COSA DICE IL DOCUMENTO DI SICUREZZA NAZIONALE

Ogni anno[1] il Governo presenta al Parlamento la *Relazione sulla politica dell'informazione per la sicurezza*[2] di cui è parte integrante il *Documento di sicurezza nazionale*[3]. Nei due anni precedenti questo documento si limitava a descrivere l'architettura nazionale cyber, **la novità di quest'anno è la comparsa di una sezione dedicata alla trattazione specifica della minaccia cibernetica** con un contributo informativo ad ampio spettro.

DOMINIO CYBERSPAZIO

La sicurezza della nazione non si articola solo nei domini terra, mare e cielo ma sempre più nel cyberspazio ed esso va protetto per salvaguardare la nostra democrazia ed economia. L'evoluzione cyber è stata molto rapida anche all'interno del comparto intelligence e questo dato si evince anche solo osservando i cambiamenti all'interno del vocabolario della Relazione per il Parlamento, che quest'anno incorpora (per la prima volta) anche un breve glossario di termini propri del cyberspazio.

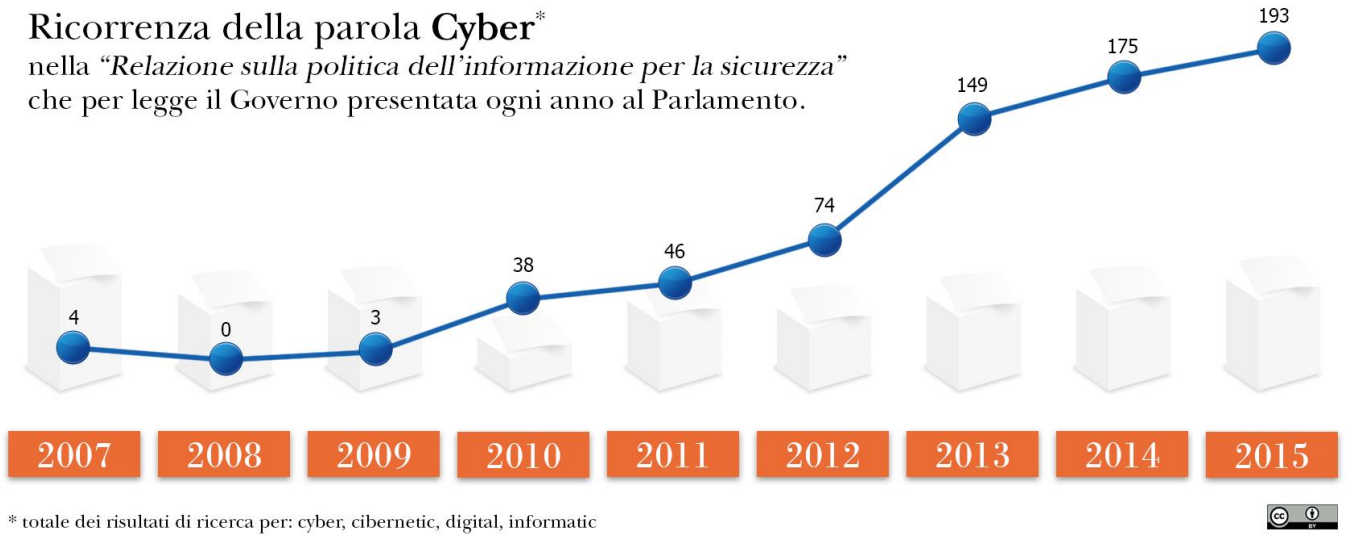

Figura 1 - Utilizzo parola Cyber nella Relazione per il Parlamento

[1] Ai sensi dell'art. 38 della Legge n. 124 del 2007 viene trasmessa, entro il mese di Febbraio, una relazione scritta riferita all'anno precedente.

[2] La Relazione: http://www.sicurezzanazionale.gov.it/sisr.nsf/archivio-notizie/presentata-al-parlamento-la-relazione-2015.html

[3] Ai sensi dell'art. 9 della Legge 133 del 2012 alla relazione è allegato il documento di sicurezza nazionale, concernente le attività relative alla protezione delle infrastrutture critiche materiali e immateriali nonché alla protezione cibernetica e alla sicurezza informatica.

COMPRENDERE I CAMBIAMENTI

Il livello di analisi della Relazione è sempre più nitido[4] ed una lettura attenta permette di cogliere importanti elementi che riguardano il profilo della minaccia. E' inoltre evidente l'impegno del Comparto verso **un'attività informativa rivolta al medio-lungo termine** e non solo alla gestione della quotidianità, nel Documento si legge "*lo sforzo dell'intelligence per incrementare, in un modello "a tendere", le proprie capacità operative e per essere all'altezza del compito: un'intelligence visionaria, che sappia cogliere dalla contingenza segnali e tendenze per il futuro*".

POTENZIAMENTO CAPACITÀ NAZIONALI

Per quanto riguarda l'architettura cyber italiana, il governo ha operato attraverso il Tavolo Tecnico Cyber per l'attività di raccordo tra istituzioni ed il Tavolo Tecnico Imprese per lo sviluppo del partenariato tra pubblico e privato. L'agenda del primo Tavolo ha riguardato principalmente la verifica di attuazione del Piano Nazionale (per il biennio 2014-2015) e la realizzazione di una connettività nazionale per la *Rete Gestione Crisi Cyber* (con il Ministero della Difesa anche per lo scambio di informazioni classificate). Si apprende inoltre che si è provveduto **ad ampliare il novero dei soggetti che, in aggiunta a quelli critici e strategici, sono i naturali destinatari di mirate attività di sensibilizzazione**, in quanto potenzialmente esposti al rischio di attacchi informatici.

PARTENARIATO CON LE AZIENDE

Nel Documento si evidenza che il Tavolo con le imprese ha fatto perno sul processo di condivisione delle informazioni che da un lato alimenta il patrimonio informativo dell'intelligence e dall'altro arricchisce la base di conoscenza dell'azienda. Seguendo la stessa logica di partenariato, il 26 Novembre è stato presentato il nuovo Polo Tecnologico quale incubatore di idee e soluzioni, nel cui ambito opera un **Laboratorio Malware** primo esperimento di livello nazionale tra Intelligence (per l'individuazione delle esigenze operative), Accademia (per la capacità di ricerca avanzata) ed Industria (per la sperimentazione e la produzione di nuovi modelli tecnologici di difesa) mirante a sviluppare una capacità in materia di malware reverse engineering, allo scopo di individuare metodologie di rilevazione, analisi e rimozione di codici malevoli.

[4] Come evidenziato anche in questo studio http://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/levoluzione-della-sicurezza-nazionale-italiana.html che approfondisce l'argomento.

FRAMEWORK NAZIONALE DI CYBER-SECURITY

Nel Documento viene dato ampio risalto all'opera dell'Accademia italiana che, su mandato del governo, ha predisposto (ad opera di CIS Sapienza e Consorzio Interuniversitario Nazionale per l'Informatica) uno strumento[5] specifico con un duplice obiettivo: da una lato consentire agli operatori pubblici e privati di **valutare le proprie capacità cibernetiche** e dall'altro superare la dimensione puramente tecnica e portarla sino al livello di rischio aziendale per consentirne la trattazione nei Consigli di amministrazione delle aziende e nei Comitati direttivi degli organismi pubblici. Nel Documento si legge che "*Una progressiva adozione del Framework da parte del tessuto imprenditoriale nazionale permetterà di aumentare la consapevolezza del rischio*".

STATO DELLA MINACCIA

Nel 2015 lo **spazio cibernetico si è dimostrato sempre più un'arena virtuale** che trascende la dimensione statuale ed amplifica il divario tra superficie di attacco e capacità di difesa. L'aumento di possibilità di accesso alla vita sociale accresce inevitabilmente anche la quantità di strumenti a disposizione degli attori ostili. Il Documento mette in evidenza in particolare alcune minacce rilevate nel corso dell'anno appena trascorso: il cyber-spionaggio, l'utilizzo dei social media da parte dei gruppi terroristici, la criminalità informatica.

SPIONAGGIO DIGITALE

E' stato rilevato un sempre maggiore ricorso agli strumenti di spionaggio cibernetico finalizzati ad **accrescere la capacità conoscitiva di aziende bersaglio**. In particolare, questa metodologia di intrusione appare concepita per svolgere attività di analisi occulta di aziende nazionali per le quali viene ipotizzata un'attività di acquisizione. Questa ingerenza consente ai potenziali acquirenti stranieri di conseguire un vantaggio informativo su cui far leva nel corso delle successive negoziazioni. Nel Documento si legge "*Il trend registrato è stato quello di un incremento qualitativo e quantitativo delle azioni contro alcune Istituzioni e l'industria ad alto contenuto tecnologico ed innovativo, con l'obiettivo di esfiltrare informazioni sensibili e know-how pregiato*". Queste attività sono svolte non più solo da

[5] Un articolo di approfondimento sul Framework nazionale http://formiche.net/2016/02/08/cyber-security-framework-nazionale-sapienza-cis-cini/ presentato ufficialmente il 4 Febbraio.

attori statuale ma da gruppi di cyber-criminali[6] che si propongono sul mercato con servizi di spionaggio al soldo del miglior offerente.

I BERSAGLI E GLI ATTACCHI

I Documento presenta inoltre una serie di dati statistici frutto di attività di analisi di AISE ed AISI ed altri attori che compongono l'architettura nazionale. Sul fronte dei bersagli gli **obiettivi privilegiati per attacchi di spionaggio digitale sono le piccole e medie imprese** (34%), le aziende operanti nei settori della difesa (18%), delle telecomunicazioni (15%), dell'aerospazio (12%), dei trasporti (9%), dell'energia (3%) e bancario (3%). Le tipologie di attacco sono basate principalmente su malware (53%) che includono strumenti di spionaggio, sistemi per le estorsioni di denaro ed altre attività illecite di natura predatoria; seguono poi gli attacchi SQL-injection (20%) che raggruppano tutta una serie di tecniche volte a saccheggiare database con informazioni rivendibili sul mercato nero; risultano in crescita i defacement (14%) ovvero quelle tecniche attraverso le quali l'attaccante modifica i contenuti di un sito; infine risultano in calo gli attacchi DDos (5%) il cui scopo è rendere temporaneamente inaccessibile una risorsa presente sulla rete.

CYBER-PROPAGANDA E JIHAD

Nel corso del 2015 i gruppi terroristici hanno continuato ad impiegare i social media come cassa di risonanza per la diffusione ed amplificazione dei loro messaggi di propaganda. In particolare si evidenzia la capacità da parte di questi gruppi di utilizzare tecniche di manipolazione della comunicazione per dirottare discussioni ad elevata visibilità verso temi correlati a tematiche vicine all'Islam. Nel Documento si legge che "*sulla base del costante monitoraggio effettuato dall'intelligence, le capacità dei gruppi terroristici di porre in essere attacchi cyber non hanno raggiunto il livello analogo a quello di un'azione terroristica convenzionale*". Non si ha evidenza di azioni terroristiche finalizzate a distruggere o sabotare infrastrutture ICT di rilevanza strategica, ma è ragionevole ipotizzare che, nel futuro, tali obiettivi possano effettivamente rientrare negli indirizzi strategici del cyber-jihad[7]. A tale proposito è da notare **l'attività di ricerca e reclutamento on-line di hacker mercenari** e la crescente casistica di attacchi informatici (sinora a basso impatto)

[6] Un articolo sul profitto attraverso il crimine informatico http://formiche.net/2015/06/22/business-cybercrime/

[7] Un articolo sull'uso degli strumenti informatici da parte dei terroristi jihadisti http://formiche.net/2015/11/21/isis-help-desk-jihad-terrorismo/

realizzati ai danni di sistemi informativi di soggetti pubblici e privati occidentali (colpiti in ragione del loro alto livello di vulnerabilità).

CRIMINALITÀ INFORMATICA

Sul piano criminale si rilevano acquisizioni fraudolente di credenziali bancarie, dati di pagamento e di identità utili a ottenere un rapido beneficio di natura economica. Particolarmente attivi risultano i gruppi di origine nigeriana che hanno ottenuto un elevato grado di specializzazione in attività illecite condotte prevalentemente in modalità phishing. In tema di estorsioni telematiche ha continuato a registrarsi la diffusione dei ransomware, virus informatici che prendono in ostaggio i file del computer attraverso sofisticate tecniche di crittografia ed impongono il pagamento di una somma di danaro sotto forma di moneta elettronica Bitcoin, anonima e non tracciabile. Nel Documento si legge inoltre che "*la minaccia di tipo avanzato e persistente denominata "Carbanak", che consente il controllo da remoto di talune applicazioni per l'attivazione di sportelli bancomat,* ***ha interessato i sistemi informatici anche di alcuni istituti bancari nazionali***".

BITCOIN

La Relazione per il Parlamento dedica ampio spazio alla cripto-valuta Bitcoin[8] sia dal punto di vista tecnologico[9] sia in considerazione dei rischi di impiego di tali strumenti per finalità illecite. Bitcoin si basa su un software open-source (disponibile on-line dal 2009) che permette **transazioni economiche prive di qualunque attività di intermediazione** e può essere utilizzata come mezzo di scambio, nonché trasferita, archiviata e negoziata elettronicamente. Può essere acquistata con moneta tradizionale, viene movimentata attraverso un conto personalizzato che permette ai titolari di effettuare transazioni con altri utenti (anche presso esercizi commerciali e/o persone fisiche che l'accettano) ed è **convertibile in moneta legale**. L'assenza intrinseca di vigilanza, espone questo strumento a possibili utilizzi strumentali per transazioni finanziarie collegate ad attività illecite, rappresentando così un vulnus per il sistema finanziario.

[8] Panoramica su Bitcoin http://www.formiche.net/files/2015/06/Panoramica-su-Bitcoin-20150429.pdf accessibile anche a i meno esperti.

[9] Blockchain è una tecnologia che consente di scambiare dati e informazioni, a prescindere dalla conoscenza delle controparti e dall'esistenza di un garante del sistema.

FATTORE UMANO

Il Documento riporta alcune considerazioni sull'evoluzione della minaccia cibernetica. In un'ottica di breve-medio periodo si rileva che la minaccia continuerà a risentire in modo particolare delle **vulnerabilità riconducibili al fattore umano**. L'uomo può essere una pericolosa minaccia attiva, a causa dell'azione volontaria che può esercitare un insider (quando c'è un interesse a sottrarre informazioni sensibili) che dall'interno elude facilmente le difese poste sul perimetro esterno; ma è anche una temibile vulnerabilità quando è il bersaglio delle attività di social engineering che ne profilano il comportamento per successivi attacchi.

TREND EVOLUTIVI

Per il futuro[10] il Documento prevede **un forte aumento della minaccia cibernetica** perché sono molteplici i fattori che concorrono ad aumentare la superficie di attacco mentre la capacità di difesa non è altrettanto rapida nel garantire una protezione efficace. Il Documento indica anche alcuni dei fattori che in Italia parteciperanno ad **estendere esponenzialmente la superficie di attacco**: l'aumento delle transazioni economiche tramite dispositivi mobile, le politiche di riduzione del digital divide, la crescente diffusione di oggetti di ogni genere collegati alla Rete, il potenziamento delle digitalizzazione di documenti e processi da parte della Pubblica Amministrazione e Privati.

FABIO DE PAOLIS

Fabio De Paolis è esperto in sicurezza informatica con oltre 20 anni di attività nel settore. E' laureato in Sicurezza dei Sistemi e delle Reti Informatiche presso l'Università di Milano; è CERTIFIED ETHICAL HACKER presso EC COUNCIL di Londra; è CHIEF INFORMATION SECURITY OFFICER in un'azienda italiana che offre servizi di ingegneria del software e sicurezza informatica; è consulente di enti ed organizzazioni private per individuare ed esaminare minacce informatiche; si interessa di cyber-security e cyber-warfare con particolare attenzione al mondo dell'intelligence; è attivo sulla Rete da quando la posta elettronica si scambiava solo fra BBS tramite modem analogico.

[10] Previsioni per il 2016 delle principali aziende che operano in materia di sicurezza informatica http://formiche.net/2016/01/09/cyber-minacce-informatica-2016/