QUALE SICUREZZA?

COME FRONTEGGIARE MALWARE, VIRUS E TENTATIVI DI INTRUSIONE GARANTENDO CHE LA RETE SIA SICURA E PROTETTA: STANDARD E LINEE GUIDA

di **Evaldo Bartaloni (**), Luca Guidi (*), Daniela Pestonesi (*)**

Oggigiorno, i sistemi di controllo di importanti processi industriali sono sempre più integrati con il tradizionale sistema informativo aziendale e fanno uso di tecnologie standard. La maggior parte dei servizi di supervisione, diagnostica e manutenzione sulle apparecchiature di controllo di processo viene eseguita in remoto. In pratica, l'uso intensivo delle moderne tecnologie di informatica e telecomunicazioni ha aperto nuove strade per lo svolgimento di attacchi. Il paradosso è che più si utilizzano i sistemi ICT, più aumenta la probabilità di intrusioni da parte di soggetti malintenzionati esterni e interni. Una violazione dell'integrità, della disponibilità o anche della riservatezza dei dati può produrre danni significativi al patrimonio delle aziende e, quando si tratta di infrastrutture critiche, i rischi si estendono all'intera società. Le organizzazioni devono quindi affrontare le minacce alla sicurezza provenienti da una vasta gamma di fonti e sono vulnerabili a virus e attacchi di pirateria di varia natura. La sicurezza informatica ottenibile esclusivamente mediante mezzi tecnici non è sufficiente, ma deve essere sostenuta da policy e procedure.

Trent'anni di minacce

È passato molto tempo da quando fu creato il primo virus per PC. Era il 1986 quando i fratelli pakistani Amjad Farooq Alvi e Basit Farooq Alvi crearono il primo virus; il mondo era molto diverso da oggi e i fratelli Alvi, che addirittura inserirono i propri riferimenti, non avevano cattive intenzioni. In realtà, sembra che il primo 'attacco' a un sistema di controllo industriale risalga a circa quattro anni prima. Thomas C. Reed, segretario di Ronald Regan, ha descritto nel suo libro *"At the abyss: An Insider's History of the Cold War"*, come gli Stati Uniti abbiano organizzato un vero e proprio sabotaggio all'Unione Sovietica tramite un software Scada manipolato. Lo Scada era quello che gestiva il gasdotto trans-siberiano; nel libro si cita un'esplosione da 3 kiloton avvenuta nel giugno 1982 in Siberia come risultato di questa azione.

Da allora tante cose sono successe e gli 'incidenti', grandi e piccoli, ai sistemi di controllo industriali sono ormai all'ordine del giorno.

Siamo passati dagli hacker dilettanti agli hacker professionisti, poi alle bande organizzate e al cyber-crime, fino alla vera e propria cyber-war. In molti hanno sentito parlare di Stuxnet, un worm estremamente sofisticato scoperto nel 2010 e destinato a mettere fuori servizio gli impianti di arricchimento dell'uranio iraniani; forse in pochi conoscono Duqu e Flame, che rappresentano l'evoluzione di Stuxnet e sono stati definiti *"Two cyber weapons unleashed by same master"* a ribadire il fatto che Stuxnet ha rappresentato un vero e proprio salto di qualità nel mondo della cyber-war.

L'ICS-Cert, che è il Cyber Emergency Response Team dei sistemi di controllo industriali gestito dal Department of Homeland Security americano, ha recentemente pubblicato un rapporto che rende noto l'aumento enorme del numero di infrastrutture che hanno subito attacchi o incidenti informatici negli ultimi anni. Il numero di tali incidenti è aumentato da 41 nel 2010 a 198 nel 2011 e questi dati sono verosimilmente di gran lunga inferiori a quelli reali, perché la maggior parte delle infrastrutture critiche è di proprietà privata e la notifica degli incidenti all'ICS-Cert è volontaria.

Cosa si sta facendo nel mondo per affrontare il problema?

La stragrande maggioranza dei produttori di Scada hanno iniziato ad affrontare i rischi di minacce informatiche attraverso lo sviluppo di linee di firewall industriali specializzati e soluzioni VPN per reti Scada basate su protocollo TCP/IP. Inoltre, vengono implementate applicazioni per sistemi di controllo capaci di prevenire le modifiche non autorizzate e le cui prestazioni non vengono compromesse dalle scansioni dei comuni antivirus. Gli utenti finali, d'altra parte, iniziano a chiedere stringenti requisiti di sicurezza nelle specifiche tecniche dei sistemi di controllo.

Nel documento *"Strategic Analysis of the World Scada Market"* di Frost & Sullivan, si indica un fatturato di 4.585 milioni di dollari nel 2009 nel settore della cybersecurity e si stima che si raggiungeranno 6.902 milioni di dollari nel 2016. I rischi informatici alla rete elet-

Fonte: www.osti.gov

trica richiederanno alle utility di effettuare nuovi investimenti significativi in sicurezza informatica per ICS; la stima di Pike Research è di passare dai circa 300 milioni del 2011 a quasi 700 milioni di dollari all'anno entro il 2018.

Linee guida e standard

La buona notizia è che oggi le aziende hanno a disposizione una risposta ai loro problemi: si tratta di standard, linee guida e best practice.

La necessità di sviluppare metodologie specifiche in grado di fornire risposte adeguate è nata parecchi anni fa. Per il settore della generazione elettrica, il gruppo WG15 di TC57 di IEC ha affrontato in modo specifico tali esigenze e, con il Report IEC TR 62210 del maggio 2003 ha proposto un approccio per l'analisi della sicurezza con speciale attenzione ai protocolli di comunicazione definiti da tale commissione.

I gruppi di utenti e le attività di normazione che si occupano di questioni relative alla sicurezza nel settore dei sistemi Scada sono cresciuti rapidamente negli ultimi anni. Tutto ciò, da una parte rappresenta una buona notizia, poiché si attesta che la sicurezza è una questione importante, dall'altra, genera una giungla di norme e linee guida. Una rassegna sui recenti sforzi per realizzare tali norme è stata fatta all'interno del Progetto ESCoRTS (*"A European network for the Security of Control and Real-Time Systems"*) finanziato dalla Comunità Europea e coordinato da CEN - Comité Européen de Normalisation. In totale sono stati individuati e analizzati 37 fra standard, direttive e altri documenti che hanno rilevanza per gli operatori o per i fornitori nel settore della sicurezza informatica dei sistemi di controllo. Tredici sono standard o linee guida internazionali, quattordici sono fornite dai comitati degli Stati Uniti e dieci sono definite da gruppi europei.

Tra i documenti più rilevanti figurano...

ISO 27000 *"Information technology - Security techniques - Information security management systems"*: ISO (International Organization for Standardization) è la maggiore organizzazione internazionale di standard: ne ha pubblicati più di 19.500. Questa famiglia di standard, di tipo 'general purpose', ha l'obiettivo di definire il sistema di gestione della sicurezza delle informazioni. È quindi simile alla famiglia ISO 9000 per la qualità e ISO 14000 per l'ambiente e non è specifico per i sistemi di controllo industriali.

ISA99/IEC 62443 *"Industrial Automation and Control Systems Security"*: ISA (International Society of Automation) lavora da anni alla produzione della famiglia di standard ISA99, di carattere generale ma indirizzato ai sistemi di controllo industriale e quindi, proprio per questo, più utile alle aziende che devono affrontare il problema di cybersecurity dei loro impianti. Purtroppo, dei trecidi documenti previsti, solo un numero esiguo è stato pubblicato; molti sono in bozza per commenti.

A seguito di un accordo con IEC questo standard appare ora come ISA/IEC 62443. Nist 800-82 "Guide to Industrial Control Systems Security": il National Institute of Standards and Technology (Nist) è un'agenzia federale USA che sviluppa e promuove misurazioni, standard e tecnologie, molto attiva e prolifica anche in materia di cybersecurity. A differenza del documento Nist 800-53 dedicato ai sistemi IT tradizionali, 800-82 è indirizzato al mondo dell'automazione industriale; fornisce una panoramica degli ICS e delle tipologie tipiche di sistema, identifica le minacce e le vulnerabilità tipiche di questi sistemi, fornisce le contromisure di sicurezza raccomandate per ridurre i rischi associati.

Cpni *"Good practice guide - Process control and Scada security"*: il Center for the Protection of National Infrastructure è stato formato in UK dalla fusione di Niscc - National Infrastructure Security Co-ordination Centre con Nsac - National Security Advice Center, una parte del noto servizio di sicurezza del Regno Unito MI5. Le linee guida sono costituite da sette documenti di 'best practice' specifici per i sistemi di controllo industriali emessi da tale organismo, attivo per la protezione delle infrastrutture critiche in un importante paese europeo. Nel settore elettrico, senza dubbio uno dei più avanzati per quanto riguarda l'implementazione di misure di sicurezza, è da prendere come riferimento anche lo standard Nerc CIP, costituito da nove documenti ed emesso dal National Electricity Reliability Council, cioè l'organismo che regola l'affidabilità del sistema elettrico USA. Contiene raccomandazioni rilevanti per gli operatori del sistema elettrico negli Stati Uniti adottati dalla Federal Energy Regulatory Commission nel 2006 e resi obbligatori per le utility americane.

Qualche riflessione...

Una prima considerazione da fare è che nessun singolo standard copre tutti gli aspetti, dal progetto all'implementazione e all'esercizio di sistemi di controllo 'sicuri'. La seconda considerazione è che esistono molte sovrapposizioni e ciò può dar luogo a indicazioni quantomeno non coincidenti. Resta, quindi, a carico delle singole aziende la scelta dell'adesione a uno degli standard proposti o la possibilità di selezionare parti di interesse da più documenti al fine di un'elaborazione personalizzata di linee guida da applicare all'interno dei propri confini. Da un punto di vista pratico, le contromisure da intraprendere per aumentare il livello di security della propria infrastruttura dipendono poco dalla soluzione prescelta. Adottando uno standard molto generale si avrà più libertà nel definire i dettagli, mentre con linee guida specifiche avremo già prescrizioni molto dettagliate che, però, dovremo verificare se coprono tutto il perimetro d'interesse. In ogni caso, per un'efficace azione di abbattimento del rischio si dovranno trattare tre grandi capitoli: governance, host, network.

- Nel capitolo della governance dovrà essere descritto come definire organizzazione e responsabilità in materia di security, strategie, processi e procedure.
- Nel capitolo degli host si dovranno affrontare le seguenti categorie di requisiti: controllo accessi, gestione dell'esercizio e acquisizione, sviluppo e manutenzione dei sistemi.
- Nel capitolo del network si parlerà di architettura, sicurezza perimetrale e protocolli, gestione dell'esercizio delle reti e gestione degli accessi ai sistemi connessi.

Ma quanto mi costi?

La domanda che le aziende si pongono è: "Ma quanto costa mettere in sicurezza i sistemi di controllo degli impianti industriali?". Non è possibile fornire una risposta valida in generale. Sicuramente è fondamentale fare delle stime dei costi che possano essere messe a confronto con i rischi, o più precisamente, con la diminuzione dei rischi che si ottiene con l'investimento in security. Proprio su questo tema è in corso un progetto europeo che ha l'obiettivo di fare queste valutazioni per le infrastrutture critiche della produzione e trasmissione di energia elettrica: *"Emerging Security Standards to the EU power Network controls and other Critical equipment (Essence)"*.

(*) Enel Ingegneria e Ricerca SpA
(**) Comitato Tecnico AO e F&N