Cyber Security – Ecco la strategia italiana

Mercoledì 05 Marzo 2014 11:29 Demetrio Zavettieri Local - Attualità

Meno di un mese fa, precisamente il 20 febbraio, sono stati resi pubblici i testi completi del Quadro Strategico Nazionale per la sicurezza dello spazio cibernetico (QSN) e del Piano Nazionale per la protezione cibernetica e la sicurezza informatica (PN), che insieme costituiscono il primo quadro organico nazionale sulla sicurezza informatica, a coordinamento centrale, in linea con quanto avviene nel resto d'Europa. Questi documenti costituiscono un primo step di un processo che vedrà coinvolte istituzioni e società civile.

UNA CYBER STRATEGY ITALIANA - L'Italia si è dotata recentemente di una linea comune di cyber security, fissando gli obiettivi strategici e operativi da perseguire. Lo scorso dicembre, infatti, sono stati approvati dal Comitato Interministeriale per la Sicurezza della Repubblica (CISR) e adottati dal Presidente del Consiglio dei Ministri, i testi relativi al Quadro Strategico Nazionale (QSN) e del Piano Nazionale (PN). La normativa di base su cui poggia fa riferimento al DPCM 24 gennaio, Direttiva recante "indirizzi per la protezione ciberbetica e la sicurezza informatica nazionale.

Nell'ambito del Quadro Strategico Nazionale, vengono identificati sei indirizzi strategici:

1)Miglioramento, secondo un approccio integrato, delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati;

2)Potenziamento delle capacità di difesa delle Infrastrutture Critiche nazionali e degli attori di rilevanza strategica per il sistema-Paese;

3)Incentivazione per la cooperazione tra istituzioni e imprese nazionali;

4)Promozione e diffusione della cultura della sicurezza cibernetica;

5)Rafforzamento delle capacità di contrasto alla diffusione di attività e contenuti illegali online;

6)Rafforzamento della cooperazione internazionale, per facilitare una l'emergere di una governance a livello.

Il Piano Nazionale definisce così il percorso operativo e le linee d'azione per l'attuazione dei sei indirizzi strategici di cui sopra:

1)Potenziamento capacità d'intelligence, di polizia e di difesa civile e militare;

2)Potenziamento dell'organizzazione e delle modalità di coordinamento e di interazione a livello nazionale tra soggetti pubblici e privati;

3)Promozione e diffusione della cultura della sicurezza informatica. Formazione e addestramento;

4)Cooperazione internazionale e esercitazioni;

5)Operatività del CERT (Computer Emergency Response Teams) nazionale, del CERT-PA e dei CERT dicasteriali;

6)Interventi legislativi e compliance con obblighi internazionali;

7)Compliance a standard e protocolli di sicurezza;

8)Supporto allo sviluppo industriale e tecnologico;

9)Comunicazione strategica;

10)Risorse;

11)Implementazione di un sistema di Information Risk Management nazionale.

Elaborato dal Tavolo Tecnico Cyber (TTC) – che opera presso il DIS (Dipartimento Informazioni e Sicurezza) e al quale partecipano i rappresentanti cyber del CISR (Affari esteri, Interno, Difesa, Giustizia, Economia e Finanze, Sviluppo economico), dell'Agenzia per l'Italia Digitale e del Nucleo per la Sicurezza Cibernetica – il QSN è la risposta italiana alle minacce presenti nello spazio cibernetico, divenuto sempre più di importanza strategica per lo sviluppo economico, sociale e culturale delle nazioni. Con il Piano Nazionale l'Italia si dota di una strategia organica, "alla cui attuazione sono chiamati a concorrere non solo gli attori, pubblici e privati, richiamati nel Quadro Strategico Nazionale ma anche tutti coloro che, su base quotidiana, fanno uso delle moderne tecnologie informatiche, a partire dal singolo cittadino".

LE MINACCE CIBERNETICHE - Il Capitolo 1 del QSN fornisce una panoramica delle principali minacce – dalla criminalità informatica allo sfruttamento delle tecnologie ICT per fini terroristici, dall'hacktivismo allo spionaggio cibernetico, dal sabotaggio per via informatica ai conflitti nella 5a dimensione – e delle vulnerabilità sfruttate per la conduzione di attacchi nello spazio cibernetico, sia di tipo tecnico che di tipo organizzativo e di processo. In particolare, il concetto di minaccia cibernetica viene suddiviso in quattro macro-categorie, a seconda degli attori e delle finalità: cyber crime, cyber espionage, cyber terrorism, cyber warfare. Vediamole nel dettaglio:

- criminalità cibernetica (cyber crime): attività criminali quali, per esempio, la truffa o la frode telematica, il furto d'identità, la sottrazione indebita di informazioni o di creazioni e proprietà intellettuali;
- spionaggio cibernetico (cyber espionage): acquisizione di dati e informazioni sensibili, proprietarie o classificate;
- terrorismo cibernetico (cyber terrorism): azioni ideologicamente motivate, volte a condizionare uno stato o un'organizzazione internazionale;
- guerra cibernetica (cyber warfare): attività e operazioni militari pianificate e condotte allo scopo di conseguire effetti sul piano militare.

L'asimmetria della minaccia e la pervasività dello spazio cibernetico nella vita di ogni giorno, rendono necessaria l'adozione di un approccio olistico e unitario, per assicurare un accettabile livello di sicurezza online. Pensiamo banalmente ai danni che potrebbe causare un'azione di cyber spionaggio ai danni di imprese italiane ad alto contenuto tecnologico e innovativo. "La sofisticazione degli attacchi informatici – si legge nel documento – e la connessione in rete delle nostre infrastrutture crescono in un modo tale che la stessa stabilità e sicurezza del Paese possono essere gravemente pregiudicate ed è dunque indispensabile assicurare la

ReFusiOrari

Senza fine. Non è Gino Paoli. E' il Drago di Arcore

FusiOrari TV

Il Sondaggio

Quale, tra questi, è il film più bello di Stanley Kubrick?

- Shining
- 2001 Odissea nello spazio
- Eyes wide shut
- Full Metal Jacket
- Arancia Meccanica
- Barry Lyndon

Vota Risultati

La Vignetta

La Borsa

Il Sole 24 ORE - Finanza e Mercati - Azioni

Il Sole 24 ORE - Finanza e Mercati - Azioni

- Crisi Ucraina: Borsa Mosca e Rublo in pesante ribasso su escalation
- Riassetto Saras, avances dei russi di Rosneft per conquistare il controllo
- Carige, banca e fondazione allo scontro
- Google guida la carica dell'hi-tech a Wall Steet e scavalca i big industriali
- Borsa, Milano migliore in Europa. Wall Street chiude positiva

migliore protezione agli assetti critici nazionale da attacchi che possono produrre gravi danni fisici e materiali, ad esempio attraverso la paralisi o l'alterazione di interi sistemi di comando e controllo militari. Ciò implica dunque la necessità di un concetto di difesa innovativo e compartecipato con il mondo privato, che in molti casi è al contempo proprietario e gestore degli assetti critici da tutelare".
Secondo una ricerca condotta Gartner, i privati e pubbliche amministrazioni mondiali hanno speso 60 miliardi di dollari nel 2012, per difendersi dagli attacchi informatici, contro i 55 del 2011 e gli 86 previsti nel 2015. Assinform stima che il 40% degli attacchi richiedono almeno quattro giorni per essere risolti. Nel 90% dei casi l'attacco ha successo a causa dell'errata configurazione del sistema di sicurezza e per la mancanza di competenze specifiche (fonte: Sole24ore).
Adesso che il primo passo verso la dotazione di una cyber strategy comune è stato fatto, spetterà ai vari soggetti coinvolti dare attuazione alle linee strategico-operative e sarà fondamentale sensibilizzare tutti gli stakeholders, compresi i cittadini, informando e formando tutti sugli aspetti della sicurezza cibernetica.

Per approfondire: http://www.fusiorari.org/world/attualita/1170-cyber-security--professione-hacker-il-lato-oscuro-della-rete.html

Ultimo aggiornamento Mercoledì 05 Marzo 2014 11:39

Aggiungi commento

Nome (richiesto)

E-Mail

Notificami i commenti successivi

Aggiorna

Invia

JComments

Login

Nome utente

Password

Ricordami

Login

- Password dimenticata?
- Nome utente dimenticato?

PhotoGallery

Sorry, but Javascript is not enabled in your browser!

Editoriali

L'Italia al palo Crisi tra ripresa invisibile e false promesse

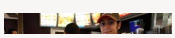
Martedì 19 Novembre 2013

La ripresa annunciata dal ministro del Tesoro, Fabrizio Saccomanni, non l'abbiamo vista. I problemi sono ancora tutti lì, fermi e presenti. Gli acquisti non ripartono, gli investimenti sono al palo. La crisi c'è. E, soprattutto, pesa. Dal 2008 oltre 11 mila aziende sono fallite e gli investimenti sono diminuiti del 26,2%. I prestiti alle imprese sono calati di 100 miliardi e il costo del denaro è sempre più alto.

Leggi tutto...

In risposta ai McLavori, una resistenza gentile

Sabato 28 Settembre 2013



Li chiamano McJob, sono i

Il Meteo