Firewall per uso industriale

Come installare correttamente un firewall per proteggere la rete di controllo e Scada, in modo da preservare la produzione da rischi di 'cyber crime'

Fonte: blazingpir.com

Enzo Maria Tieghi (*)

Molti dei più diffusi standard del mondo industriale, come http, FTP, OPC (con Dcom), Ethernet IP, Modbus TCP, DNP3 e molti dei protocolli proprietari impiegati dai PLC e dai software Scada/HMI, presentano notevoli rischi per la security di reti e sistemi. Molti di essi sono però sconosciuti ai dispositivi del mondo IT, ad esempio i firewall, per cui scrivere regole che permettano di trasferire dati via OPC (con Dcom) attraversando appunto un firewall, può diventare un'impresa complessa.

Nello specifico, Dcom è un protocollo utilizzato sia da OPC, sia da Profinet. Impiega il servizio Microsoft RPC (Remote Procedure Call) del quale sono già note alcune vulnerabilità, che fra l'altro sono state la base dell'exploit del 'worm Blaster'. In aggiunta, OPC e Dcom aprono dinamicamente una serie di porte fittizie (tra la 1.024 e la 65.535), che possono essere difficili da far filtrare al firewall. D'altra parte, lasciare aperte 'porte' non presidiate introdurrebbe alcune vulnerabilità nei sistemi. È per questi motivi che il traffico OPC dovrebbe essere permesso solo tra la rete di controllo PCN (Process Control Network) e una DMZ (De-Militarized Zone), ossia un segmento di rete 'isolato', ed esplicitamente bloccato tra la DMZ e la rete aziendale (EN-Enterprise Network). Inoltre, si dovrebbe restringere il range delle porte utilizzate, modificando i 'registry' sui PC che utilizzano Dcom.

Per ovviare alle limitazioni introdotte e avere al contempo una comunicazione 'protetta', anche utilizzando OPC (e Dcom), è possibile introdurre la tecnica del 'tunnelling' per instradare le comunicazioni OPC anche attraverso il firewall. Il tunnelling permette infatti di incapsulare i protocolli per l'attraversamento in modo protetto delle zone in cui sia stata segmentata la rete di controllo PCN. A tale scopo, sono disponibili sul mercato prodotti software ad hoc.

Installazione e configurazione di un firewall

Una volta previsti i firewall nel progetto di rete industriale che si intende utilizzare, prima di scegliere quale apparato di protezione impiegare, acquistarlo e installarlo fisicamente, occorre definire esattamente quale e quanto traffico dovrà essere permesso su di esso: questo è forse il punto più critico da affrontare. Infatti, configurare il firewall in base alla regola 'deny all' non è possibile e sarebbe inutile. Di solito, si prende la decisione di vietare tutto quanto non sia assolutamente indispensabile per il business aziendale, per fare funzionare il sistema di controllo e condurre l'impianto. Quali impatti hanno però questi accorgimenti sulla security della rete di controllo, sullo Scada o sul DCS?

Molte aziende richiedono di configurare i sistemi di controllo e permettono il trasferimento e la scrittura di dati tramite comandi SQL dallo Scada/DCS all'Historian e al database relazionale, Oracle o MS-SQL che sia, attraverso il firewall. Sfortunatamente, il traffico SQL può anche essere un vettore di vulnerabilità, come è stato riscontrato nel 2003, quando si è diffuso il 'worm di Slammer'.

Vediamo due esempi. Nel primo, si sta installando un firewall a due porte senza DMZ per i server condivisi. Bisogna

pensare bene con quali regole configurarlo. Come minimo bisogna definire per ogni dispositivo di rete una matrice di regole sia riguardo all'indirizzo IP, sia alle porte (applicazioni) utilizzate. La parte di regole relative all'indirizzo dovrebbe restringere il traffico verso un numero ristretto di dispositivi, ad esempio i dati per l'Historian, sulla rete di controllo PCN da parte di un limitato set di indirizzi sulla rete aziendale EN. Infatti, permettere agli utenti della rete aziendale di accedere direttamente ai server all'interno della rete PCN non è prassi raccomandabile. Inoltre, bisognerebbe restringere le porte di accesso, limitando l'ingresso tramite protocolli sicuri come https: lasciare liberi protocolli come http, FTP, OPC/Dcom e protocolli Scada non criptati comporta infatti un rischio elevato, che potrebbe esporre a potenziali attacchi tramite 'sniffing' di traffico e/o a tecniche di 'man in the middle'.

Il secondo esempio prende in considerazione un'architettura con DMZ. Bisogna quindi configurare i sistemi per fare in modo che il traffico non possa attraversare l'area demilitarizzata, passando dalla rete PCN direttamente a quella aziendale. A parte alcune eccezioni, tutto il traffico di ogni segmento della rete deve terminare nella DMZ. Ciò permette un utilizzo più flessibile dei protocolli che possono attraversare il firewall, come Modbus TCP od OPC. Si potrebbe quindi mettere direttamente in comunicazione il server Historian e il server Web/terminal server nella DMZ con i PLC che sono sulla rete di controllo, mentre http può essere utilizzato solo dalla DMZ verso i client sulla rete aziendale. Entrambi i protocolli presentano vulnerabilità specifiche, ma in questo caso, con due firewall da attraversare, possono essere utilizzati ognuno per il suo scopo, poiché non attraverseranno mai due zone passando dalla rete PCN a quella aziendale e viceversa.

Fonte: e-victims.squarespace.com

Ormai asset riconosciuto del mondo dell'informatica, il firewall "è certamente un 'must have'", come ha asserito Raoul Chiesa, anche nel campo delle reti industriali

Firewall e DMZ per reti PCN/Scada

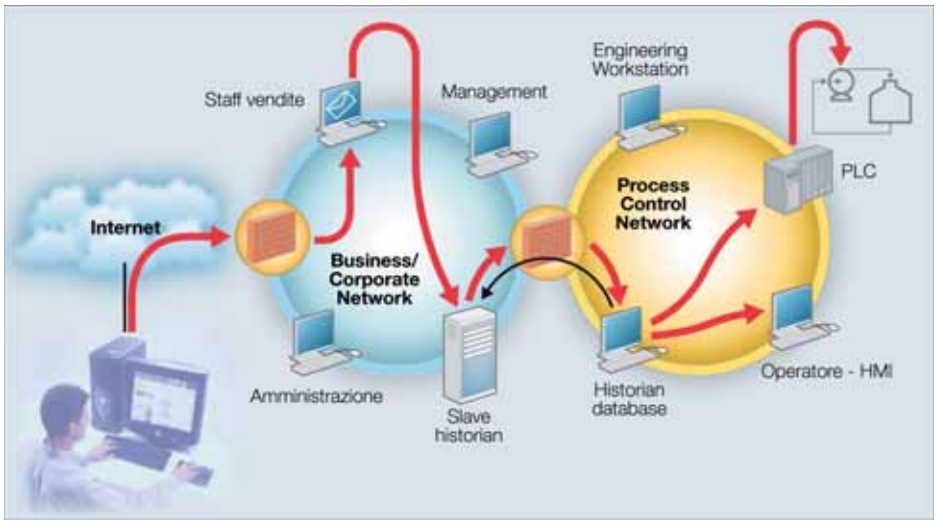
La presenza di server condivisi, ad esempio per la raccolta di dati per l'Historian, o database con informazioni d'impianto (produzione) tra la rete di controllo PCN/Scada e la EN ha un impatto considerevole in fase di progettazione della rete e nella scelta di utilizzare dei firewall, la loro configura-

UNA VOCE FUORI DAL CORO

Socio fondatore e membro del comitato direttivo e tecnico-scientifico di Clusit (Associazione Italiana per la Sicurezza Informatica), nonché senior advisor strategic alliances&cybercrime issues di Unicri (United Nations interregional crime & justice research institute), **Raoul Chiesa** *si occupa della tematiche 'Scada, automazione industriale e sicurezza logica' da alcuni anni. Venendo dal mondo IT, dove la sicurezza rappresenta un tema sempre attuale e di notevole spicco, gli abbiamo come vede la sicurezza relativamente al 'pianeta industria', dove del tema si sta cominciando a parlare seriamente solo da poco.*

Raoul Chiesa: *"Mi fa molto piacere che vi occupiate di sistemi firewall in ambito industriale, in quanto si tratta di un segno che qualcosa forse sta cambiando. Nel corso degli ultimi tre o quattro anni, infatti, nell'ambito di Clusit, mi sono occupato a fondo delle relazioni e iterazioni, spesso non semplici, tra la sicurezza informatica (InfoSec-Information Security) e il mondo Scada, DCS, PLC o, più in generale, dell'automazione industriale. Come sono solito sottolineare, esiste un divario di circa dieci anni tra questi due mondi, infatti se asset come i firewall sono uno standard 'de facto' nel mondo informatico, non si può certo dire altrettanto nel settore dell'automazione industriale, dove vendor e system integrator stanno appena iniziando a spingerli e proporli. Come dimostra il banale esempio della diatriba RID-DIR, ovvero 'Riservatezza, Integrità, Disponibilità' del dato contro 'Disponibilità, Integrità' e, solo in ultimo, 'Riservatezza', le necessità gli obiettivi che i due mondi perseguono sono esattamente speculari. La situazione che abbiamo osservato in questi anni, dunque, è tutto sommato 'normale' ed il mercato è ancora tutto da sviluppare. Il firewall è certamente un 'must have', ma entrano in gioco anche altre logiche, tipiche dell'InfoSec, che sono da trasportare in un'ottica differente e presso realtà diverse, dalle quali, spesso, può dipendere la stabilità dello stesso Sistema-Paese. Indubbiamente, il mondo dell'industria ha bisogno di cultura, best practice, esperienze condivise e, soprattutto, formazione. Per questo in Unicri partiranno da febbraio 2010 due corsi di specializzazione sulla tematica "Security in ambienti Scada e Infrastrutture Critiche Nazionali", che si terranno presso il campus internazionale dell'ONU a Torino"*

zione e installazione. In un'architettura a tre zone (PCN/DMZ/EN) viene naturale porre i server nella DMZ; se invece si utilizza un'architettura a due zone (PCN/EN), la scelta può divenire complessa. Mettere i server Historian e server Web/terminal server sulla rete aziendale, quindi al di qua del firewall di demarcazione tra le due zone, significa permettere il traffico di protocolli non sicuri quali Modbus TCP od OPC con Dcom, ed esporre ogni dispositivo della rete di controllo, che debba far confluire dati ai server, a minacce e vulnerabilità della rete aziendale. D'altra parte, lasciando il server Historian e server Web/terminal server sul lato della rete PCN, ci si trova nella situazione di dover lasciare passare protocolli altrettanto insicuri come http o SQL; inoltre, il server sulla PCN rimane accessibile da quasi chiunque in azienda.



Vulnerabilità in un'applicazione con replica di server Historian in due zone diverse (fonte INL)

In generale, conviene abbandonare l'idea delle due zone e adottare la soluzione a tre, connettendo gli apparati di raccolta dati alla rete PCN e quelli di storicizzazione dei dati ai server Historian e server Web/terminal server nella DMZ. In determinate situazioni, però, anche quest'architettura può mostrare il fianco a qualche preoccupazione. In caso di un numero elevato di accessi al server nella DMZ da parte di un gran numero di utenti dalla rete aziendale EN, infatti, si può arrivare a saturare le risorse del firewall che delimita la zona DMZ/EN. In questo caso si può arrivare, se necessario, a installare due server, di cui uno per una raccolta locale di dati, posto sulla rete di controllo PCN o nella DMZ, e un secondo in 'mirroring', con continuo allineamento tra i due, ubicato sulla rete aziendale EN, in grado di far fronte alle elevate richieste di dati da parte di client sulla Intranet.

Con questa configurazione si entra nel tema di vulnerabilità e minacce relative a comunicazioni server-to-server, poiché si avrebbero i due server in comunicazione diretta. Se si affronta correttamente e con una protezione adeguata, il rischio di incidenti risulta notevolmente mitigato.

Policy adeguate per la gestione dei firewall

Come in casa una buona porta blindata non deve essere lasciata aperta, né bisogna avere troppe copie di chiavi in giro, così non si deve sottostimare l'importanza di dotarsi, una volta installato un firewall, delle giuste regole di gestione e manutenzione, perché questo dispositivo possa continuare a espletare al meglio i propri compiti.

Dunque, se il firewall è un componente fondamentale della rete di controllo PCN e sicuramente il centro focale della protezione della rete stessa, occorre ricordare anche che richiede notevoli risorse. Questo non solo in fase di progettazione iniziale della rete, nonché di acquisto, installazione e configurazione, ma anche e soprattutto lungo l'intero ciclo di vita del sistema, per la sua corretta gestione, l'analisi dei log generati, la gestione degli incidenti, l'aggiornamento, il supporto e l'assistenza tecnica. Spesso invece l'impegno viene sottostimato. All'inizio vi è molta sensibilità sul tema della security, poi però, con il tempo, il livello di attenzione decresce e anche i migliori presidi divengono inutili.

Solitamente, trattando della protezione di reti e sistemi e di 'cyber security', si tende oggi a spendere molto in tecnologia, pensando di adottare valide contromisure e di risolvere quindi i problemi di sicurezza, rimanendo però esposti a molti rischi non solo a causa di configurazioni non corrette, ma anche per comportamenti non adeguati e una gestione non confacente. Nell'elenco dei compiti che dovrebbero essere assegnati ed eseguiti per implementare e gestire correttamente i firewall a protezione delle reti di controllo, si trova al primo posto la necessità di porre attenzione alla gestione della configurazione e alla documentazione.

In particolare, la configurazione e le regole definite per amministrare la rete PCN, i sistemi Scada e DCS possono avere un impatto considerevole sugli apparati di gestione aziendale e sulla continuità della produzione, a livello ad esempio di controllo della qualità, ISO9001 ecc., come sulle emissioni, per quanto concerne nello specifico l'ambiente, le norme ISO14001 ecc., e sulla sicurezza fisica (SGS-OHS18001, legge 196 ecc.) degli impianti e delle fabbriche. Bisogna quindi gestire correttamente tutti gli accessi alla programmazione, raccogliere in modo puntuale la documentazione relativa alle variazioni che vengono apportate, fare i back up per poter eventualmente ripartire in caso di bisogno. Soprattutto, è necessario rivedere

periodicamente se le regole fissate sono ancora attuali e allineate ai requisiti del sistema, alle minacce e alle vulnerabilità del momento. Inoltre, per verificare se sono presenti falle e incidenti e/o si sono concretizzati dei tentativi di attacco è consigliabile eseguire dei test periodicamente o secondo necessità sui log dei firewall e dei dispositivi antintrusione IDS.

È anche utile preparare un piano di risposta all'emergenza (Incident Response Plan), in cui vengano definite le responsabilità e si descriva che cosa debba essere fatto in caso d'incidente e da chi, per evitare eventuali operazioni avventate prese 'sotto emergenza' e in stato di panico. Il piano potrebbe anche prevedere di scollegare la rete di controllo PCN da tutte le altre reti dell'azienda; poiché spesso il distacco fisico è impraticabile, nel piano occorre definire la strategia migliore per effettuare in modo congruo l'operazione. Infine, il gruppo o la persona preposte al controllo del firewall dovrebbero tenere sotto osservazione anche quanto avviene e/o viene loro comunicato dall'esterno, ad esempio tramite mail di allarme da parte dei fornitori di software e hardware dei sistemi installati, segnalazioni di vulnerabilità e minacce ecc.

La gestione degli aggiornamenti e delle patch sui sistemi di controllo e i loro componenti è uno dei temi più delicati da affrontare, insieme a quello relativo alla competenza e consapevolezza del personale, nonché al training cui gli addetti dovrebbero periodicamente partecipare. Si tratta di uno degli aspetti più importanti della sicurezza dei sistemi e spesso è anche uno dei più trascurati, in quanto non si ritiene necessario spendere denaro per il supporto, la formazione, l'acquisto di corsi. Del resto, acquisire nuovi dispositivi è spesso inutile, quando non viene utilizzato in modo efficace quanto è già stato implementato. Una migliore gestione del parco installato può infatti elevare il livello di protezione del sistema. Rivolgersi a specialisti per fare assessment, eseguire una valutazione dei rischi e identificare le strategie migliori per la security è sicuramente una delle pratiche consigliate, che porta quasi sempre a evitare errori e spese avventate, migliorando considerevolmente la conoscenza del sistema da parte sia di chi lo ha implementato, sia di chi lo utilizza quotidianamente. Sforzi e risorse spesi in consapevolezza e training sui temi della sicurezza hanno l'impatto maggiore e possono aumentare considerevolmente il livello di protezione e security di tutta l'infrastruttura. ■

(*) Estratto dal Quaderno Clusit: "Introduzione alla protezione di reti e sistemi di controllo e automazione (DCS, Scada, PLC ecc.)"

Clusit readerservice.it n. 16