



APPROFONDIMENTI SCIENTIFICI
SULLA SICUREZZA

POLO TECNOLOGICO SICUREZZA

Approfondimenti scientifici sulla Sicurezza

Biometria. Tra Privacy e Garanzie

Bruno Amici

Riflessione sulla sicurezza aziendale in Italia.
Cosa sta succedendo?

Alessandro .Lega

Privacy e Sicurezza.
Un binomio inscindibile

Aldo Agostini

Come affrontare in maniera efficace la
formazione dell'agente di sicurezza
navale e portuale

Ivano Roveda

Italia. La minaccia terroristica

Vittorfranco Pisano

Le nuove sfide dell'Information Security

Roberto Lorini

Brevi cenni sulla crescente diffusione
della Biometria

Mario Savastano

La sfida della gestione della sicurezza
nelle nostre città

Maurizio Grasso

Beni Culturali. Protezione e fruibilità possono
convivere?

Giovanni Bracone

La sicurezza attiva e passiva all'interno di una
moderna struttura destinata alla reclusione

Luigi Miccoli

Riflessioni sulla Sicurezza Aziendale in Italia. Cosa sta accadendo?

Coloro che all'indomani dell'11 settembre avevano previsto un'immediata crescita dei fatturati per servizi alle aziende Italiane, nel comparto della Sicurezza Aziendale, dimostrarono forse troppa fretta. Nacque l'illusione di riuscire a rinvigorire un mercato che da anni si è attestato ad un livello accettabile e che non dimostra di avere la capacità di fare passi da gigante.

Gli stessi operatori inizialmente fiduciosi, poi gradualmente rassegnati, che si affannavano a misurare una crescita dei loro fatturati han dovuto prendere atto che gli incrementi si dovevano comunque misurare con il bilancino del farmacista; un aumento di qualche unità percentuale rispetto all'anno precedente.

Poi ci sono stati i fatti di Madrid dell'11 marzo 2004, seguiti da quelli di Londra in luglio di quest'anno, solo per rimanere in Europa. L'aspettativa di una crescita del mercato della sicurezza si è fatta di nuovo sentire.

Tutto questo potrebbe portare a concludere che non ci sarebbero stati cambiamenti significativi se negli ultimi quattro anni non fossero accaduti fatti così drammatici. Certamente non è così!

Qualche cambiamento si stava già delineando all'orizzonte, prima dell'11 settembre. Un cambiamento nella qualità della domanda, per esempio, invocato da parte delle aziende più esposte, in particolar modo da quelle con dimensioni più significative.

Perché l'attacco alle Torri, poi ai treni Madrid e quelli alla Metropolitana di Londra hanno accelerato questo processo? Possiamo pensare che è accaduto ciò che accade dopo un brutto sogno: al risveglio la realtà ci può suggerire di adottare paradigmi diversi. Forse possiamo aggiungere che le motivazioni c'erano già ma che una certa inerzia nel resistere al cambiamento (non solo da parte delle imprese utilizzatrici ma anche da parte degli operatori del settore) è spesso più forte della effettiva spinta nel cambiare ?

Potremmo continuare l'analisi e trovare tanti altri *perché* ai quali possono essere contrapposte logiche e valide risposte.

Sofferamoci sul punto messo in evidenza, quello di una richiesta di qualità, che non è cosa di poco conto.

Le aziende Italiane (come nel mondo Anglosassone era avvenuto da qualche tempo) cominciano a percepire la necessità di dover disporre di capacità organizzative e di competenze professionali per proteggere le proprie iniziative imprenditoriali. Proteggerle sul fronte dei valori patrimoniali, delle risorse umane e delle informazioni aziendali. E' un cambiamento di estrema importanza, specialmente se viene rilevato in un momento in cui assistiamo ad una contrazione degli investimenti. Se determiniamo il delta fra i due diversi fenomeni, una minore crescita tendenziale degli affari in generale da una parte, ed una maggiore attenzione nel ridurre al minimo il livello di rischio dall'altra, potremmo concludere che siamo di fronte ad un reale apprezzamento del valore attribuito al contributo che la Sicurezza Aziendale può portare alle performance delle imprese.

E' pur vero che questa percepibile tendenza delle aziende si dovrebbe trasformare in reali opportunità di business per gli operatori che si propongono come fornitori di Sicurezza. Ma è anche pur vero che in un mercato che per anni ha limitato l'offerta ad una presenza fisica di personale in uniforme, oppure di pura tecnologia, gestendo la sicurezza solo tramite pratiche di tipo reattivo, questo cambiamento deve essere considerato abbastanza significativo. Anche se tutto ciò potrebbe non essere sufficiente per costituire un'effettiva opportunità, specialmente per quegli operatori del settore che si ostinano a mantenersi a riverente distanza da una disciplina che si chiama Security Management.

Dove sta quindi la chiave di volta che può dare un effettivo impulso al business della Sicurezza Aziendale: risiede nella capacità di saper diversificare l'offerta abbinandola a spunti propositivi capaci di far crescere la scala del valore trasferibile sulle aziende utenti.

Fin quando l'offerta si limiterà ad un presidio di tipo tradizionale, più o meno visibile, le valutazioni per le scelte si soffermeranno unicamente su considerazioni del costo orario e durata del servizio.

Un mero confronto fra un budget disponibile, ma in costante contrazione, verso una scontata convinzione che questa, da sola, potrebbe essere una risposta veramente limitata.

Dove sono allora le vere opportunità di crescita per il settore della Sicurezza Aziendale?

Esistono almeno due comparti nei quali è urgente mettere ordine e per i quali non è necessaria nessuna iniziativa del legislatore, cosa peraltro che sta molto a cuore ad alcune categorie della sicurezza, ma che non prescindono dalla necessità di un processo di qualificazione.

Il primo deve avvenire principalmente per convinzione delle aziende, sia per quelle che decidono di crearsi competenze interne, che per quelle che si propongono come fornitrici di servizi di sicurezza. Questo passo richiede la nascita di capacità organizzative in grado di assicurare alla professione del manager che si occupa di sicurezza (proprietaria od esterna) la piena dignità del ruolo di gestore di risorse (umane, finanziarie e tecnologiche), accettato e ritenuto capace come altre figure di contribuire al sostegno della scala del valore aziendale. Non sono necessarie alchimie organizzative ma solo la semplice applicazione di un regola che in economia è ben conosciuta: le perdite vanno sempre a decremento del profitto, quindi meno sono le perdite (di qualsiasi tipo) migliore è la performance aziendale. Esistono possibili forme organizzative, tecnologiche ed operative per poter realizzare questa condizione. Facciamolo subito, perché ogni giorno perso può corrispondere ad una costante perdita di competitività.

L'altro aspetto è in capo a coloro che si propongo come esperti del settore, sia come Security Manager interno alle aziende, che come Operation Manager di aziende fornitrici di sicurezza. Si può in questo caso dire: impara l'Arte e mettila da parte. L'Arte di saper anticipare le situazioni che devono essere prevenute, non tramite la lettura di una sfera magica, ma con modalità più sistemiche tipiche della valutazione del rischio. Quella disciplina che parte dalla ricognizione delle vulnerabilità e che passa attraverso la loro valutazione, sotto il profilo della criticità e della probabilità di accadimento. Un ruolo quindi non passivo, di attesa che avvenga un evento per poi doverlo affrontare. Un atteggiamento invece di tipo propositivo nel cercare di prevenire le situazioni meno favorevoli. Assieme a questo atteggiamento, che è anche una specifica competenza, si deve affiancare anche la capacità di contrastare chi si renda responsabile delle iniziative a danno delle organizzazioni che intendono proteggersi, oltre alla predisposizione di buone capacità di ripristino delle operazioni vitali in caso di evento capace di ridurre o bloccare la capacità operativa.

Un cambiamento non del tutto banale che richiede sia capacità professionali ma anche attitudini manageriali per poter governare un processo che tocca trasversalmente tutti gli altri processi aziendali. E poiché alcuni di questi processi hanno in comune una buona dose di necessità di sicurezza, meglio se nel prepararsi ad affrontare queste problematiche si riesce anche a cogliere l'opportunità di capirne meglio le implicazioni nell'ambito dell'intero processo aziendale. In altri termini capacità interdisciplinari e non monoculturali. Un esempio tipico sono le interrelazioni fra la Sicurezza Aziendale e la Sicurezza Informatica. Perché tenerle così distinte e separate? Non è forse vero che le informazioni sono un bene importante che l'azienda deve proteggere, indipendentemente dal fatto che siano scritte su carta oppure contenute in un computer?

Se tutto questo è vero e condivisibile, affrettiamoci a metterlo in atto!

Alessandro Lega
Managing Director di TraiCon srl - Gruppo DAB

Privacy e Sicurezza. Un binomio inscindibile

Il nuovo Codice della Privacy prevede che ogni dato (cioè informazione) che ci riguarda può essere trattato da terzi solo per motivi leciti, legittimi e non eccedenti gli obiettivi prefissati.

Si basa su tre importanti istituti (con varie eccezioni):

- Informazione (diritto ad essere informati sul perché e come terzi trattano i nostri dati);
- Consenso (si possono trattare i dati di terzi solo con il consenso degli interessati);
- Accesso (diritto di conoscere i propri dati detenuti da terzi e a farsi spiegare i motivi del trattamento).

Inoltre, i dati sensibili o giudiziari possono essere trattati solo in presenza di particolari situazioni, anche se la Pubblica Amministrazione conserva delle facoltà molto ampie.

Se i principi generali sono semplici, l'applicazione pratica è piuttosto complessa.

Ma esiste un principio tassativo: la necessità di garantire la sicurezza dei dati sotto ogni profilo (logico, fisico e organizzativo - le regole valgono per tutti i trattamenti, anche quelli cartacei).

Sotto l'aspetto informatico, che è quello più importante, i capisaldi di queste regole si riassumono nell'adozione delle seguenti Misure Minime di Sicurezza:

- a) autenticazione informatica per qualsiasi utente (in pratica: password diversa e veramente segreta per ognuno), con una gestione riservata delle credenziali;
- b) utilizzazione di un sistema di autorizzazioni (ognuno può accedere solo alle informazioni che può lecitamente trattare);
- c) queste facoltà devono essere periodicamente controllate dal titolare del trattamento;
- d) tutti i sistemi informatici devono essere protetti da virus, worms e altri programmi maligni, con software e hardware adeguati e aggiornati;
- e) le aree e gli accessi ai sistemi informatici debbono essere adeguatamente tutelati;
- f) bisogna conservare le copie di sicurezza e, in caso di guasto, garantire il ripristino dei dati in tempi rapidi e tassativi;
- g) è prevista l'adozione di protezioni ancora più rilevanti e complesse per alcune categorie di dati, come quelli sullo stato di salute o sulla vita sessuale delle persone;
- h) bisogna adottare e aggiornare periodicamente il Documento Programmatico sulla Sicurezza (DPS) che riassume lo stato di fatto dei sistemi informatici e analizza le capacità di coloro che sono chiamati ad impiegarli, nonché la loro filosofia futura di utilizzo.

Riguardo al DPS, va ricordato che bisogna redigerlo già da ora. Il regime delle proroghe, infatti, riguarda aspetti minimali e, comunque, scadrà alla fine di quest'anno.

Si tratta di regole obbligatorie (la disapplicazione è sanzionata penalmente), che spesso sono anche di buon senso. Purtroppo, però, sono molto distanti dalla realtà dei fatti (basti pensare che i sistemi operativi Windows '95 e '98 sono ormai fuori regola)

Problematiche ancora più complesse riguardano le imprese, anche piccole.

Ma la privacy è un concetto molto più ampio, che investe numerosi aspetti del vivere civile e del mondo economico. Serviranno anni per capirlo ma, intanto, occorre mettersi in regola.

Aldo Agostini

Il Dott. Agostini è Presidente di Security Studio System – SSSy – ed è un ex Vice Questore di Polizia specializzato in biometria, videosorveglianza avanzata e privacy.

Scrivo frequentemente sulle riviste del settore della sicurezza e svolgo corsi di formazione in queste materie

Come affrontare in maniera efficace la formazione dell'agente di sicurezza navale e portuale

LA MINACCIA

La pirateria e gli attacchi armati sono fenomeni che si verificano troppo frequentemente; l'una, solitamente in mare a danno delle navi, gli altri principalmente nelle zone portuali.

Entrambi i fenomeni vengono attuati attraverso l'attività di gruppi estremisti che cercano di perseguire i propri obiettivi politici con la violenza. Oltre a tutto costoro agiscono in sinergia con sette estremiste religiose che spesso inducono gli adepti a comportamenti suicidi.

Inoltre costituisce minaccia il contrabbando di merce rubata, attività criminale che provoca una perdita finanziaria all'armatore la cui nave sia utilizzata dai terroristi a questo scopo.

La droga e le armi costituiscono i più frequenti oggetti di contrabbando; possono essere entrambi portati a bordo in tanti differenti modi, talvolta imprevedibili.

Un altro problema grave è il furto del carico che causa al commercio marittimo perdite finanziarie di grande entità.

Anche se i furti non sono associati ad atti di violenza o effettuati da terroristi a fini politici comunque rappresentano una minaccia alla sicurezza e richiedono soluzioni adeguate.

Un recente studio effettuato dal Centro Ricerche della Comunità Europea ha individuato nel container la maglia più debole e più esposta della catena del traffico globale di merci. Si consideri che il 90% delle merci spedite via mare è trasportato tramite container; di essi mediamente solo il 2% viene controllato approfonditamente. Il container non è considerato un obiettivo pagante per un atto terroristico ma piuttosto è utilizzato dai terroristi quale mezzo ideale per il contrabbando di beni e persone.

Il furto del carico rappresenta una delle tante minacce alla sicurezza così come l'incendio, l'esplosione, o l'attacco nelle vicinanze di una nave o di un impianto portuale.

I REGOLAMENTI

Le crescenti minacce contro la sicurezza marittima hanno indotto i governi e le organizzazioni internazionali a legiferare in materia; in tale ambito normativo il Codice ISPS rappresenta lo strumento maggiormente strutturato e più aggiornato per gli operatori del settore.

Ricordiamo che la Conferenza diplomatica dell'Organizzazione Marittima Internazionale (IMO) ha adottato, il 12 dicembre 2002, alcuni emendamenti alla Convenzione SOLAS sulla sicurezza della vita in mare ed ha anche emanato un Codice internazionale relativo alla sicurezza delle navi e degli impianti portuali; appunto il Codice ISPS. Questo strumento normativo contiene, da un lato, disposizioni di natura obbligatoria; d'altro, disposizioni aventi valore di mere raccomandazioni. L'obiettivo principale del Codice è quello di indurre tutti i paesi del mondo ad adottare ed applicare strumenti comuni finalizzati a migliorare la sicurezza delle navi adibite al commercio internazionale ed al traffico nazionale, nonché degli impianti portuali associati, contro le minacce di azioni illecite.

Si tratta di misure speciali adottate per rafforzare l'incolumità di persone e cose tramite la valutazioni delle possibili minacce, l'elaborazione di piani di sicurezza, la designazione di agenti di sicurezza delle società, delle navi e degli impianti portuali.

LA FORMAZIONE

Come universalmente noto la prevenzione è il metodo fondamentale per garantire la sicurezza, in senso lato, delle persone e dei beni e in tale contesto la formazione è lo strumento più efficace per raggiungere l'obiettivo.

ISPS Code prescrive che ogni nave e impianto portuale abbia l'obbligo di inserire nel proprio organico un Agente di Sicurezza il quale deve possedere nozioni e formazione in materia, in accordo agli orientamenti della parte A e B del citato Codice.

In particolare deve conoscere in maniera approfondita le seguenti tematiche:

- ❑ convenzioni, codici e raccomandazioni internazionali pertinenti;
- ❑ metodologia della valutazione della sicurezza della nave o dell'impianto portuale ;
- ❑ metodologia dei controlli e delle ispezioni di sicurezza della nave e dell'impianto portuale;
- ❑ operazioni navali e portuali e condizioni in cui esse si svolgono;
- ❑ misure di sicurezza applicate a bordo della nave e nell'impianto portuale;
- ❑ preparazione, intervento e pianificazione dell'emergenza;
- ❑ tecniche didattiche per la formazione in materia di sicurezza, comprese le misure e le procedure di sicurezza;
- ❑ trattamento delle informazioni e delle comunicazioni sensibili sotto il profilo della sicurezza
- ❑ conoscenza delle varie forme di minacce alla sicurezza;
- ❑ riconoscimento ed individuazione di armi, sostanze e apparecchiature pericolose;
- ❑ riconoscimento, su base non discriminatoria, delle caratteristiche e dei modelli comportamentali dei soggetti che potrebbero costituire una minaccia per la sicurezza;
- ❑ tecniche utilizzate per aggirare le misure di sicurezza;
- ❑ apparecchiature e sistemi di sicurezza e loro limiti di utilizzazione;
- ❑ tecniche di perquisizione fisica e di ispezione non intrusiva;

Senza entrare nel merito della conoscenza di base degli allievi, della professionalità degli insegnanti e del tipo di materie trattate, in ogni caso un simile corso non appare sufficiente a formare nei discenti la necessaria "mentalità alla sicurezza".

Infatti, nell'immaginario collettivo, persiste l'idea che la tecnologia e tutte le sue innovative applicazioni tecniche, dalla videosorveglianza automatica a tracking attivo al controllo accessi biometrico, possano risolvere egregiamente il problema della sicurezza marittima.

Ci si dimentica troppo spesso che anche la più sofisticata apparecchiatura non possiede quelle doti umane, chiamate intuito e creatività, che sono nella maggior parte dei casi gli elementi risolutivi per sventare un furto, un attentato o una azione terroristica.

Queste doti possono essere opportunamente sviluppate e orientate alla sfera della sicurezza con l'aiuto di professionisti che, nell'ambito di un adeguato corso, focalizzino l'attenzione in particolare sui temi del comportamento e delle modalità d'azione dei terroristi e/o dei ladri.

Oramai i governi e le organizzazioni che operano nel settore della sicurezza hanno imparato che la vera minaccia è rappresentata dalla sempre più vasta abilità e professionalità dei terroristi ed è proprio questa tematica che deve costituire il principale oggetto di insegnamento all'interno di un corso riferito alla sicurezza.

Possedere un così vasto e specifico bagaglio di conoscenze sul tema della sicurezza normalmente è frutto di un processo di apprendimento teorico-pratico che si acquisisce solo nel tempo.

L'entrata in vigore dell'ISPS Code nel luglio dell'anno scorso ha costretto gli armatori e i responsabili dei porti a "correre ai ripari"; una minoranza ha reperito sul mercato del lavoro professionisti della sicurezza ma la maggioranza ha designato un proprio dipendente quale Agente di Sicurezza.

Un corso di formazione ad hoc, della durata di un paio di giorni, ha permesso a questi dipendenti di ottenere l'idoneità ad operare sulle navi o nei porti in qualità di esperto di sicurezza .

Ivano Roveda

*Direttore della Outsourcig Development & Management S.r.l. (Engeneering e Sicurezza)
Socio A.I.PRO.S. Associazione Italiana Professionisti della Sicurezza*

Italia. La minaccia terroristica

Sin dagli anni Sessanta, epoca in cui sorge il terrorismo contemporaneo, la minaccia nei confronti tanto dell'Italia quanto della comunità internazionale è di duplice matrice: endogena ed esogena. Pur non essendosi totalmente esaurita la minaccia del terrorismo interno (lo attestano i rigurgiti dell'estremismo di destra e di sinistra, particolarmente di stampo anarcoide, e le azioni violente di aggregazioni separatiste etno-nazionaliste), la fonte principale della minaccia proviene oggi dal radicalismo islamico, le cui dinamiche coinvolgono elementi sia interni sia transnazionali. Basta ricordare, per restare nel mondo occidentale, gli attentati di New York e Washington (11 settembre 2001), di Madrid (11 marzo 2004) e di Londra (7 e 21 luglio 2005).

Nel calcolo terroristico, il quale è accompagnato da costante progettazione come dimostrato dal *modus operandi* della rete che si ispira ad al Qaeda, diversi fattori rendono l'Italia un potenziale e pagante bersaglio. Primo: gli impegni militari/umanitari nel mondo islamico, particolarmente in Afghanistan con circa duemila uomini ed in Iraq con oltre tremila. L'Italia correntemente partecipa a 25 missioni internazionali in 18 Paesi in buona parte di cultura/religione islamica. Tutto ciò comporta visibilità internazionale. Secondo: la stretta collaborazione con gli USA nel contrasto al terrorismo. Per quanto riguarda specificamente l'impegno in Iraq, l'Italia è in ambito europeo-continentale il più importante e palese alleato degli USA. Terzo: gli arresti, processi, condanne ed espulsioni di elementi radicali islamici indiziati di terrorismo o attività di supporto. Gli arrestati sono stati 16 nel 2000, 33 nel 2001, 64 nel 2002 e 71 nel 2003. Statistiche cumulative per il periodo luglio 2001/giugno 2005 rispecchiano 203 arresti. Gli osservati speciali sono a loro volta circa 350. Quarto, ma non da sottovalutare: il ruolo fondamentale dell'Italia nello sviluppo della cultura e civiltà occidentale. Non a caso si trova a Roma la sede storica del cristianesimo.

Infatti, l'Italia è stata e rimane oggetto di ripetute minacce, talune persino dirette al suo attuale Presidente del Consiglio dei Ministri. Osama Bin Laden ha personalmente minacciato l'Italia annualmente dal 2001 al 2004, mentre le Brigate al Masri hanno emesso dichiarazioni intimidatorie una volta nel 2003 e due nel 2004, al Muqrin tre volte nel 2003 e altre aggregazioni almeno quattro volte nel 2004. Ulteriori minacce hanno avuto luogo anche dopo i su ricordati attentati di Londra nel luglio di quest'anno.

Parimenti, bande armate irregolari e terroristiche hanno posto in essere violenze non solo contro il personale e le strutture istituzionali italiane in Iraq (Nassiriya e altrove), ma anche ai danni di privati cittadini nei settori della sicurezza imprenditoriale, del giornalismo e del volontariato di affiliazione "Ong", come dimostrato in sequenza dai sequestri Quattrocchi-Agliana-Cupertino-Stefio, Baldoni, le "due Simone" Pari-Torretta e Sgrena. Detti sequestri e le relative uccisioni di Quattrocchi e Baldoni sono avvenuti dall'aprile del 2004 ad oggi. Per quanto riguarda la vulnerabilità degli obiettivi, va ricordato che nei calcoli e nelle dinamiche del terrorismo internazionale, a prescindere dalla matrice politica o politico-religiosa, è spesso più agevole colpire cittadini, beni e interessi di specifiche nazioni all'estero piuttosto che sul loro territorio nazionale.

All'interno dell'Italia, le risultanze investigative, confermate da quelle giudiziarie, rispecchiano soprattutto la costituzione di basi e reti i cui fini comportano l'agevolazione dell'ingresso clandestino di connazionali/correligionari; il reperimento o la contraffazione di documenti d'identità o di viaggio; la raccolta e il riciclaggio di fondi attraverso attività commerciali o caritative; l'acquisizione di armi, esplosivi e agenti chimici da utilizzare in patria, nella stessa Europa o altrove;

matrimoni con cittadini italiani per l'ottenimento della cittadinanza, residenza e relative coperture; e il monitoraggio e reclutamento di musulmani nell'ambito delle comunità islamiche trapiantate - inclusi i discendenti di seconda generazione - per essere inviati a frequentare corsi di addestramento, tenutisi fino all'inizio dell'attuale decennio prevalentemente in Afghanistan, o a svolgere direttamente compiti eversivi o violenti in Europa e altrove. A tali fini, gli estremisti islamici attivi nel Paese sfruttano una serie di istituzioni ed esercizi commerciali, fra i quali risaltano centri culturali, moschee, macellerie specializzate, negozi di abbigliamento e café internet. A questi si aggiunge il noto strumento finanziario informale dell'*hawala*.

Verosimilmente l'attività di prevenzione è stata sinora tale da non rendere possibile la concretizzazione di atti terroristici eclatanti, anche se esistono episodi di non certa interpretazione.

Gli strumenti giuridicamente e tecnicamente impiegabili debbono mirare alla dissuasione, prevenzione, e repressione del terrorismo interno e transnazionale, nonché al contenimento dei danni da esso causati in quanto il terrorismo non è del tutto debellabile. Questi strumenti includono l'*intelligence*, l'apporto dei cittadini e delle organizzazioni private, la responsabilizzazione nei *mass media*, la preparazione tecnica del personale assegnato agli enti statali competenti, un'impostazione antiterroristica equilibrata e coerente, gli accordi internazionali, la diplomazia, le sanzioni e gli incentivi economici e di altra natura, la collaborazione bilaterale e multilaterale tra Stati, il ruolo appropriato delle forze armate, le operazioni speciali saggiamente mirate e dosate e la protezione civile.

Oltre all'esigenza di forze armate, le operazioni speciali saggiamente mirate e dosate e la protezione civile. Oltre all'esigenza di programmazione con debito anticipo, gli strumenti di contrasto debbono essere concreti, di reciproco rinforzo e coordinati fra loro. Solo raramente un singolo strumento può rivelarsi determinante o prestarsi ad un impiego esclusivo, poiché la propria applicabilità ed efficacia sono variabili a seconda delle situazioni specifiche.

Data la delicatezza del momento storico, riveste particolare importanza la sensibilizzazione dell'opinione pubblica, ausilio indispensabile per il controllo del territorio e per un'efficace impostazione antiterroristica. Solo se adeguatamente sensibilizzati e informati, i cittadini e gli enti privati possono esercitare la vigilanza del caso, ridurre la propria vulnerabilità e collaborare, riferendo eventuali segnali di avvertimento e di pericolo, con le forze statali preposte alla prevenzione e alla repressione della minaccia.

Per quanto riguarda, poi, la collaborazione delle imprese con le autorità costituite ai fini del contrasto preventivo e del contenimento del fenomeno terroristico, è di notevole importanza lo sviluppo di criteri aziendali di monitoraggio della minaccia attinente ai loro specifici settori, ad esempio, bancario, energetico, chimico o farmaceutico, nonché quanto concerne le infrastrutture e i trasporti. In tutti questi settori altamente tecnici, le imprese sono in condizione di formulare valutazioni approfondite che normalmente esulano dalle conoscenze istituzionali degli apparati di sicurezza statali. Ma tutto ciò non è attuabile in assenza di una adeguata formazione di settore mirata alla tutela della sicurezza privata nei confronti del terrorismo.

Prof. Vittoriofranco Pisano

Colonnello t.SG di Polizia Militare USA (Ris.) - Docente nel Master in Intelligence & Security presso Link Campus University of Malta

Le nuove sfide dell'information security

L'Information Security ha acquisito un ruolo centrale nel mondo delle aziende e delle istituzioni nazionali e internazionali. In un'economia basata sulla conoscenza, dati e informazioni diventano il patrimonio essenziale e la stessa ragion d'essere di imprese ed organizzazioni complesse.

La protezione di questi asset e l'assicurazione della continuità operativa della società/istituzione richiedono l'adozione di strategie e contromisure efficaci e capaci di conciliare problematiche di carattere tecnologico e temi a sfondo organizzativo. La gestione dell'Information Security va in altre parole ben al di là del puro aspetto tecnologico e di messa in sicurezza dei sistemi. Al contrario si va imponendo un'impostazione di tipo manageriale centrata sulla formazione e sensibilizzazione del personale e su di un nuovo sistema di security governance.

Realtà diverse presentano tuttavia complessità e aspetti differenziati, richiedendo approcci specifici. Aziende ed istituzioni "data intensive" come banche, operatori di telecomunicazioni e pubblica amministrazione sono più esposte al rischio di furto, distruzione o uso illecito di dati ed informazioni. Come conseguenza questi comparti sono anche quelli che hanno adottato sistemi di protezione più sofisticati.

Nel caso delle banche ad esempio sono ricordare gli sforzi compiuti, anche a livello normativo (Basilea 2, Banca d'Italia) per assicurare una migliore gestione del rischio operativo, definito come la possibilità di incorrere in perdite a causa di failure di sistemi, processi e/o risorse aziendali. Nel caso degli operatori di telecomunicazione e della pubblica amministrazione (soprattutto Sanità e Fisco) la capacità di assicurare l'implementazione e la gestione di infrastrutture informatiche complesse e la contemporanea protezione della privacy dei cittadini hanno spinto all'adozione di sistemi di Information Security integrata. In questi casi non solo sono state implementate soluzioni tecnologiche di sicurezza avanzata (ad esempio sistemi di regolazione di accesso e gestione delle informazioni), ma anche: definite policies che normano il comportamento di utenti ed amministratori dei sistemi; varati assetti organizzativi innovativi basati sul concetto di "famiglie professionali"; implementati meccanismi di pianificazione e controllo degli obiettivi di sicurezza basati su indicatori di rischio e performance (es. Security Tableau de Bord).

Per rispondere ad esigenze e sfide sempre più complesse, consulenti e provider di servizi di sicurezza devono sviluppare un approccio nuovo, coniugando specializzazione e visione d'insieme. Trattandosi di una tematica di non facile comprensione e in continua evoluzione, l'Information Security richiede dedizione ed aggiornamento continuo. Viene quindi scoraggiato un approccio di taglio generalista e premiato invece chi sceglie di focalizzarsi, assicurando nel contempo una visione d'insieme che colloca e integra in modo efficace l'Information Security all'interno dell'organizzazione cliente. I consulenti infine hanno una responsabilità in più. Un presidio efficace delle esigenze di sicurezza delle aziende clienti richiede infatti la capacità di assicurare la progettazione e realizzazione di soluzioni chiavi in mano, diventando il "general contractor" che permette al cliente di avere un partner unico dalla fase di analisi del problema, all'individuazione della risposte più opportuna, sino al roll-out e gestione delle soluzioni.

Roberto Lorini
Executive Vice President VP Tech

Brevi cenni sulla crescente diffusione della Biometria

La situazione politica particolarmente delicata a livello internazionale e la crescente richiesta generalizzata di maggiore sicurezza nella nostra vita di ogni giorno stanno vistosamente forzando le tappe per una diffusione sempre più capillare di nuove tecnologie in grado di determinare l'identità certa degli individui.

Le cosiddette "tecniche biometriche", basate sul riconoscimento di caratteristiche degli individui come impronte digitali, iride o volto stanno quindi entrando velocemente nelle prassi procedurali di uffici o banche introducendo abitudini e gestualità che, quasi tutti gli esperti concordano, nel giro di poco tempo diverranno familiari, soprattutto alla luce dell'ormai prossima introduzione dei nuovi passaporti di tipo elettronico che ingloberanno elementi biometrici

I settori di stretta competenza dalla biometria possono essere microscopicamente identificati in quello del controllo degli accessi, fisici e logici, e della sorveglianza.

Il primo consiste nella verifica della identità degli utenti nelle operazioni di accesso a luoghi o comprensori (accesso fisico) o per la fruizione di servizi informatici (accesso logico) mentre le tecniche di sorveglianza biometrica sono deputate all'identificazione automatica di particolari classi di individui all'interno di zone caratterizzate da un alto livello di sensibilità.

Ci si attende quindi una certa diffusione delle tecniche biometriche a protezione delle zone o ambienti sensibili, soprattutto a livello governativo anche se, e questo è un aspetto particolarmente delicato, dovrebbe essere ormai evidente che l'applicazione, per ottemperare in maniera corretta alla normativa sulla privacy, deve soddisfare a pieno i due principi di proporzionalità e necessità

Il rapporto fra biometria e Garante della Privacy è tuttavia caratterizzato, da parte del Garante, da una grande e comprensiva attenzione e, a tal proposito, di particolare interesse appare, nel contesto internazionale, l'autorizzazione concessa all'uso della biometria in alcune filiali di banche caratterizzate da un considerevole profilo di rischio.

In proposito, la richiesta di rilasciare le impronte digitali, in forma assolutamente anonima, sembra avere ottenuto, da una parte risultati concreti (oltre ad un significativo effetto di deterrenza) in merito alla reiterazioni dei fenomeni criminosi, dall'altra ha dimostrato, ancora una volta, la generalizzata buona accettazione, da parte degli utenti, del controllo biometrico, soprattutto se effettuato nel contesto di un quadro normativo ad-hoc ed in linea con i tempi.

La frontiera della tecnologia è rappresentata dalla cosiddetta "sorveglianza biometrica" che associa al tradizionale concetto di videosorveglianza la possibilità di riconoscere la presenza di particolari classi di individui nelle aree sottoposte al controllo e c'è già chi in Italia ipotizza, come già avviene in altri Paesi, un uso della sorveglianza biometrica in zone o aree a particolare rischio o per il controllo delle manifestazioni sportive più delicate.

Un eventuale uso delle tecniche di sorveglianza biometrica, anche se di stretta competenza delle Forze dell'Ordine, non mancherà comunque di destare probabilmente qualche perplessità per le ovvie interferenze con aspetti etici e con la privacy anche se, in ogni caso bisognerebbe ammettere che – piaccia o meno – viviamo in un contesto sociale e tecnologico destinato quasi certamente nel tempo a sacrificare qualche aspetto della riservatezza in cambio di un incremento della sicurezza.

Per concludere, qualche nota sulla posizione dell'Italia nello scenario della biometria. Il nostro Paese, nel panorama internazionale, viene unanimemente giudicata una nazione particolarmente impegnata nello studio della biometria e delle sue applicazioni e non è un dato contestabile che alcuni Centri di Ricerca Universitari e del Consiglio Nazionale delle Ricerche abbiano, nel settore, una visibilità assolutamente paragonabile, se non superiore, a quella tipica dei paesi ad alto sviluppo tecnologico.

Ing. Mario Savastano

Ricercatore BB - CNR (National Research Council of Italy) c/o DIEL - Università Federico II

La sfida della gestione della Sicurezza nelle nostre Città

Sempre più la gestione della Sicurezza nelle nostre città, sta diventando una vera e propria sfida per le Amministrazioni. Molti e complessi sono infatti gli aspetti coinvolti ma, dobbiamo aggiungere, non sempre le risposte sono all'altezza della sfida stessa.

Ma allora, senza per questo voler peccare di presunzione, dal nostro punto di osservazione di operatori del settore, ma anche di semplici cittadini, ci chiediamo: come si vince questa sfida?

Non si possono certo esprimere soluzioni universalmente valide, anche considerando le casistiche molto differenziate delle nostre città, ma sicuramente alcuni principi sono universalmente applicabili.

Il principio basilare, ma purtroppo non sempre applicato, è quello di un'attenta valutazione dei rischi. Tale fase non può che nascere da un tavolo di lavoro misto, costituito da esperti delle problematiche della città stessa, ovvero le amministrazioni, ed esperti di sicurezza, o meglio di analisi dei rischi. Questa fase deve considerare rischi diversi in luoghi diversi. In generale non potrà prescindere dal monitoraggio delle aree principali della città, della viabilità, delle periferie critiche e dei luoghi principali di assembramento, ma anche dalla protezione del patrimonio artistico e culturale, degli immobili ed infrastrutture della Città (non escludendo per esempio gli Stadi e le strutture sportive), dal monitoraggio di luoghi di particolare attenzione sociale, come per esempio le scuole, e da un monitoraggio dei trasporti pubblici. Si dovrà infine tenere in conto un sufficiente livello di flessibilità, ovvero la capacità di affrontare rischi nuovi ed intervenuti, come sta per esempio avvenendo con il terrorismo. La fase di analisi dei rischi dovrà dunque definire quali sono i rischi che si desidera fronteggiare e con quali priorità.

Il secondo principio nasce come conseguenza dalla complessità delle problematiche emerse nella prima fase, ovvero, vista l'impossibilità di fronteggiare con un unico strumento i rischi individuati, è necessario definire come ridurre tali rischi con un uso sapiente di Sistemi di Sicurezza, di Uomini e Procedure, in quello che può essere definito come un "Processo di Sicurezza".

Non vi è certo qui lo spazio per approfondire, ma sicuramente molti dei rischi individuati potranno essere sostanzialmente ridotti con le moderne Tecnologie della Sicurezza.

Il secondo principio ha una ulteriore conseguenza, poiché serviranno diversi investimenti (Sistemi di Sicurezza, Strumenti, ecc.) e non è pensabile effettuarli in una sola annualità di bilancio, le amministrazioni devono dunque definire una strategia, che nel tempo le porti a consolidare diverse realizzazioni in una costruzione organica, chiara però sin dall'inizio.

Ciò introduce al terzo principio: l'integrazione. La tecnologia odierna permette infatti di interconnettere e "centralizzare" diversi sistemi, trasportando le informazioni (immagini, allarmi, dati) piuttosto che gli uomini che le devono analizzare e gestire, a tutto vantaggio dell'ottimizzazione dei costi (da una centrale operativa si possono supervisionare gli aspetti di sicurezza di una intera città).

L'integrazione va progettata e perseguita strenuamente, imponendosi di far colloquiare sistemi realizzati con diverse modalità ed in epoche successive. L'integrazione va però realizzata con l'utilizzo di "Piattaforme di Centralizzazione Aperte", ovvero in grado colloquiare con diversi prodotti e sottosistemi, senza preclusione di fornitori, marche, ecc., a tutto vantaggio della concorrenza e della flessibilità verso nuove necessità che potranno emergere in futuro.

L'utilizzo di piattaforme aperte ha una naturale conseguenza che può considerarsi un quarto principio: l'interdisciplinarietà.

Per quanto possibile bisogna infatti evitare il proliferare di sistemi diversi, che i vari dipartimenti delle amministrazioni possano voler realizzare per proprio conto, non badando all'integrazione tra di essi. Come scelta politica, va quindi perseguito il dialogo tra le diverse esigenze che porti ad una "Piattaforma Aperta", che permetta di integrare tutti i diversi aspetti della sicurezza, garantendo a ciascuno di operare secondo la propria competenza.

Oltre ai principi enunciati vi sono poi gli aspetti tecnici specifici, come la progettualità tecnica (meglio utilizzare gli esperti!), la capacità di selezionare chi deve realizzare i Sistemi (il costo non può essere l'unico parametro considerato), la capacità di portare a compimento quanto progettato nonché di gestire e mantenere quanto così faticosamente ottenuto (che peccato vedere spesso sistemi costosi che per pochi spiccioli di manutenzione vengono lasciati inutilizzati e non funzionanti!).

Volendo sintetizzare, quanto viceversa osserviamo avvenire in media sul panorama italiano e che purtroppo non sempre si fa un'attenta analisi dei rischi (non ricorrendo a persone esperte), molto raramente si definisce una strategia di lungo termine con la quale effettuare degli investimenti e difficilmente si pensa a creare una piattaforma integrata, aperta e multidisciplinare. Infine solo a volte si riesce a progettare bene quanto è necessario, a selezionare con le opportune procedure amministrative un fornitore affidabile ed quindi a realizzare e gestire opportunamente i sistemi.

Concludendo, serve un diverso approccio in cui le amministrazioni utilizzino meglio le competenze che esistono sul mercato e considerino le aziende ad alta specializzazione del settore, più partner che semplici fornitori.

Solo così si potrà vincere questa difficile sfida.

Ing. Santi Maurizio Grasso

Direttore Commerciale DAB Sistemi Integrati Srl

Beni Culturali. Protezione e fruibilità possono convivere?

L'Italia è il Paese con più ricchezze al mondo dal punto di vista culturale. Il nostro patrimonio costituisce il 50% della ricchezza culturale mondiale dichiarata dall'UNESCO Patrimonio dell'Umanità.

Dal punto di vista dell'Economia Nazionale, la grande attrattiva esercitata dalle nostre città d'arte, dai nostri musei, dalle nostre aree archeologiche è il propulsore principale del settore turistico da sempre importantissimo per il nostro Paese. Ormai è un valore condiviso e diffuso che i beni culturali siano una ricchezza per la società da godere e valorizzare.

E' necessario che i nostri tesori artistici, archeologici, architettonici siano resi fruibili ad un pubblico sempre più vasto e che, al tempo stesso, siano mantenuti nelle migliori condizioni di conservazione e ne sia assicurata la protezione contro ogni possibile danno, accidentale o intenzionale. Tuttavia l'Italia, per la vastità del suo patrimonio, deve affrontare il problema del fabbisogno di risorse necessario per la tutela dello stesso. Capita spesso che i nostri capolavori per timore che siano oggetto di furti ed atti vandalici, non siano aperti al pubblico. D'altro canto è lecita la preoccupazione dei responsabili della custodia e della conservazione dei beni i quali, piuttosto che metterli in pericolo non li espongono affatto, non potendone garantire la sicurezza.

Programmare correttamente gli investimenti dedicati alla sicurezza dei beni culturali permette di ottenere un risultato economico a breve e medio termine, garantendo la possibilità di maggiori aperture al pubblico e minimizzando i rischi di danni o furti.

Dal punto di vista tecnico importanti aiuti possono derivare dalle applicazioni specialistiche che il mondo della sicurezza dedica alla protezione di opere d'arte ed in generale del territorio in cui viviamo.

Poiché parliamo di un ambito vastissimo che va dai Musei alle Biblioteche, dalle Aree Archeologiche alla Mostre temporanee, dagli Archivi Storici ai Luoghi di Culto, un approccio progettuale specifico è il punto di partenza indispensabile per individuare:

- tutti gli elementi di rischio per il bene da proteggere nel contesto in cui deve essere goduto dal pubblico;
- le misure più adatte per garantire la protezione dai vari rischi individuati;
- la soluzione integrata che consente di ottimizzare la gestione del sistema di sicurezza.

I grandi progressi fatti dal punto di vista tecnologico consentono oggi di avere strumenti per proteggere i beni culturali da rischi di ogni tipo, ad esempio:

- sistemi antincendio ed antintrusione di grande efficienza;
- sistemi televisivi a circuito chiuso e trattamento digitale delle immagini;
- sistemi di regolazione e controllo dei parametri ambientali e climatici;
- sistemi di controllo accessi e software di supervisione molto potenti;
- reti di comunicazione locali e geografiche a banda larga che consentono l'implementazione di centrali di controllo "in loco" o remote

Una corretta progettazione ed un'installazione professionale dei sistemi consentono inoltre, di scegliere le tecnologie in modo che siano il meno "invasive" possibile dal punto di vista estetico e funzionale.

Ad esempio:

- è possibile utilizzare tecnologie *wireless* per i collegamenti ai sensori ed alle telecamere, in quanto la trasmissione radio oggi è sempre più sicura da interferenze ed intrusioni;
- gli assorbimenti elettrici sempre più contenuti delle apparecchiature elettroniche permettono di ricorrere a pannelli solari o energia eolica per alimentare le centraline di rilevamento o i punti di sorveglianza in aree in cui è difficoltoso approvvigionare energia elettrica;
- la miniaturizzazione consente di installare sensori e telecamere in prossimità delle opere d'arte o sulle facciate di palazzi senza che ne risenta l'aspetto estetico del bene protetto.

L'implementazione di tali tecnologie è particolarmente vantaggiosa soprattutto se correlata con una gestione accorta dei servizi di sorveglianza di cui possono aumentare l'efficacia. Basti pensare alla possibilità di avere in tempo reale le informazioni relative ad un allarme presso la sala operativa del sito, comunicandole contemporaneamente alle Forze dell'Ordine, alla pattuglia di ronda o al custode mediante terminale portatile.

Un cenno è necessario alla manutenzione dei sistemi di sicurezza, che purtroppo nel nostro Paese non è sempre tenuta nella debita considerazione ma che è un elemento di fondamentale importanza per garantire la protezione dei beni e l'investimento fatto. Se concepita in ottica moderna ed evolutiva e non come semplice corollario alla realizzazione del sistema, la manutenzione diventa il vero punto di forza di una politica volta ad assicurare aggiornamento tecnologico e continuità di servizio.

Alla luce di quanto rapidamente accennato è quindi possibile dare una risposta affermativa all'interrogativo di apertura della presente nota: *è possibile massimizzare la fruibilità dei beni culturali garantendone la sicurezza attraverso un corretto utilizzo delle tecnologie e delle competenze presenti sul mercato ed implementando le procedure ed i servizi necessari per il mantenimento delle condizioni ottimali d'esercizio.*

Perché questo accada tutti gli attori coinvolti (istituzioni, operatori culturali e turistici, professionisti ed aziende della sicurezza) devono comprendere l'importanza della posta in gioco, che riguarda uno dei principali settori della vita del Paese dal punto di vista economico e sociale.

Ing. Giovanni Bracone
Responsabile Divisione Progetti di DAB Sistemi Integrati S.r.l.
Gruppo DAB

La sicurezza attiva e passiva all'interno di una moderna struttura destinata alla reclusione

La progettazione della sicurezza attiva e passiva all'interno di strutture destinate alla reclusione deve sempre tenere presenti le esigenze operative e funzionali delle strutture stesse. Infatti, la tecnologia non deve in alcun modo limitare le attività operative e la funzionalità degli ambienti in cui agisce il Personale dell'Amministrazione Penitenziaria, ma deve essere un valido strumento affinché detto Personale possa operare in modo agevole in totale e completa sicurezza.

L'altro aspetto di notevole importanza nella progettazione della sicurezza è la ricerca di una elevata integrazione e centralizzazione dei sistemi, sia perché detta integrazione consentirà di visualizzare in tempo reale gli eventi di allarme ed automaticamente interconnettere i diversi sistemi per la corretta gestione degli eventi, sia perché un'unica piattaforma di gestione consentirà di ottimizzare la struttura del sistema stesso.

Nello specifico, una struttura tipo di una casa di reclusione può essere distinta in due macro aree opportunamente separate da vincoli fisici ed elettronici:

- Detenzione e servizi;
- Area uffici ed alloggi Personale Amministrazione Penitenziaria.

Prima di individuare le tipologie impiantistiche a servizio della struttura bisogna individuare la tipologia di atto criminoso che può essere compiuto al suo interno.

In questo ci viene incontro la cultura anglosassone nel campo della sicurezza, che impiega due sostantivi distinti per indicare la diversa funzionalità di difesa degli impianti dagli atti criminosi. Infatti, se l'atto criminoso nei confronti di persone e beni è di tipo volontario si parlerà di impianti destinati alla *security*, mentre se l'atto criminoso è di tipo casuale si parlerà di impianti destinati alla *safety*.

A servizio del complesso edilizio si possono quindi individuare le seguenti tipologie impiantistiche:

- Impianti destinati alla *security*;
- Impianti destinati alla *safety*;
- Impianti elettrici e speciali.

La gestione di questi impianti sarà affidata ad una sala di controllo posta all'interno di una struttura protetta ed opportunamente separata dalle aree detentive. I criteri generali di impostazione dell'impiantistica destinata alla sicurezza si dovranno appoggiare su quelli di seguito descritti:

Espansibilità: consentire ulteriori implementazioni attraverso la semplice acquisizione e configurazione di elementi terminali (ad esempio dispositivi in/out quali sensori, telecamere, terminali per il controllo degli accessi, ecc.), ma non attuare incrementi delle infrastrutture di trasmissione, visualizzazione, gestione, memorizzazione, ecc;

Ridondanza: di tipo *caldo* per tutti i sistemi vitali nella gestione, ripresa e memorizzazione degli eventi, con ridondanza di tipo *funzionale* per i sistemi di ripresa video dislocati in campo;

Continuità del servizio: garantita per tutti gli impianti di sicurezza, stante la criticità dell'applicazione, in caso di mancanza di energia elettrica, tramite l'impiego di gruppi statici di continuità a loro volta alimentati attraverso linea privilegiata (gruppo elettrogeno).

Infine, la progettazione della sicurezza, così come previsto dalla normativa vigente in materia di appalti pubblici, dovrà prevedere tutti quegli interventi di manutenzione degli impianti necessari per preservare la loro funzionalità con il conseguente mantenimento degli adeguati livelli di sicurezza.

Ing. Luigi Miccoli

Presidente CDA EPRO S.r.l