La sicurezza informatica nei sistemi industriali

I sistemi industriali di controllo e supervisione di processo presentano problematiche di sicurezza informatica che non devono essere sottovalutate

MASSIMO GIUSSANI

Nell'agosto del 2005 la diffusione del worm 'zotob' e delle sue varianti ebbe grande risalto mediatico soprattutto per via del fatto che vennero attaccati i sistemi informatici del New York Times e delle reti televisive ABC e CNN. Il worm, diffuso attraverso Internet, interessò prevalentemente sistemi Windows 2000 provocando ripetuti spegnimenti e riavvii degli elaboratori infettati. Ma a essere affetti non furono solo i sistemi in prima linea sul fronte del Web: anche alcuni sistemi di controllo di processo in ambito industriale subirono danni rilevanti. Ben tredici impianti produttivi della Daim-ler Chrysler in sei stati americani dovettero sospendere le attività per un periodo di tempo compreso tra i cinque e i cinquanta minuti mentre gli amministratori di si-stema provvedevano ad applicare le patch. Incidenti di questo tipo hanno una probabilità maggiore di interessare i sistemi industriali di controllo rispetto al passato per via della crescente complessità dei componenti utilizzati e delle interazioni con le porzioni della rete aziendale che si rivolgono al mondo esterno. Da un lato i dispositivi per il controllo distribuito sono dotati di connettività alla rete Intranet e/o Internet per il trasferimento dei dati di produzione e la gestione degli allarmi; dall'altro la connessione della rete di controllo con la rete di gestione aziendale connessa a Internet può esporre dispositivi critici a manipolazioni da parte di personale non autorizzato. La sicurezza informatica è stata oggetto di un incontro, organizzato da Vision Automation lo scorso novembre, con Jonathan Pollet, esperto di cybersecurity a livello internazionale. Pollett, in Italia per partecipare all'European Utility Telecom Conference tenutasi a Roma, ha avuto

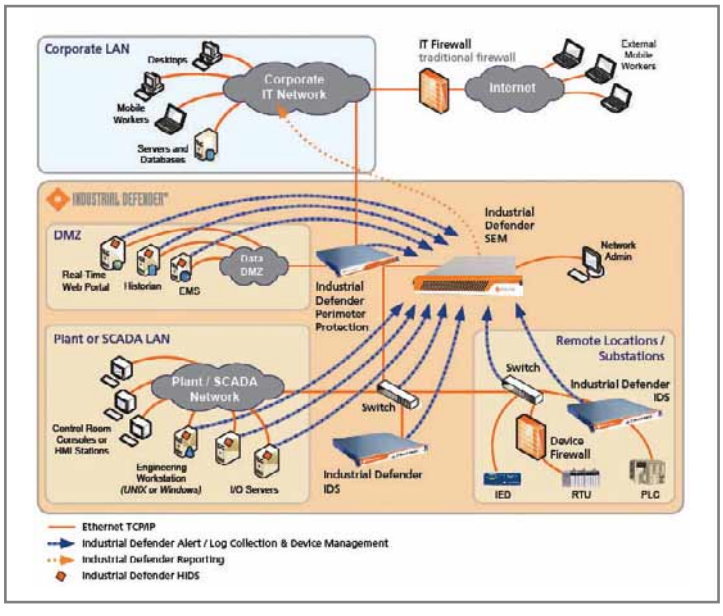

Fig. 1 - Esempio di protezione con Industrial Defender

modo di illustrare le vulnerabilità tipiche di un sistema di controllo industriale e le relative contromisure con riferimento alla suite Industrial Defender messa a punto da Verano, azienda americana specializzata in Scada mission-critical.

Pianificare la sicurezza

Le istituzioni governative e le associazioni industriali sono attivamente impegnate, in questi anni, a promulgare e a promuovere degli standard di sicurezza per la protezione delle infrastrutture critiche dagli attacchi informatici. L'adozione di un sistema di difesa informatica può essere necessaria per tutelarsi dalle cause legali per omessa custodia dei dati sensibili e può presentare effetti collaterali positivi, come la riduzione dei premi assicurativi per i casi di perdita dei dati.
Quello della sicurezza è un tema complesso che trascende l'aspetto squisitamente tecnologico: per gestire correttamente la sicurezza in un'azienda è infatti necessario operare su più livelli. Innanzitutto deve essere curata la sicurezza 'fisica', limitando l'accesso in azienda ed, eventualmente, nei reparti sensibili, al solo personale autorizzato. In questo sono utili i sistemi di identificazione automatizzati, meglio se biometrici e incrociati con i sistemi tradizionali (come la classica tessera magnetica con foto). Il secondo, importante, passo da intraprendere è quello della formazione del personale, che deve essere istruito a utilizzare diligentemente i sistemi di identificazione e a riconoscere i tentativi di phishing, ossia di estorsione delle informazioni da parte di terzi. Particolare attenzione deve essere rivolta alla gestione delle password che devono essere scelte in maniera non banale, venire rinnovate periodicamente e non essere mai comunicate a terzi, né devono esser messe in bella vista su post-it attaccati alla cornice del monitor (potrà sembrare strano, ma questo caso è più frequente di quanto si possa immaginare). Dato che la maggior parte degli attacchi informatici in un'azienda proviene dall'interno della rete e non dall'esterno, il personale deve essere informato dei rischi di infezione per mezzo di CD, Dvd, penne Usb e altri dispositivi di memorizzazione rimovibili. Quello tecnologico è dunque l'ultimo, ma non per questo meno importante, aspetto della sicurezza informatica: firewall, router, cifratura dei dati e agenti software che controllano le transazioni in atto e registrano ogni possibile anomalia sono l'ultimo baluardo di difesa dagli attacchi interni ed esterni. Il mondo industriale presenta tutta una serie di nuove sfide e pericoli sotto questo profilo, dato che a essere esposti agli attacchi sono i sistemi di controllo distribuito, i controllori logici programmabili connessi in rete, le reti con gli archivi storici e le infrastrutture di rete per la gestione d'impresa. Se un sistema informatico

Industrial Defender, la soluzione scalabile di Verano

Verano Industrial Defender è la prima suite di prodotti espressamente pensati per la gestione della sicurezza dei sistemi industriali e realizzati da un unico produttore. La suite consiste di componenti hardware e software (la console, i dispositivi di protezione perimetrale, i sensori di rete, gli agenti software, l'applicativo di supervisione) che permettono di creare un sistema di protezione a misura di applicazione e di budget. Industrial Defender è una soluzione completa di monitoraggio, rilevamento e notifica che supporta svariati tipi di firewall, router, switch, IDS (Intrusion Detection System) e dispositivi di controllo industriale. Il sistema di gestione gira sotto Linux e offre agli utilizzatori un'intuitiva interfaccia grafica basata sul browser Mozilla. La console consente il monitoraggio, il controllo, la gestione degli allarmi, l'analisi, la memorizzazione e la creazione di report relativi ai dati di sicurezza e alle prestazioni del sistema. Gli agenti software sono in grado di rilevare problemi nelle applicazioni di controllo, intrusioni provenienti dalla rete interna o esterna, variazioni, cancellazioni e alterazioni nei server e nei parametri delle interfacce uomo-macchina, oltre che colli di bottiglia prestazionali che possono preludere a un utilizzo improprio della rete. I sensori di rete (NIDS, Network Intrusion Detection Sensor) sono in grado di rilevare un'ampia gamma di schemi di attacco, registrano le attività sospette e inviano messaggi di allarme alla console preposta alla gestione della sicurezza. Una delle peculiarità del sistema messo a punto da Verano è che i sensori di rete sono in grado di gestire funzioni specifiche delle apparecchiature di controllo; per esempio il sistema è in grado di riconoscere l'impiego delle password di fabbrica (suggerendone la modifica), sa gestire i protocolli industriali come Modbus e DNP3, ed è in grado di riconoscere il trasferimento dati dovuto all'aggiornamento del software dei PLC. I sensori Snmp rilevano le prestazioni e i problemi di sicurezza negli switch, nei router e in tutte quelle apparecchiature di controllo e automazione che supportano il protocollo Smnp, come PLC, robot e terminali remoti. Gli agenti passivi per le apparecchiature di controllo e automazione, disponibili per i sistemi operativi Unix, Windows e Linux, funzionano come sensori di rilevamento delle intrusioni e comunicano direttamente con la console di Industrial Defender. Sono appositamente pensati per richiedere risorse minime dal punto di vista del traffico di rete e dell'occupazione della CPU, in modo da non interferire in maniera percettibile con le prestazioni del sistema e da permettere la loro implementazione anche sulle piattaforme meno recenti. Più in dettaglio, gli agenti utilizzati da Industrial Defender sono espressamente pensati per utilizzare meno dell'1% del throughput di rete e meno del 3% di utilizzo della CPU del dispositivo che li ospita. L'offerta di Verano-Vision Automation è completata dai servizi di identificazione delle problematiche di sicurezza, di pianificazione degli interventi, di formazione del personale e di supporto alla gestione.

tradizionale può andare incontro al rischio di una perdita di dati (mitigabile ricorrendo a salvataggi periodici), un sistema industriale può essere soggetto a rischi che contemplano l'interruzione della produzione, l'incolumità fisica del personale e addirittura disastri ecologici (si pensi al controllo di processo di un impianto chimico o nucleare, per esempio). La diffusione delle reti wireless, anche a livello di fabbrica, peggiora ulteriormente il quadro rendendo possibile l'accesso alla rete interna senza doversi necessariamente trovare a un terminale aziendale o dover passare attraverso un firewall su rete cablata: la cifratura dei dati diviene in questo caso una necessità inderogabile.

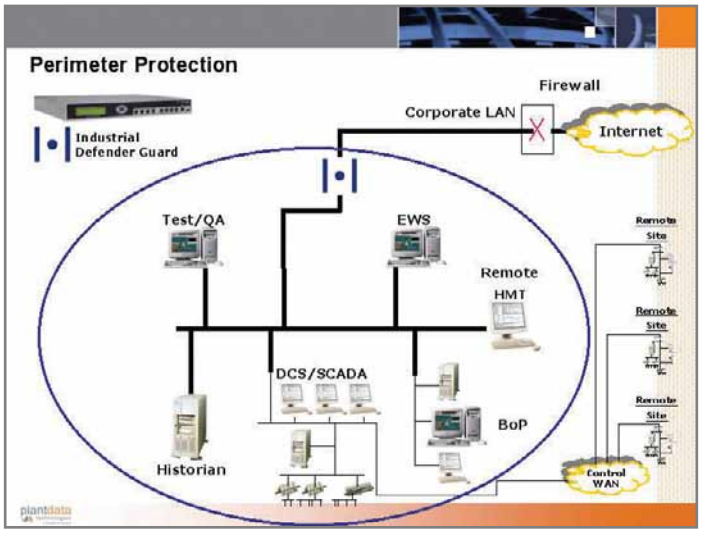

Fig. 2 - Protezione perimetrale

Sicurezza multistrato

Ogni impianto è un caso a sé stante e deve essere valutato nella sua specificità per trovare il giusto compromesso tra sicurezza, prestazioni e costi di implementazione e gestione. Il tipico approccio per la messa in sicurezza di un impianto esistente consiste di quattro passi: una valutazione preliminare che permette di individuare e classificare le falle del sistema; una fase in cui si decide quali provvedimenti devono e possono essere presi; la messa in atto delle misure di protezione (con la successiva gestione); la verifica della sicurezza del sistema.
La fase più importante, e spesso più onerosa, è la prima: difatti, anche se ci dovesse essere la disponibilità a mettere in sicurezza tutte le falle, la sola conoscenza dei potenziali pericoli può essere utilizzata per limitare i rischi di intrusione. L'implementazione delle misure protettive può interessare diversi strati dell'infrastruttura di rete: un firewall esterno permette di disaccoppiare la rete interna da quella esterna, e fornisce un primo elementare, ma spesso insufficiente, livello di protezione. La rete di controllo può essere dotata di una propria protezione perimetrale, che gestisca le transazioni con le rimanenti porzioni di rete aziendale e provveda alla validazione degli accessi. Una soluzione di protezione che si limiti a questi due strati presenta il vantaggio di non alterare l'infrastruttura esistente e di non richiedere l'arresto del sistema per la sua messa in opera (figura 2). Maggior sicurezza può essere ottenuta isolando i vari sottosistemi, connettendoli a un di-spositivo che provveda a gestire il traffico tra di loro (figura 3), filtrando tutto ciò che non rientra nel funzionamento ordinario della rete; l'alterazione della topologia rende però inevitabile metter mano al cablaggio delle sottoreti. E' anche possibile dotare ciascun sottosistema di una propria protezione, ma in sistema di controllo di media complessità il numero di modem distribuiti nell'impianto renderebbe troppo onerosa questa scelta rispetto a quella di un controllo centralizzato della sicurezza, più facilmente gestibile anche dal punto di vista della manutenzione. Il controllo perimetrale, eventualmente frazionato, può essere arricchito con un sistema di supervisione che raccolga i dati pertinenti alla sicurezza e alle prestazioni per individuare possibili minacce, per concertare le operazioni di aggiornamento e per notificare gli allarmi al personale autorizzato. L'aggiunta di opportuni agenti software che estraggano informazioni utili dai vari componenti dell'impianto rende più capillare la gestione della sicurezza e presenta l'ulteriore vantaggio di disaccoppiare l'hardware legato al controllo di processo vero e proprio dagli elementi preposti alla difesa dalla minacce informatiche e quindi maggiormente soggetti ad aggiornamenti. ■

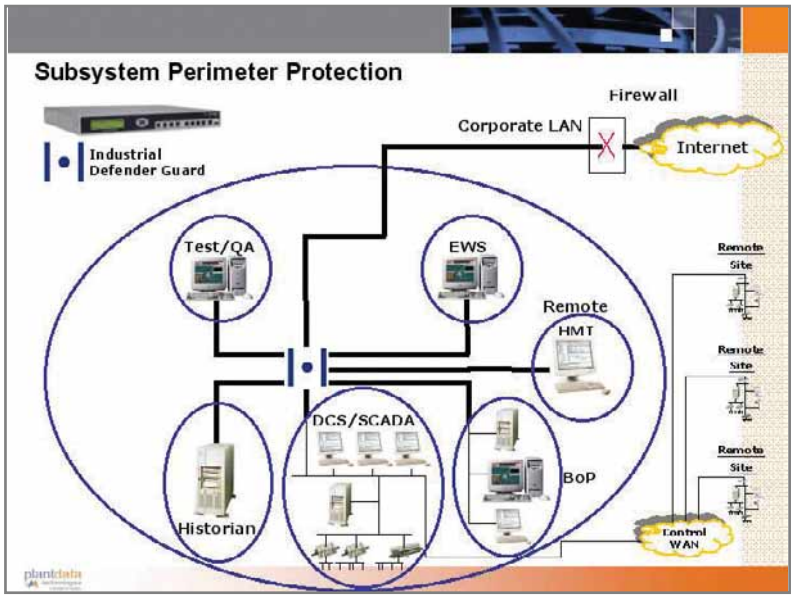

Fig. 3 - Protezione perimetrale frazionata

Vision Automation
readerservice.it n. 26