VULNERABILITA' INFORMATICA DEI SISTEMI SCADA CONNESSI ALLE RETI PUBBLICHE

Stefano Panzieri*[1], Ilaria Scarano*, Roberto Setola°†

* Dip. Informatica e Automazione, Università degli Studi "Roma Tre"
Via della Vasca Navale 79, 00146 Roma

° Facoltà di Ingegneria , Università CAMPUS Biomedico di Roma,
Via E. Longoni, 83, 00155 Roma

panzieri@uniroma3.it

SOMMARIO

I sistemi informatici SCADA, generalmente impiegati per il controllo ed il monitoraggio di reti di distribuzione dell'energia elettrica, del gas, o dell'acqua, oppure impiegati nella supervisione di impianti industriali, sono stati storicamente progettati come elementi autonomi ed isolati rispetto alle altre reti telematiche aziendali. Per una serie di ragioni di natura economica, sociale, organizzativa e tecnologica questo scenario è andato rapidamente modificandosi nell'ultimo decennio. I sistemi SCADA risultano, infatti, ora profondamente integrati con le altre reti informatiche aziendali al punto da risultare affetti dalle stesse vulnerabilità che caratterizzano queste ultime. Ciò impone la necessità di modificare le strategie di sicurezza iniziando a considerare, in parallelo alle minacce fisiche, anche quelle provenienti dal cyberspace.

A causa della crescente rilevanza che rivestono le diverse infrastrutture per le società industrializzate, queste vulnerabilità vengono a configurarsi come un potenziale obiettivo per azioni criminose o terroristiche perpetrate sia in modo tradizionale sia tramite il cyberspace.

1. INTRODUZIONE

Le infrastrutture tecnologiche che sono alla base delle società industrializzate sono caratterizzate da una crescente complessità che impone l'adozione di sofisticati sistemi di monitoraggio e controllo. Questo si traduce nella necessità di un massiccio ricorso alle tecnologie ICT (Information and Communication Technologies) che ha avuto come conseguenza l'incrementato esponenziale delle dipendenze ed interdipendenze funzionali esistenti fra le diverse infrastrutture, al punto che un guasto, di natura accidentale o dolosa, può facilmente propagarsi tra di esse amplificando, di conseguenza, gli effetti negativi [1].

Questo scenario comporta, inoltre, che uno dei maggiori problemi alla sicurezza delle infrastrutture sia rappresentato dalle minacce informatiche. Le vulnerabilità derivanti dalla connessione di queste al cyberspace, spesso tramite connessioni alle reti corporate, sono dovute a diversi fattori. Tra i vari, ricordiamo la condivisione dei canali di trasmissione, la progressiva maggiore interoperabilità dei sistemi SCADA con le procedure aziendali e l'introduzione di sistemi operativi commerciali al posto di quelli proprietari [9]. Tutto ciò, unito alla carenza di un'opportuna politica di sicurezza per i sistemi installati [2], comporta un incremento potenzialmente pericoloso della possibilità di condurre attacchi, attraverso il cyberspace, ai sistemi informatici che presiedono la conduzione della stragrande maggioranza degli impianti infrastrutturali e produttivi di una nazione. Sotto quest'ottica, i sistemi SCADA (Supervisory Control and Data Acquisition) non sono assolutamente esenti da vulnerabilità, anche se fino a qualche anno fa si riteneva, in maniera quasi pregiudiziale, che essi fossero al riparo da potenziali attacchi [3].

Il risultato della connessione sopra descritta è che la sicurezza dei sistemi SCADA ha gli stessi punti di forza, ma soprattutto di debolezza, di quelli della rete societaria. In definitiva, va preso atto che l'attuale evoluzione della tecnologia SCADA tende all'impiego sempre più diffuso di protocolli e reti di comunicazione di tipo aperto. Se da un lato tali reti sono in grado di minimizzare i costi dei sistemi informatici delle imprese, dall'altro pongono numerosi problemi relativi alla sicurezza.

Si dovranno seguire, pertanto, regole di progettazione basate su criteri definiti in opportune politiche di sicurezza. La definizione di queste rappresenterà il primo stadio dell'intero ciclo di gestione della sicurezza

[1] Membro del Gruppo di Lavoro sulla Protezione delle Infrastrutture Critiche istituito presso la Presidenza del Consiglio dei Ministri – Dipartimento per l'Innovazione e le Tecnologie

[13], e sarà necessario garantire non solo la sicurezza passiva (firewall, access list, metodi progettuali e flussi applicativi), ma anche la sicurezza attiva, ricorrendo a sistemi di Intrusion Detection configurati in base a regole e/o criteri prestabiliti. Non possiamo tacere la necessità di definire tali procedure in maniera dinamica così da poter affrontare un'evoluzione praticamente continua sia dei fattori di rischio, sia dei presidi atti a ridurli, ed al contempo sviluppare una vera cultura della sicurezza aziendale.

In questo articolo verrà presentato il problema dell'interdipendenza dei sistemi SCADA con il cyberspace e verrà evidenziato il rischio informatico che ne deriva. Una analisi degli attacchi noti in letteratura, insieme alla presentazione dei nuovi scenari tecnologici collegati a questi sistemi, consentirà di porre l'accento sulle problematiche di sicurezza che necessariamente dovranno essere affrontate e risolte nel corso dei prossimi anni, pena l'esposizione di molte delle infrastrutture critiche nazionali a rischi sempre crescenti di malfunzionamenti indotti intenzionalmente o meno. Gli autori vogliano porre l'accento sulla necessità di schierare molteplici contromisure che dovranno considerare come un unico terreno di sfida sia quello fisico, sia quello virtuale delle tecnologie del cyberspace.

2. INTERDIPENDENZA DEI SISTEMI SCADA CON IL CYBERSPACE

I processi che attualmente sono alla base della maggior parte della produzione industriale hanno raggiunto un livello di complessità talmente elevato da richiedere un rigido controllo sulla loro evoluzione mediante la conoscenza e il governo di numerose variabili e/o parametri che li caratterizzano.
Si ricorre allora a sistemi automatici di controllo e di acquisizione dati denominati sistemi SCADA, i cui benefici sono particolarmente rilevanti in impianti diffusi su vaste aree territoriali, di tipo sia lineare sia areale, quali le infrastrutture deputate alla produzione ma anche al trasporto e/o distribuzione, che per molteplici ragioni di tipo tecnico, economico e strategico necessitano di sorveglianza e controllo dei processi che ne sono alla base.

La complessità delle operazioni da eseguire richiede in molti casi l'applicazione di tecnologie sempre più raffinate e che, attualmente, si rendono disponibili grazie allo sviluppo raggiunto dagli attuali sistemi SCADA.

Fino a pochi anni fa i sistemi SCADA erano ritenuti sicuri per una serie di ragioni, ormai diventate false credenze, ma che hanno a lungo rappresentato, e in molti casi lo rappresentano tuttora, un ostacolo allo sviluppo e all'applicazione di migliori strategie di sicurezza. Si pensi che ancora nel 1994 la IEEE dava la seguente definizione di Sicurezza delle comunicazioni nei sistemi SCADA: "*Security is the ability to detect errors in the original information transmitted, caused by noise on the communication channel*" [10],

Tali pregiudizi nascevano dal fatto che si riteneva che:

Un sistema SCADA si trova in una rete stand alone fisicamente separata dalle altre [3].

Effettivamente la maggior parte dei sistemi SCADA furono progettati e costruiti prima delle altre reti corporate o, comunque, tenuti separati da esse. Questa caratteristica si è tuttavia perduta negli anni per un insieme di ragioni, a cui si è già accennato, che rispondono più a logiche di mercato, di gestione e di organizzazione aziendale che a vere e proprie necessità tecniche.

I collegamenti fra i sistemi SCADA e le reti corporate sono protetti mediante controlli di accesso "forti" [3].

Molte interconnessioni tra le reti societarie e la rete SCADA richiedono un processo d'integrazione dei due sistemi caratterizzati quasi sempre da standard di comunicazione differenti. Il risultato di questa integrazione è spesso basato su una serie di compromessi tecnologici che consentono di trasferire con successo i dati e le informazioni fra i due sottosistemi, senza però che i progettisti vogliano o siano in grado di comprendere appieno quali possono essere i reali rischi di sicurezza del sistema integrato.

Di conseguenza i controlli di accesso progettati per proteggere i sistemi SCADA sono di solito molto deboli, anche perché vengono spesso trascurati o sottovalutati proprio nei punti di connessione fra le due reti.

I sistemi SCADA richiedono conoscenze specializzate, rendendo così difficile l'accesso e il controllo da parte di intrusori che affollano la rete [3].

In passato si è creduto che eventuali intrusori non avessero le capacità tecniche necessarie per poter

accedere ad informazioni dei sistemi SCADA o almeno comprenderne funzionamento e caratteristiche. All'opposto, si riteneva che gli specialisti di tali sistemi non avessero alcuna motivazione a portare attacchi più o meno nocivi, se non distruttivi, a quei sistemi. Attualmente questa distinzione si è molto attenuata. La circostanza che la maggior parte delle imprese che erogano servizi rappresentano elementi chiave nel contesto delle infrastrutture critiche di una nazione, ha fatto sì che esse siano un obiettivo altamente probabile per attacchi di natura terroristica. I possibili assalitori o intrusori sono motivati, molto ben remunerati e possono disporre anche di una conoscenza approfondita dei sistemi e del loro funzionamento grazie ad informazioni ottenute da personale interno alle imprese (social engineering). Naturalmente gli attacchi non hanno sempre e soltanto una matrice terroristica ma possono provenire anche da attività di spionaggio industriale.

Un ulteriore elemento a favore del rischio di attacco è la possibilità, in continuo aumento, di ottenere informazioni che descrivono le operazioni proprie dei sistemi SCADA. Informazioni che sempre più facilmente possono essere reperite sulla rete Internet grazie ai progetti e alla documentazione resi disponibili dalle società che realizzano tali sistemi, sia per semplificare la loro manutenzione, sia per fornire toolkits per lo sviluppo di software d'implementazione utilizzato in ambienti SCADA. Infine, per far fronte alla competitività di mercato, garantendosi una più ampia diffusione dei propri prodotti, le stesse società hanno cominciato ad utilizzare standard ordinari e non proprietari per l'interconnessione dei sistemi SCADA e delle unità remote (RTU).

In realtà, l'evoluzione dei sistemi SCADA, non solo ha eliminato tutti questi pregiudizi, ma addirittura ne ha incrementato la vulnerabilità. Infatti, per ragioni economiche e commerciali, come la liberalizzazione dei mercati, la presenza di molteplici fusioni aziendali, la diffusione di politiche di outsourcing e lo sviluppo dell'e-business, le imprese si sono orientate verso sistemi integrati con le reti IT ricorrendo a reti di comunicazione di tipo aperto [9]. Pertanto le vulnerabilità proprie di queste reti sono diventate vulnerabilità anche delle reti SCADA. Nella Tabella 1 vediamo riportati una serie di fatti relativi sia al settore delle reti per il controllo delle infrastrutture, sia a quello della sicurezza informatica. Se ne può dedurre immediatamente come la correlazione tra fattori di sviluppo incrociati conduca ad un evidente aumento delle vulnerabilità in esame.

Cosa succede nell'industria delle infrastrutture	**Cosa succede nel settore della sicurezza informatica**
Maggiore quantità ed estensione di sistemi SCADA	Le organizzazioni più attaccate sono quelle che gestiscono Infrastrutture Critiche
Forte tendenza all'utilizzo di piattaforme standardizzate, e.g. Windows 2000	I sistemi maggiormente vulnerabili sono Microsoft ed i software basati sul Web
Progressivo spostamento verso sia il protocollo IP, sia il protocollo di gestione della rete SNMP	I protocolli più semplici da rompere sono IP e SNMP
Tendenza ad avere grande connettività tra la rete business e quella di gestione dell'impianto	Incrementano le opportunità di accesso
Diffusione della connettività Wireless	Il miglior modo per realizzare un accesso semplice ed illegale è la connessione Wireless
Le strutture informatiche sono comunque vincolate e ben controllate	Le risorse IT per la sicurezza sono complesse e difficili da gestire correttamente anche se stanno emergendo delle tecnologie significative
Il personale IT ben addestrato è difficilmente reperibile	Di tutti I professionisti IT quelli addetti alla sicurezza sono I più rari e costosi

Tabella 1. Minacce alla sicurezza in ambiente SCADA [9]

Particolare attenzione va riservata, inoltre, all'utilizzo di sistemi di comunicazione di tipo wireless. Tale tipologia di canale di comunicazione, infatti, rappresenta una promettente soluzione per la trasmissione dati all'interno delle RTU se non anche per la connessione di queste con il sistema centrale. Ad esempio possiamo citare l'utilizzo di reti wireless per la gestione dei terminali mobili di alcuni aeroporti americani, e di un numero crescente di ospedali negli Stati Uniti così come in Europa. Oppure possiamo trovarle impiegate nel controllo di impianti di estrazione distribuiti su un'area di vaste dimensioni (petrolio) ed alle volte in impianti dedicati alla estrazione o manipolazione a distanza di materiali pericolosi (stazioni di pompaggio dell'acqua per l'estrazione di uranio). Ma anche nel settore delle ferrovie per il controllo degli scambi, ed ancora per la gestione dei sistemi idrici, dei sistemi di trattamento delle acque di scarico ed infine per la distribuzione del gas di città.

Le reti wireless consentono, infatti, la connessione di una molteplicità di dispositivi diversi senza la necessità di posa di cavi, riuscendo così a semplificare le connessioni con le RTU situate in luoghi difficili da raggiungere ed eliminando i problemi di manutenzione connessi usualmente con la presenza di collegamenti fisici. A tali favori si aggiunge che gli attuali dispositivi informatici hanno reso la connessione ad una rete wireless addirittura più semplice rispetto alla configurazione di una rete locale tradizionale e, soprattutto, a costi estremamente contenuti. Anche all'interno di sistemi SCADA, infatti, iniziano ad abbondare l'utilizzo di tecnologie quali il Wi-Fi (conosciuta anche come IEEE 802.11, per larghezze di banda medie e alte) e il Bluetooth (larghezza di banda media a piccolo raggio).

Nonostante gli evidenti vantaggi che tali tecnologie possiedono va però tenuto conto che l'evoluzione del wireless, pur consentendo ormai livelli di affidabilità, di sicurezza, di continuità ed integrità di scambio dati significativamente superiori rispetto al passato, l'assenza di un supporto fisico (al quale l'eventuale intrusore deve guadagnare materialmente accesso) fa sì che, in ogni caso, queste reti rappresentino una porta aperta per gli hacker.

Tale problema assume una rilevanza notevole se si pensa che una tipica azienda americana oggi investe circa un quarto del suo budget nell'acquisto di infrastrutture e servizi per la gestione del traffico dati in modalità wireless come sostiene una ricerca effettuata dalla società specializzata in tematiche ICT Yankee Group [20]. Su questi argomenti l'ANIPLA, ha organizzato nell'aprile 2003 una Giornata di studio dal titolo "La comunicazione WireLess per l'automazione: la Tecnologia, la Legislazione, le Applicazioni"[21].
In cui sono stati messi in luce, tra le altre cose, i vantaggi e, soprattutto,i rischi derivanti dall'utilizzo di tale tecnologia.

3. VALUTAZIONE DEL RISCHIO INFORMATICO

Gli studi sulla vulnerabilità delle infrastrutture di solito prendono in considerazione soltanto elementi di tipo strettamente tecnico benchè talvolta l'analisi sia orientata a determinare anche le ricadute in un più vasto contesto socio-economico [5].

Gli elementi di base da esaminare sono:

- la conoscenza quanto più ampia e approfondita possibile delle proprietà e caratteristiche del sistema;
- l'individuazione di possibili minacce e rischi;
- l'analisi della vulnerabilità del sistema e le conseguenze da essa derivanti;
- la ricerca e la messa a punto di rimedi volti a creare sistemi più robusti.

	Azioni Umane		Interventi non Umani
	Intenzionali	Non Intenzionali	
Cause Interne	Infiltrazione	Fattori Umani Mancanza di manutenzione Errori di Costruzione o Progettazione	Guasti tecnici Errori di produzione
Cause Esterne	Sabotaggio Terrorismo Azioni di Guerra	Fattori Umani	Disastri Naturali Distruzioni in altri sistemie e servizi (interdipendenze)

Tabella 2. Classificazione di minacce e rischi [14]

Una procedura analitica completa non deve inoltre trascurare la durata, in relazione al tipo di minaccia, dell'intervallo di tempo in cui il sistema è fuori uso. Allo scopo sono state sviluppate diverse metodologie di tipo probabilistico-statistico, che utilizzano la teoria dei grafi o che si basano sulla failure analysis.

In relazione ai rimedi volti ad accrescere la robustezza delle infrastrutture, le misure o i dispositivi necessari dipendono largamente dalle loro caratteristiche e dalla varietà di minacce e di rischi. L'intero processo si basa in gran parte sui risultati di una vera e propria analisi di rischio (Figura 1)

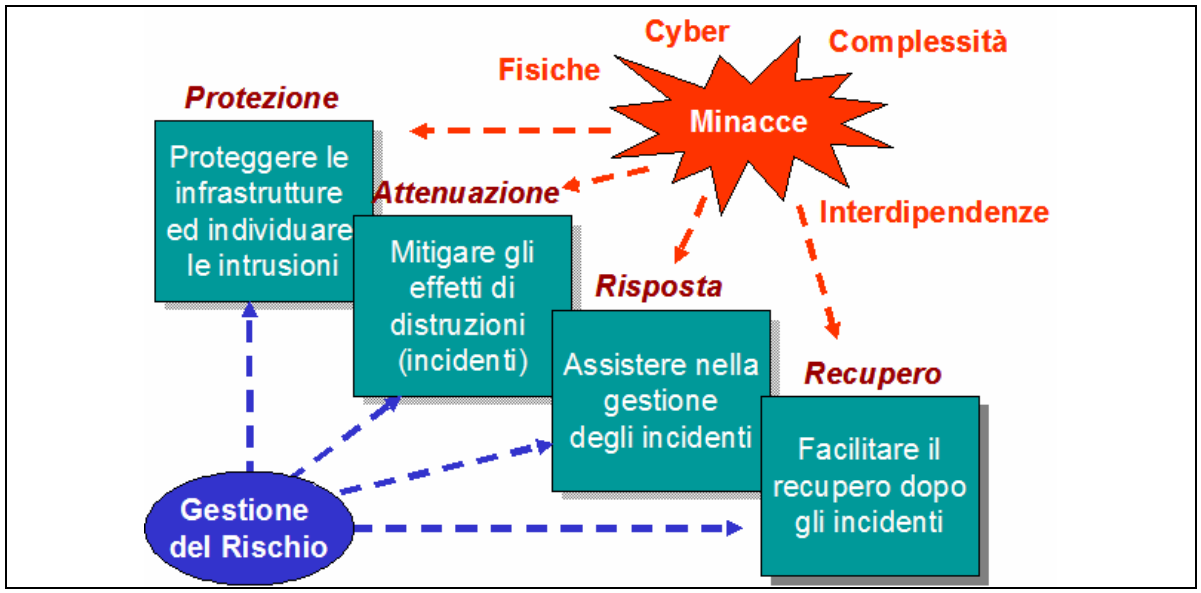

Figura 1. Procedura di gestione del rischio [15]

Molto schematicamente le opzioni strategiche che si possono considerare sono:

1. evitare completamente il rischio, ovvero non consentire un certo tipo di attività;
2. ridurre il rischio, ovvero mettere in atto misure preventive;
3. accettare il rischio, ovvero scegliere in maniera intenzionale o meno di non fare alcunché riguardo al rischio specifico;
4. distribuire o trasferire il rischio ad un'altra organizzazione, per esempio mediante forme assicurative;
5. condividere il rischio, ovvero accettarlo e in parte trasferirlo attraverso delle joint ventures.

La maggior parte delle misure di protezione per le infrastrutture critiche si possono basare sulle opzioni anzidette.

In ogni caso la sicurezza non è un'opzione da aggiungere alla fine, ma deve essere parte integrante del processo di progettazione e realizzazione di una rete SCADA che va garantita a tutti i livelli: fisico, network-based e host-based. La sicurezza fisica riguarda sia gli accessi fisici delle persone nelle aree protette (perimetrale) come la sala controllo dove sono ospitati i server, sia la sicurezza da eventi naturali. Per assicurare la sicurezza perimetrale si ricorre spesso a protezioni alle porte, a sistemi di controllo e a registrazione degli ingressi [19]. La sicurezza network-based fa riferimento ai meccanismi di protezione a livello di rete informatica; essa riguarda firewall, standard di progettazione della rete, modalità di interconnessione. La sicurezza host-based, infine, riguarda tutti i meccanismi di hardening necessari su un singolo server per evitare l'utilizzo di servizi non strettamente legati alle funzionalità proprie di quest'ultimo.

Le procedure per aumentare la sicurezza dei sistemi SCADA sin qui elencate considerano, quindi, una molteplicità di punti di attacco e individuano i possibili presidi. Esse però non sono di tipo sistemico, in quanto trattano soltanto aspetti di componentistica. Per cercare di risolvere il problema soprattutto per reti SCADA molto complesse e con numerose interconnessioni ad altre infrastrutture, anche di tipo non informatico, e specialmente per quelle che si estendono su ampie porzioni di territorio, può essere opportuno eseguire test su configurazioni riprodotte in scala 1:1, oppure progettare modelli di simulazione con lo scopo di mettere in evidenza le suddette interconnessioni.

A questo scopo l'INEEL (Idaho National Engineering and Environmental Laboratory), che si occupa di soluzioni ingegneristiche e scientifiche a problematiche di sicurezza, ha realizzato un sito di circa 890 miglia quadrate che è un vero e proprio microcosmo, sicuro ed isolato, di molte delle infrastrutture critiche della nazione [6]. In questo sito, denominato "Test Range", vengono sviluppate, provate e convalidate tecnologie, sistemi e politiche di protezione delle infrastrutture in condizioni reali.

Utilizzando le risorse offerte dal Test Range, personale specializzato della National Security Division dell'INEEL, in collaborazione con i SANDIA National Laboratories , ha sviluppato un progetto denominato National SCADA Test Bed. Esso è mirato ad identificare e valutare le vulnerabilità dei sistemi esistenti per incrementarne la sicurezza e la robustezza e individuare le soluzioni progettuali per futuri sistemi, più sicuri ed affidabili. Nello stesso tempo vengono messe a punto strategie per mitigare l'impatto di attacchi fisici o cibernetici e consentire il rapido recupero funzionale delle infrastrutture colpite.

Dal punto di vista delle metodologie di simulazione dobbiamo ricordare il lavoro svolto dal Center for Secure and Dependable Systems ed il Computer Science Department dell'università dell'Idaho [22] presso i quali è stato sviluppato un modello matematico che permette di calcolare le vulnerabilità dei dispositivi di un sistema SCADA. Il modello si basa sulla teoria dei grafi per rappresentare i sistemi di controllo e i loro dispositivi di protezione, nonché il grado di connettività ad essi associato. Inoltre esso pone le basi per la definizione di un prototipo di un sistema esperto, in grado di individuare in un particolare sistema SCADA, il dispositivo più vulnerabile in un determinato scenario di attacco e le cause della sua vulnerabilità.

L'obiettivo è quello di aiutare gli operatori di sistemi di controllo industriale e gli amministratori di reti informatiche ad identificare i dispositivi più vulnerabili in modo da incrementare la sicurezza dei sistemi.

2000	A Maroochy Shire (Australia) un ex-dipendente riuscì ad introdursi nel sistema di tele-controllo di un impianto di depurazione provocando, da remoto, il riversamento di circa 1.200.000 litri di liquami non trattati direttamente nell'ambiente.
2001	Un attacco hacker alla Cal-ISO, la principale società per il trasporto dell'energia elettrica in California, fu scoperto solo dopo 17 giorni. Non è stato possibile stabilire che tipo di informazioni siano state carpite durante questo periodo né quali erano i reali obiettivi dell'azione.
2003	Il worm informatico Slammer, con la sua rapida diffusione, ha causato problemi a diversi sistemi di controllo. Negli USA il worm è riuscito a penetrare anche all'intero del sistema di controllo di una centrale nucleare in dismissione (senza creare seri problemi grazie alla presenza di circuiti di back-up in analogico). Esso è riuscito, inoltre ad interrompere il traffico dei sistemi di monitoraggio e controllo di due società di distribuzione dell'energia elettrica (in un caso penetrando all'interno del sistema informatico e nell'altro saturando la banda del canale ATM utilizzata, tramite una connessione Frame Relay, per colloquiare con le unità periferiche).
2003	Un rapporto intermedio della commissione congiunta US-Canada, istituita per far luce sulle cause del black-out del 14 agosto 2003, ha evidenziato che la causa scatenante va ricercata nel contatto fra un albero ed una linea a 345 kV. Tale evento, per altro relativamente usuale, è stato in una certa misura indotto e, soprattutto, non gestito correttamente a causa di una pluralità di problemi registrati dal sistema SCADA utilizzato per il monitoraggio e il controllo della rete elettrica da parte dell'operatore FirstEnergy. In particolare, si è riscontrato che lo "stimatore" utilizzato per prevedere l'evoluzione della rete rimase non operativo per circa 4 ore riprendendo a funzionare solo pochi minuti prima del black-out (a causa sia di errori umani che di problemi tecnici). Un differente guasto ai server del sistema SCADA ha reso non operativa la gestione degli allarmi (cioè le segnalazioni agli operatori che determinate grandezze assumevano valori anomali) rallentando, inoltre, la funzionalità complessiva dello SCADA (ed in particolare le operazioni di aggiornamento dei valori misurati sul campo) rendendo di fatto "ciechi" gli operatori nella sala di controllo rispetto a quanto stava accadendo alle linee.
2004	Il 3 maggio il worm Sasser, sfruttando una vulnerabilità del sistema Micorsoft Windows, riesce a penetrare diverse installazioni in tutto il mondo. In particolare, il sistema di gestione dell'aeroporto di Dubai risulta compromesso mandando in tilt il traffico aereo [24].

Tabella 3: Alcuni esempi connessi con minacce di natura informatica nei confronti di sistemi SCADA.

Gli attacchi elettronici contro le infrastrutture critiche e soprattutto contro i relativi sistemi di controllo, si possono raggruppare in cinque classi Hackers, Spionaggio, Sabotaggio, Furto elettronico e Vandalismo. A questi vanno aggiunti il Cyberterrorismo e l'Attivismo. Per qualificare un atto come Cyberterrorismo, occorre che sia caratterizzato da due aspetti: avere una motivazione di carattere politico e provocare risultati distruttivi, mentre per Attivismo si intende azioni che, pur avendo una motivazione poltico-ideologica (no-global, ecologisti, ecc.), hanno più che altra una valenza simbolica mirata non tanto a "danneggiare" il sistema quanto a richiamare l'attenzione dell'opinione pubblica su determinati fatti o eventi.

Nella Tabella 3 sono riportati alcuni esempi, tratti dalla letteratura scientifica, di azioni criminose o guasti accidentali che hanno avuto per oggetto i sistemi di monitoraggio e controllo di importanti infrastrutture.

Essi sono emblematici, oltre che per la loro rilevanza intrinseca, per il fatto che ognuno di essi è esemplificativo di una classe di minacce che possono affliggere i sistemi SCADA. Si va infatti, dall'intrusione di un hacker all'interno del sistema informativo di uno SCADA (che nel caso specifico di Maroochy Shire è stata perpetrata anche da un ex-dipendente e quindi in un certo senso da un insider) ad una intrusione informatica le cui conseguenze possono essere anche di difficile individuazione, come occorso alla Cal-ISO nel 2001. In realtà queste intrusioni possono mettere in luce delle ulteriori vulnerabilità con conseguenze potenzialmente distruttive. Citiamo a questo scopo anche l'intrusione avvenuta il 24 dicembre del 2000 ai danni della Marina degli Stati Uniti durante la quale un hacker venne in possesso di parti di codice del software OS/COMET il quale viene usato per dagli operatori delle stazioni terrestri per controllare alcuni sistemi satellitari ed inviare loro dei comandi.

L'episodio del worm Slammer mostra da un lato come anche ambienti notoriamente considerati sicuri ed inviolabili, quali gli impianti nucleari, siano in realtà vulnerabili, e dall'altro, che a causa delle crescenti interdipendenze, le cause che possono essere alla base delle vulnerabilità ricadono al di fuori di quelle direttamente controllabili dalla singola azienda.

L'ultimo episodio riportato, sebbene la causa del guasto al sistema SCADA sembra sia di natura accidentale e non dolosa, è, però, emblematico di come a causa della crescente complessità intrinseca dei sistemi e della conseguente necessità di ricorrere a sistemi di controllo molto sofisticati e complessi, un guasto nel sistema di controllo (per quanto banale) può avere effetti drammatici su un'intera nazione.

Il Governo Canadese ha condotto un interessante studio su quelle che sono le minacce che possono affliggere le varie infrastrutture e i loro trend futuri [16]. Tale studio evidenzia che le minacce di tipo **accidentale**, cioè dovute a rotture meccaniche, guasti software, ecc,. nonostante l'aleatorietà che caratterizza tali eventi, presentano un trend negativo, ovvero la loro incidenza sembra ridursi.

Nel contempo, si evidenzia un trend positivo, e quindi una crescente rilevanza, per quegli eventi negativi connessi sia con cause **naturali**, soprattutto legate all'estremizzazione di molti eventi climatici, che per quel che riguarda le azioni **dolose**. In particolare fra queste ultime, quelle condotte tramite il cyberspace vengono considerare le più insidiose (anche se non necessariamente le più distruttive) a causa della difficoltà di predire e rilevare le stesse. Infatti:

- L'identificazione degli attori risulta oltremodo complessa in un ambiente, quale quello del cyberspace, ove è relativamente semplice mantenere una identità anonima e dove esiste una lasso di tempo (a volte anche non breve) fra l'azione perpetrata dall'intrusore e la manifestazione dei suoi effetti (sempre che questi si manifestino in modo evidente).
- Le minacce non sono circoscritte a prestabiliti confini, geografici o politici, quindi un attacco può originarsi, anche simultaneamente, da una pluralità di siti sull'intero globo.
- Il cyberspace è un ambiente in rapida e mutevole evoluzione e al momento relativamente poco conosciuto.
- Le tecnologie impiegate per un attacco sono relativamente semplici, facili da usare e reperire (su Internet esistono svariati siti che permettono di scaricare anche sofisticati strumenti di attacco).
- Gli strumenti di attacco sono divenuti, nel contempo, sempre più sofisticate ed al tempo stesso automatizzati, al punto che anche un utente con limitate conoscenze può produrre un attacco le cui conseguenze potrebbero essere anche di vaste proporzioni.
- Gli strumenti impiegati per gli attacchi sono sempre più simili, se non proprio identici, alle tecnologie impiegate per garantire la *resilience* delle reti.
- Il costo necessario per acquisire e sferrare un attacco significativo è in continua diminuzione.
- La crescente interconnessione fra le diverse infrastrutture rappresenta, comunque, la causa principale dell'incremento di vulnerabilità.

Tali considerazioni possono condensarsi nel grafico di Figura 2: in parallelo ad una crescita costante del livello di sofisticazione dei tools utilizzabili per un attacco, si è assistito ad una drastica riduzione del livello di conoscenza richiesto per il loro utilizzo.

Si consideri che il CERT (Center for Computer Emergency Response Team) dell'Università Carnegie Mellon, segnala oltre 26.000 incidenti di intrusione nei computer verificatisi e segnalati nei primi tre mesi del 2002, più di quanti sono avvenuti in tutto l'anno 2000 [5]. Inoltre, l'analisi condotta in [23] evidenzia che le società di utilities (ed in particolare quelle addette alla trasmissione e distribuzione dell'energia elettrica) costituiscono uno dei bersagli prediletti per cyber-attack e che oltre il 70% di queste è stata oggetto di un attacco "severo"nei primi sei mesi del 2002.

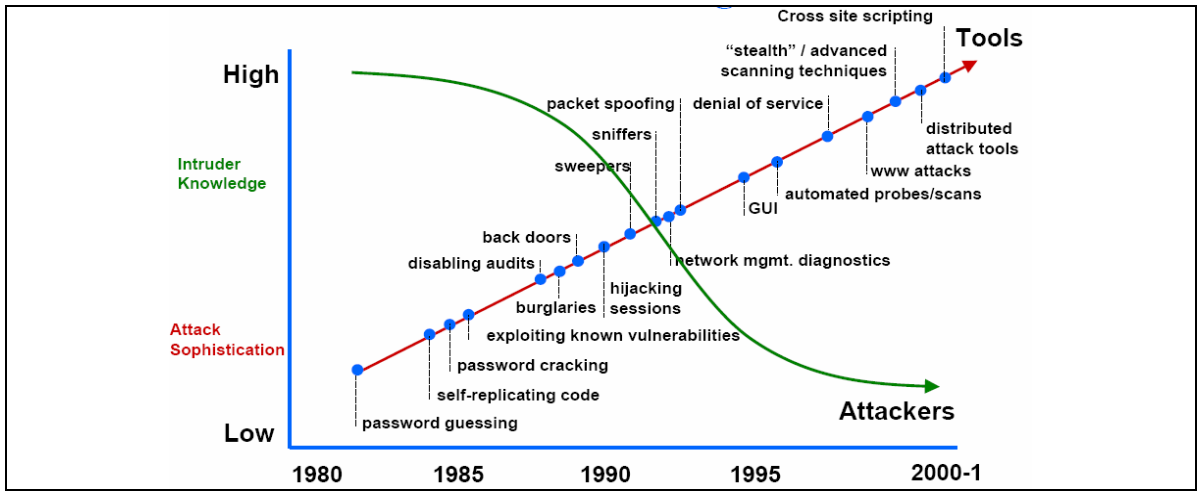

Figura 2. Evoluzione del grado di sofisticazione degli attacchi tramite il cyberspace (in rosso) e del livello di conoscenza richiesto agli assalitori (in verde) [19]

È possibile individuare tre distinte categorie di attori che potrebbero perpetrare azioni delittuose tramite il cyberspace alle infrastrutture critiche colpendo i loro sistemi di controllo e monitoraggio e precisamente:

Script kiddies: questa categoria include quei soggetti che si procurano gli strumenti utilizzati dagli hacker da siti web senza neanche comprenderne a fondo le potenzialità.
Sono generalmente teen-ager fra i 12 e i 16 anni motivati più che altro dalla curiosità o dal desiderio di fare un "bravata". La loro pericolosità risiede soprattutto nel numero, infatti anche se le loro capacità sono modeste esiste una elevata probabilità che almeno uno di loro riesca, accidentalmente, a sfruttare una vulnerabilità lasciata non adeguatamente protetta. Contro questa tipologia di assalitori, una corretta politica di gestione delle patch in genere consente di limitare radicalemnte il rischio;

Hackers: a differenza dei *kiddies*, un hacker sa sfruttare a fondo i diversi tools ed è anche in grado di sviluppare codice ad hoc. Le motivazioni che li spingono vanno da quelle di tipo economico-finanziario al semplice gusto della sfida.

Malicious Insider Actors: ovvero quei soggetti che sfruttando conoscenze acquisite in modo legittimo (perché dipendenti, fornitori, ecc.) cercano di acquisire informazioni, danneggiare il sistema, o comunque operare in modo non lecito.
Questa rappresenta forse la categoria di attori più difficile da arginare. Si pensi che in uno studio della Ernst & Young del 1999 il 70% delle violazioni dei sistemi informativi aziendali ha avuto origine dall'interno dell'azienda stessa.

4. STANDARDIZZAZIONE E CERTIFICAZIONE

Da un punto di vista più propriamente tecnico, a livello internazionale sta crescendo il dibattito circa l'opportunità di utilizzare software Open Source per i sistemi SCADA. I fautori di quest'ultima soluzione evidenziano come in tal modo si ridurrebbe drasticamente la presenza di back-doors e, forse, dei bachi; gli oppositori ritengono, invece, che la natura degli SCADA consigli di limitare al massimo la diffusione di qualunque tipo di informazione perseguendo politiche di *security by obscurity* [12].

Parallelamente si va prospettando l'opportunità di *certificare* i software SCADA, o quanto meno i loro aspetti di sicurezza [11]. In questo scenario da più parti si suggerisce l'adozioni di standard di sicurezza quali la BS7799 o i Common Criteria.

La BS7799 è una metodologia sviluppata negli anni ’90 che diventa un British Standard nel 1995. Il suo obiettivo, partendo dagli assunti che non è possibile raggiungere una sicurezza del 100% e che le informazioni di per se stesse rappresentano un valore aziendale da proteggere, è quello di ottimizzare il rapporto costi/benefici per quel che concerne le misure di sicurezza informatica. Essa si compone di due parti: la prima parte, ripresa nel 2000 dalla norma ISO/IEC 17799, suggerisce “best-practice” per implementare un programma per la sicurezza delle informazioni; la seconda elenca i processi ed i controlli per implementare e certificare un sistema di gestione della sicurezza informatica. La filosofia alla base della BS7799 è il passaggio da un concetto di sicurezza quale strumento di processo a strumento di *governance* il cui compito è quello integrare e ottimizzare gli altri strumenti di *governance* a disposizione dell’azienda. Esso si basa sulla determinazione dei Requisiti di Security (legati alle policy aziendali, ai requisiti contrattuali, alle leggi, ecc.) che a loro volta contribuiscono a determinare il Risk Assessment (che parte dall’individuazione delle minacce e vulnerabilità con l’individuazione della relativa probabilità e incidenza sulla realtà industriale) e da questi si derivano le strategie per la Gestione della Security, che si estrinseca in azioni tecniche, organizzative e nelle policy di sicurezza aziendale.

La ISO/IEC 15408, più nota come Common Criteria, ha lo scopo di fornire uno strumento di comparazione, per quel che riguarda gli aspetti di sicurezza, fra prodotti indipendenti. Essa consente di verificare se le esigenze dell’utente, descritte attraverso un insieme di requisiti di alto livello (il protection profile PP) sono soddisfatte per un determinato prodotto (TOE Target of Evaluation) sulla base dell’insieme dei requisiti e delle specifiche utilizzate dal produttore per l’implementazione del prodotto (ST Security Target). I Common Criteria rappresentano, pertanto, uno strumento per la valutazione e comparazione dei prodotti, e consentono di definire un “mercato” dei componenti sicuri. Essendo, quindi, pensati per la valutazione di un singolo prodotto e non di sistemi, non rappresentano una metodologia di sviluppo.

Semplificando possiamo affermare che la BS7799 fornisce una metodologia per definire le politiche di sicurezza aziendali in relazione a specifiche minacce, senza, per altro, fornire indicazioni puntuali su come implementare tali politiche, mentre i Common Criteria forniscono uno strumento per la selezione di componenti sicuri.

2. CONCLUSIONI

La protezione delle infrastrutture tecnologiche di una nazione da attacchi cyberterroristici sta divenendo una priorità molto alta per i governi come evidenziato dalle diverse iniziative in atto nei vari paesi (si veda ad esempio [CIIP Handbook]) e da parte di organismi sopranazionali (l’ultima in ordine di tempo è la risoluzione 58/199 dell’ONU [17]).

Ciò deriva sia dalla crescente incidenza che tali infrastrutture hanno, e andranno sempre più ad avere nei prossimi anni, sul benessere delle popolazioni, sia dal fatto che la sempre maggiore interdipendenza esistente fra le diverse infrastrutture può provocare l’amplificazione di un eventuale guasto (di natura accidentale o dolosa) che può propagarsi da un’infrastruttura all’altra con un effetto domino arrivando a colpire utenti remoti sia dal punto di vista geografico che logico, rispetto alla causa originante il guasto. Di conseguenza ogni vulnerabilità presente in un’infrastruttura costituisce un elemento di rischio per l’intero cluster di sistemi costituito dalle diverse infrastrutture tecnologiche interdipendenti [1].

D’altro canto l’attenzione che gli operatori privati, che per altro gestiscono direttamente oltre l’80% delle infrastrutture tecnologiche, pongono al problema della sicurezza rispetto a minacce provenienti dal cyberspace è ancora limitata, soprattutto per quel che riguarda i sistemi di monitoraggio e controllo (SCADA e DCS).

Tale disattenzione trae origine da pregiudizi legati alla natura proprietaria e alla separazione fisica di cui hanno goduto questi sistemi storicamente. Per una serie di ragioni, di natura sia tecnologica, ma soprattutto economica e sociale, tale presupposti non hanno più ragion d’essere portando tali sistemi ad essere affetti dalle medesime vulnerabilità che caratterizzano i sistemi informativi aziendali ed Internet.

Stante anche l’impatto che un’eventuale manomissione di un sistema di controllo potrebbe avere su ampie porzioni della popolazione, diversi governi hanno posto particolare attenzione alla protezione dei sistemi SCADA dalle minacce di natura informatica. Ad esempio il governo americano indica come una delle cinque priorità nazionali per migliorare la sicurezza del cyberspace, proprio l’incremento del livello di cyber-security degli SCADA e DCS [11], ed il governo britannico ha focalizzato uno dei tre canali attivati dal NISCC (National Infrastructure Co-ordination Centre) per la cooperazione con i soggetti privati proprio nei confronti degli utilizzatori di sistemi SCADA e DCS.

4. BIBLIOGRAFIA

[1] R. Setola "La Protezione delle Infrastrutture Critiche Informatizzate", *Automazione e Strumentazione*, pp. 27 - 35, luglio 2003; http://www.ilb2b.it/autom_strum/detalle.asp?id=20030708006&ricerca=6.

[2] White Paper. "Information Security in Industrial Communications," Siemens AG, Nuremberg, 1999.

[3] "Understanding SCADA System Security Vulnerabilities," Riptech Inc., January 2001.

[4] P. Oman, E.O. Schweitzer, J. Roberts. "Safeguarding IEDS, Substations And SCADA Systems Against Electronic Intrusions," Schweitzer Engineering Laboratories, USA, 2001.

[5] http://www.newsfactor.com/story.xhtml?story_id=17371

[6] http://www.inel.gov/nationalsecurity/homeland_security/testing_capabilities.shtml

[7] R.G. Little. "Toward More Robust Infrastructure: Observations On Improving The Resilience and Reliability of Critical Systems," *AICP Proc. of 36th Hawaii International Conference on System Sciences*, Havaii, 2002.

[8] S. Panzieri, R. Setola, "Vulnerabilità indotta dal Cyberspace sui Sistemi di Monitoraggio e Controllo", Atti del Convegno Nazionale ANIPLA – ENERSIS 2004, pp. 320 – 332, Milano 1-2 aprile 2004.

[9] Saunders J. H., "A Dynamic Risk Model for Information Technology Security in a Critical Infrastructure Environment"; http://www.johnsaunders.com/papers/riskcip/RiskConference.htm

[10] R. Carlson, *Sandia SCADA Program High-Security SCADA LDRD Final Report*, Sandia Report SAND2002-0729, aprile 2002.

[11] USA The National Strategy to Secure Cyberspace, 2003; http://www.whitehouse.gov/pcipb

[12] USA General Accounting Office, "Critical Infrastructure Protection – Challenges for Selected Agencies and Industry Sectors" GAO-03-233, febbraio 2003; http://www.gao.gov/new.items/d03233.pdf

[13] White Paper "Information Security in Industrial Communications," pubblicato da Siemens AG, Nuremberg, 1999.

[14] Holmgren Å., Molin S. & Thedéen T., "Vulnerability of Complex Infrastructure Power Systems and Supporting Digital Communication Systems"; 5th International Conference on Technology Policy and Innovation – Critical Infrastructures; Delft (The Netherlands); giugno 2001

[15] Jones D., "Electric Infrastructure Vulnerability Assessment Methodology", NERC Workshop, Meeting the Security Challenge; Orlando; 14, aprile 2003

[16] Government of Canada, Office of Critical Infrastructure Protection and Emergency Preparedness, *Threats to Canada's Critical Infrastructure*, TA03-001, 12 marzo 2003.

[17] UN Resolution n. 58/199 "Creation of a global culture of cybersecurity and the protection of critical information infrastructures", General Assembly 23 dicembre 2003, http://www.un.org/Depts/dhl/resguide/r58.htm

[18] A. Wenger, J. Metzger, M. Dunn, I. Wigert *International CIIP Handbook 2004*, ETH, the Swiss Federal Institute of Technology Zurich, 2004, http://www.isn.ethz.ch/crn/_docs/CIIP_Handbook_2004_web.pdf

[19] http://www.vnunet.it/detalle.asp?ids=/Articoli/Reti_e_TLC//20010731003

[20] http://rcrnews.com/cgi-bin/news.pl?newsId=17663

[21] http://www.fullpress.it/articolo.asp?ID=4483

[22] Conte de Leon D. et al., "Modeling Complex Control Systems to Identify Remotely Accessible Devices Vulnerable to Cyber Attack", ACM Workshop on Scientific Aspects of Cyber Terrorism, (SACT), Washington DC, novembre 2002

[23] http://www.securitystats.com/reports/Riptech-Internet_Security_Threat_Report_vII.20020708.pdf.

[24] http://www.ilsole24ore.com/fc?cmd=art&artId=404617&chId=30&artType=Articolo&back=0