenti di Security informatica recenti ha riferito che il 33% di tutti gli incidenti di Security ICS sono dovuti ad accesso remoto. (* Fonte: http://www.isssource.com/risi-industry-attacks-growing/)

Così, mentre ci sono benefici inerenti all'accesso remoto, questi stessi vantaggi inducono preoccupazioni ed alcuni degli incubi più comuni di Security a livello ICS.

No. 4: Change Management nella rete di Impianto

La gestione del cambiamento e delle configurazioni all'interno di ambienti industriali è un ostacolo importante sia per l'IT che le Operations. La tecnologia moderna ha permesso e permette un rapido aumento di connettività di dispositivi, e poiché la gestione del cambiamento e la modifica delle reti industriali è spesso difficile, a volte le reti dei sistemi in produzione sono cresciute senza tenere conto della Security.

Ad esempio, a fronte dell'esigenza di integrare anche i PC e strumenti del laboratorio per la qualità dell'acqua nella rete processo, per gestire e correlare adeguatamente di dati di qualità con quelli della produzione, sarebbe stato probabilmente necessario iniziare un nuovo progetto IT per estendere la VLAN di processo al laboratorio, con nuovi requisiti di scambio dati, nuova infrastruttura, gestione del rischio e security conseguente. Spesso la crescita è "organica" e si procede solo a collegamento dei nuovi utenti, e la rete inizia a non essere più sotto controllo.

In un mondo ideale, si dovrebbe essere in grado di effettuare rapidamente questa modifica e poi concedere gli ingegneri e utenti esterni un accesso controllato, molto limitato, anche solo a richiesta, se necessario.

In realtà questa implementazione ideale è spesso difficile da realizzare dal punto di vista dei costi e operativo e, di conseguenza, l'estensione della rete viene completata in "qualche modo".

In alternativa, proviamo a prendere in considerazione un secondo scenario potenziale in cui si sta semplicemente cercando di migliorare alcune attrezzature obsolete. Ci piacerebbe sostituire i dispositivi con attrezzature più moderne con una maggiore connettività e, allo stesso tempo, tenerli lo stesso isolati. Poi scopriamo che l'isolamento accoppiato con connettività dinamica si rivela difficile da configurare, allora decidiamo di configurare il nuovo dispositivo nello stesso modo del dispositivo precedente. Però è connesso.

Mentre questo è spesso considerata la 'migliore soluzione per ora' in quanto risolve il problema immediato, esso non fornisce stabilità per futuri cambiamenti.

Mentre l'espansione della rete, vale a dire la possibilità di aggiungere o rimuovere attrezzature, e una maggiore connettività hanno molti benefici, il procedere senza pensare alla Security è la base per un incubo per la Security ICS. Oggi, il numero di dispositivi esposti è in aumento mentre dovrebbe essere in calo: ecco perché questi cambiamenti devono essere accompagnati da un aumento delle misure di Security.

Il Change Management deve garantire non solo i dispositivi di oggi, ma fornire una solida base per la crescita futura della vostra azienda e dell'aumento inerente il numero di dispositivi collegati.

Conclusioni.

Lavorare in un mondo sempre più connesso e trarre vantaggio dalle tecnologie emergenti apre la porta a grandi possibilità ma anche a grandi rischi.

E' grande infatti il potenziale di una forza lavoro mobile, abilitata alla gestione di dati in tempo reale all'interno di un ambiente di lavoro sempre più automatizzato, in ogni settore dell'industria e delle utility, dall'impianto di trattamento acque, alle raffinerie di petrolio, a impianti di produzione.

Si parla di Industrial Internet of Things (IIOT): nel prossimo futuro avremo un proliferare di sensori, attuatori, dispositivi sugli impianti, ovunque e distribuiti, collegati alle nostre reti che saranno collegati ad Internet.

Oggi la tecnologia permette a operatori e responsabili, allo stesso modo, di accedere ai dati operativi critici su qualsiasi dispositivo in qualsiasi momento, ovunque.

Tuttavia, questa possibilità porta con sé il potenziale per intrusioni: una minaccia così grande che fa sì che alcuni evitano di aprire la porta, visto che una porta chiusa non permette di entrare. Ma spesso non è la via giusta, e non sempre è la più sicura: a volte ci sono porte di servizio e finestre non adeguatamente protette.

Ed allora vediamo che una terza opzione può prevedere un portone ben custodito. Le soluzioni di Security industriali moderne consentono alle organizzazioni di proteggere le loro reti in modo tale che gli operatori possono sfruttare le tecnologie disponibili durante il funzionamento in un ambiente molto sicuro.

Ed anche una adeguata formazione di ciò che è veramente una minaccia in contrapposizione con la vaga idea di ciò che significa una minaccia è anche la chiave per essere più sicuri.