ItaliaOggi Sette

26-GIU-2017
pagina 16
foglio 1 / 3

Le indicazioni del Piano nazionale per la sicurezza informatica. Risorse per 150 mln

Cybercrime, l'unione fa la forza

Soggetti pubblici e privati insieme contro le violazioni

Pagina a cura
DI ANTONIO CICCIA MESSINA

Partenariato pubblico-privato contro il cybercrime; più cooperazione tra istituzioni e imprese, contrasto rafforzato contro i contenuti illegali online. Sono alcune delle direttrici del nuovo Piano nazionale per la protezione cibernetica e la sicurezza informatica, pubblicato sulla *Gazzetta Ufficiale* n. 125 del 31/5/2017. Con il Piano si stabilisce la roadmap per l'adozione da parte dei soggetti pubblici e privati in attuazione del dpcm 17/2/2017.

Questo decreto ha individuato un Nucleo per la sicurezza cibernetica, protagonista nella gestione di eventuali crisi, nel corso delle quali deve assicurare che le attività di reazione e stabilizzazione di competenza delle diverse amministrazioni ed enti vengano espletate in maniera coordinata. Nel dpcm sono chiamati a fare la loro parte gli operatori privati e cioè quelli che forniscono reti pubbliche di comunicazione o servizi di comunicazione elettronica accessibili al pubblico, gli operatori di servizi essenziali e i fornitori di servizi digitali, quelli che gestiscono infrastrutture critiche di rilievo nazionale ed europeo. Hanno funzione di sentinelle perpetue: devono comunicare ogni significativa violazione della sicurezza o dell'integrità dei propri sistemi informatici, utilizzando canali di trasmissione protetti; devono adottare best practices e misure finalizzate all'obiettivo della sicurezza cibernetica; devono fornire informazioni agli organismi di informazione per la sicurezza e consentire l'accesso ai Security operations center aziendali e ad altri eventuali archivi informatici di specifico interesse ai fini della sicurezza cibernetica; in generale devono collaborare alla gestione delle crisi cibernetiche contribuendo al ripristino della funzionalità dei sistemi e delle reti da essi gestiti.

Il Piano 2017 scrive la strategia contro gli attacchi informatici. I punti salienti sono: il potenziamento delle capacità di difesa delle infrastrutture critiche nazionali e degli attori di rilevanza strategica; il miglioramento delle capacità tecnologiche, operative e di analisi degli attori istituzionali interessati; l'incentivazione della cooperazione tra istituzioni e imprese nazionali; la promozione e diffusione della cultura della sicurezza cibernetica; il rafforzamento della cooperazione internazionale in materia di sicurezza cibernetica; il rafforzamento delle capacità di contrasto alle attività e contenuti illegali online.

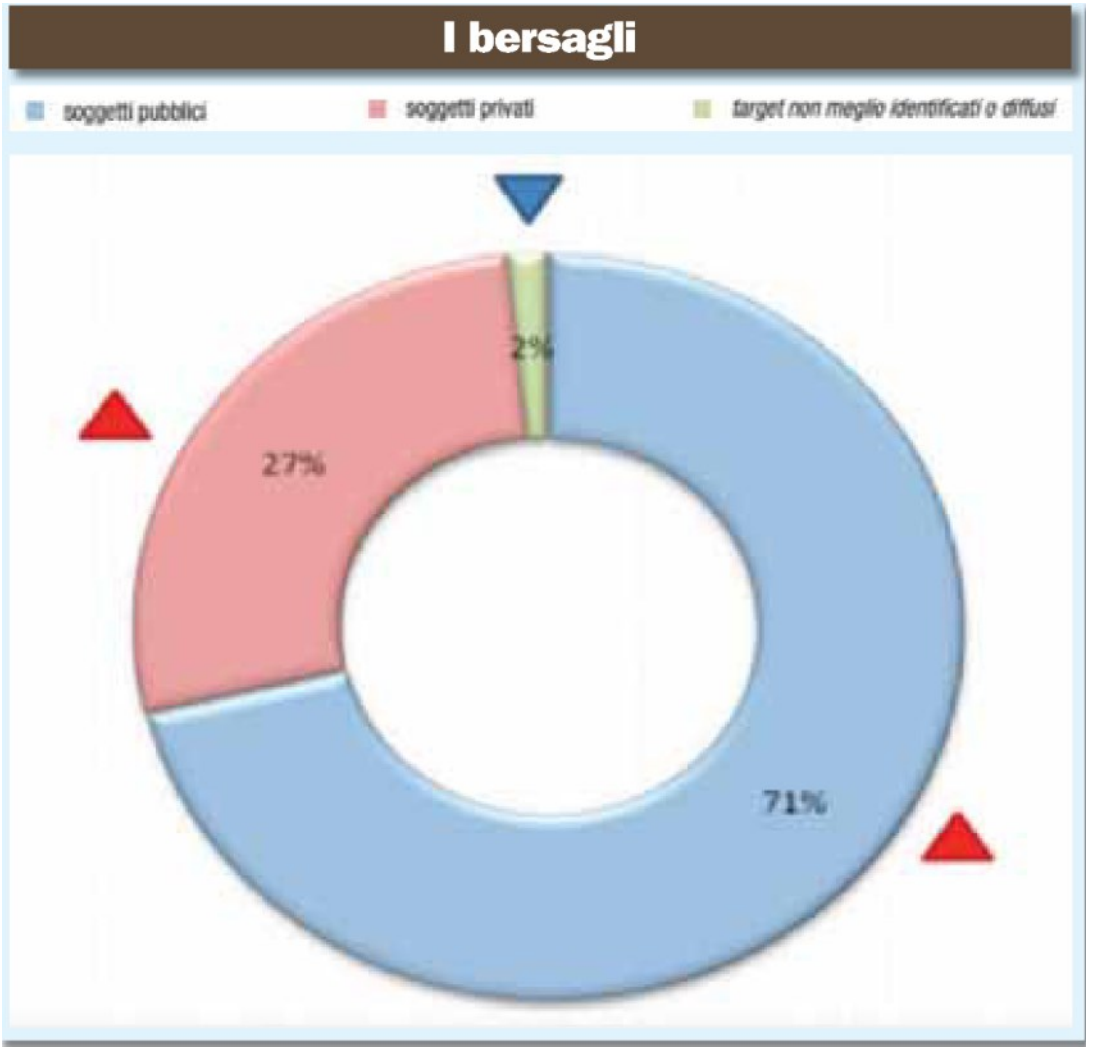
Il documento punta le sue carte sul potenziamento delle strutture nazionali di incident prevention, response e remediation, e il potenziamento delle capacità di intelligence, di polizia e di difesa civile e militare. Inoltre nel Piano nazionale è previsto uno specifico piano d'azione dedicato a un nucleo essenziale di iniziative, cui attribuire carattere di priorità ed urgenza. Le iniziative si propongono di aumentare il coordinamento e l'interazione tra soggetti pubblici, privati e mondo della ricerca sia a accorciare e razionalizzare, rispetto al passato, la «catena di comando» deputata alla gestione delle crisi.

Peraltro a sostegno di tutto ciò ci sono anche le risorse economiche (il totale è di 150 mln) destinate a iniziative per rafforzare la prevenzione nel campo della sicurezza informatica e cibernetica nazionale, e in particolare all'assunzione di risorse professionali e alla realizzazione di progetti Ict.

ItaliaOggi Sette

Diritti d'autore online, responsabilità a monte

Scacco al cybercrime che colpisce il copyright. È responsabile per violazione del diritto d'autore il gestore della piattaforma internet di condivisione di opere protette. È quanto deciso dalla seconda sezione della Corte di giustizia dell'Ue, con la sentenza del 14/6/2017 (causa C-610/15), che può segnare una svolta contro il caricamento di contenuto illegali online. Questo perché si anticipa la tutela e si mette sul banco degli accusati non chi carica i file, ma chi mette a disposizione la struttura su cui altri caricano dati illeciti. Secondo la Corte di giustizia, in base alla direttiva 2001/29/CE sull'armonizzazione del diritto d'autore e dei diritti connessi rappresenta una comunicazione al pubblico l'adibizione di una piattaforma di condivisione online per la condivisione di file protetti, senza l'autorizzazione del titolare. La direttiva 2001/29/Ce prevede che agli autori è riconosciuto il diritto esclusivo di autorizzare o vietare qualsiasi comunicazione al pubblico, su filo o senza filo, delle loro opere, compresa la messa a disposizione del pubblico delle loro opere in maniera tale che ciascuno possa avervi accesso dal luogo e nel momento scelti individualmente. I giudici europei hanno chiarito che la nozione di «comunicazione al pubblico» comprende la messa a disposizione e la gestione, su Internet, di una piattaforma di condivisione che, mediante l'indicizzazione di metadati relativi a opere protette e la fornitura di un motore di ricerca, consente agli utenti di tale piattaforma di localizzare tali opere e di condividerle nell'ambito di una rete tra utenti (peer-to-peer).



Nel mirino degli attacchi banche e sanità

Banche e sanità sotto attacco cyber. Nel settore pubblico nel mirino c'è il governo centrale, ma crescono gli attentati agli enti locali. Gli ultimi dati ufficiali sul cybercrime (relazione annuale del governo sulla politica dell'informazione per la sicurezza) fotografano il 2016: ai primi posti le statistiche trovano il settore bancario con il 17% delle minacce a soggetti privati (+14% rispetto al 2015), le Agenzie di stampa e le testate giornalistiche che, insieme alle associazioni industriali, si attestano sull'11%. Il settore farmaceutico, con il 5%, si posiziona a pari merito di difesa, aerospazio e energia.

Nel settore pubblico l'87% degli attacchi cyber riguarda la pubblica amministrazione centrale (comprese attività ostili verso movimenti politici). Nel 2016 si è verificata una inversione di tendenza, poiché gli attacchi contro le Pubbliche amministrazioni centrali (Pac) risultano, infatti, in lieve diminuzione (-2%) mentre quelli avverso le Pubbliche amministrazioni locali (Pal) sono in aumento (+5%).

Secondo il governo i settori a rischio continueranno a essere quelli ad alto contenuto tecnologico e di know how, con livelli di time to market contenuti, quali il segmento farmaceutico e del software, e altri obiettivi sensibili al danno reputazionale con conseguenti significativi impatti economici e di mercato. La relazione del 2016 del governo indica i settori bancario e sanitario come bersagli privilegiati del cybercrime, anche per il valore intrinseco dei dati finanziari e personali posseduti, sfruttabili, attraverso il furto di identità, nell'ambito di attività di frode, e, nel caso dell'area finanziaria, per le potenziali ingenti sottrazioni di valuta perseguibili tanto a livello massivo (frodi connesse alle carte di credito/debito), quanto a livello dei circuiti interbancari, nonché attraverso la potenziale manipolazione degli algoritmi di trading combinata con attività di speculazione sui mercati.

Il settore sanitario sta diventando molto appetibile alla malavita cibernetica perché sempre di più ricorre al supporto Ict sia nel management dei processi organizzativi (cartelle cliniche, dati sanitari) sia nella gestione dei presìdi biomedicali (controllo remoto dei pacemaker, robotica sanitaria, sistemi automatici di monitoring di parametri critici).

L'evoluzione tecnologica caratterizzata dal progressivo aumento delle possibilità di gestione e controllo in remoto delle attività produttive mette il settore manifatturiero al rischio di crescenti compromissioni cyber.