

Editoriale. Il ruolo della security tecnologica tradizionale nella società del web

*Franco Dischi**

In ambito scientifico, ma ancor prima nei salotti buoni della social information, i blog e i forum di discussione IT, si dibatte da tempo sull'imminente passaggio dall'era della globalizzazione all'era della global-interconnessione del mondo. Un passaggio che a ben vedere fa già parte dell'oggi, se si guarda all'autorevole definizione di globalizzazione di Pier Giorgio Ardeni¹ quale "crescente interconnessione di persone e luoghi risultante dagli avanzamenti nelle tecnologie dell'informazione, della comunicazione e dei trasporti, dalla sempre minore importanza delle barriere e delle frontiere nelle relazioni economiche internazionali, e dalla mondializzazione degli stili, degli schemi e dei modelli economici e legali che portano alla convergenza politica, culturale ed economica tra Paesi".

L'interconnessione globale, deflagrata in pochissimo tempo con la diffusione a macchia d'olio di Internet e con l'esplosione dei social network e dei dispositivi mobili intelligenti che veicolano contenuti da qualunque luogo e in ogni momento della nostra giornata, ci consegna del resto un mondo nuovo, fatto di esperienze condivise e di "real time senza compromessi". Ciò che in parte e certo non esaustivamente descrive l'ampio concetto di Web Society, tema al centro di questo primo numero del trimestrale Sicurezza e Scienze Sociali.

1. Vulnerabilità della Web Society

All'entusiasmo di un mondo libero, dove condividere apertamente informazioni, documenti, risorse, applicativi, si contrappongono tuttavia insidie

* Associazione Assosicurezza. assosicurezza@assosicurezza.it

¹ Pier Giorgio Ardeni, Professore Ordinario di Economia Politica e di Economia dello Sviluppo presso l'Università di Bologna Dipartimento di Scienze Economiche. Testo disponibile al sito: www2.dse.unibo.it/ardeni/Corsi_anni_passati/Economia_dello_sviluppo/Globalizzazione.htm

e problematiche del tutto peculiari della Web Society e che impongono un profondo ripensamento su temi “macro”, quali la tutela della privacy personale e la sicurezza.

Queste tematiche, già al centro dei principali dibattiti tecnici e normativi, diventeranno sempre più pressanti con la diffusione dell’IPv6 e con un uso sempre più massivo della banda larga – fattori che preluderanno a quell’Internet of Things dove gli oggetti potranno acquisire un’intelligenza “attiva” accedendo direttamente alle informazioni reperibili in rete. Basta pensare ad un oggetto banale come la sveglia che diventerà capace di suonare in anticipo “perché ha autonomamente verificato che c’è traffico” per dare una dimensione e un’identità al nuovo paradigma determinato dall’Internet delle cose e dai suoi sviluppi in chiave 3.0.

Scenari intriganti, misteriosi e dagli applicativi potenzialmente illimitati, che però – su questo non c’è dubbio – aumenteranno esponenzialmente l’allarme sulla sicurezza dei dati e le minacce alla riservatezza personale. In questo fiume di informazioni liberamente accessibili, quanto dovremo perdere di noi stessi, del nostro business, del nostro danaro, del nostro copyright e in generale delle nostre idee?

2. L’industria della security fisica

Il tema, apparentemente riservato ai soli decisori politici e, sul piano tecnico, a chi si occupa di IT security, si estende in verità a chiunque a vario titolo si occupi di sicurezza, arrivando a lambire anche chi produce e distribuisce soluzioni tecnologiche di sicurezza in senso tradizionale, ossia in senso fisico. Ci riferiamo ad un’industria complessa da perimetrare, dal momento che nasce, per derivazione o per espansione, da settori limitrofi (elettrico, elettronico, meccanico e mecatronico) e dal momento che è oggetto di sempre maggior attrazione da parte di nuovi comparti, partendo proprio dall’ICT, quindi il suo nucleo tecnologico originario è andato via via integrandosi con quello di altre *industry*.

Questa industria così variegata è tuttavia la prima interessata a produrre soluzioni che tengano conto del contesto “aperto” nel quale deve ormai per forza inserirsi l’operatività tecnica dei prodotti di sicurezza.

Se infatti è stato da tempo pensionato il *device* di sicurezza *stand-alone* per abbracciare logiche di sistema e poi di rete a maglie sempre più larghe, fin ad arrivare alla Rete delle Reti, è al contempo cambiato lo scenario nel quale insiste lo stesso modo di “fare, pensare e proporre sicurezza”.

3. Un nuovo paradigma

Un nuovo paradigma è quindi stato adottato anche nel campo della sicurezza tradizionale. Sistemi d'allarme, videosorveglianza, controllo accessi fisico, protezioni perimetrali, *building e home automation*: tutto deve ormai fare i conti con la sicurezza dell'autostrada che trasporta i dati e le informazioni legate alle immagini delle telecamere e ai segnali di allarme.

E tutti ormai devono fare i conti con l'utilizzo di dispositivi mobili (spesso ad uso personale, quindi ancora più a rischio intrusione) per la ricezione e la gestione dei dati da remoto.

In sintesi, utilizzare la rete IP per trasportare dati, come ormai accade in quasi tutte le industrie – anche le più chiuse, come quella della security fisica – significa portarsi dietro tutte le problematiche di sicurezza legate all'IT, quindi significa portarsi in casa tutti rischi legati all'integrità dei segnali, e quindi mettere a rischio la stessa funzione di sicurezza delle tecnologie proposte.

4. L'Associazionismo, volano per la cultura della sicurezza

Muove dall'insieme di questi presupposti e di queste riflessioni l'interesse di Assosicurezza, Associazione Nazionale Costruttori e Distributori di Sistemi di Sicurezza, per questa nuova rivista che si affaccia sulla scena della stampa scientifica. Un interesse tutt'altro che disinteressato, avendo questa rivista ad oggetto – sin dal nome della testata – un tema che di fatto incarna la nostra mission associativa: promuovere la cultura della sicurezza in tutte le sue forme.

Calare il tema della sicurezza fisica, che curano le nostre aziende, in chiave prospettica di Web Society, ha reso il nostro interesse ancor più netto e definito, non essendoci ancora, nel settore in cui operano le nostre aziende, una completa percezione del rischio al quale sono esposte le apparecchiature di sicurezza tradizionali a seguito della convergenza in atto tra sicurezza fisica e sicurezza logica. Portando l'IP nel campo della sicurezza tradizionale, la sicurezza fisica si compenetra infatti con la sicurezza logica e le problematiche e le competenze dell'IT manager si fondono con quelle del security manager, coinvolgendo anche la gestione dei processi e delle risorse umane. Nel frattempo la necessità di compattare comandi e sistemi di gestione, dovuta anche ad una sempre più forte richiesta di remotizzazione e di risparmio, vede la security tradizionale compenetrarsi non solo con l'ICT, ma anche con la safety, la domotica e la biometria. Un passaggio delicatissimo che richiede una gestione estremamente attenta.

5. Un approccio olistico alla sicurezza

In gergo tecnico, questo passaggio viene definito di Security Convergence, ed impone un approccio olistico alla sicurezza che armonizzi competenze e responsabilità con una progressiva integrazione di processi, strumenti e risorse. Integrazione alla quale il nostro settore, soprattutto nelle frange tecnologiche meno evolute e negli anelli terminali del canale di mercato, non è ancora pienamente pronto.

Naturalmente gli strumenti tecnici per dotare i dispositivi fisici di standard di sicurezza adeguati sono pienamente disponibili e incorporati sin dalla progettazione nelle tecnologie di ultima generazione, ma se mancano cultura, formazione e sensibilità di tutti i soggetti coinvolti, il rischio di intrusioni si autoalimenta di anello in anello della catena distributiva, fino a diventare virale a livello di utenza finale.

Il primo passo tocca evidentemente a noi, produttori e distributori di tecnologie per la sicurezza fisica: sta a noi educare la filiera ad una cultura della sicurezza che sia realmente “olistica”, dalla progettazione fino alla manutenzione periodica di ciascun dispositivo.

In questo senso, iniziative scientifiche e divulgative come quella del trimestrale Sicurezza e Scienze Sociali devono essere sempre salutate con interesse dalle Associazioni di categoria.

6. Il ruolo del partenariato

Ma assieme all’aspetto più squisitamente divulgativo che deve essere operato sulla filiera del mercato, è essenziale diffondere una cultura dei processi che coinvolga anche l’utenza, in particolare quella pubblica.

L’interlocutore pubblico, del resto, spesso si pone in posizione di partnership tecnologica e ancor più spesso in veste di partner di progetto, gettando le basi per quel modello di partenariato che ha già visto diverse pratiche virtuose nella gestione della sicurezza urbana e nelle politiche di controllo del territorio.

Ci riferiamo ad accordi come “Mille Occhi sulla Città”, che coinvolgono tutti gli “occhi” (pubblici e privati) che vigilano e presidiano il territorio o alle Associazione Temporanee di Scopo messe in campo in alcune Regioni per riqualificare le aree più degradate.

Il partenariato, favorendo un approccio “di sistema” ai problemi di sicurezza ove ciascun partecipante, sia esso pubblico o privato, mette a fattor comune esperienze e proposte specifiche o settoriali, può portare alla definizione di forme articolate di programmazione e cooperazione molto efficaci tra enti e soggetti privati.

Un modello che potrebbe essere preso in considerazione anche per ipotizzare forme virtuose di gestione condivisa delle innumerevoli vulnerabilità che sempre più intensamente minacciano la Web Society.

7. Un modello esistente

Un modello di interazione tra soggetti pubblici e privati per rispondere agli eventi latamente intesi come “destabilizzanti” per il sistema paese (catastrofi, atti terroristici, calamità naturali, crisi finanziarie ed incidenti industriali), in qualsiasi contesto sociale essi si verificano, è stato da poco messo a punto dalla Commissione UNI “Sicurezza della società e del cittadino” ed è confluito nella norma 11500:2013.

Questa norma pattizia, allo studio anche a livello internazionale ISO, pur standardizzando un modello di relazioni strutturate tra soggetti pubblici e privati coinvolti nei processi, favorisce anche l’armonizzazione delle tecnologie utilizzate sotto il profilo funzionale. Potrebbe quindi porsi anche come modello mutuabile per promuovere la cultura della sicurezza anche attraverso un uso virtuoso dell’esperienza tecnologica.

8. La sicurezza come valore fondante

Questa ed altre iniziative sono al centro dell’attività associativa di Assosicurezza, da sempre impegnata nella promozione della cultura della sicurezza in tutte le sue forme.

Assosicurezza promuove infatti un concetto attivo di cultura della sicurezza quale fattore abilitante il business, quale elemento di competitività aziendale, quale punto di partenza e di approdo di qualunque pensiero individuale e collettivo e quale valore fondante di dimensione costituzionale. Citando Tommaso F. Giupponi² (2008), del quale si condivide appieno la definizione, “(...) calata all’interno del tessuto costituzionale (e di un particolare tessuto costituzionale), la sicurezza dovrà quindi essere declinata non quale impalpabile a priori logico, del tutto indecifrabile agli oc-

² *La sicurezza e le sue “dimensioni” costituzionali* di Tommaso F. Giupponi (*Diritti umani. Teorie, analisi, applicazioni*, a cura di S. Vida, Bologna, 2008). Il Forum di Quaderni costituzionali (Coordinatore editoriale Roberto Bin; Responsabile redazione Tommaso Giupponi) è la sezione telematica di Quaderni Costituzionali (Direttore Augusto Barbera). Dal 2012 pubblica Forum di Quaderni costituzionali – Rassegna, rivista telematica mensile (ISSN 2281-2113). Testo disponibile al sito: www.forumcostituzionale.it/site/images/stories/pdf/documenti_forum/paper/0078_giupponi.pdf

chi della scienza giuridica; né come semplice oggetto di disciplina da parte dell'ordinamento generale, in quanto da esso richiamata o presupposta (in una prospettiva semplicemente formalistica e avalutativa); bensì come specifico valore costituzionale, sintesi di una pluralità di diversi interessi, nell'ambito di un ventaglio ben preciso di opzioni fondamentali codificate nella Carta fondamentale”.

Questa la sintesi della vocazione associativa di Assosicurezza, che si fonde ad un nuovo pensiero di sicurezza tecnologica che guarda alla società, in particolare a quella Web Society che sempre più pervasivamente fa parte della nostra vita, offrendo opportunità illimitate ma anche minacce sempre più liquide e insidiose.

È con questi presupposti e con queste aspettative che Assosicurezza formula i migliori auspici per questo primo numero della rivista Sicurezza e Scienze Sociali, dedicata alla Web Society e al Security Management.