Business Intelligence a supporto della Business Security

Abstract

Project Work

Master Homeland Security – III Edizione Anno 2010/2011

Autore:	Ing. Gabriele De Luca	Dic-2011
Tutor:	Ing. Francesco Ceccarelli - Resp. Sicurezza Logica, Analisi e Business Intelligence	Dic-2011

Lista di distribuzione

Consegnato in formato elettronico (e-mail) e cartaceo.

Nominativo	Riferimento
Dott.ssa Rossella Liaci	Master Homeland Security – Presidenza Nitel
Ing. Francesco Ceccarelli	Enel - Responsabile Sicurezza Logica, Analisi e Business Intelligence

Riferimenti

Elenco dei documenti di riferimento (da fonti aperte).

[1] Information Warfare Conference - Strategie e tattiche di info-war e network intelligence: dalla sicurezza delle imprese alla sicurezza nazionale - Roma, 27/10/2011.
[2] Fabrizio Minniti - "Le Fonti Informative e l'Open Source Intelligence" - CeMiSS, 2006
[3] Jardines Eliot A. - "Testimony of Eliot A. Jardines", Using Open Source Effectively: Hearings before the Subcommittee on Intelligence, Information and Terrorism Risk Assessment of the Committee on Homeland Security" - United States House of Representatives, 2005
[4] http://www.boozallen.com/consulting/advance-our-government/megacommunities
[5] Robert David Steele - "Open Source Intelligence " in "Strategic Intelligence: The Intelligence Cycle" - Praeger 2007
[6] Alvin Toffler (New York, 3 ottobre 1928) è uno scrittore statunitense e "futurologo" (come egli stesso si definisce), che da anni studia i mezzi di comunicazione e il loro impatto sulla compagine sociale e il mondo della cultura. Tra i suoi studi più significativi *The third wave* (1980), in cui disegna la storia dei media scandendola in tre "ondate": vecchi media, mass-media e nuovi media.
[7] National Intelligence Council - "Global Trends 2015: A Dialogue About the Future with Nongovernment Experts", p. 14 (http://www.cia.gov/nic/NIC_globaltrend2015.html), 2000
[8] Eric L. Dahlstrom - "From Reconnaissance to Surveillance: Intelligence Transformation in the New Millennium" - National War College - Washington, 2003
[9] Richard L. Russel – Review of "Best truth: intelligence in the information age" - Intelligence in Recent Public literature, 2001
[10] http://megacommunities.com/26655021
[11] S. Mercado, "Reexamining the difference between open information and secrets", "Studies in Intelligence", Vol. 49, n. 2, 2004
[12] NATO Open Source Intelligence Handbook - NATO, 2001
[13] NATO Open Source Intelligence Reader - NATO, 2002
[14] NATO Intelligence Exploitation of the Internet - NATO, 2002
[15] http://www.brightplanet.com/images/stories/pdf/deepwebwhitepaper.pdf
[16] http://www.opensource.gov
[17] Deborah G. Barger - "Towards a Revolution in Intelligence Affairs" - RAND, 2005
[18] Colleen Mc Cue - "Data Mining and Predictive Analysis" - Elsevier, 2007
[19] Frank A. Verrastro - "Security Implications of the changing Energy Landscape", da "Global Forecast 2011", CSIS, 2011
[20] Harry Yarger, Professor of National Security Policy in Department of National Security and Strategy at US Army War College

Indice

1. Abstract

Viene illustrato il *Project Work* svolto nell'ambito del *Master in Homeland Security* "Sistemi, Metodi e Strumenti per la Security ed il Crisis Management" dell'*Università Campus Bio-Medico* di Roma, III Edizione Anno 2010/2011.
Il *Project Work* è focalizzato sulla *Business Intelligence* nella *Corporate Security* e presenta esempi, della metodologia e delle applicazioni, estratti dallo studio condotto nella realtà Enel.

1.1. Scenario dell'Intelligence

Attraverso un'esplorazione del tema dell'*Intelligence [1][2][8][9][12][13][14]*, ripercorrendone l'evoluzione storica dalla *Guerra Fredda* alla *Revolution in Intelligence Affairs [1][17]*, se ne attualizza la visione al contesto del moderno mercato economico (*Competitive Intelligence [11]*) e dei nuovi complessi scenari geo-politici (es. *11 Settembre, Primavera Araba, Cyberwarfare [1]*), sempre più da interpretare ed affrontare con nuovi paradigmi (*VUCA* [20] e *Megacommunity [4][10]*).

1.2. OSInt: la novità

Tra le metodologie e le tecnologie dell'*Intelligence*, viene presentato in particolare *OSInt* [1][11][16] che, sebbene esistente da diversi anni, sta ora beneficiando delle nuove tecnologie (es. *Internet*, motori di ricerca semantici, nuovi metodi per cercare nel *deep web* [15], *Cloud Computing*, etc.) e ricevendo particolare attenzione non solo dalle forze armate, ma anche da governi ed imprese private, in virtù del suo paradigma *open* (fonti aperte, legalmente accessibili e non classificate). L'*OSInt* consente inoltre di produrre *Intelligence* partendo da fonti eterogenee (approccio *all-source [14]*), supportando quindi la costruzione di una visione d'insieme della *situazione*.
L'aspetto metodologico, concepito in ambito militare, è ormai consolidato e maturo per essere utilizzato anche da governi ed imprese private, garantendo uno standard per la condivisione dell'intelligence. Dal paradigma di *classified information* ci si orienta verso un paradigma di *shared information*, consapevoli che gli aspetti chiave sono la verifica e la correlazione delle informazioni e soprattutto la sua finalizzazione verso le figure responsabili di decidere (*decisori*).

"I conflitti futuri ruoteranno intorno alla ricerca di conoscenza.
Con la crescente rapidità delle comunicazioni e dei flussi di dati
a seguito dello sviluppo tecnologico,
i conflitti futuri saranno decisi da coloro i quali avranno la capacità
di raccogliere, analizzare e diffondere intelligence
nella maniera più efficace ed efficiente." [5]
Alvin Toffler

1.3. Vantaggi per le Imprese: Best Practices

Vengono presentate e confrontate alcune *Best Practice* interessanti dell'*OSInt* per le imprese private (aziende, tra cui Enel) e le organizzazioni pubbliche, che operano in un ambito sempre più internazionale, in cui sono necessarie informazioni contestualizzate e rapide per supportare le decisioni.
Le applicazioni spaziano trasversalmente in numerosi campi: supporto al *Marketing Strategico [11]*¸ valutazioni dei competitors sul mercato, valutazioni delle controparti, *opinion mining* (monitoraggio del *sentiment* e della *Brand Reputation*), studio delle popolazioni di clienti attuali

e potenziali, analisi della comunicazione mediatica e dell'*advertising*, attività di *Ricerca e Sviluppo*, monitoraggio di aspetti sociali e politici dei Paesi in cui si svolge il business, *Security Intelligence* con ricerca di informazioni anche multi-lingua.

1.4. Case Study: Business Intelligence e Corporate Security

Il tema è poi contestualizzato alla *Corporate Security*, evidenziando sia l'importanza di un approccio preventivo alla gestione del rischio, sia il beneficio che l'*OSInt* può apportare. L'*OSInt*, per rispondere agli *Information Requirements* [11] che ne avviano il *Ciclo di Intelligence* [16], effettua efficientemente il monitoraggio e l'analisi di grandi quantità di informazioni per capire il contesto e prevederne gli sviluppi [18], supportando così le decisioni del *management*. Si può così potenziare la capacità di *Business Intelligence* e quindi l'intero processo di *Security* in cui si inserisce.
La capacità di "leggere" nell'ambiente complesso è il primo passo per poter evolvere i processi di Security verso il paradigma di prevenzione sempre più necessario a seguito della *Revolution in Intelligence Affairs*: da reazione (ex-post) ad anticipazione (ex-ante).
Viene introdotto lo scenario di minacce delle *Energy Company* [7][19] per comprendere la realtà in cui si inserisce il processo di una funzione *Security* come quella di Enel, in cui i recenti fenomeni (per citare alcuni: movimenti ambientalisti, virus per ambienti *SCADA*, *Infrastrutture Critiche Europee*, etc.) richiedono un'enfasi sul processo di *Business Intelligence* già esistente, al fine di conseguire il vantaggio della prevenzione mediante nuovi strumenti metodologici e tecnologici come l'*OSInt*.
Vengono quindi illustrati il metodo di lavoro ed i criteri adottati nella conduzione di un progetto per l'introduzione di un modello e di un sistema informatico basati su metodologia e tecnologia *OSInt*.

1.5. Tesi: il fattore abilitante alla Business Security

La prospettiva di una *Business Security* è di generare valore nella *Corporate* ed assumere il ruolo integrato e strategico di tutela del *Business*.

Lo stesso strumento metodologico e tecnologico *OSInt*, può essere utilizzato per contribuire a realizzare gli obiettivi di aree differenti (*Business Intelligence*, *Competitive Intelligence*, *Security Intelligence*, etc.) e quindi può supportare la *Security*, che è trasversale alle funzioni aziendali ed ha un approccio multidimensionale-coordinato, per tutelare il raggiungimento dei vari obiettivi orientati al *Core Business*.

In quest'ottica si rinnovano alcuni approcci tradizionali: dalla "protezione" aziendale all'idea di "contributo alla crescita" del *Business*; dal *need to know* al *need to share* [1], elaborando e condividendo informazioni strategiche per il *Business* con le varie funzioni dell'organizzazione.

Un sistema complesso, quale quello di una grande azienda, diventa *proattivo* quando fornisce *risposte forti a segnali deboli*. L'evoluzione verso un approccio *proattivo* è fondamentale per una *Business Security* affinché possa affrontare le sfide degli attuali scenari e garantire un adeguato livello di gestione del rischio.

La *Business Intelligence*, con la sua capacità di "lettura" ed "ascolto" dei *segnali deboli*, è uno dei principali fattori abilitanti a questo processo di evoluzione.