



Il Futuro della Cyber Security in Italia

*Un libro bianco per raccontare le principali sfide che il
nostro Paese dovrà affrontare nei prossimi cinque anni*

Laboratorio Nazionale di Cyber Security
Consorzio Interuniversitario Nazionale per l'Informatica

Ottobre 2015

A cura di:

Roberto Baldoni, Università degli Studi di Roma "La Sapienza"
Rocco De Nicola, IMT, Institute for Advanced Studies, Lucca

Il volume è stato realizzato da:



con il supporto del
Dipartimento delle Informazioni per la Sicurezza
della Presidenza del Consiglio dei Ministri



NonCommercial-ShareAlike CC BY-NC-SA

This license lets others remix, tweak, and build upon the work non-commercially, as long as they credit the work and license their new creations under the identical terms.

ISBN 9788894137309

Titolo: Il Futuro della Cyber Security in Italia

Stampato in Italia, Ottobre 2015

A cura di: Roberto Baldoni e Rocco De Nicola

Autori in ordine alfabetico:

Luca Allodi	Giovanni Lagorio
Alessandro Armando	Antonio Lioy
Roberto Baldoni	Michele Loreti
Antonio Barili	Federico Maggi
Sandro Bologna	Marco Mayer
Matteo E. Bonfanti	Alberto Marchetti Spaccamela
Silvia Bonomi	Luigi Martino
Francesco Buccafurri	Fabio Massacci
Enrico Cambiaso	Massimo Mecella
Costantina Caruso	Luca Montanari
Michele Colajanni	Gian Domenico Mosco
Luigi Coppolino	Ida Panetta
Fabrizio d'Amore	Vincenzo Piuri
Salvatore D'Antonio	Paolo Prinetto
Sabrina De Capitani di Vimercati	Luigi Romano
Rocco De Nicola	Pierangela Samarati
Carolina De Stefano	Donatella Sciuto
Tommaso De Zan	Fabio Scotti
Federica Di Camillo	Stefano Silvestri
Giorgio Di Natale	Maurizio Talamo
Andrea Di Nicola	Alberto Trombetta
Andrea Dimitri	Fiamma Terenghi
Gianluca Dini	Aaron Visaggio
Riccardo Focardi	Stefano Zanero
Giuseppe F. Italiano	

Introduzione

Internet sta rivoluzionando la nostra società e la nostra economia, favorendo l'interazione, lo scambio di idee, la condivisione delle informazioni, e creando nuove modalità di coinvolgimento politico e sociale e di scambio economico e commerciale. *Spazio cibernetico (Cyberspace)* è il termine convenzionalmente usato per riferirsi all'ambiente all'interno del quale avvengono le operazioni che fanno uso di Internet. La riduzione dei costi di accesso alla rete e lo sviluppo della banda larga comporteranno un'ulteriore crescita del cyberspace, rendendolo un fattore sempre più cruciale per la crescita economica e sociale.

Tuttavia l'adozione del cyberspace porta con sé problemi di vulnerabilità delle applicazioni e dei sistemi informatici, dovute anche al fatto che la stragrande maggioranza delle reti e dei sistemi che formano il cyberspace sono stati progettati e realizzati pensando a criteri di usabilità e al più di resilienza, senza tenere in debito conto fin dall'inizio aspetti di sicurezza.

Queste vulnerabilità sono sempre più utilizzate da singoli e da gruppi a fini criminali per ottenere guadagni illeciti. A questo scopo vengono ad esempio sottratte, a imprese e organizzazioni, informazioni riservate, quali elenchi clienti, brevetti o asset strategici. La cronaca recente evidenzia che attacchi di questo tipo sono stati condotti in molti stati. Proprio per questa ragione, molti paesi stanno progettando e realizzando piani strategici nazionali che coinvolgono pubblico, privato e ricerca. Questi prevedono non solo la messa a punto di adeguate misure di contrasto ai crimini cibernetici, ma anche azioni di sensibilizzazione e di coordinamento. Lo scopo finale è arrivare, in breve tempo, all'innalzamento delle difese delle infrastrutture critiche nazionali, delle organizzazioni governative, delle aziende e dei singoli cittadini.

L'implementazione di un piano strategico è un processo molto complesso che richiede una relazione stretta tra pubblico, privato e mondo della ricerca. Se si considerano, a titolo di esempio, le infrastrutture critiche nazionali (reti elettriche, idriche, informatiche, ...), si vede che esse sono gestite da soggetti privati, pur essendo pubbliche, e necessitano delle competenze avanzate dei ricercatori per poter fronteggiare in modo adeguato minacce sempre più complesse e sofisticate.

Tutti i soggetti coinvolti devono essere consapevoli della minaccia e, per quanto di propria competenza, migliorare i propri livelli di protezione. Anche un soggetto apparentemente marginale all'interno di un'organizzazione e non dotato di adeguate protezioni di sicurezza, può essere utilizzato come base per portare attacchi al cuore dell'organizzazione stessa. A sua volta, un'organizzazione "compromessa" può mettere a repentaglio organizzazioni a essa collegate che, seppur dotate di difese evolute, condividono informazioni grazie alla reciproca fiducia di relazione commerciale.

In un sistema economico globale nel quale le informazioni hanno un valore essenziale, la sicurezza delle reti è diventata una delle sfide più serie per l'economia. Questa consapevolezza è emersa in tutta la sua drammaticità nel 2007, quando in Estonia una serie di attacchi cibernetici ha rischiato di abbattere l'intera infrastruttura informatica del Paese [73]. Come ha rilevato il presidente Obama nel 2009 [57], l'interdipendenza tra i sistemi informatici delle economie mondiali che utilizzano la stessa infrastruttura di base, gli stessi software, hardware e standard, con miliardi di dispositivi connessi, è alla base del carattere di universalità del *cyber crime* e lo rendono un fenomeno del quale è impossibile prevedere con esattezza le conseguenze nel medio-lungo termine. La vera differenza tra il *cyber crime* e la criminalità tradizionale non risiede tanto nella tipologia di aggressioni che li caratterizza, quanto nella circostanza che le violazioni perpetrate tramite il *cyber space* sono di fatto prive di confini fisici e di limiti geografici; spesso il crimine informatico è dunque più conveniente, anche per via della mancanza della sua percezione fisica da parte della vittima.

Non può quindi stupire il progressivo incremento, quantitativo e qualitativo, di attacchi e minacce criminali con le finalità più disparate, in quella "terra di mezzo" che è oramai diventato il cyberspace: dalle frodi e dalle estorsioni informatiche ai furti di identità e di dati sensibili, fino ad arrivare allo spionaggio e al sabotaggio, compresi gli atti vandalici meramente emulativi. Attacchi che possono anche non essere mirati a colpire un soggetto preciso, selezionato in base a determinate caratteristiche, ma a danneggiare in modo casuale un numero indefinito di soggetti sensibili alla minaccia predisposta dal criminale. Non bastano singole misure protettive. Occorre mettere in atto vere e proprie strategie difensive in mancanza delle quali, secondo il Report Global risks 2014 del World Economic Forum [29], nel 2020 le perdite economiche causate da attacchi cyber potrebbero arrivare fino a tremila miliardi di dollari.

Sotto il profilo delle vittime potenziali, un rilievo particolare hanno le istituzioni pubbliche di ogni dimensione e le imprese multinazionali, già più volte oggetto di crimini informatici dai quali sono derivati danni ingenti. Tuttavia, anche le imprese di piccole e medie dimensioni, che costituiscono il fulcro del tessuto economico italiano, sono un potenziale bersaglio di attacchi informatici, sia casuali sia mirati. Le imprese di piccole e medie dimensioni appaiono anzi le più vulnerabili e per loro le conseguenze negative sono in proporzione ancora maggiori, a causa delle ridotte risorse organizzative ed economiche delle quali dispongono. Il dato dimensionale accentua l'asimmetria informativa della vittima rispetto all'attaccante, in quanto l'impresa di dimensioni minori deve sopportare costi più rilevanti per dotarsi di un sistema di protezione e ha maggiori difficoltà a reagire ai danni, economici e reputazionali, causati da una violazione informatica. È quindi indispensabile che gli interventi di *regulation* volti a tutelare le vittime degli attacchi informatici tengano conto delle diverse caratteristiche dei destinatari. Altrettanto importante è che le imprese minori siano concretamente incoraggiate a incrementare la cultura della sicurezza, che stentano ancora a fare propria. La *cyber security* costituisce, del resto, una componente essenziale del "valore" che l'impresa è istituzionalmente chiamata a generare per i propri *stakeholders*, nei confronti dei quali l'impresa ha precisi obblighi di protezione.

L'assenza di una politica digitale in un Paese può produrre danni gravissimi nel breve e nel medio periodo, esponendolo al rischio di perdere rilevante opportunità di crescita, quali posti di lavoro qualificati in tutti i settori industriali e nei servizi, ricerca universitaria e privata, produzione di know how, imprese innovative e startup [23]. La sicurezza informatica non va dunque considerata un costo superfluo, o peggio un freno all'attività, ma, al contrario, una precondizione indispensabile per il suo esercizio, che per le imprese si traduce in un vantaggio in termini di competitività. Il diffondersi di una cultura della sicurezza informatica è un fattore decisivo per il Paese, in chiave non solo difensiva ma soprattutto di crescita economica.