Nuova edizione
Settembre 2014

Rapporto

2014

sulla sicurezza ICT
in Italia

Indice

Prefazione di Gigi Tagliapietra 3

Introduzione al rapporto 5

Panoramica degli eventi di cyber-crime e incidenti informatici più significativi del 2013 e del primo semestre 2014 7

- Analisi dei principali attacchi noti a livello internazionale 11
- Analisi della situazione italiana in materia di cyber-crime e incidenti informatici . . 27
- Analisi FASTWEB 36
- BIBLIOGRAFIA 54

Mercato italiano della sicurezza ICT e Mercato del lavoro 57

FOCUS ON 73

- Smartphone, Tablet e Social Networks in Azienda 74
- La strategia europea per la cybersecurity 79
- Lo stato della digital forensics in Italia: accademia, Forze dell'Ordine, magistratura e avvocatura, esperti e aziende 86
- I controlli interni sui processi ICT in ambito aziendale 90
- Security By Design 94
- La Security vista dal Management 100
- Formazione e consapevolezza, strumenti indispensabili per la Sicurezza delle Informazioni 105

Gli autori del Rapporto Clusit 2014 113

Ringraziamenti 121

Descrizione CLUSIT e Security Summit 123

Copyright © 2014 CLUSIT
Tutti i diritti dell'Opera sono riservati agli Autori e al Clusit.
È vietata la riproduzione anche parziale di quanto pubblicato
senza la preventiva autorizzazione scritta del CLUSIT.

ASTREA Advanced Security, Training Research, Events Agency
Via Enrico Tazzoli,11 - 20154 Milano

Prefazione

Il rapporto CLUSIT che vi accingete a leggere è il frutto di un intenso impegno dei soci e delle aziende che hanno collaborato dando la loro disponibilità con dati, commenti e analisi: oltre 100 esperti e 500 aziende hanno lavorato intensamente per fare in modo che questo documento non fosse una elencazione di lamenti o di «bisognerebbe», ma uno strumento di lavoro concreto e realistico per chi si muove professionalmente nel campo della sicurezza delle informazioni.

L'anno appena concluso è stato indubbiamente l'anno del «Datagate», lo scandalo internazionale in cui il grande pubblico ha avuto evidenza del fatto che la sicurezza informatica non sia più solo uno scontro tra «buoni» e «cattivi» ma sia un fattore strategico di portata planetaria ed è anche a questo tema che è dedicata l'apertura del capitolo relativo al Cyber Crime che troverete nel rapporto.

I governi si stanno muovendo decisamente per rendere più sicure le infrastrutture dei propri paesi ma sappiamo bene che, data la complessità della rete, la sua capillarità, la sua dinamica, nulla sarà efficace senza una piena consapevolezza di tutti che porti a comportamenti responsabili.

Per questo motivo il rapporto CLUSIT costituisce uno strumento prezioso per i professionisti ma anche per le imprese, per i giornalisti, per gli amministratori pubblici, per i semplici cittadini, per tutti coloro che hanno compreso che la sicurezza dipende dalle azioni di ciascuno di noi.

I dati di mercato che troverete sono a questo proposito incoraggianti, nonostante le difficoltà della congiuntura economica il settore vede un incremento delle risorse messe a disposizione della sicurezza e soprattutto nelle medie aziende che rappresentano l'asse strategico primario della nostra economia.

Infine nei «focus on» troverete gli approfondimenti e i commenti sui temi cruciali all'orizzonte: dai tablet ai social networks, dalle questioni del management della sicurezza a quelle della formazione, temi ai quali abbiamo già rivolto l'attenzione nei precedenti rapporti CLUSIT ma che per la loro straordinaria dinamica ed evoluzione rappresentano scenari completamente nuovi.

2.000 copie cartacee, oltre 50.000 copie in elettronico scaricate dal sito CLUSIT sono la prova della funzione pratica che svolge il rapporto e nell'incoraggiarvi a leggerlo con attenzione, vi invitiamo a diffonderlo, a parlarne, a farlo conoscere perchè ciascuno, nel proprio ambito, faccia la sua parte per rendere la rete sempre più sicura.

Buona lettura

Gigi Tagliapietra
Presidente CLUSIT

Introduzione al rapporto

Il Rapporto 2014 inizia con una panoramica degli eventi di cyber-crime e incidenti informatici più significativi degli ultimi diciotto mesi. Si tratta di un quadro estremamente aggiornato ed esaustivo della situazione globale, con particolare attenzione alla situazione italiana. In totale, abbiamo classificato ed analizzato oltre 3.200 incidenti noti avvenuti nel mondo ed in Italia negli ultimi 42 mesi (dal primo gennaio 2011 al 30 giugno 2014), selezionati tra quelli che hanno avuto un impatto particolarmente significativo per le vittime in termini di perdite economiche, di reputazione, o di diffusione di dati sensibili (personali e non).
A questa analisi si è aggiunto quest'anno un nuovo formidabile strumento di rilevazione. Infatti, per la prima volta in Italia, abbiamo avuto a disposizione anche i dati relativi agli incidenti rilevati, aggregati in forma anonima e classificati dal Security Operations Center di FASTWEB, che ha gentilmente acconsentito a condividerli con Clusit.

Il Rapporto contiene anche i risultati di una survey che ha coinvolto ben 438 aziende e che ci ha consentito di analizzare le tendenze del mercato italiano dell'ICT Security, individuando le aree in cui si stanno orientando gli investimenti di aziende e Pubbliche Amministrazioni. Riguardo il mercato del lavoro, lo studio ha evidenziato quali sono le figure professionali più richieste, con l'intento di facilitare le scelte di studenti e professionisti.

Si forniscono inoltre importanti approfondimenti su una quantità di temi caldi: Smartphone, Tablet e Social Networks in Azienda; La strategia europea per la cybersecurity; Lo stato della digital forensics in Italia; La sicurezza delle informazioni in azienda ed i controlli interni; Security By Design; La Security vista dal Management; Formazione e Consapevolezza, strumenti indispensabili per la Sicurezza delle Informazioni.

Panoramica degli eventi di cyber-crime e incidenti informatici più significativi del 2013 e del primo semestre 2014

Anche in questa sesta edizione il Rapporto CLUSIT inizia con un'attenta e dettagliata analisi degli eventi ed incidenti informatici più significativi degli ultimi diciotto mesi.
A questa analisi si è aggiunto un nuovo formidabile strumento di rilevazione. Quest'anno (per la prima volta in Italia) abbiamo a disposizione anche i dati relativi agli incidenti rilevati (di qualsiasi dimensione ed impatto) nel corso del 2013, aggregati in forma anonima e classificati dal Security Operations Center di FASTWEB, che ha gentilmente acconsentito a condividerli con Clusit, realizzando per il Rapporto 2014 un'analisi molto interessante, presentata nella seconda parte di questo capitolo.
Ringraziamo sentitamente FASTWEB per la collaborazione e confidiamo che in futuro anche altri operatori di telecomunicazioni vorranno seguirne l'esempio, il che costituirebbe un significativo servizio non solo per gli addetti ai lavori, ma per la sicurezza della rete nazionale.

Prima di analizzare quanto avvenuto nel 2013 e nei primi sei mesi del 2014 a livello globale ed italiano, quest'anno vogliamo partire da cinque fatti di cronaca[1] solo apparentemente scorrelati ed a nostro avviso particolarmente significativi, per utilizzarli come chiave di lettura utile a comprendere come la situazione si stia evolvendo rapidamente in tema di Cyber Security.
Da un lato, la recente proposta da parte del Cancelliere Merkel (rivolta principalmente alla Francia, ma necessariamente estesa a tutti i partner europei della Germania) di costituire una "Internet europea"[2], alla luce delle rivelazioni da parte del "whistleblower"[3] Edward Snowden in merito alle attività di cyber espionage e sorveglianza di massa che sarebbero condotte dagli alleati anglo-americani (anche) ai danni di governi e cittadini europei.
Dall'altro, la recente pubblicazione negli USA di un framework nazionale per la cyber security delle infrastrutture critiche[4] (che inevitabilmente nel tempo, data l'ampiezza della definizione americana di infrastruttura critica, sarà estesa anche ad altri generi di imprese, oltre che alle istituzioni nazionali e federali), realizzato su diretta indicazione (Executive Order) del Presidente Obama[5]. Illuminanti le prime parole del testo dell'ordine presidenziale: "*Repeated cyber intrusions into critical infrastructure demonstrate the need for improved*

---

1 Scritto nel Febbraio 2014, aggiornato nel Luglio 2014

2 http://www.repubblica.it/tecnologia/2014/02/15/news/merkel_a_hollande_costruire_una_rete_web_indipendente_dagli_usa-78679542

3 http://it.wikipedia.org/wiki/Gola_profonda_%28informatore%29

4 http://www.whitehouse.gov/the-press-office/2014/02/12/launch-cybersecurity-framework

5 http://www.whitehouse.gov/the-press-office/2013/02/12/executive-order-improving-critical-infrastructure-cybersecurity

cybersecurity. The cyber threat to critical infrastructure continues to grow and represents one of the most serious national security challenges we must confront"[6].
Anche in Italia abbiamo assistito ad un evento significativo: a seguito dell'emanazione della "Direttiva recante indirizzi per la protezione cibernetica e la sicurezza informatica nazionale" del gennaio 2013, il 18 dicembre 2013 il Governo Letta ha approvato il "Piano nazionale per la protezione cibernetica e la sicurezza informatica", ovvero la nostra Cyber Strategy nazionale[7] (pubblicata sulla Gazzetta Ufficiale n.41 del 19 febbraio 2014).
Anche il Governo francese ha annunciato di voler investire un miliardo di euro nei prossimi 5 anni per la realizzazione di un ambizioso programma nazionale di cyber security[8] per "elevare il proprio livello di sicurezza a quello di altri partner NATO". Interessante il dato che traspare dalle parole del Ministro della Difesa francese sulla quantità di attacchi subiti nel 2013: "*Most of the money will go toward shoring up security at the Defence Ministry and its strategic partners, which were targeted by some 800 cyber attacks in 2013 amid unprecedented belt-tightening for the military*"[9].
Infine, va segnalata la crescente gravità dei danni provocati dagli attacchi informatici, fenomeno che cresce più velocemente del loro aumento in termini di frequenza. Tra i casi più eclatanti degli ultimi 18 mesi ricordiamo:

- il furto di 40 milioni di carte di credito dei propri clienti subito dal retailer americano Target, che oltre ad aver portato alle dimissioni del CEO e del CIO avrà un costo stimato per l'azienda di oltre un miliardo di dollari[10];
- il furto dei dati personali e delle credenziali di accesso di 230 milioni di utenti eBay[11];
- il ritrovamento da parte della Polizia tedesca di due database contenenti le credenziali email di circa 18 milioni di vittime, complessivamente[12];
- la campagna di cyber-espionage (denominata "Dragonfly" dai suoi scopritori), che ha colpito globalmente i sistemi SCADA di oltre 1.000 aziende del settore Energy (Italia inclusa), tramite il malware Havex[13].

Da questi recenti fatti si evince che il crescente impatto socio-economico e geopolitico derivante dalla attuale patologica situazione di diffusa insicurezza informatica, già ampiamen-

---

6 "Ripetute intrusioni informatiche nelle infrastrutture critiche dimostrano la necessità di una maggiore cyber security. La minaccia cyber alle infrastrutture critiche continua ad aumentare e rappresenta una delle più gravi sfide per la sicurezza nazionale che ci troviamo ad affrontare".

7 http://www.sicurezzanazionale.gov.it/sisr.nsf/wp-content/uploads/2014/02/piano-nazionale-cyber.pdf

8 http://www.reuters.com/article/2014/02/07/france-cyberdefence-idUSL5N0LC21G20140207

9 "La maggior parte del denaro sarà dedicato a migliorare la sicurezza del Ministero della Difesa e dei suoi partner strategici, che sono stati oggetto di 800 cyber attacchi nel 2013, in un contesto di importanti riduzioni di budget per la difesa".

10 http://www.aorato.com/blog/untold-story-target-attack-step-step/

11 http://www.techreviewer.co.uk/233-million-users-at-risk-of-identity-theft-after-ebay-is-involved-in-worlds-biggest-online-security-breach/

12 http://thehackernews.com/2014/04/worst-data-breach-in-german-history-18.html

13 http://grahamcluley.com/2014/07/dragonfly-hackers-target-1000-western-energy-firms-industrial-control-systems/

te sottolineato negli ultimi due Rapporti sui Rischi Globali del World Economic Forum[14], (oltre che, nel suo piccolo, anche da CLUSIT nei suoi precedenti Rapporti), è ormai tale da essere finalmente giunto sui tavoli (e nelle agende) dei principali attori della politica internazionale e nazionale, e non solo per ragioni di facciata, o come mero argomento di moda, come era fino a poco fa.
Pertanto, pur consci delle inevitabili resistenze che si dovranno fronteggiare, quest'anno osserviamo con soddisfazione le prime conseguenze di un fenomeno importante: la grande politica ha compreso l'importanza della Cyber Security e delle gravi implicazioni derivanti dalla sua diffusa carenza (se non totale mancanza) in tutti i contesti del mondo iper-connesso di oggi, il quale basa ormai la propria stessa esistenza sul buon funzionamento delle proprie infrastrutture ICT (critiche e non).
Tutti questi segnali, tra loro anche contraddittori (per esempio l'ipotesi di "Internet europea", volta a limitare l'impatto in Europa delle attività straniere di intelligence, ed in particolare americane, cozza sia logicamente che praticamente con i processi in atto in ambito NATO per il rafforzamento e l'integrazione della Cyber Security su base transatlantica, ed appare per molte ragioni di difficile realizzazione, oltre a risultare del tutto incompatibile con la prevista estensione dell'art.5 del trattato NATO anche ai cyber-attacchi[15]), indicano che è finalmente giunto il momento del fare, e che non è più possibile rimandare ulteriormente la concreta attuazione di efficaci politiche di sicurezza informatica, sia da parte del pubblico che dei privati, senza sottostare a rischi potenzialmente gravissimi.
Il cambiamento di prospettiva è tale che nella prefazione del nostro Piano nazionale per la protezione cibernetica e la sicurezza informatica si legge: "Con questo ulteriore documento 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".
La Cyber Security, come auspichiamo da tempo[16], è finalmente diventata anche nella percezione dei principali decisori nazionali un problema di "salute pubblica", e questo fenomeno rappresenta un "salto quantico", che va assolutamente apprezzato, sostenuto e valorizzato.
Ora si tratta di vigilare affinché principi ed iniziative di tale portata non rimangano lettera morta, e di implementare celermente le opportune misure (educative, normative, organizzative e tecnologiche), stanziando le risorse necessarie, in una corsa contro il tempo che allo stato attuale vede i difensori in una posizione di crescente svantaggio, dato che, come vedremo nei prossimi capitoli, il fronte delle minacce è sempre più esteso, agguerrito, complesso da contrastare ed efficace nel perseguire le proprie finalità dannose.
Recuperare il tempo perduto negli ultimi 4-5 anni è oggi la principale priorità, a tutti i livelli, per invertire le tendenze in atto, che sono certamente molto preoccupanti - la speranza, alla

---

14 http://www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf

15 http://www.repubblica.it/tecnologia/2014/09/02/news/cyberattacchi_nato-94856544/

16 http://www.tomshw.it/cont/articolo/le-tenaglie-di-efesto-stato-della-sicurezza-informatica-in-italia/44483/1.html

luce delle recenti evoluzioni, è che finalmente inizino ad esserci le condizioni per perseguire questo obiettivo fondamentale.
Auspicando che questo aggiornamento del Rapporto Clusit 2014 sulla Sicurezza ICT in Italia, giunto alla sua sesta[17] edizione, possa dare anche quest'anno un piccolo contributo nell'affrontare le difficili sfide che ci attendono, auguriamo a tutti una buona lettura!

17 Considerando gli aggiornamenti di fine anno pubblicati nel 2012, nel 2013 e nel 2014

Analisi dei principali attacchi noti a livello internazionale

Questo studio si riferisce alla classificazione ed all'analisi di un campione di oltre 3.200 incidenti noti avvenuti nel mondo ed in Italia negli ultimi 42 mesi (dal primo gennaio 2011 al 30 giugno 2014)[18], selezionati tra quelli che hanno avuto un impatto particolarmente significativo per le vittime in termini di perdite economiche, di reputazione, o di diffusione di dati sensibili (personali e non).
La sintesi qui presentata è il risultato di complesse attività di correlazione e di verifiche incrociate tramite attività mirate di OSInt[19] oltre che, non ultimo, del confronto con i dati che emergono dai report di molti Vendor (tra i quali ricordiamo Akamai, Cisco, IBM, Kaspersky, McAfee, Symantec, Trend Micro e Websense).

Va tenuto presente che il campione, per quanto abbastanza rappresentativo della realtà, non può essere considerato esaustivo in quanto presenta delle (inevitabili) distorsioni.
Ciò è dovuto da un lato al fatto che alcuni settori economici sono particolarmente efficaci nel minimizzare la diffusione pubblica di informazioni relative agli attacchi subiti, e risultano pertanto sotto-rappresentati, e dall'altro che alcuni tipi di attacchi (i più dannosi, per esempio quelli legati allo spionaggio industriale, o ad attività di Information Warfare) sono compiuti nell'arco di periodi piuttosto lunghi, in modalità estremamente cauta, e di conseguenza vengono alla luce ad anni di distanza[20].
Va dunque tenuto presente che i dati di seguito sintetizzati costituiscono solo la "punta dell'iceberg" rispetto al totale degli attacchi gravi compiuti in Italia e nel mondo nel corso dell'anno passato.
Dei 3.240 attacchi gravi di pubblico dominio che costituiscono il nostro campione, nel primo semestre 2014 ne abbiamo raccolti, classificati e analizzati 437 (il 13,5% del totale); di questi solo 7 si riferiscono a bersagli italiani (un mero 1,6% degli attacchi analizzati per il primo semestre 2014, numero che sicuramente non è rappresentativo della realtà dei fatti).
Anticipando una riflessione che svolgeremo più avanti, da questi numeri appare evidente come sia assolutamente attuale ed urgente implementare nel nostro Paese logiche di Cyber Intelligence Sharing e di Breach Disclosure, come indicato anche ai punti 5.3.d e 9 del nostro Piano nazionale per la protezione cibernetica e la sicurezza informatica.

2013-2014: l'insicurezza informatica è il "new normal"

Prendendo come riferimento il 2011, primo anno della nostra analisi, il numero di attacchi gravi di pubblico dominio che abbiamo analizzato è cresciuto nel 2013 del 245%. In altri termini, mentre nel 2011 abbiamo raccolto e classificato una media di 46 attacchi gravi al

[18] I dati di dettaglio ricavati da questa analisi, qui non riportati per ragioni di spazio, sono disponibili tramite CLUSIT per chiunque ne faccia richiesta.

[19] OSINT – Open Source Intelligence – Analisi di fonti aperte

[20] https://www.securelist.com/en/blog/208216078/The_Careto_Mask_APT_Frequently_Asked_Questions

mese, nel 2013 (a parità di criteri di classificazione) la media mensile è stata di 96, ovvero oltre 3 al giorno, con un picco di 123 attacchi registrati nel mese di gennaio. Nel primo semestre 2014 il picco si è avuto sempre a gennaio, con 85 attacchi gravi.
Nel corso dell'anno passato, come abbiamo già anticipato nella seconda edizione del Rapporto Clusit 2013[21] pubblicata lo scorso ottobre, mentre il numero complessivo degli attacchi informatici gravi di cui abbiamo avuto notizia è rimasto sostanzialmente invariato rispetto al 2012, la loro gravità è aumentata in modo significativo, sia in termini di quantità e di valore economico dei dati sottratti, sia in termini di ampiezza delle conseguenze nel caso di sabotaggi ed attacchi di tipo "denial of service".
Questo perché sono aumentate, in parallelo, sia la sofisticazione e la determinazione degli attaccanti sia, di conseguenza, la severità dei danni subiti dalle vittime. , ed i I dati del primo semestre 2014 confermano il persistere di questa situazione: il numero di attacchi gravi rilevati non aumenta, anzi diminuisce rispetto al secondo semestre 2013, ma il loro impatto continua a crescere.
D'altra parte va segnalato che sono in netta crescita gli attacchi distribuiti su un gran numero di vittime, che se da un lato causano danni relativamente modesti a ciascuna vittima, complessivamente colpiscono centinaia di migliaia di soggetti (sia privati che aziende). A titolo esemplificativo di questo genere di attacchi, che qui non sono rappresentati, ricordiamo quelli compiuti dalla "gang" responsabile della diffusione del ransomware[22] Cryptolocker[23], che ha realizzato decine di milioni di dollari di introiti in pochi mesi. Data la loro crescente rilevanza, in futuro ci occuperemo anche di questo genere di fenomeni.
A titolo esemplificativo dell'intensità crescente dei problemi che dobbiamo affrontare, una recente ricerca condotta da RBS in collaborazione con DatalossDB ha mostrato che nel 2013 in 2.164 diversi incidenti documentati sono stati sottratti 882 milioni di record personali[24] (una media di oltre 400.000 record per incidente), con punte di oltre 150 milioni di profili sottratti in un singolo attacco[25] (il secondo peggiore di sempre, ad oggi). Dei primi 10 incidenti avvenuti negli ultimi quattro anni in materia di sottrazione di account o profili personali, tre sono avvenuti nel primo semestre 2014.
Allo stesso modo, nel corso del 2013 gli attacchi DDoS volumetrici (basati cioè sulla quantità di traffico generato per disabilitare il bersaglio) superiori a 10 Gbps sono cresciuti, rispetto all'anno precedente, del 41,6%, con picchi di oltre 300 Gbps[26], mentre nei primi ~~due~~ sei mesi del 2014 sono già stati osservati alcuni attacchi superiori ai 400 Gbps[27], mentre

[21] http://www.clusit.it/rapportoclusit/

[22] http://en.wikipedia.org/wiki/Ransomware

[23] http://it.wikipedia.org/wiki/CryptoLocker

[24] https://www.riskbasedsecurity.com/2014/02/2013-data-breach-quickview/

[25] http://nakedsecurity.sophos.com/2013/10/04/adobe-owns-up-to-getting-pwned-login-and-credit-card-data-probably-stolen-all-passwords-reset/

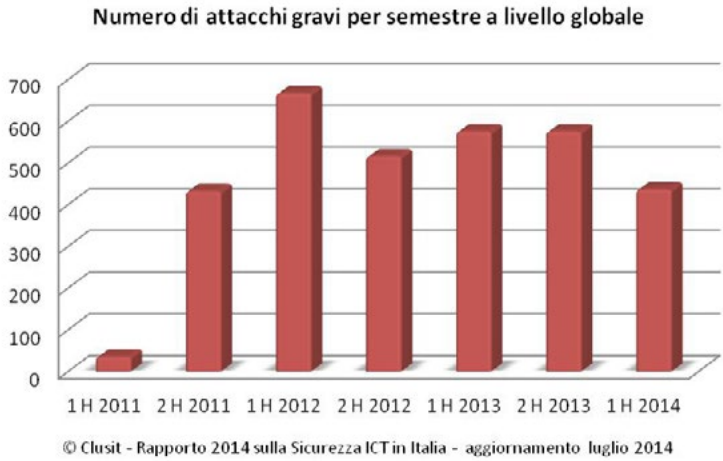
[26] http://www.darkreading.com/vulnerability/average-ddos-attack-size-growing-dramati/240159399

[27] http://blog.cloudflare.com/technical-details-behind-a-400gbps-ntp-amplification-ddos-attack

quelli superiori ai 100 Gbps sono ormai diventati di ordinaria amministrazione[28].
Questo in un contesto nel quale la spesa globale nel 2013 per prodotti e servizi di Cyber Security è stata stimata da Gartner prossima a 70 miliardi di dollari (+16% rispetto al 2012), contro un totale di perdite dirette ed indirette causate dal solo Cyber Crime che il Ponemon Institute stima in quasi 500 miliardi di dollari[29] (+ 26% rispetto al 2012).
Allo stato attuale dobbiamo dunque prendere atto del fatto che l'investimento in contromisure cresce meno rapidamente di quanto crescano i danni provocati dagli attaccanti, oppure, detto diversamente, che l'efficacia degli attaccanti è maggiore di quella dei difensori, in termini di ROI.

La situazione globale in cifre

Per dare un riferimento numerico relativamente al campione di 3.241 incidenti noti[30] che Clusit ha classificato come particolarmente gravi ed analizzato, osserviamo il grafico relativo agli ultimi 42 mesi, ordinato per semestre:

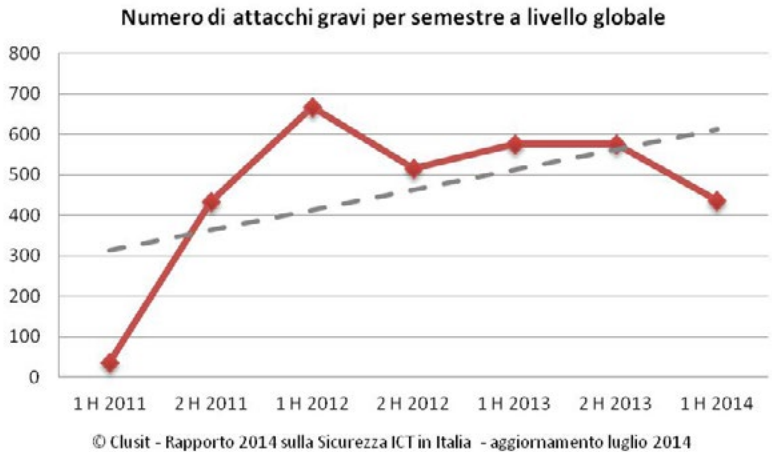


Il picco di attacchi significativi divenuti di dominio pubblico nel primo semestre 2012 è dovuto sostanzialmente alla fase di maggiore intensità delle azioni dimostrative su larga scala realizzate da parte degli Hacktivist della galassia Anonymous (che sono poi stati duramente colpiti dalle Forze dell'Ordine nella seconda metà del 2012, riducendo di molto le attività).

28 http://www.akamai.com/html/about/press/releases/2014/press-041714.html

29 The Ponemon Institute, " The 2013 Cost of Cyber Crime Study"

30 http://hackmageddon.com/2013-cyber-attacks-timeline-master-index/



Pur considerando che all'inizio del 2011 gli attacchi noti considerati gravi in base ai nostri criteri di classificazione erano molti meno rispetto agli anni successivi, la linea di tendenza degli ultimi 42 mesi è inequivocabile. Gli ultimi due semestri mostrano che siamo entrati in una fase di stabilizzazione se non di flessione del fenomeno, quantomeno dal punto di vista del numero di attacchi. La nostra interpretazione di questa flessione numerica è che i principali gruppi di attaccanti stiano attraversando una fase di consolidamento e di "concentrazione" rispetto al 2012-2013, il che potrebbe anche spiegare perché la gravità degli impatti causati dagli attacchi sia mediamente in aumento: i soggetti criminali responsabili di questi attacchi, associandosi e coordinandosi meglio, realizzano meno "colpi", ma con maggiore aggressività, conseguendo una maggiore "redditività" (dal loro punto di vista).
Sicuramente questo dato è anche conseguenza del lento innalzamento generale del livello di protezione delle vittime, che se non impedisce ai criminali più capaci di mettere a segno attacchi anche clamorosi, d'altra parte in un crescente numero di casi riduce le possibilità di successo di molti attaccanti improvvisati.

I fenomeni più interessanti emersi nel 2013-2014

Fatto salvo quanto già descritto nel Rapporto CLUSIT 2013 a seguito dell'analisi degli attacchi del 2012, relativamente al fatto che tutti sono ormai diventati bersagli, che le protezioni tradizionali sono sempre meno efficaci e che tutte le piattaforme sono ormai nel mirino dei malintenzionati, i nuovi fenomeni più interessanti del 2013, che vediamo confermati anche in questi primi sei mesi del 2014, possono essere sintetizzati come segue:

- **In tutto il mondo si moltiplicano gruppi di attaccanti con capacità tecniche sofisticate.**

Mentre fino a poco tempo fa la maggior parte degli hackers erano occidentali, negli ultimi anni (e nel 2013 in particolare) si è assistito ad una moltiplicazione esponenziale di capacità, anche molto avanzate, tra persone originarie di paesi in via di sviluppo e del terzo mondo.
Anche senza considerare l'addestramento di un crescente numero di cyber warriors, derivante dallo sviluppo di capacità in ambito Information Warfare che ormai sono, con differenti livelli di capacità, in via di adozione da parte di decine di nazioni, questa inevitabile diffusione di know-how sofisticato tra hacktivist e cyber criminali non occidentali ha implicazioni profonde, sia dal punto di vista strettamente numerico, data la quantità di popolazione che si sta affacciando su Internet in quei paesi, sia perché la razionalità di questi soggetti è differente da quella alla quale siamo abituati, il che implica che sono disposti a correre rischi maggiori ed a non curarsi dell'impatto delle proprie azioni sui bersagli (rispetto ai loro omologhi di cultura occidentale, per esempio dell'est europeo, che hanno un approccio più cauto e di basso profilo). Questo cambiamento nella razionalità prevalente degli attaccanti va sicuramente considerato nel predisporre le prossime iniziative di difesa, sia per il pubblico che per i privati.

- **Cyber Crime ed Hacktivism diventano concetti sempre più sfumati.**
  A differenza del recente passato, quando questo fenomeno rappresentava un'eccezione, dal 2013 sempre più spesso si assiste ad una commistione tra finalità cyber criminali e forme di hacktivism. I due ambiti, originariamente distinti per background, finalità e modalità di azione, sempre più spesso trovano conveniente allearsi per raggiungere i propri obiettivi. Eclatante il caso del complesso attacco alle banche ed alle televisioni sud coreane (operation "Dark Seoul")[31], nel quale l'inedito e premeditato coordinamento tra hacktivist, cyber criminali e cyber spie è risultato estremamente efficace. Inoltre le frange di attivisti digitali più oltranzisti (in particolare di matrice nazionalista, come la S.E.A., Syrian Electronic Army[32]) iniziano ad utilizzare le modalità operative del cyber crime per auto-finanziarsi. Tutto ciò, generando ulteriori ambiguità nelle "firme" degli attacchi, rende ancora più complesse le attività di Cyber Intelligence e di reazione da parte dei difensori.

- **Le grandi organizzazioni vengono sempre più spesso colpite tramite i propri fornitori / outsourcer.**
  Nel 2013 si è assistito all'emergere di una chiara tendenza, ampiamente confermata nel 2014, per cui gli attaccanti hanno individuato negli outsourcer l'anello più debole da colpire per raggiungere (tipicamente sfruttandone le utenze privilegiate e le connessioni VPN) i loro bersagli primari.
  Tra gli esempi più eclatanti, in un caso le applicazioni per piattaforme mobile di un noto

[31] http://www.nytimes.com/2013/03/21/world/asia/south-korea-computer-network-crashes.html

[32] http://en.wikipedia.org/wiki/Syrian_Electronic_Army

network televisivo satellitare sono state infettate con malware, e diffuse su milioni di smartphone tramite il meccanismo degli aggiornamenti automatici, compromettendo la software house che le realizza[33]. Curiosamente il network, mostrando una notevole incertezza nelle proprie procedure di Crisis Management, dopo aver invitato via Twitter i propri utenti a disinstallare le proprie app, lo stesso giorno ha fatto clamorosamente marcia indietro[34].

In un altro caso, una nota catena americana della grande distribuzione organizzata è stata duramente colpita con la sottrazione dei codici di 40 milioni di carte di credito, rubate infettandone i POS a partire dalla connessione VPN di un fornitore specializzato nella manutenzione di banchi frigoriferi[35].

Questo fenomeno, data la propensione degli attaccanti a minimizzare gli sforzi, è destinato a crescere in modo esponenziale, dal momento che spesso questi fornitori sono aziende medio-piccole, con una cultura della sicurezza sensibilmente inferiore a quella dei loro grandi clienti, pur avendo di frequente accessi poco o per nulla presidiati alle loro reti ed infrastrutture.

- **I Social Network, per la loro natura e diffusione, sono ormai il principale veicolo di attività malevole.**

  Ciò che avevamo anticipato nei Rapporti precedenti si è realizzato compiutamente nel 2013, e risulta confermato dai dati dei primi sei mesi del 2014: i Social Network, grazie alle loro caratteristiche ed alle modalità "disinvolte" di interazione tra gli utenti, sono utilizzati dagli attaccanti per massimizzare l'effetto delle loro campagne di diffusione di spam, di phishing e di social engineering, con la finalità prevalente di infettare il maggior numero possibile di sistemi, per poterli associare a botnet composte da milioni di macchine[36], che poi sono utilizzate per generare BitCoins, compiere attacchi DDoS, inviare spam, rubare identità[37], etc.

  Inoltre, dato che i Social Network gestiscono i profili (e gli account) di un numero enorme di utenti, sono utilizzati per attività di "scraping" di credenziali e di dati personali su scala planetaria[38]. Questo include anche le principali piattaforme di messaggistica per smartphone e tablet (che costituiscono la nuova frontiera dei Social Network), spesso afflitte da importanti vulnerabilità: a titolo di esempio, una popolare piattaforma ha consentito la diffusione non autorizzata di 6 milioni di numeri di telefono appartenenti ai suoi utenti[39], mentre un'altra consentiva a chiunque di aggirare la cifratura dei messaggi

---

33 http://www.androidcentral.com/sky-tv-apps-hacked-all-now-removed-play-store

34 http://www.techradar.com/news/software/applications/sky-s-android-apps-hacked-users-advised-to-uninstall-until-its-safe-1154507

35 https://krebsonsecurity.com/2014/02/target-hackers-broke-in-via-hvac-company/

36 http://threatpost.com/facebook-security-fbi-take-down-butterfly-botnet-arrest-10-121212/77308

37 http://www.zdnet.com/hacker-database-exposed-thousands-of-stolen-facebook-twitter-google-passwords-found-7000023922/

38 http://www.businessweek.com/news/2014-01-07/linkedin-sues-unknown-hackers-over-thousands-of-fake-accounts

39 http://nakedsecurity.sophos.com/2013/06/27/researchers-facebook-leaks-are-a-lot-leakier-than-facebook-is-letting-on/

scambiati tra gli utenti e di leggerli in chiaro[40].
Data la diffusione nell'uso dei Social Network oltre che tra i privati anche tra utenti di organizzazioni pubbliche e private di ogni dimensione, (spesso in associazione con strumenti mobile, il che rappresenta un moltiplicatore di rischio), queste minacce incombono costantemente anche sui relativi sistemi informativi e sulle informazioni che contengono (perfino, ed a maggior ragione, in ambiti molto delicati quali quelli governativi e militari[41]).

Ma quali sono, in sostanza, le conseguenze pratiche di tutti questi fenomeni?

Classificazione e analisi dei principali incidenti noti a livello globale

Di seguito tre tabelle che rappresentano i criteri di sintesi che abbiamo utilizzato per rendere fruibili i molti dati raccolti. Come l'anno scorso abbiamo segnalato in arancio gli incrementi percentuali che risultano essere superiori alla media, evidenziando così le principali tendenze in atto, e confrontato i dati del 1° semestre 2014 (1H) con quelli del semestre precedente. Queste le consistenze numeriche emerse:

ATTACCANTI PER TIPOLOGIA	2011	2012	2013	2012 su 2011	2013 su 2012	2H 2013	1H 2014	1H 2014 su 2H 2013
Cybercrime	170	633	609	272,35%	-3,79%	315	268	-14,92%
Hacktivism	114	368	451	222,81%	22,55%	227	128	-43,61%
Espionage / Sabotage	23	29	67	26,09%	131,03%	26	30	15,38%
Cyber warfare	14	43	25	207,14%	-41,86%	8	11	37,50%
TOTALE	469	1.183	1.152			576	437	

VITTIME PER TIPOLOGIA	2011	2012	2013	2012 su 2011	2013 su 2012	2H 2013	1H 2014	1H 2014 su 2H 2013
Institutions: Gov - Mil - LEAs - Intel	153	374	402	144,44%	7,49%	224	111	-50,45%
Others	97	194	146	100,00%	-24,74%	75	35	-53,33%
Entertainment / News	76	175	147	130,26%	-16,00%	71	49	-30,99%
Online Services / Cloud	15	136	114	806,67%	-16,18%	58	52	-10,34%

40 http://thehackernews.com/2013/10/vulnerability-in-whatsapp-allows.html

41 http://www.timesofisrael.com/israels-army-of-facebook-addicts-battles-to-keep-its-secrets/

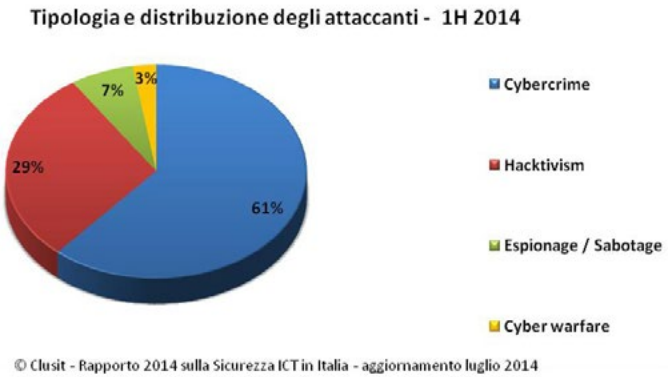
Research - Education	26	104	70	300,00%	-32,69%	31	32	3,23%
Banking / Finance	17	59	108	247,06%	83,05%	43	27	-37,21%
Software / Hardware Vendor	27	59	46	118,52%	-22,03%	22	29	31,82%
Telco	11	19	19	72,73%	0,00%	13	14	7,69%
Gov. Contractors / Consulting	18	15	2	-16,67%	-86,67%	2	3	50,00%
Security Industry:	17	14	6	-17,65%	-57,14%	1	2	100,00%
Religion	0	14	7	-	-50,00%	2	5	150,00%
Health	10	11	11	10,00%	0,00%	7	21	200,00%
Chemical / Medical	2	9	1	350,00%	-88,89%	1	4	300,00%
Critical Infrastructures	-	-	37	-	-	17	11	-35,29%
Automotive	-	-	17	-	-	1	3	200,00%
Org / ONG	-	-	19	-	-	8	19	137,50%
GDO / Retail	-	-	-	-	-	-	20	-

TECNICHE DI ATTACCO PER TIPOLOGIA	2011	2012	2013	2012 su 2011	2013 su 2012	2H 2013	1H 2014	1H 2014 su 2H 2013
SQL Injection	197	435	217	120,81%	-50,11%	55	56	1,82%
Unknown	73	294	239	302,74%	-18,71%	133	100	-24,81%
DDoS	27	165	191	511,11%	15,76%	84	46	-45,24%
Known Vulnerabilities / Misconfigurations	107	142	256	32,71%	80,28%	175	104	-40,57%
Malware	34	61	57	79,41%	-6,56%	49	65	32,65%
Account Cracking	10	41	115	310,00%	180,49%	69	49	-28,99%
Phishing / Social Engineering	10	21	3	110,00%	-85,71%	1	4	300,00%
Multiple Techniques / APT	6	13	71	116,67%	446,15%	9	8	-11,11%
0-day	5	8	3	60,00%	-62,50%	1	4	300,00%
Phone Hacking	0	3	0	-	-	0	1	-

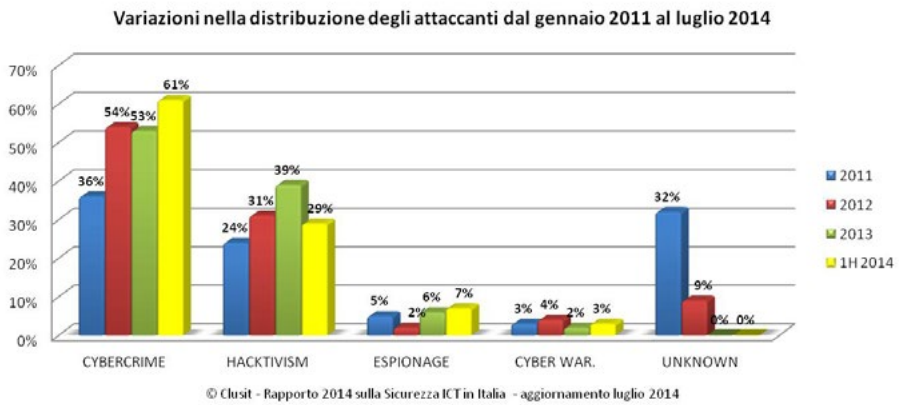
© Clusit - Rapporto 2014 sulla Sicurezza ICT in Italia – aggiornamento luglio 2014

Distribuzione degli attaccanti

Questo grafico rappresenta la distribuzione percentuale degli attaccanti osservata nel primo semestre 2014. Da notare che la distribuzione numerica degli attaccanti non dà informazioni significative sull'impatto degli attacchi che hanno compiuto. Per esempio le crescenti attività di Cyber Espionage, pur essendo solo il 7% (+37% rispetto al secondo semestre 2013) degli attacchi noti, hanno causato danni certamente superiori rispetto a quelli realizzati da Hacktivist, che sono in calo rispetto al 39% del 2013, essendo responsabili del 29% degli attacchi.

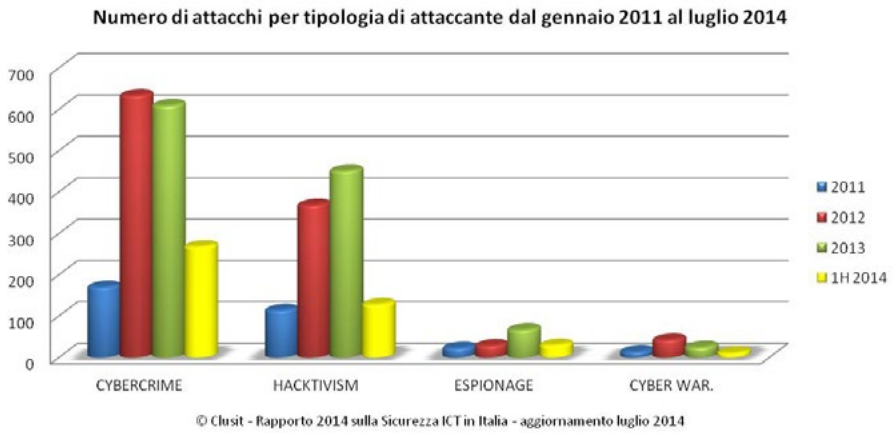


Da notare come il Cyber Crime superi ormai il 60% del totale (dal 36% del 2011 al 54% del 2012 al 53% nel 2013).



I casi noti di Cyber Espionage (escluse le vicende legate al c.d. Datagate, che non sono considerate dalle nostre statistiche) sono cresciuti dal 2% del 2012 al 7% del 2014.

Da notare infine l'assenza della categoria "Unknown". Gli attaccanti non identificati erano ben il 32% nel 2011, ed ancora il 9% nel 2012.
Questo risultato, senz'altro positivo, è dovuto all'affinamento delle tecniche di OSInt impiegate nella fase di attribuzione degli attacchi, e rappresenta la dimostrazione di come sia possibile ottenere (pur con i mezzi limitati a nostra disposizione) una buona comprensione delle motivazioni e della natura degli attaccanti, elementi fondamentali per poter porre in essere le contromisure più opportune.
Questi, in valori assoluti, gli attacchi analizzati per il primo semestre 2014 a livello internazionale ed italiano, rispetto agli anni precedenti:

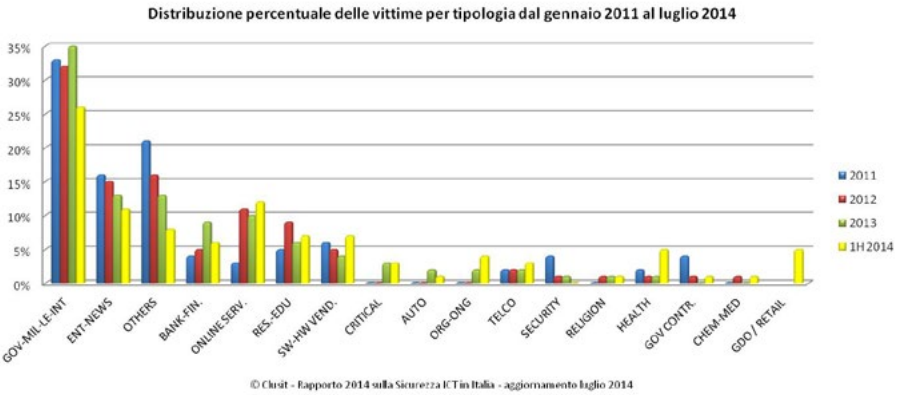


Distribuzione delle vittime

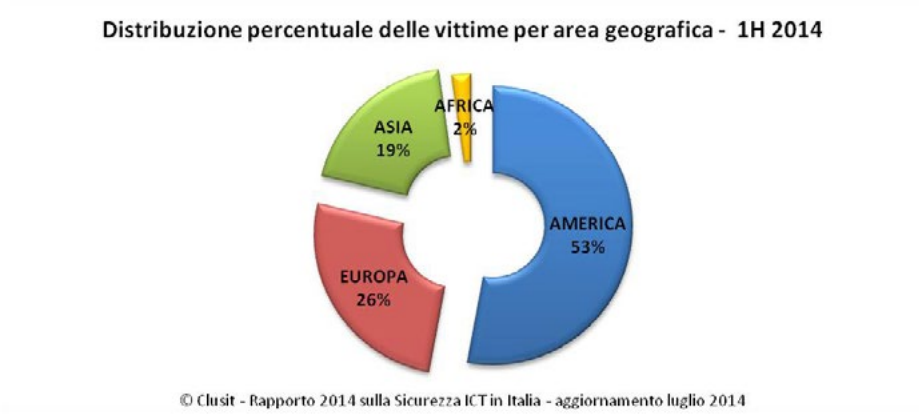
Per quanto riguarda la distribuzione delle vittime, nel 2012 diminuivano leggermente gli attacchi verso enti governativi, partiti politici, forze dell'ordine etc (sempre comunque al primo posto), ma aumentavano quelli contro l'industria dell'informazione e dello spettacolo, i servizi cloud / web 2.0 / social e le istituzioni di ricerca o scolastiche.
Nel 2013 invece abbiamo assistito ad un leggero aumento di attacchi verso il settore governativo (+7,5%) e ad un aumento numericamente consistente (+83%) di attacchi verso il settore Banking/Finance, che passa dal 5% del totale nel 2012 al 9% nel 2013.
Nel primo semestre 2014 sono diminuiti in percentuale quasi tutti i settori, con la significativa crescita dei settori Health, Online Services / Cloud e SW / HW Vendor rispetto al secondo semestre 2013. Si è inoltre reso necessario aggiungere la categoria Retail / GDO, fatta oggetto di numerosi attacchi gravi negli ultimi mesi da parte di cyber criminali molto aggressivi:

Nel 2013 sono apparsi per la prima volta nel campione attacchi noti contro Infrastrutture Critiche (categoria non presente nelle precedenti edizioni del Rapporto), che si posizionano anche nel 2014 al 3% del totale, e verso altri due settori, quello Automotive (principalmente con finalità di spionaggio industriale) e quello delle ONG (principalmente con finalità di spionaggio politico o di Hacktivism). In leggera crescita anche le Telco, che passano dal 2% al 3% delle vittime.

L'evoluzione della distribuzione delle vittime nel corso dei tre anni e mezzo considerati si evince dal grafico sottostante:



Con questo aggiornamento del Rapporto Clusit 2014, per la prima volta presentiamo anche la distribuzione percentuale delle vittime rispetto all'area geografica di appartenenza:

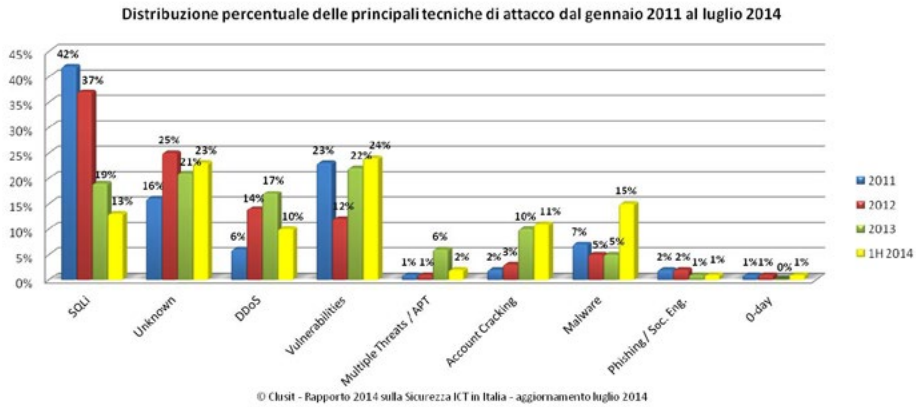


Come si può notare, la maggior parte degli attacchi gravi di dominio pubblico che abbiamo analizzato hanno interessato organizzazioni pubbliche e private americane (inclusi tutti i Paesi del nord, centro e sud america, anche se le vittime del nostro campione sono principalmente statunitensi). L'Europa (inclusa la Russia) viene al secondo posto, seguita dall'Asia e dall'Africa.
Questa distribuzione è certamente determinata anche dal fatto che sono disponibili molti più dati relativi ad incidenti occorsi ad organizzazioni basate in USA che per il resto del mondo, grazie alla normativa americana sull'obbligo di notifica dei data breach, altrove ancora assente.

Distribuzione delle tecniche di attacco

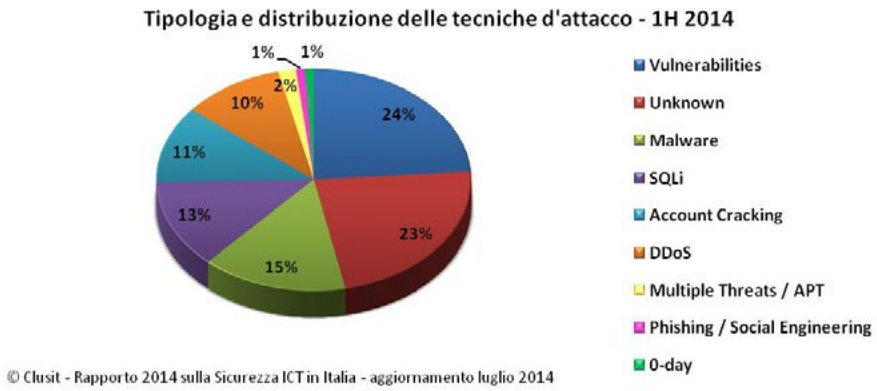
Per quanto riguarda la classificazione degli attacchi in base alle tecniche utilizzate dagli attaccanti nel primo semestre 2014 rispetto agli anni precedenti, spiccano l'ulteriore incremento della categoria Vulnerabilities, l'aumento di attacchi basati su Account Cracking e soprattutto una notevole crescita della categoria Malware, che passa dal 5% del 2013 al 15% del 1H 2014. Questo è dovuto al rilascio di numerose nuove famiglie di malware, che negli ultimi mesi hanno messo a dura prova le difese tradizionali. Va sottolineato che la diminuzione della categoria DDoS all'interno del nostro campione non deve trarre in inganno: questo tipo di attacco è sempre più diffuso, ma più spesso che in passato viene oggi utilizzato verso bersagli meno importanti (in quanto meno difesi), e quindi qui risulta sottorappresentato.

Questo grafico rappresenta in valori percentuali le tecniche di attacco rilevate globalmente negli ultimi 42 mesi:



La principale macro-famiglia di tecniche di attacco rilevate nel primo semestre 2014 è relativa allo sfruttamento di vulnerabilità note o di misconfigurazioni dei sistemi bersaglio, che rappresentano circa un quarto dei casi analizzati (24%). Per la prima volta dal 2011 questa categoria passa al primo posto tra le cause di compromissione che hanno portato i cyber criminali a realizzare attacchi gravi con successo.
Si confermano sempre efficaci le tecniche di attacco basate su SQL Injection (erano il 37% nel 2012 e sono ancora il 13% nel 2014) e quelle basate su phishing e social engineering (tipicamente realizzati via email o tramite Social Network, oppure infettando siti Web), per quanto complessivamente queste categorie siano in flessione nel nostro campione.
In generale, i vettori di attacco più semplici da sfruttare (e più facili da mitigare, quantomeno in astratto) ovvero SQLi, DDoS e Vulnerabilities, nel primo semestre 2014 rappresentano ancora il 47% del totale, contro il 58% dell'anno precedente.
Questo suggerisce due riflessioni: da un lato molti difensori non pongono ancora sufficiente attenzione all'hardening dei sistemi, non applicano le patch di sicurezza e soprattutto non dispongono di sistemi di monitoraggio in real-time, in grado di individuare e bloccare questi attacchi spesso poco sofisticati, dall'altro il numero di vulnerabilità note continua ad aumentare ogni anno, il che accresce la superficie di attacco dei bersagli e quindi le opportunità per gli attaccanti.

Questa la distribuzione percentuale delle tecniche di attacco emersa dal nostro campione per il 1H 2014:



La diminuzione percentuale delle categorie SQLi, DDos, ed APT rispetto al 2013 si spiega con l'adozione di contromisure efficaci da parte dei difensori, quantomeno nelle realtà di grandi dimensioni.
Rimangono ancora un buon 23% di casi (in leggero aumento rispetto al 21% del 2013) nei quali non è stato possibile individuare con certezza il tipo di tecnica di attacco utilizzata. Questa mancanza di informazioni pubbliche sui metodi utilizzati dagli attaccanti è da un lato sintomo della carenza, ancora oggi, di intelligence sharing e di trasparenza da parte delle vittime (fenomeno che danneggia tutti), e dall'altro sottolinea la complessità raggiunta dalle tecniche utilizzate dai malintenzionati, che spesso non consente di stabilire con certezza le modalità effettive di compromissione di un sistema o di un'organizzazione.
Da questo grafico appare comunque evidente come i difensori stiano ponendo rimedio alle vulnerabilità più banali ancora troppo lentamente, ed allo stesso tempo gli attaccanti stiano continuamente alzando il livello di complessità e di pericolosità dei loro attacchi, in una sorta di "corsa agli armamenti" che al momento vede i malintenzionati ancora in vantaggio in molte delle categorie analizzate.

Principali tendenze per il 2014

Dopo aver analizzato i dati del primo semestre 2014, siamo in grado di ipotizzare con una buona approssimazione quali saranno i principali trend del 2014.

Cloud e Social Network

Sicuramente uno dei fenomeni a cui assisteremo con maggiore frequenza quest'anno sarà una serie di attacchi ai sistemi Cloud ed ai Social Network, oppure realizzati per loro tramite per colpirne gli utenti finali. Questi sistemi contengono infatti grandi quantità di dati e

sono quindi un bersaglio appetibile per i malintenzionati che, con un attacco solo, possono riuscire a raccogliere grandi quantità di informazioni, e/o a colpire un grandissimo numero di utenti.

Malware, APT e "0-day"

Nel 2014 osserveremo quasi certamente un crescente numero di ~~Advanced Persistent Threat e di~~ nuove famiglie di malware con finalità di cyber crime, e di un numero significativo di Advanced Persistent Threat (APT), alcune delle quali basate su vulnerabilità "zeroday", cioè malware scritti appositamente per condurre un determinato attacco e non riconosciuti dai tradizionali antivirus, con finalità di cyber espionage. Questo fenomeno è dovuto al fatto che, nella corsa agli armamenti che si sta verificando nel cyberspace, un enorme ecosistema criminale lavora senza sosta per mantenere il vantaggio sui difensori, disponendo di risorse e capacità di alto livello.

La maggiore visibilità di questi attacchi, che in realtà, silenziosamente, vanno avanti da anni, sarà anche dovuta all'evoluzione delle tecnologie per la rilevazione di queste minacce, che ci permetteranno di prendere coscienza di un fenomeno che fino ad ora è rimasto per lo più nascosto.

Crypto-monete

Se la "bolla" delle crypto-monete non imploderà a breve, vedremo sicuramente la percentuale di malware scritta allo scopo di generare e di rubare queste valute tramite i sistemi informativi di vittime ignare aumentare ancora, dato l'altissimo guadagno per i criminali a fronte di investimenti minimi.

Distributed Denial of Service

Con l'aumentare della banda disponibile, sia a livello domestico che professionale, gli attacchi di tipo DDoS, ormai divenuti attuabili da chiunque, verranno utilizzati massivamente, oltre che per fini dimostrativi anche per fini criminali (principalmente di ricatto, nel 2014) e di concorrenza sleale.

Piattaforme Mobile

Il 2013, è stato l'anno in cui si sono venduti più dispositivi mobili (tablet e smartphone) che computer. Per questo motivo, seguendo il trend, nel 2014 osserviamo un aumento sensibile della percentuale di malware scritta per colpire questo tipo di sistemi, indipendentemente dal tipo di piattaforma (pur con una prevalenza di minacce per la piattaforma Android).

I vari colossi che gestiscono i mercati delle App, come Google ed Apple, fanno del loro meglio per allontanare la minaccia, generalmente con buoni risultati. Una gran parte degli utenti ha l'abitudine tuttavia di servirsi di App store non ufficiali, ove le App rilasciate e caricate non subiscono purtroppo alcun controllo, oppure di "rootare"[42] il proprio device

[42] http://www.androidplay.it/android-root-rootare-rooting-3533/

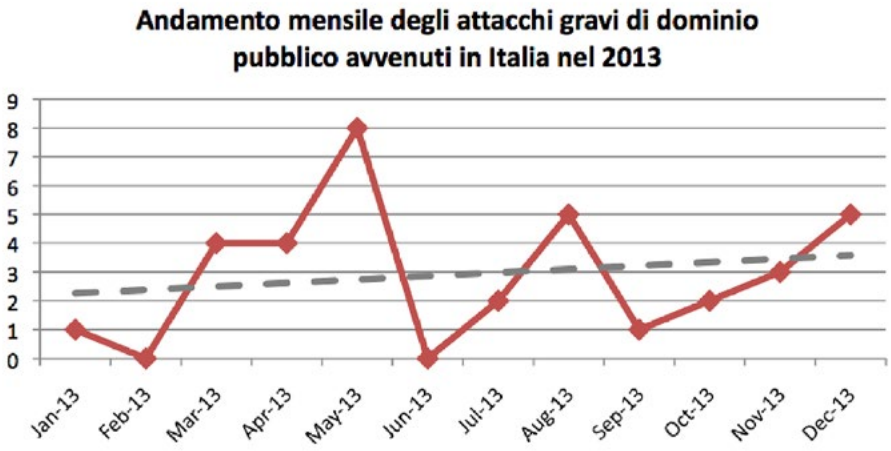
mobile, il che lo espone a rischi molto elevati.
I malware per Android crescono, ma i numeri di varianti rimangono ancora lontani da quelli prodotti per attaccare i PC. I dispositivi mobili sono ancora un terreno non sfruttato a pieno dai cyber criminali in quanto non pare ci siano ancora strategie semplici per ottenere denaro dai dispositivi compromessi. La sicurezza messa in campo dalla combinazione di app store ufficiali e il costante aggiornamento dei sistemi operativi, rende difficile la compromissione delle principali piattaforme. Tuttavia ciò non può essere considerato sufficiente nel lungo termine e per tale motivo sarà sicuramente necessario adottare ulteriori accorgimenti di sicurezza, tra i quali piattaforme MDM (Mobile Device Management), ovvero sistemi sviluppati per la gestione e per la protezioni dei dati presenti sulle flotte dei dispostivi mobili dei dipendenti.

Trasformazioni nel mercato della Security

L'impressione che si ha a metà del 2014 è che il mercato dei servizi di sicurezza cloud e cloud-based sarà uno dei punti focali dei prossimi anni.
L'adozione sempre più universale di applicazioni "software as a service" (SaaS) e di servizi basati su cloud incoraggeranno le aziende ad adottare sistemi di controllo della security in cloud tra i quali particolare l'e-mail security, i web security services e l'identity and access management (IAM).
A seguito di una costante evoluzione di tali servizi si potrà assistere anche ad un incremento dei servizi di security basati su crittografia e token, i tool SIEM (Security Information and Event Management), dei sistemi di Vulnerability Assessment ed i firewall per le applicazioni basate su Web.
Il modello del Cloud applicato alla Security è oramai una realtà abbastanza matura, che tenderà sicuramente a consolidarsi nel corso del 2014-2015. Ciò è soprattutto dovuto al consistente numero di vantaggi che queste piattaforme possono fornire, soprattutto per le piccole-medie imprese che altrimenti non potrebbero dotarsi delle soluzioni più avanzate per ragioni di budget.

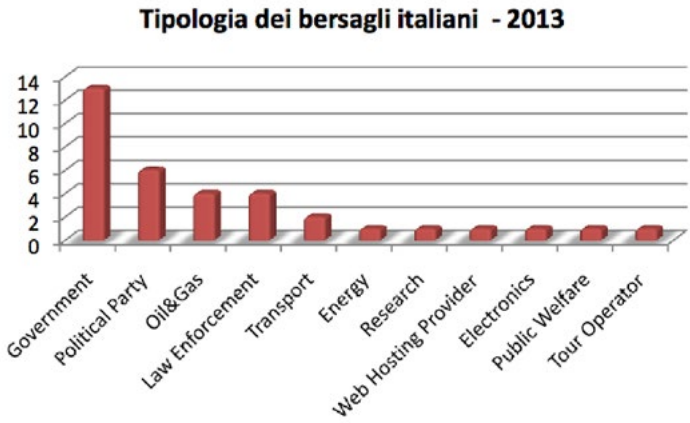
Analisi della situazione italiana in materia di attacchi informatici gravi

Mentre nel 2013 abbiamo classificato come gravi ed analizzato 35 attacchi di dominio pubblico contro bersagli italiani, che rappresentano un mero 3% del nostro campione complessivo di 1.152 incidenti del 2013, nel primo semestre 2014 abbiamo rilevato solo 7 attacchi gravi sui 437 (1,6%), ad oggi un numero troppo basso per produrre statistiche significative. Appare comunque piuttosto improbabile che il numero di attacchi gravi nel nostro Paese sia stato così basso, soprattutto se confrontiamo tale cifra con quelle note per altri paesi occidentali con un'economia di dimensioni paragonabili (per esempio l'Inghilterra), il che ci porta a supporre che tale cifra incongrua sia dovuta alla cronica mancanza di informazioni pubbliche in merito, ed, in misura minore, al fatto che le organizzazioni in Italia spesso non hanno ancora gli strumenti organizzativi e tecnologici per rendersi conto di essere state compromesse.
Auspichiamo che, con l'attivazione del CERT nazionale e nel dare attuazione agli indirizzi espressi dal "Piano nazionale per la protezione cibernetica e la sicurezza informatica", si riesca a porre rimedio a questa situazione di carenza informativa ed in alcuni casi di "omertà", che per un malinteso senso di protezione della propria reputazione porta le organizzazioni nostrane a non denunciare gli incidenti subiti se non quando assolutamente inevitabile, il che danneggia concretamente tutta la collettività.
Ciò premesso, analizziamo e commentiamo i 35 incidenti italiani del nostro campione del 2013, cominciando dalla distribuzione temporale degli attacchi e dalla loro linea di tendenza.



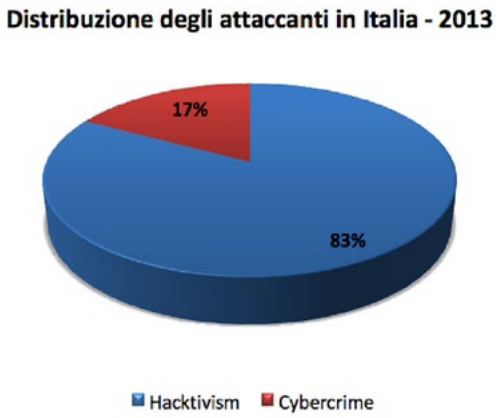
© Clusit - Rapporto 2014 sulla Sicurezza ICT in Italia

Ricordando che i casi analizzati rappresentano un punto di vista particolare e parziale, dato che si riferiscono agli attacchi di dominio pubblico che hanno avuto un impatto significativo (mediatico e/o economico), riportiamo una sintesi dei bersagli colpiti.



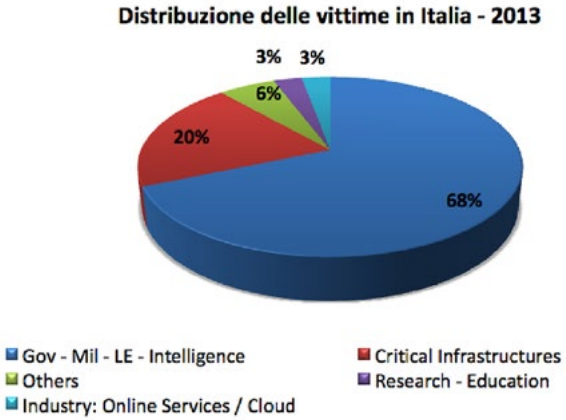
© Clusit - Rapporto 2014 sulla Sicurezza ICT in Italia

Il grafico sopra riportato, che si discosta dalle statistiche globali che abbiamo presentato analizzando gli attacchi avvenuti all'estero, si spiega analizzando le finalità degli attaccanti, che in base ai dati a nostra disposizione sono state le seguenti:



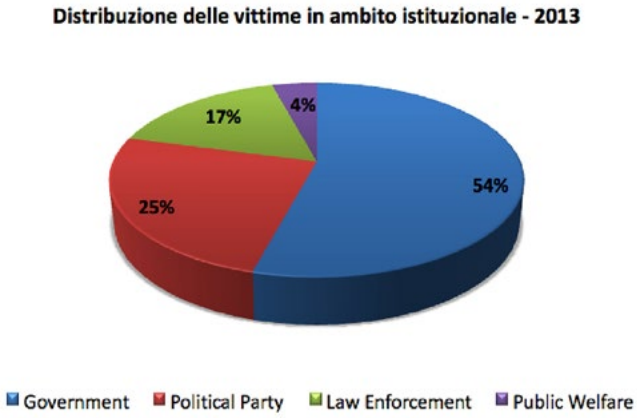
© Clusit - Rapporto 2014 sulla Sicurezza ICT in Italia

In pratica in base agli incidenti noti nel nostro Paese sembrerebbe che gli attacchi siano stati prevalentemente causati da azioni di Hacktivism, a fronte di una quota di attacchi noti realizzati dal Cyber Crime che è meno di un terzo (17%) rispetto a quella rilevata a livello internazionale (53%). Questo ci porta a supporre che la maggior parte di questo tipo di attacchi non sia di dominio pubblico (anche alla luce dei risultati dell'analisi realizzata da FASTWEB, che come vedremo più avanti, analizzando il traffico sulla propria rete, segnala una situazione diametralmente opposta).
Questa la distribuzione percentuale dei bersagli, con una netta prevalenza di vittime nell'ambito istituzionale e della politica:



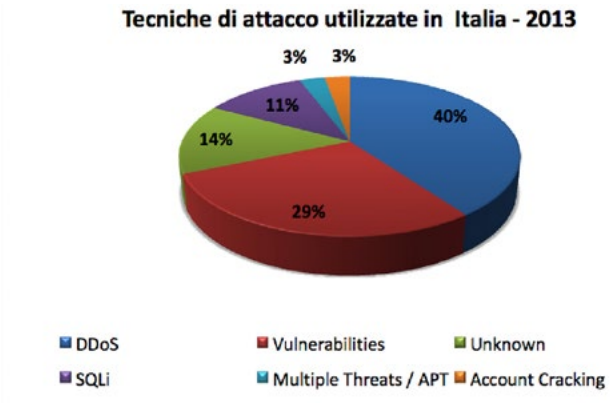
© Clusit - Rapporto 2014 sulla Sicurezza ICT in Italia

Per maggiore chiarezza espositiva abbiamo effettuato una classificazione di dettaglio delle vittime in ambito istituzionale:



© Clusit - Rapporto 2014 sulla Sicurezza ICT in Italia

Nel grafico seguente la distribuzione delle tecniche di attacco utilizzate:



© Clusit - Rapporto 2014 sulla Sicurezza ICT in Italia

In un campione dominato dalla presenza di attaccanti di tipo Hacktivist, prevalgono gli attacchi di tipo DDoS, seguiti da quelli basati sullo sfruttamento di vulnerabilità / misconfigurazioni e su SQL Injection.
D'altra parte va detto che i bersagli italiani risultano essere in media particolarmente suscettibili di compromissione anche quando gli attaccanti utilizzino tecniche banali e di semplice attuazione.
Di seguito una descrizione sintetica degli incidenti analizzati, suddivisi in tre gruppi: attacchi realizzati da hacktivist con finalità di protesta politica (principalmente ma non solo, per "solidarietà" con il movimento NoTAV), attacchi realizzati con altre finalità (principalmente in base ad istanze ambientaliste), ed attacchi realizzati con finalità di lucro (cyber crime).

1) I gruppi facenti riferimento alla "galassia" di antagonisti che utilizza il nome collettivo "Anonymous" (e sigle collegate), hanno effettuato una serie di attacchi contro istituzioni governative, partiti ed uomini politici, aziende e forze dell'ordine, riconducibili per lo più alle campagne di protesta denominate "#OpItaly", "#OpRevenge" ed "#OpTrasparenza". In particolare, in ordine cronologico:

11 marzo: Casapounditalia.org
Un attacco DDoS ha causato il disservizio del portale per diverse ore.

15 marzo: Forza Nuova, Fiamma Tricolore e Lealtà e azione
Azione dimostrativa che ha fatto seguito all'attacco verso il portale Casapounditalia.org durante la quale ben tre portali web appartenenti allo stesso schieramento politico sono stati resi irraggiungibili per diverse ore a causa di un attacco DDoS.

3 maggio: Movimento 5 stelle

Attacco durante il quale, tramite tecniche di hacking, sono stati sottratti e pubblicati dati (principalmente documenti interni ed email) di membri del movimento, per un totale di 4GB di informazioni[43].

28 marzo: coisp.it

Il primo di una serie di attacchi informatici contro le Forze dell'Ordine, realizzato colpendo in questo caso il sito di uno dei sindacati della Polizia Italiana, tramite un attacco DDoS che ha reso il servizio irraggiungibile per alcune ore[44].

20 Maggio: poliziadistato.it

L'attacco, rivendicato dal gruppo di hacktivisti, ha consentito a questi ultimi di sottrarre e pubblicare username, password e numeri telefonici (privati e non) di appartenenti alle forze dell'ordine[45].

24 Maggio: siulp.it

Attacco in cui sono stati sottratti e pubblicati dati (documenti) relativi a membri del Sindacato Unitario Lavoratori di Polizia. Successivamente il sito è stato vittima di un defacement[46].

26 Maggio: sap-nazionale.org

Attacco durante il quale sono stati sottratti e pubblicati dati relativi agli account (username & password) degli utenti del portale del Sindacato Autonomo di Polizia[47].

28 maggio: Ministero degli Interni

Attacco che ha condotto al furto di dati (documenti) dal portale del Ministero degli Interni, per un totale di circa 650 Mb di informazioni[48].

28 giugno: Casaleggio & Associati

Defacement del sito dell'azienda[49].

19-25 Ottobre: mit.gov.it, cortedeiconti.it, cassaddpp.it, sviluppoeconomico.gov.it, Ministero delle Infrastrutture e dei Trasporti, Regione Piemonte

---

43 http://www.pcprofessionale.it/2013/04/24/anonymous-e-lattacco-alle-mailbox-dei-parlamentari-m5s-e-democrazia-diretta/

44 http://www.ilfattoquotidiano.it/2013/03/28/aldrovandi-anonymous-blocca-sito-del-coisp-insabbiate-verita/545716/

45 http://www.giornalettismo.com/archives/945831/anonymous-pubblica-i-dati-dei-poliziotti-italiani/

46 http://www.ilmessaggero.it/tecnologia/hitech/anonymous_hacker/notizie/283732.shtml

47 http://www.pianetatech.it/internet/attualita/anonymous-vs-sap-sindacato-polizia-attacco-hacker-documenti-online-foto-video.html

48 http://daily.wired.it/news/internet/2013/05/28/anonymous-dati-ministero-interno-hack-52652.html

49 http://daily.wired.it/news/internet/2013/06/28/anonymous-casaleggio-attacco-56728.html

Serie di attacchi DDoS portati verso differenti bersagli che sono stati resi irraggiungibili per alcune ore[50].

9 novembre: Giuseppe Scopelliti
Attacco portato contro il sito web del governatore della Regione Calabria, durante il quale sono stati sottratti e pubblicati documenti di vario genere[51].

22 novembre: enricoletta.it, Regione Piemonte, sviluppoeconomico.gov.it, ltf-sas.com
Per solidarietà con i NoTAV, nell'ambito del #OpPayBack il collettivo Anonymous ha compiuto attacchi DDoS verso diversi siti istituzionali, rendendoli irraggiungibili per qualche ora[52].

25 novembre: Roberto Maroni
Attacco portato contro una casella di posta del presidente della regione Lombardia Roberto Maroni che ha permesso agli hacktivisti (con la sigla "CyberGuerrilla") di sottrarre diversi tipi di documenti riservati[53].

11 dicembre: Matteo Renzi
Attacco DDoS verso il portale del sindaco di Firenze e segretario del partito Democratico, messo offline per 24 ore[54].

18 dicembre: interno.gov.it, poliziadistato.it
Ennesimo attacco DDoS contro portali governativi che hanno subito un disservizio di qualche ora.

23 dicembre: Matteo Renzi
Un altro attacco verso il sito web di Matteo Renzi, questa volta un hacker denominato RenziHack è riuscito tramite una tecnica di tipo SQL Injection ad effettuare il dump di 430.000 tra username, emails, password e numeri telefonici[55].

2) Alle precedenti attività antagoniste orientate verso le istituzioni ed il mondo della politica, si aggiungono una serie di attacchi rivendicati su Twitter con l'hashtag #OperationGreenRights, effettuati tramite DDoS e compromissione di di differenti portali, con il relativo leak di credenziali di accesso. I bersagli di tali attività sono industrie/aziende ed enti regionali/ governativi, colpiti per motivazioni legate a tematiche ambientali.

---

50 http://www.squer.it/of/anonymous-con-i-notav-down-i-siti-di-mit-mse-e-regione-piemonte/

51 http://www.corrieredellacalabria.it/stories/reggio_e_area_dello_stretto/18894_ecco_cosa_c_nel_computer_di_scopelliti/

52 http://www.giornalettismo.com/archives/1230735/anonymous-allattacco-contro-la-tav/

53 http://www.lettera43.it/politica/anonymous-contro-maroni-mail-violata_43675114453.htm

54 http://www.internazionale.it/news/partito-democratico/2013/12/12/attacco-hacker-contro-sito-renzi-irragiungibile-per-24-ore/

55 http://www.wired.it/attualita/2013/12/24/renzi-hack-quando-anonymous-attacca-politici/

15 aprile: Porto di Gioia Tauro e Consiglio Regionale della Calabria
Attività effettuata per protestare contro il rigassificatore nella città di Gioia Tauro, per questo motivo il gruppo di Hacktivist ha portato contro i due target appartenenti alla regione interessata attacchi DDoS ed ha sottratto dati dal database dei siti web[56].

18 aprile: Ministero dell'Ambiente e oltoffshore.it
L'attività di protesta contro i rigassificatori continua e questa volta ad esser vittima, di attacchi DDoS sono la Olt Offshore ed il Ministero dell'Ambiente, i cui portali subiscono un disservizio di alcune ore a causa di attacchi DDoS[57].

20 aprile: Comune di Livorno, ASA SpA, Porto di Livorno, Grimaldi Lines, Grandi navi veloci e Comune Rosignano
Ancora una protesta, questa volta contro la morte dei cetacei, realizzata verso numerosi target resi irraggiungibili tramite attacchi DDoS. A tali attacchi seguono la diffusione di credenziali e dati personali di 697 utenti (username e password) sottratti ai siti colpiti[58].

3 agosto: Ministero dell'ambiente
Protesta contro i rigassificatori attuata con un attacco che ha portato a sottrarre un ampio pacchetto di dati (specifiche rigassificatori) e circa 4.000 account di utenti[59].

8 agosto: irenemilia.it , oltoffshore.it, saipem.com
Protesta contro l'inceneritore di Parma, attacco che portato il gruppo di hacktivisti a sottrarre circa 800 Mb di dati ed a realizzare il defacement di alcune pagine del sito web irenemilia.it Inoltre le proteste hanno colpito anche i portali web Oltoffshore e Saipem, con un DDoS che ha causato disservizio per circa 24 ore[60].

11 agosto: difesa.it e Comune di Niscemi
Protesta contro le antenne dell'installazione militare Muos di Niscemi. L'attacco DDoS ha messo fuori uso i siti colpiti per qualche ora. Nel contempo sono stati sottratti e divulgati documenti ufficiali tra ambasciata U.S.A., membri del governo e della Regione Sicilia[61].

30 Ottobre: eni.it, saipem.com
Attività di protesta contro i portali web delle due aziende, accusati da Anonymous di causare danni all'ambiente, sono stati oggetto di furto di vari tipi di dati tra cui spiccavano vecchi progetti di sviluppo di oleodotti e gasdotti[62].

---

56 http://www.dailygreen.it/news/item/1539-anonymous-attacca-gioia-tauro-%C3%A8-operationgreenrights.html

57 http://www.pianetatech.it/internet/attualita/ministero-dell-ambiente-risposta-anonymous-dopo-attacco-hacker-sito-comunicato.html

58 http://iltirreno.gelocal.it/cecina/cronaca/2013/04/21/news/gli-hacker-di-anonymous-rubano-i-dati-al-comune-1.6924870

59 http://www.zeusnews.it/n.php?c=19627

60 http://www.parmatoday.it/cronaca/anonymous-inceneritore-parma-iren-emilia.html

61 http://www.linksicilia.it/2013/08/no-muos-anonymous-colpisce-i-siti-del-comune-di-niscemi-e-della-difesa/

62 http://espresso.repubblica.it/attualita/2013/10/29/news/eni-saipem-hackerata-da-anonymous-1.139330

5 Novembre: enel.it

Attacco che ha permesso di sottrarre e divulgare dati relativi alla costruzione della centrale nucleare di Mochovce (Slovacchia)[63].

8 dicembre: Regione Piemonte

Protesta contro la TAV, realizzata tramite un defacement del portale web della regione Piemonte[64].

3) Infine riportiamo anche alcuni attacchi di dominio pubblico non legati a finalità di Hacktivism, tra i quali utilizzo abusivo di risorse informatiche, tentativi di estorsione, hijacking di account Facebook atti a redirigere utenti su siti malevoli, defacement e furti di dati personali con finalità varie (frodi, furti di identità), etc.

1 gennaio: CNR Genova

L'hacker ha agito via smartphone o comunque utilizzando un dispositivo mobile. Dal 28 al 31 dicembre è penetrato almeno sei volte nella rete del CNR di Genova. E' stato calcolato che nel poco tempo disponibile lo sconosciuto abbia spedito tramite i server del Consiglio Nazionale delle Ricerche oltre un milione di email[65].

17 Gennaio: Partitodemocraticotrentino.it

In prossimità del periodo elettorale un hacker chiamato @TheNeoGod è riuscito a sottrarre, tramite lo sfruttamento di tecniche di tipo SQL Injection, i dati degli utenti registrati nel portale Partitodemocraticotrentino.it

16-17 febbraio: Tribunale di Milano

Defacement del sito del Tribunale, accompagnato da un messaggio che richiama graficamente, ma non nei contenuti, le modalità utilizzate da Anonymous. La sigla che rivendica l'attacco è sconosciuta[66].

Aprile-Marzo: in.enasarco.it

L'attacco ha colpito il sito internet istituzionale di Enasarco indirizzandosi verso l'URL specifica dedicata al recupero delle password dimenticate dagli utenti registrati. In alcuni momenti la frequenza delle richieste fraudolente è stata così elevata da sovraccaricare l'intera struttura del sito (web server farm e database server)[67].

---

63 http://www.pianetatech.it/internet/attualita/anonymous-vs-enel-attacco-hacker-mail-file-online-operationgreenrights.html

64 http://www.tomshw.it/cont/news/anonymous-con-i-notav-defacing-regione-piemonte/51674/1.html

65 http://www.ilsecoloxix.it/p/genova/2013/02/25/APpWvwqE-hacker_sabotati_attacco.shtml

66 http://www.professionegiustizia.it/notizie/notizia.php?id=211

67 http://www.enasarco.it/allegati/10674465-636f-42b0-aa76-f45b457485e2.olts

8 luglio: websolutions.it

Dopo aver sottratto dati di decine di migliaia di utenti, l'attaccante ha effettuato un tentativo di estorsione verso l'azienda, chiedendo un pagamento per non diffondere i dati. Il tentativo di ricatto è fallito a causa del rifiuto dell'azienda[68].

13 luglio: sony.it

Un database della multinazionale, ospitato in Italia, contenente dati relativi a promozioni effettuate da Sony Italia con dati relativi al 2006/2007 è risultato essere stato violato consentendo il furto di dati anagrafici quali nome, cognome, indirizzo, mail, numero di telefono ed anno di nascita, tuttavia il database violato non conteneva dati relativi a carte di credito[69].

12 settembre: Alpitour, Francorosso, Viaggidea, e Villaggi Bravo

Gli account delle diverse pagine Facebook del Gruppo Alpitour sono stati sottratti da cyber criminali egiziani, che hanno iniziato a pubblicare a nome dell'Azienda link malevoli, al fine di redirigere gli utenti su pagine infette da malware (Zeus). Il malware tentava di infettare i sistemi e di effettuare il furto di credenziali bancarie delle vittime. L'attacco è durato almeno 48h prima di essere risolto, con il recupero del controllo delle pagine Facebook[70].

30 novembre: Regione Lombardia

Ignoti attaccanti hanno messo fuori servizio il portale della Regione per diverse ore[71].

---

68 http://news.softpedia.com/news/Rex-Mundi-Hackers-Blackmail-Italian-Hosting-Service-Websolutions-it-366685.shtml

69 http://www.dday.it/redazione/10093/Violato-un-datato-database-di-Sony-Italia.html

70 http://www.lastampa.it/2013/09/15/italia/cronache/alpitour-cyberattacco-via-facebook-false-offerte-per-rubare-dati-agli-utenti-6XHELfHFLlVuGq5RfstdMO/pagina.html

71 http://www.ecodibergamo.it/stories/Cronaca/il-sito-di-regione-lombardia-sotto-attacco-da-parte-degli-hacker_1035303_11/

Analisi FASTWEB della situazione italiana in materia di cyber-crime e incidenti informatici

I dati analizzati

Per riuscire a comprendere al meglio i contenuti dell'analisi svolta è necessario una premessa in merito al tipo di dati utilizzati per realizzarla.
Il perimetro dei dati analizzati è costituito da tutti i dati relativi ai circa 200.000 indirizzi IP appartenenti all'Autonomous System dell'Internet Service Provider FASTWEB SpA (quindi sia quelli dei Clienti che di FASTWEB stessa), raccolti ed analizzati dal Security Operations Center.
In particolare:

- i dati relativi a malware e botnet (virus, trojan e più in generale software malevolo) sono stati ricavati da un mix di strumenti interni e da servizi esterni come Shadowserver Foundation;
- I dati relativi ai defacement sono stati ricavati sia da segnalazioni ricevute internamente che da fonti aperte ed archivi disponibili su Internet;
- I dati sui Distributed Denial of Service sono stati ricavati da tutte le anomalie DDoS rilevate dai sistemi di DDoS mitigation.

È importante sottolineare che tutti i dati, prima di essere analizzati, sono stati automaticamente aggregati e anonimizzati per proteggere la privacy e la sicurezza sia dei Clienti che di FASTWEB stessa.

Visione d'insieme

Nel 2013 la situazione italiana nel complesso appare paradossale. Se da una parte infatti il mercato della sicurezza informatica rimane uno dei pochi che continua a crescere e la richiesta di figure professionali continua ad essere maggiore rispetto alla disponibilità di risorse sul mercato, dall'altra parte pur incrementando o mantenendo costante il budget, il livello di sicurezza delle aziende italiane continua a scendere.
Questo fenomeno è legato al fatto che la sensibilità rispetto alle tematiche di sicurezza continua a viaggiare ad una velocità estremamente inferiore rispetto all'evoluzione delle minacce. Nel necessario trade-off tra necessità di business e requisiti di sicurezza, questi ultimi finiscono per essere messi da parte, il che favorisce gli attaccanti, incrementando la percentuale di attacchi che riescono ad andare a segno.
Per quanto riguarda la tipologie e le finalità degli attaccanti, lo scenario si è in pochi anni modificato radicalmente. Mentre in origine gli attaccanti erano principalmente Hackers, oggi si tratta principalmente di criminali che acquistano strumenti offensivi sviluppati da terzi per realizzare le loro attività illecite.

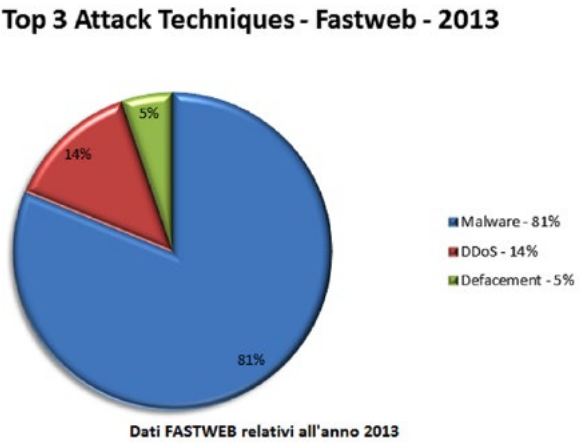
Due fenomeni In particolare hanno impresso un'ulteriore accelerazione a questo fenomeno: il primo è la diffusione delle crypto-monete (la più famosa è il "Bitcoin", nata nel 2009),

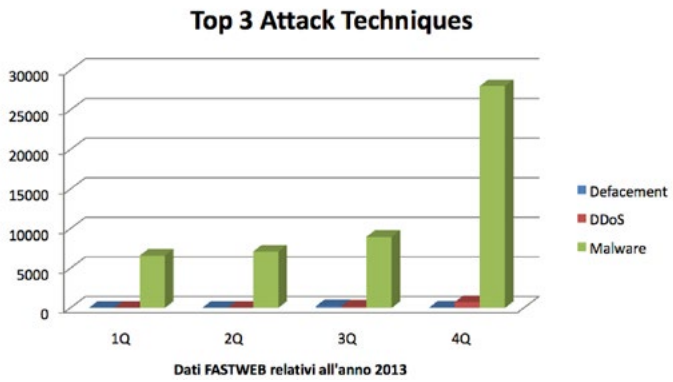
diventate molto popolari tra i criminali perché consentono di svolgere attività di cash-out in modo sostanzialmente non tracciabile, il secondo è l'aumentare dei "click-fraud" cioè delle frodi legate ai click sui banner e pubblicità online di altro tipo.
Si è notato infatti un incremento enorme di malware sviluppato sia con lo scopo di rubare questo tipo di moneta che di sfruttare la potenza computazionale dei sistemi compromessi per generare questo tipo di crypto-monete, aumentando così il valore del proprio portafoglio virtuale.
Tecniche e conoscenze che un tempo erano appannaggio di appassionati e curiosi, ormai sono utilizzate oltre che dagli ambiti criminali anche da quelli antagonisti, terroristi e per finalità militari, con tutt'altri scopi rispetto a quelli con cui erano originariamente nati.
Fortunatamente però anche quest'anno non vi sono stati, in Italia, casi documentati di Cyber Terrorism nè di Information Warfare (escludendo il caso Datagate).
Da sottolineare inoltre la tendenza ad un cambiamento in positivo della visione delle pubbliche amministrazioni, che si dimostrano sempre più affamate di saperi, consapevoli e decise a condividere le proprie conoscenze ed esperienze.

Le minacce

Le principali minacce

Com'era immaginabile, la maggior parte delle minacce arrivano ancora tramite software malevoli utilizzati principalmente per due tipologie di attività: crimine e spionaggio industriale.
Gli attacchi DDoS crescono invece in maniera esponenziale rispetto agli scorsi anni e costituiscono il 14% degli eventi rilevati, confermando la tesi per cui la possibilità di essere colpiti da uno di essi è più probabile di quanto si pensi.
Scendono invece i defacement, cioè le azioni volte a modificare una o più pagine web di un sito (per lo più per motivi dimostrativi).
Questi numeri assumono tali proporzioni in quanto sia virus che più in generale i malware costituiscono la categoria più "consolidata" di minacce informatiche ed accessibile per chiunque si dedichi a questo tipo di attività. Lanciare attacchi tramite malware è, oltre che molto remunerativo, estremamente poco rischioso in quanto raramente gli autori di un malware vengono rintracciati. L'impennata rilevata nell'ultimo trimestre del 2013 non deve preoccuparci in quanto è dovuta all'evoluzione delle tecniche di rilevazione di nuovi malware che prima rimanevano "invisibili" alle nostre statistiche.
Ovviamente, a causa della loro natura, non è dato sapere quale sia il valore di altre categorie, sicuramente meno appariscenti in termini di quantità ma non meno in termini di minaccia come gli APT (Advanced Persistent Threat) o più in generale attacchi 0day.
Questo tipo di minacce infatti, sono estremamente difficili da intercettare ed allo stesso tempo costituiscono una percentuale estremamente bassa in quanto tali tecniche vengono utilizzate per attacchi mirati che raramente vengono scoperti.



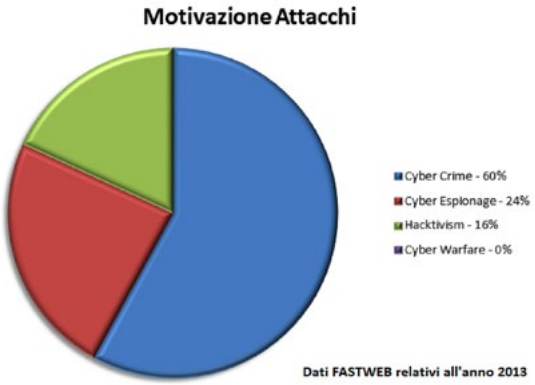


Motivazioni degli attacchi monitorati

Prima di andare avanti occorre sottolineare che i successivi dati sono relativi **unicamente agli attacchi individuati sulla rete FASTWEB**, e contengono quindi tutti i tipi di attacco, indipendentemente dal loro impatto. Tali dati pertanto possono risultare discordanti con il campione Clusit riportato in precedenza, in quanto questi riporta una macrovisione unicamente legata agli attacchi più gravi divenuti di dominio pubblico registrati nel mondo (Italia inclusa) nel corso del 2013.

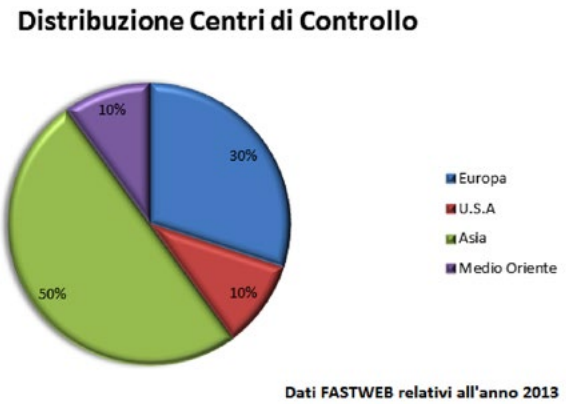
Come già sottolineato nella visione d'insieme, oggi la motivazione principale per cui vengono compiuti attacchi informatici è di natura criminale. In particolare il 60% degli attacchi è dovuto ad azioni di cybercrime ed il 24% ad azioni di spionaggio industriale volto a sottrarre informazioni (progetti, dati di business, o documenti).

Le azioni dimostrative, portate avanti tramite attacchi informatici (Hacktivism), sebbene abbiano conquistato dall'estate in poi, quasi settimanalmente, le prime pagine dei giornali, costituiscono in realtà solamente il 16% degli attacchi rilevati.



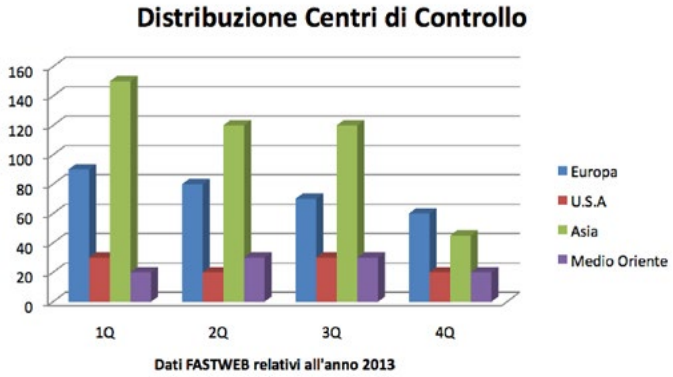
Origine degli attacchi

Pur essendo quasi impossibile riuscire a capire quale sia l'origine esatta di un attacco in quanto l'attaccante potrebbe lanciare un attacco rimbalzando su un qualsiasi altro server in giro per il mondo, abbiamo analizzato il dato che più gli si avvicina, cioè la localizzazione dei server utilizzati come centri di controllo (Command and Control).
I risultati confermano quanto gli studi già ci dicevano, cioè che la maggior parte di questi attacchi (50%) ha come origine l'Asia. L'Europa costituisce la seconda origine (30%) mentre Stati Uniti e Medio Oriente sono rispettivamente al terzo e quarto posto (10% ognuno).



Distribuzione dei centri di controllo durante l'anno

Interessante notare che mentre nel primo trimestre questa percentuale era fortemente sbilanciata in favore dell'Asia, questa differenza si è andata affievolendo fino ad invertire la tendenza nel quarto trimestre grazie ad un calo verticale della regione asiatica.
Inoltre un altro fattore molto interessante da analizzare è la sostanziale diminuzione dei centri di controllo rilevati. Se si considera il forte exploit avvenuto durante il primo trimestre ed un periodo di "assestamento" del numero dei centri di controllo rilevato durante il secondo ed il terzo, assistiamo ad un vero e proprio crollo del numero di questi durante l'ultima parte dell'anno.
Non bisogna tuttavia commettere l'errore di credere che la rilevazione di un minor numero di centri di controllo sia direttamente proporzionale ad un minor numero di infezioni, ciò è sbagliato, tuttavia è un fenomeno di cui tener conto e che può lasciar spazio a diverse interpretazioni.

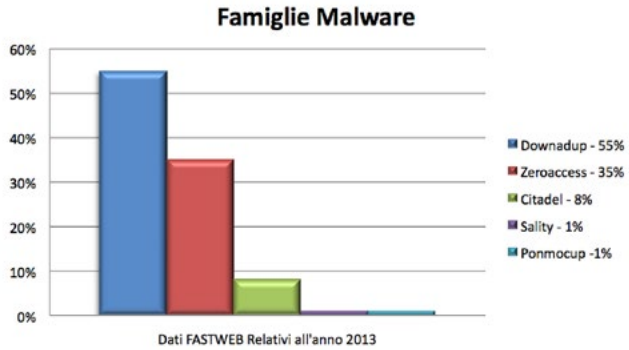


Tipologie di malware rilevate

Abbiamo visto che I malware costituiscono la grande maggioranza delle minacce rilevate, questo fenomeno è infatti probabilmente dovuto a due motivi: il fatto che i malware sono una minaccia storica e consolidata ed il fatto che, di rimando, le tecnologie per il loro contrasto siano altrettanto consolidate ed evolute.

In questo caso sono state fatte due differenti statistiche:
La prima è relativa ai malware che infettano sistemi Windows, in cui è lampante il predominio di due tipologie di malware molto conosciute: Downadup e ZeroAccess.
Downadup anche conosciuto come Conficker, Downdup o Kido worm del 2008, sfrutta vulnerabilità del 2008 e del 2009 (a seconda della variante), si diffonde ancora probabilmente in gran parte grazie alle condivisioni di rete senza protezione o con password debole.
ZeroAccess, (anche conosciuto come Sirefef), è invece un Trojan horse che colpisce i sistemi operativi Microsoft Windows. Le sue capacità di diffusione sono molteplici: tramite

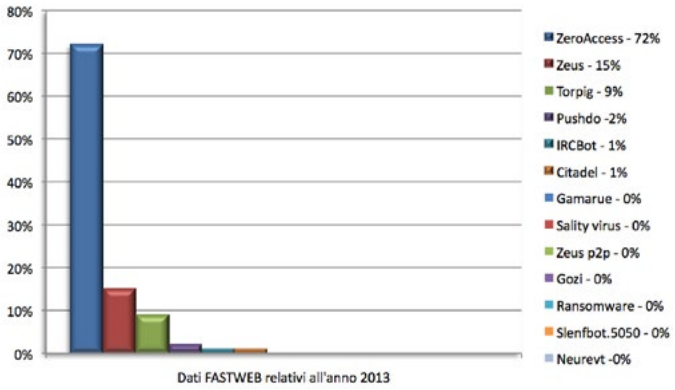
siti web che sfruttano delle vulnerabilità di browser o plugin, attraverso l'esecuzione di eseguibili contenenti codice malevolo (come ad esempio i file di tipo keygen che facilmente trovano terreno fertile nell'ambito P2P) o tramite l'installazione diretta da parte di terzi che hanno ottenuto un accesso diretto.
La sua attività consiste nell' effettuare il download di altri malware sugli host infetti al fine di formare botnet per lo più coinvolte in "Bitcoin mining" (generazioni di crypto-moneta) e "click fraud", inoltre ha la capacità di nascondersi grazie ad alcune caratteristiche tipiche dei rootkit.



La botnet ZeroAccess (conosciuta anche come ZAccess o Siref) conta, nel mondo, più di 2 milioni di host infetti, e proprio agli inizi di Dicembre 2013, un colosso del settore informatico[1], in collaborazione con altre organizzazioni governative e non, ha effettuato un'attività di bonifica di 18 "Centri di Controllo" isolandone la componente "click fraud".
Tuttavia è stato calcolato che ancora più del 60% dei "Centri di Controllo" è rimasto attivo, grazie alla capacità di ZeroAccess di propagarsi tramite connessioni P2P. Ciò ha portato a definire il tentativo di Microsoft & co., un fallimento.

La seconda statistica elaborata, rappresenta invece le tipologie di botnet rilevate.
Considerando quindi che la botnet di ZeroAccess, nonostante il tentativo di bonifica effettuato in Dicembre, conti ancora milioni di host infetti, non c'è da sorprendersi che questa ricopra quasi il 75% dei malware facenti parte di botnet rilevate, soprattutto se si considera la capacità di questi di propagarsi tramite P2P ed un mix di ulteriori altri tecniche.

[1] Fonte: http://arstechnica.com/security/2013/12/microsoft-disrupts-botnet-that-generated-2-7m-per-month-for-operators/

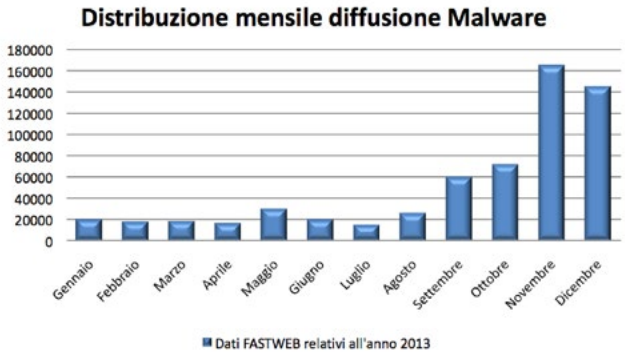


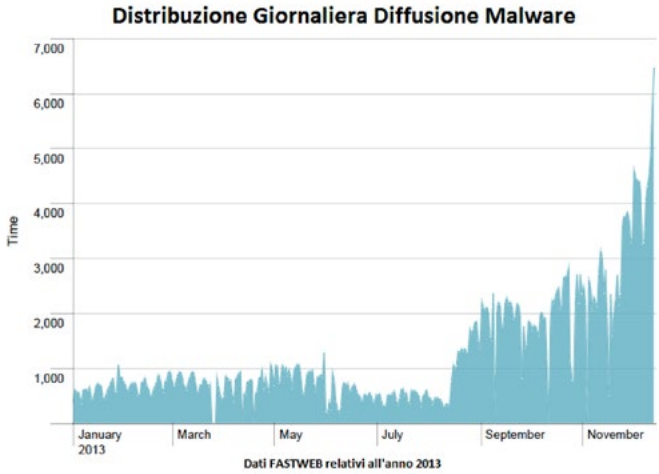
Una parte meno corposa è invece rappresentata dalla già nota botnet del malware trojan Zeus aka Zbot, malware che può essere generato tramite l'utilizzo di un kit, distribuito intorno al 2008, il quale permette di crearne il codice senza avere particolare competenze. Questa particolarità ha favorito, negli anni, il proliferare di centinaia di differenti tipologie di versioni dello stesso malware, facendo sì che sia attualmente riconosciuta come la più grande famiglia malware presente su internet.

Distribuzione mensile della diffusione di malware

I dati FASTWEB, relativi alla diffusione malware, e riportati nel grafico sottostante, sono eloquenti. Nonostante durante la maggior parte del 2013 si sia verificato un trend abbastanza costante, relativo al numero degli host infetti, dal mese di settembre assistiamo ad una crescita esponenziale dovuta all'improvvisa diffusione sulla rete del malware Zeroacces, il quale in soli 3 mesi costituisce più del 70% dei malware rilevati.

Si ricorda che i dati esposti sono aggregati e statistici, per quanto più granulari possibili, la rilevazione malware viene ottenuta su base giornaliera, tali dati poi sono stati successivamente aggregati e distribuiti su scala mensile, pertanto non stiamo parlando di host infetti "univoci".



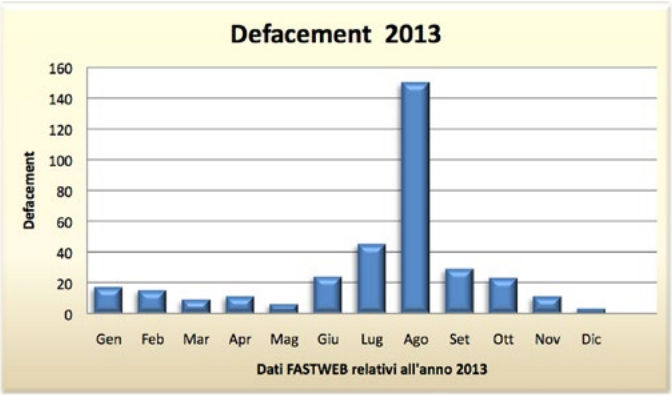


Defacement

Quanti sono i defacement

Un altro diffuso scopo degli attacchi sono i defacement, cioè la variazione di una pagina web (tipicamente la home page) a scopi dimostrativi. Come possiamo facilmente notare dai grafici, questo tipo di attività non ha una enorme diffusione e raggiunge un picco solo nel mese di Agosto, probabilmente a causa del fatto che le motivazioni legano queste attività al "tempo libero".

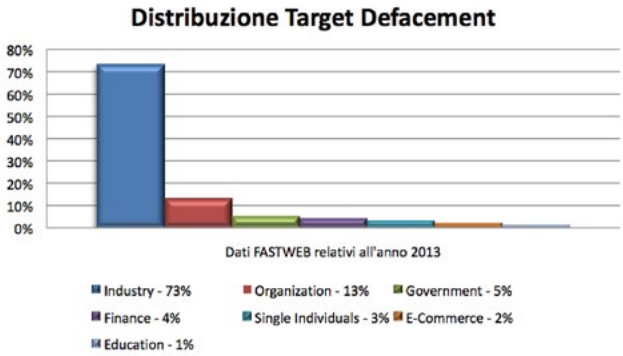
In questo caso la base di dati analizzata sono, come già specificato, tutti i siti web di Clienti che hanno un IP appartenente all'Autonomous System di FASTWEB.



Chi è obiettivo di un defacement

I dati esaminati durante l'anno, relativi ai defacement, indicano che i principali obiettivi di tale tipologia di attacco sono appartenenti al settore privato, in particolare aziende ed industrie.

Il settore relativo alle organizzazioni (associazioni private, no profit etc.) viene subito dopo seppur rappresentandone una fetta decisamente più piccola. Successivamente abbiamo defacement portati contro target di ambito governativo (principalmente siti web relativi ai comuni di determinate città italiane) e finanziario.
Le briciole vere e proprie sono rappresentate da attacchi portati contro siti web di persone private (personaggi dello spettacolo o appartenenti al mondo della politica), portali e-commerce e educazione (in particolare siti web di scuole).



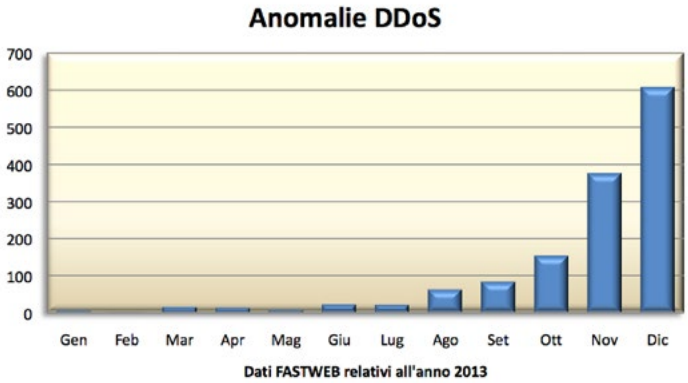
Attacchi DDoS (Distributed Denial of Service)

Un capitolo a parte viene costituito dagli attacchi di tipo Distributed Denial of Service (DDoS), attacchi volti a rendere inaccessibili alcuni tipi di servizi (principalmente web e mail).

Questo genere di attacchi possono essere divisi in due tipologie differenti: **volumetrici** e **applicativi**.
Gli attacchi di tipo **volumetrico** mirano a generare un volume di traffico maggiore o uguale alla banda disponibile in modo da saturarne le risorse.
Gli attacchi di tipo **applicativo** mirano a generare un numero di richieste maggiore o uguale al numero di richieste massimo a cui un server può rispondere (es. numero di richieste web HTTP/HTTPS concorrenti).
Come più volte sottolineato, compiere questo genere di attacchi è divenuto sempre più semplice, soprattutto grazie a servizi facilmente acquistabili tramite carte di credito prepagate e bitcoin che permettono di effettuare questi attacchi senza possedere pressoché alcuna capacità tecnica particolare.

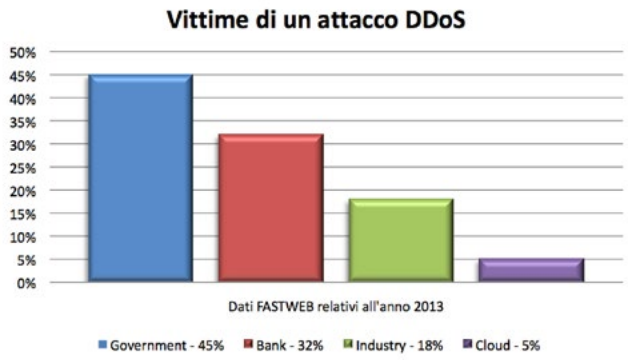
Quanto è diffuso il fenomeno

Durante il 2013 abbiamo rilevato più di 1000 anomalie riconducibili a probabili attacchi DDoS, dirette verso i Clienti di FASTWEB, un crescendo esponenziale che ha avuto un culmine negli ultimi due mesi dell'anno con quasi 400 anomalie a Novembre e 600 a Dicembre. Questi dati ci fanno capire chiaramente che il fenomeno è molto più diffuso di quanto si pensi. La tendenza è pensare che questo tipo di attacchi vengano portati solamente verso siti istituzionali e siti vetrina, la realtà è che invece questo tipo di attacchi colpisce un po' tutti i settori e non sono più solo indirizzati verso i siti vetrina ma anche verso il cuore della comunicazione, per esempio la posta elettronica.



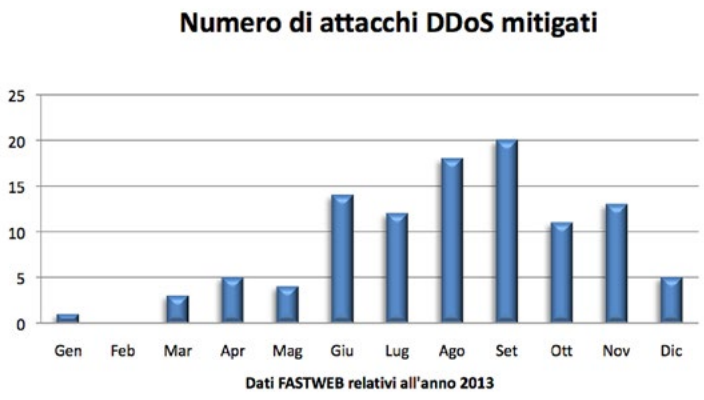
Le vittime di un attacco DDoS

La rilevazione effettuata durante l'anno indica che i tre principali obiettivi degli attacchi DDoS sono le istituzioni governative (Ministeri, Pubbliche Amministrazioni locali e centrali, etc), le banche ed il settore industriale.
Questra rilevazione rappresenta una statistica immaginabile in quanto il network di attivisti "Anonymous", che svolge principalmente delle azioni dimostrative di protesta tramite attacchi di questo tipo verso le istituzioni, è stato parecchio attivo, soprattutto durante la seconda parte dell'anno.
È interessante sottolineare che, dalle analisi svolte, la totalità degli attacchi diretti verso il settore governativo non aveva, almeno apparentemente, finalità di cyber warfare ma era solamente frutto di azioni dimostrative.



Distribuzione mensile delle mitigation attivate

Di seguito viene riportata la distribuzione mensile delle mitigation attivate dal Security Operations Center di FASTWEB. Con mitigation vengono intese le attività di contromisura applicate al fine di neutralizzare gli attacchi DDoS. Tali contromisure vengono applicate solo nel caso in cui, a seguito di analisi specialistica, l'anomalia di traffico rilevata e registrata dagli strumenti sia classificata come attacco conclamato ed il Cliente abbia richiesto l'attivazione della protezione.

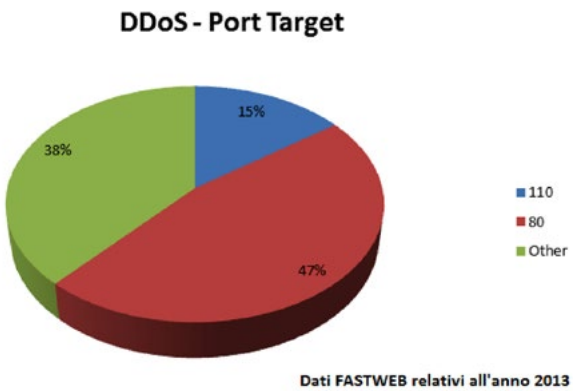


Come vengono effettuati gli attacchi DDoS

Passiamo quindi ad un'analisi delle modalità con cui gli attacchi vengono effettuati.

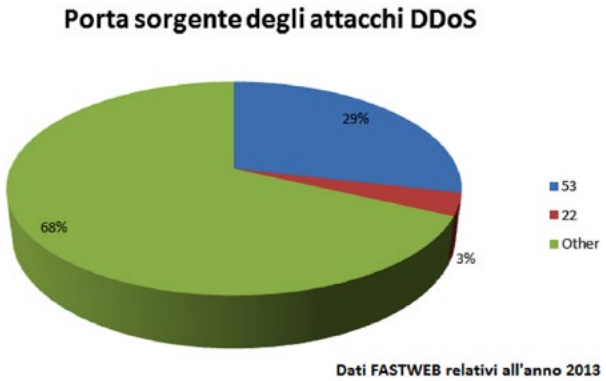
Quali sono i servizi attaccati da un ddos

Com' è possibile verificare dal grafico sotto riportato, gli attacchi DDoS vanno maggiormente ad impattare i servizi web, attaccando il protocollo http e quindi mirando a rendere tali servizi irraggiungibili dagli utenti. Tuttavia non è l'unico caso registrato, sono stati verificati anche casi in cui gli attacchi DDoS sono stati mirati a negare altre tipologie di servizi come, ad esempio, la posta elettronica, cercando di saturare il servizio POP3 associato alla posta in ingresso.



Distribuzione source port

Le due porte sorgenti più utilizzate durante gli attacchi sono la 53 e la porta 22. La rilevazione di un così alto numero di attacchi provenienti dalla porta 53, è dovuta a tecniche di dns amplification. Nel 68% degli attacchi, la porta sorgente era invece casuale, tipico comportamento di tecniche di syn flood.



Tecniche di attacco utilizzate

Le tecniche di attacco utilizzate durante l'esecuzione dei DDoS rilevati, non presentano grosse novità tecniche.

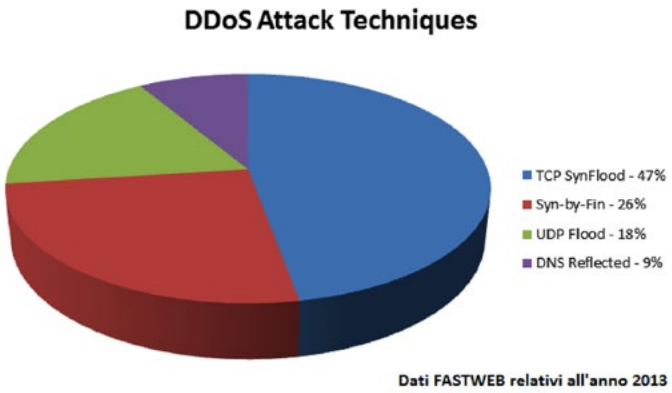
La maggior parte degli attacchi rilevati è rappresentata da "TCP Synflood" (o half open) tramite il quale l'attaccante, forgiando pacchetti SYN in cui è falsificato l'IP mittente (spesso inesistente), impedisce la corretta chiusura del three-way handshake, in quanto, nel momento in cui il server web vittima invia il SYN/ACK all'IP sorgente (ricordiamo inesistente), questi non ricevendo alcun ACK di chiusura lascerà la connessione "mezza aperta", se quindi l'host attaccante, invia un numero elevato di pacchetti SYN e se a questo associamo anche alti tempi di timeout delle connessioni, il buffer del server sarà presto saturo e reso inagibile ad accettare ulteriori connessioni TCP, anche se legittime.

Successivamente c'è la variante "al contrario" della precedente tipologia di attacco, denominata "SYN-BY FIN" durante la quale l'attaccante crea delle connessioni legittime e di breve durata con il server target, successivamente cerca di abbattere tali connessioni inviando dei pacchetti FIN verso l'host vittima. Quest'ultimo invierà all'attaccante un pacchetto FIN/ACK e rimarrà (come nel caso delle connessioni mezze aperte) in vana attesa del l'ACK finale per chiudere la connessione. Ed anche in questo caso, un elevato numero di pacchetti FIN può portare a saturare il buffer e quindi a causare un disservizio.

Successivamente abbiamo attacchi di tipo "UDP Flood" molto facile da attuare in quanto a differenza del protocollo TCP non prevede l'instaurazione di una connessione vera e pro-

pria, possiede tempi di trasmissione e risposta estremamente ridotti ed ha quindi maggiori probabilità di esaurire il buffer tramite il semplice invio massivo di pacchetti UDP verso l'host target dell'attacco.

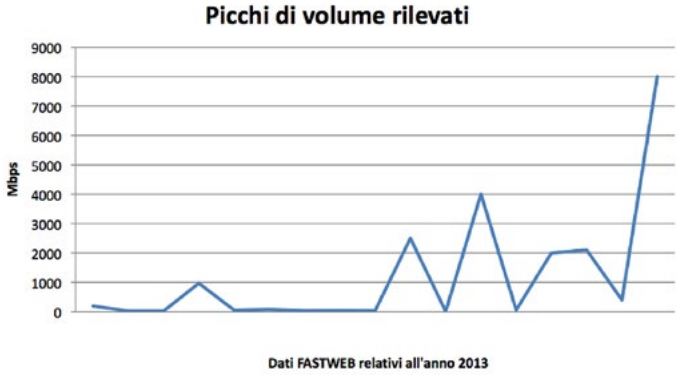
In ultima analisi vi sono i **DRDoS – Distributed Reflection Denial of Service**, anche se nel caso specifico si tratta di **DNS Reflected**, la cui particolarità è quella di sfruttare appunto server DNS come riflettori, tuttavia proprio la struttura dei DNS permette di amplificare il volume dell'attacco. Tramite lo spoofing dell'indirizzo IP di una vittima, un utente malintenzionato può inviare piccole richieste ad un server DNS chiedendogli quindi di inviare alla vittima "risposte" ripetute e assolutamente non volute/richieste. Questa tipologia di DDoS permette al malintenzionato di amplificare la potenza del suo attacco anche di 70 volte.



Qual è il volume degli attacchi ddos

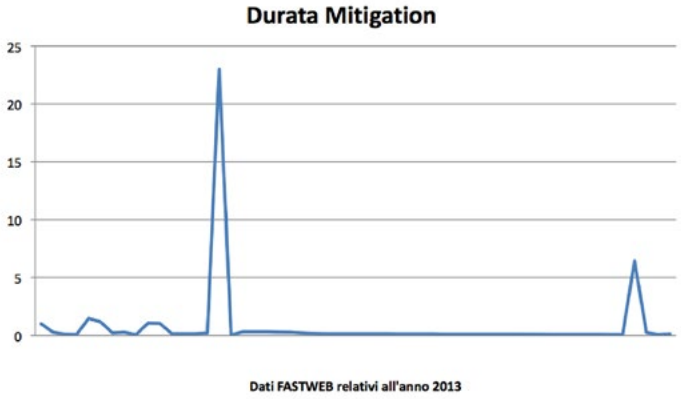
I volumi degli attacchi registrati durante il 2013 hanno avuto una particolare tendenza a crescere. Nonostante durante la prima parte dell'anno non abbiano mai superato 1Gb di traffico, abbiamo assistito, durante la seconda parte dell'anno ad un sostanziale aumento dei picchi di intensità, questo anche grazie alla sempre più facile possibilità di ottenere una maggiore potenza d'attacco.

Grazie all'utilizzo di botnet e host zombie a pagamento, la totalità degli attacchi rilevati è riuscita a saturare, la banda a disposizione degli host vittima.



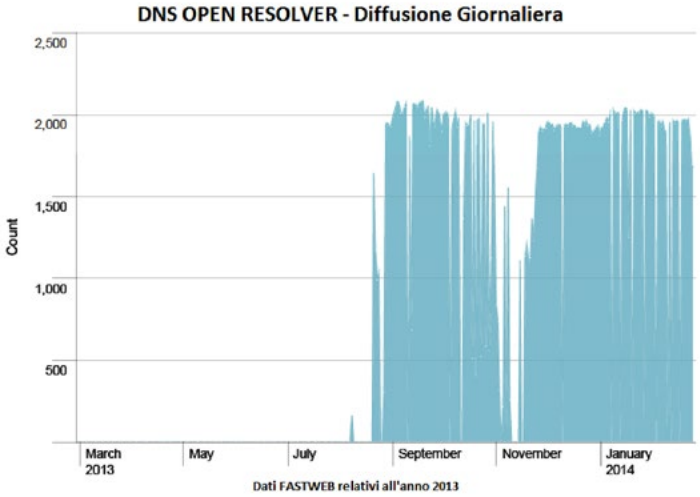
Quanto dura un attacco DDoS

I dati forniti dal Security Operations Center di FASTWEB sono eloquenti, descrivendo uno scenario di attacchi, fatta esclusione di qualche eccezione, relativamente brevi, la cui durata è in media di 1 ora.
Si può inoltre affermare che la durata degli attacchi è stata sicuramente influenzata dal fatto che questi siano stati neutralizzati con successo, il che ha portato l'attaccante ad interrompere la sua attività nel momento in cui questa gli sia risultata inefficace.



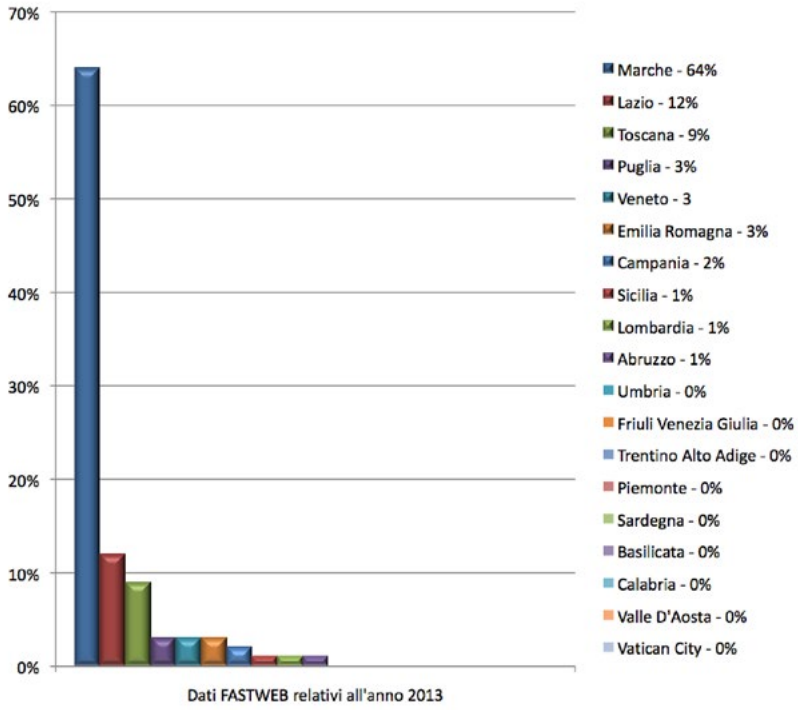
Il Problema dei DNS open resolver

Tramite l'interrogazione di tutti i computer con indirizzi IPv4, non protetti da firewall e con servizio DNS attivo su porta 53/udp, e catturando la risposta data dal servizio DNS è stato possibile stilare una classifica delle regioni e città Italiane dove sono presenti potenziali server utili ad attacchi di tipo DNS Amplification.
I dati rilevati nel corso della seconda metà del 2013 mostrano un numero abbastanza omogeneo di DNS Open Resolver rilevati giornalmente, la cui media, fatta eccezione per alcuni casi, è intorno ai 2000 indirizzi IP.



Inoltre si evince che la regione dove risultano essere presenti più server utili ad essere sfruttati, inconsapevolmente, per fini malevoli, è la regione Marche. La differenza con le altre regioni, in termini di quantità, risulta essere notevole. La regione Lazio rappresenta "solo" il 12% della totalità dei dns open resolver, seguito da un 9% della Toscana per poi andare a ridursi ad un mero 3% rispettivamente di Puglia, Veneto ed Emilia Romagna.

Si ricorda che i dati, unicamente relativi all'AS di FASTWEB, sono rilevati nell'ordine di migliaia di indirizzi IPv4, aggregati e riportati in un grafico esplicativo.
Si fa inoltre presente che l'attività di rilevazione di tali dati è iniziata durante il mese di Agosto 2013.



Considerazioni Finali

Per prima cosa dobbiamo assolutamente essere coscienti della situazione non affatto rosea in cui ci troviamo: il gap tra il livello di protezione delle aziende e l'evoluzione delle nuove minacce è in continua crescita questo gap si concretizza di un aumento della percentuale di attacchi che, con un minimo di buona volontà, possono andare a segno.
I fattori che contribuiscono a fare in modo che questo accada sono moltemplici: i tempi necessari a pianificare gli investimenti sono troppo lunghi rispetto all'evoluzione delle minacce, c'è una tendenza a far nascere per ogni nuova minaccia una nuova tecnologia che finisce spesso per essere dimenticata dopo poco tempo, c'è una mancanza di un punto di riferimento serio ed affidabile che funga, non tanto da coordinamento, ma quantomeno da faro per poter fornire una visuale chiara di quello che sta succedendo ed infine vi è una quasi totale assenza di volontà di condividere le informazioni.
Allora quali sono le azioni che dovremmo mettere in campo per riuscire ad invertire questa tendenza?
Dobbiamo consolidare e concentrare le tecnologie, frenando l'inutile tendenza a riempirci di piattaforme troppo verticali. I tempi di progettazione, approvvigionamento, configura-

zione e messa in esercizio finiscono spesso per arrivare fuori tempo massimo rispetto alla minaccia. Inoltre dopo breve tempo c'è il forte rischio che ne venga trascurata la manutenzione rendendo la tecnologia inefficace.
Piuttosto, soprattutto nel caso delle piccole e medie aziende, meglio definire il livello di sicurezza che si intende raggiungere e rivolgersi a professionisti per l'ottenimento dello stesso. Questo permetterà di dedicarsi unicamente alle attività core per l'azienda evitando di sprecare risorse in un campo che segue delle dinamiche di evoluzione troppo elevate rispetto alle energie che un'azienda di queste dimensioni può investire.
Ci auguriamo infine che si assista alla nascita di un centro unico, super partes, che sia in grado di raccogliere informazioni provenienti dai maggiori attori nel campo IT, Telecomunicazioni ed infrastrutture sparse sul territorio nazionale, per elaborarle, presentarle e renderle facilmente fruibili a chiunque, al fine di poter ottenere una vista globale ed indipendente dello stato relativo alle minacce presenti ed alle tendenze per il futuro.

BIBLIOGRAFIA

Oltre alle fonti già citate in questa «Panoramica degli eventi di cyber-crime e incidenti informatici più significativi del 2013 e tendenze per il 2014», segnaliamo altre fonti e Report che abbiamo preso in considerazione.

[1] *Frodi nel mondo Mobile - Minacce nel mondo Mobile e il mercato underground* – APWG
http://docs.apwg.org/reports/mobile/apwg_mobile_fraud_report_2013_Italia_CLUSIT.pdf

[2] Supplemento a Frodi con Dispositivi Mobili – Maggio 2013 - *Crimeware dei dispositivi mobili ed il mercato dei servizi illeciti* – APWG
http://docs.apwg.org/reports/mobile/apwg_mobile_report_supplement_2013_Italia_CLUSIT.pdf

[3] *Cisco 2014 Annual Security Report* - CISCO
www.cisco.com/web/offers/lp/2014-annual-security-report/index.html

[4] *Panorama de la Cyber-Crminalité* – CLUSIF
www.clusif.asso.fr/fr/production/ouvrages/type.asp?id=CYBER%2DCRIMINALITE

[5] *Can Recent Attacks Really Threaten Internet Availability?* - ENISA
www.enisa.europa.eu/publications/flash-notes/flash-note-can-recent-attacks-really-threaten-internet-availability/at_download/fullReport

[6] ENISA Threat Landscape, Mid-year 2013 - Reality check of 2012's assessment and more - ENISA
www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-mid-year-2013/at_download/fullReport

[7] *Cloud Security Incident Reporting - Framework for reporting about major cloud security incidents* - ENISA
www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/incident-reporting-for-cloud-computing/at_download/fullReport

[8] *ENISA Threat Landscape 2013 - Overview of current and emerging cyber-threats* - ENISA
www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape-2013-overview-of-current-and-emerging-cyber-threats/at_download/fullReport

[9] *Smart Grid Threat Landscape and Good Practice Guide* - ENISA
www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/sgtl/smart-grid-threat-landscape-and-good-practice-guide/at_download/fullReport

[10] *Risks of using discontinued software* – ENISA
www.enisa.europa.eu/publications/flash-notes/flash-note-risks-of-using-discontinued-software/at_download/fullReport

[11] *Feasibility study and preparatory activities for the implementation of a European Early Warning and Response System against cyber- attacks and disruptions* – EUROPEAN COMMISSION
http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=4438

[12] http://hackmageddon.com/2013-cyber-attacks-timeline-master-index/

[13] *TID14028USEN-02 IBM Security Directory Integrator - Simplifying identity silos and cloud integrations* - IBM
www-01.ibm.com/common/ssi/cgi-bin/ssialias?subtype=SP&infotype=PM&appname=SWGE_TI_SE_USEN&htmlfid=TID14028USEN

[14] *IBM X-Force 2013 Mid Year Trend and Risk Report* - IBM
https://www14.software.ibm.com/webapp/iwm/web/signup.do?lang=it_IT&source=swg-IT_WEB-ORG_Tivoli&S_PKG=ov16986

[15] *A new standard for security leaders: Insights from the 2013 IBM Chief Information Security Officer Assessment* - IBM
www14.software.ibm.com/webapp/iwm/web/signup.do?lang=it_IT&source=swg-WW_Security_Organic&S_PKG=ov17975&S_TACT=102KX1JW

[16] *IBM Security Services Cyber Security Intelligence Index - Analysis of cyber security attack and incident data from IBM's worldwide security operations* - IBM
http://public.dhe.ibm.com/common/ssi/ecm/en/sew03031usen/SEW03031USEN.PDF

[17] *Responding to—and recovering from—sophisticated security attacks - The four things you can do now to help keep your organization safe* - IBM
www-01.ibm.com/common/ssi/cgi-bin/ssialias?infotype=SA&subtype=WH&htmlfid=SEW03029USEN

[18] *Data Breaches - Identity Theft Resource Center* –(idtheftcenter.org)
www.idtheftcenter.org/id-theft/data-breaches.html

[19] *Cyber threat intelligence and the lessons from law enforcement* - KPMG
www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-threat-intelligence-final3.pdf

[20] *Future State 2030: The global megatrends shaping governments* - KPMG
www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/future-state-government/Documents/future-state-2030-v3.pdf

[21] *McAfee® Labs: le previsioni sulle minacce per il 2014* - MCAFEE
www.mcafee.com/it/resources/reports/rp-threats-predictions-2014.pdf

[22] *Rapporti semestrali* – MELANI
www.melani.admin.ch/dokumentation/00123/00124/01555/index.html?lang=it

[23] *2013 Italian Cyber Security Report - Critical Infrastructure and Other Sensitive Sectors Readiness - Research Center of Cyber Intelligence and Information Security* "SAPIENZA" - Università di Roma
www.dis.uniroma1.it/~cis/media/CIS%20Resources/2013CIS-Report.pdf

[24] *2014: attacco agli smartphone e al mobile banking - Dai dispositivi mobile presi sempre più di mira fino alle grandi violazioni di dati*. – TREND MICRO
www.trendmicro.it/newsroom/pr/-attacco-agli-smartphone-e-al-mobile-banking/index.html

[25] *L'Italia conquista il bronzo nella classifica delle nazioni che spammano di più* – TREND MICRO
www.trendmicro.it/newsroom/pr/italia-conquista-il-bronzo-nella-classifica-delle-nazioni-che-spammano-di-pi/index.html

[26] *Nel mirino degli hacker la piattaforma Android e l'online banking: ecco quanto rivela il nuovo report Security Roundup di Trend Micro* – TREND MICRO
www.trendmicro.it/newsroom/pr/nel-mirino-degli-hacker-la-piattaforma-android-e-lonline-banking-ecco-quanto-rivela-il-nuovo-report-security-roundup-di-trend-micro/index.html

[27] *Trend Micro lancia l'allarme: le minacce mobile crescono a un ritmo esponenziale ed emergono nuove tipologie di malware* – TREND MICRO
www.trendmicro.it/newsroom/pr/trend-micro-lancia-lallarme-le-minacce-mobile-crescono-a-un-ritmo-esponenziale-ed-emergono-nuove-tipologie-di-malware-/index.html

[28] *Websense 2014 Security Predictions Report* - WEBSENSE
http://it.websense.com/content/websense-2014-security-predictions-report.aspx

[29] *Global Risks 2014: Digital Wildfires in a Hyperconnected World* - WORLD ECONOMIC FORUM
www3.weforum.org/docs/WEF_GlobalRisks_Report_2014.pdf

Mercato italiano della sicurezza ICT e Mercato del lavoro

Introduzione

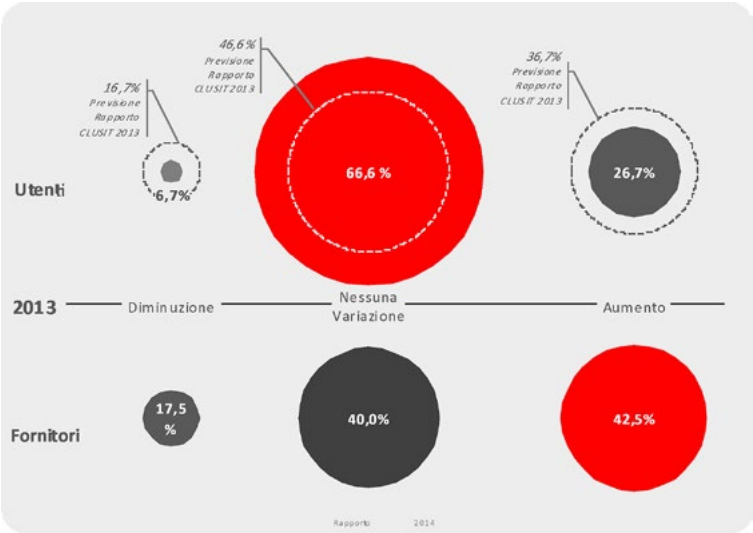
In uno scenario economico nazionale quanto mai incerto, il mercato dell'ICT Security ha un andamento ancora positivo, anche se la performance è meno brillante rispetto agli anni precedenti.

Questo risultato deve molto al coraggio dei player del settore, che hanno dimostrato nel 2013 maggiore versatilità, rispetto al passato, nell'adattare l'offerta per mantenerla competitiva. In più grande misura ha tuttavia contribuito una maggiore sensibilità alle problematiche di sicurezza delle aziende utenti, che hanno saputo, non senza sforzo, mantenere stabili, quando non hanno aumentato, i propri investimenti in questo ambito.

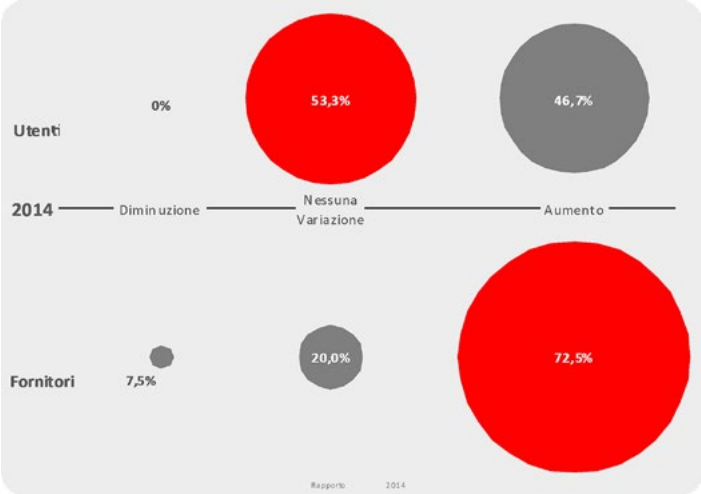
Il livello di sensibilizzazione, infatti, continua a salire in modo rilevante e, potremmo dire, tale sensibilità si è resa ancora più pervasiva che in passato: si consolida infatti un trend di crescita, già osservato negli scorsi anni, della propensione alla spesa in sicurezza da parte delle medie imprese, forse la più interessante delle novità di questa survey.
Il mercato ha raggiunto anche un maggiore livello di maturità, come testimoniano gli orientamenti di spesa del 2013 e gli obiettivi definiti dalle aziende utenti per la sicurezza nel 2014: pur essendo la maggioranza, si riduce il numero di coloro i quali pongono come principale priorità la conformità alle normative, ed aumentano invece le imprese che favoriscono la scelta di iniziative a tutela del patrimonio informativo e del business aziendale.

La nuova edizione del nostro Rapporto mette a confronto in questo capitolo i dati a consuntivo che emergono dalle interviste effettuate a oltre 400 aziende della domanda e dell'offerta di sicurezza ICT, con le previsioni per il 2014 che queste stesse aziende hanno formulato. Ne esce un quadro dinamico, positivo, con molte conferme e qualche piccola novità.

Un mercato maturo e pronto ad agganciare la crescita

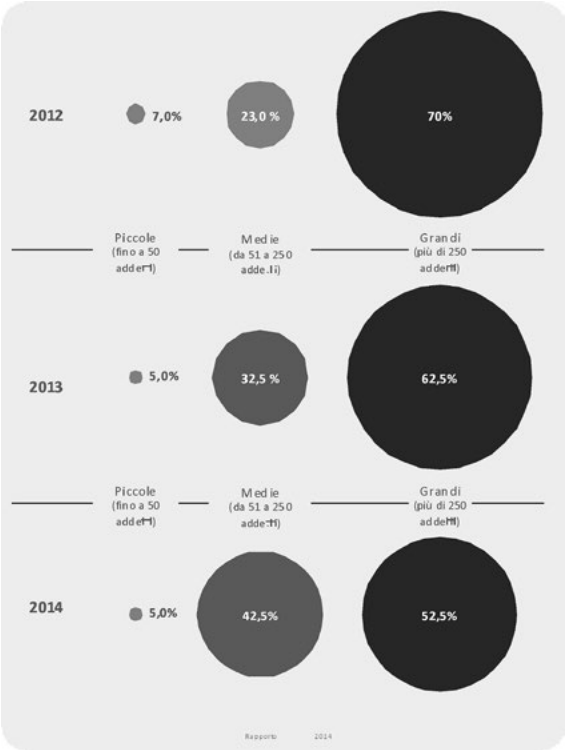


Nonostante i venti di crisi, il mercato della sicurezza ICT conferma anche per il 2013 un trend, seppure timido, di crescita, confermando il dato che abbiamo registrato fin dalla prima edizione del Rapporto CLUSIT.
In particolare, per quando riguarda il 2013, i fornitori hanno pressoché confermato i dati previsionali forniti nel precedente Rapporto, con una lieve preponderanza di coloro i quali hanno rilevato una crescita (42%), rispetto alle aziende che hanno riscontrato un mercato stazionario rispetto all'anno precedente (40%).
Le aziende utenti della sicurezza, al contrario, rilevano un dato diverso da quello delle previsioni (nell'immagine, identificate con una linea tratteggiata): è minore il numero di aziende che dichiara di aver ridotto gli investimenti nella security rispetto al 2012, ma cresce in modo rilevante il dato delle aziende che non hanno variato il budget rispetto all'anno precedente. Sempre rispetto alle previsioni del precedente Rapporto CLUSIT per il 2013, si riduce al 27% circa il numero delle aziende utenti che dichiarano di aver aumentato i propri investimenti.



Relativamente al 2014, il primo dato che leggiamo con interesse è la scomparsa, dal nostro campione, di aziende che intendono ridurre i propri investimenti per la sicurezza ICT! Lo stesso campione conferma infatti, per il 2014, una maggiore tendenza a mantenere inalterato il budget della sicurezza.
Tali risultati (pur previsionali) paiono confermare l'opinione diffusa che il mercato di riferimento della sicurezza ICT abbia ormai raggiunto un adeguato livello di maturità.
Tale mercato, tuttavia, si sta ampliando grazie ad una maggiore ricerca e specializzazione dei fornitori che, complice la crisi, adattano la propria offerta alla pluralità di esigenze delle nicchie di mercato o delle aree geografiche fino a poco tempo fa scarsamente raggiunte. E' con questa chiave di lettura che possiamo interpretare il numero ancora ampio (quasi il 47%) di aziende utenti che prevedono di aumentare i propri investimenti nel settore, ma soprattutto la proiezione del mercato per il 2014 resa proprio dai fornitori. In questo caso, le previsioni sono nettamente orientate alla crescita, quasi un plebiscito per un valore superiore al 70% degli intervistati! Se il risultato è sorprendente, bisogna comunque sottolineare che, dalla prima edizione del Rapporto CLUSIT, i fornitori hanno prodotto previsioni che nei successivi riscontri si sono sempre rivelate pressoché esatte.

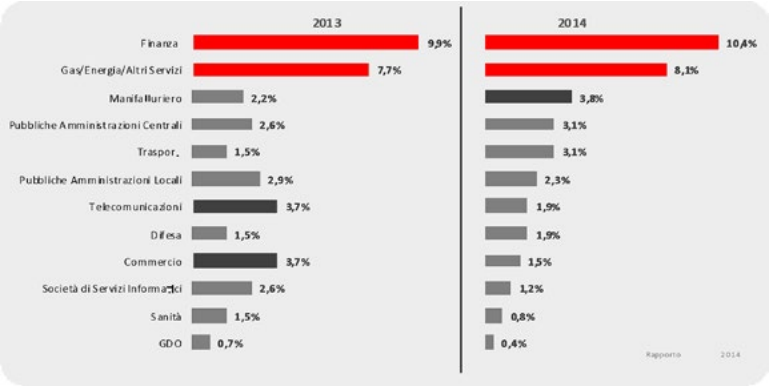
Medie imprese crescono…



A conferma della lettura che abbiamo fornito sui dati relativi alla crescita del mercato prevista nel 2014, abbiamo chiesto ai fornitori di security di indicare, dal loro privilegiato punto di osservazione, la dimensione delle imprese clienti che hanno dimostrato maggiore propensione alla spesa in sicurezza nel 2013. Di nuovo, i fornitori non smentiscono la loro capacità previsionale, confermando in pieno le ipotesi pubblicate nella scorsa edizione del Rapporto CLUSIT: il numero delle "grandi" è pressochè il doppio (62,5%) delle "medie" (32%), dato comunque in crescita (+10% circa) rispetto al 2012, quando il numero relativo alle aziende medie si attestava attorno al 23%.
Per queste, nel 2014 i fornitori prevedono un ulteriore aumento della propensione alla spesa in sicurezza (+10% rispetto al 2013): che sia per effetto di una maggiore penetrazione del mercato degli stessi fornitori e dei relativi prodotti, o di una maggiore consapevolezza delle "medie" imprese, se la previsione del 2014 sarà confermata, si potrà ormai parlare di una tendenza consolidata. Tale tendenza è forse la più rilevante novità di questo anno, poiché attesa da tempo da parte degli osservatori del settore anche a livello internazionale, come

dimostrano numerose iniziative condotte a livello europeo per sensibilizzare il settore delle PMI (dove lo stesso CLUSIT ha in più occasioni rappresentato il nostro paese). Tenuto conto che il tessuto delle imprese italiane è, per la maggior parte, costituito da piccole e medie imprese, questa tendenza è inoltre il migliore auspicio sia per la diffusione di una nuova consapevolezza dell'importanza dell'ICT Security, sia per le prospettive e gli spazi che si potrebbero aprire in fase di ripresa del mercato.

Mobilis in mobile



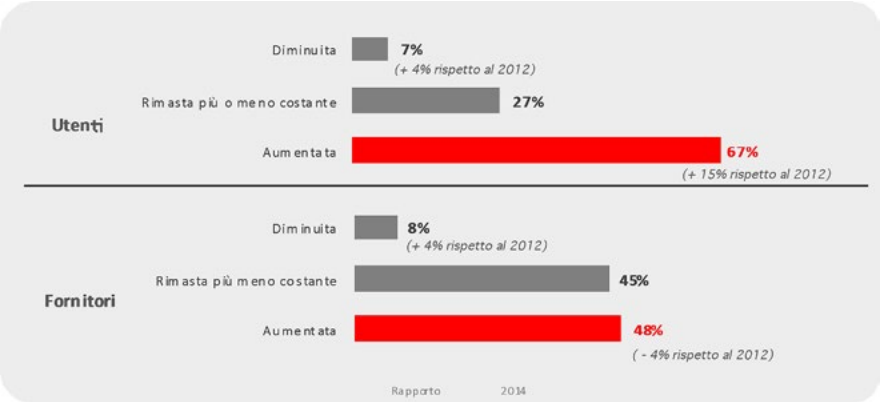
Il carrello della spesa del mercato della sicurezza ICT resta comunque saldamente in mano ai grossi player, almeno secondo la quota dei fornitori del nostro campione. I settori Finance e dell'Energia/Gas/Altri Servizi confermano, se non aumentano, il loro margine tra i settori che più investono nella security, sia nel 2013 che nelle previsioni del 2014, complici anche nuove normative in ambito bancario e le aspettative riposte nella diffusione della *SCADA Security*.

Rispetto al passato, tuttavia, il 2013 è il primo anno nel quale è possibile osservare cambiamenti significativi nella distribuzione degli investimenti tra gli altri settori: l'immagine che ci viene offerta è quella di uno scenario in rapido mutamento, dove la domanda e l'offerta hanno cambiato gli orientamenti sia rispetto al consolidato degli anni passati, sia rispetto alle previsioni.

Il 2013 è l'ultimo anno in cui le aziende di telecomunicazioni si mantengono sul podio, per collocarsi, nel 2014 in settima posizione tra le aziende che dimostrano la maggiore propensione alla spesa in sicurezza. Il 2013 è stato anche l'anno in cui le aziende utenti nel

settore del commercio hanno fatto registrare il migliore risultato dal 2011 (3° posto a pari merito con le Telco), contro le previsioni date dal nostro stesso campione lo scorso anno. Evidentemente tale situazione non è ritenuta strutturale, poiché i fornitori prevedono una nuova flessione nel 2014. Delude il risultato nell'ambito delle società di servizi informatici nel 2013, tendenza confermata per il 2014. Sorprendono il settore Manifatturiero e dei Trasporti, che registrano nel 2013 una propensione alla spesa in sicurezza decisamente più alta rispetto al 2012 e non prevista dal nostro campione nel 2013, in crescita nelle stime del 2014.
Più in generale, questo outlook per settori di attività risulta essere quello che ha disatteso maggiormente le aspettative e che può riservare maggiori sorprese nel futuro: se si considera che per il 2013 nel 42% dei casi i fornitori hanno rilevato un aumento degli investimenti dei propri clienti, come precedentemente osservato, evidentemente abbiamo un'ulteriore conferma che il mercato della sicurezza sta modificando in modo anche sensibile i propri orientamenti. Inoltre, pare dimostrare una sana e buona capacità di adattamento, dal momento che tali orientamenti sono stati evidentemente intercettati dall'offerta. Sarà pertanto interessante verificare, nella prossima indagine, l'effettiva quota di investimenti dei settori attualmente ritenuti meno promettenti o tradizionalmente più "chiusi", come la sanità, la grande distribuzione e la difesa.

Continua a crescere la sensibilità verso la sicurezza ICT

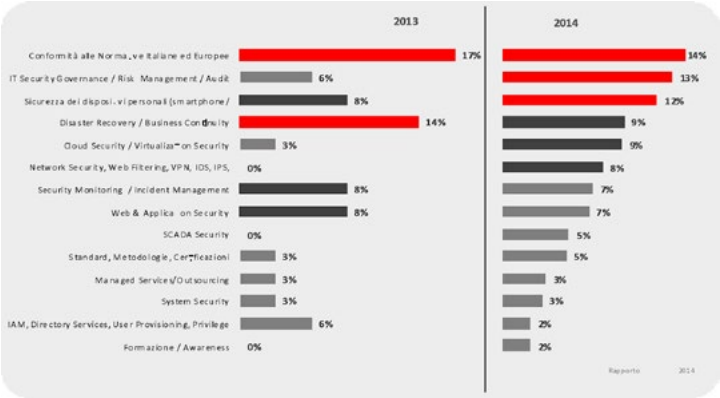


Anche per quest'anno si conferma un aumento della sensibilità delle aziende utenti al tema dell'ICT security: questo è il dato più confortante, dato che il 67% del campione non ha dubbi, confermando un trend che cresce, rispetto all'anno precedente, di circa il 15%.

Meno della metà, il 27%, sono invece le aziende utenti che rilevano di aver mantenuto la stessa soglia di attenzione ai temi della sicurezza ICT rispetto all'anno precedente.
Il punto di vista dei fornitori è meno orientato: solo il 48% rileva un aumento dell'attenzione da parte dei propri clienti, in lieve flessione (-4%) rispetto al 2012. Sono poco meno i fornitori che dichiarano che i propri clienti hanno al più mantenuto la medesima sensibilità rispetto all'anno precedente.

Il dato sorprendente, soprattutto in questi tempi di crisi (si sa, spesso l'ICT security costituisce la Cenerentola tra gli ambiti di investimento delle imprese, soprattutto a confronto con altri capitoli di spesa) è il numero di aziende per le quali l'attenzione alla sicurezza risulta diminuita: per queste, utenti e fornitori concordano su un valore decisamente basso, attorno al 7%. Pur enfatizzando un quadro generale decisamente positivo, è doveroso precisare che questo dato, rispetto all'anno precedente, è in lieve aumento.

Quando la conformità, da sola, non basta più



La conformità continua ad essere il principale driver di investimento delle imprese italiane, come emerge dal dato aggregato ottenuto dai questionari compilati da utenti e fornitori di sicurezza.
Il 2013, in generale, ha visto tendenze di investimento piuttosto nette e concentrate su alcune tematiche specifiche. Predominano, oltre alla conformità, le iniziative relative al disaster recovery (il 14% degli intervistati lo considera un driver importante di investimento), il monitoraggio e la gestione degli incidenti (8%), la sicurezza del mondo applicativo (8%). Seguono in coda in coda l'Identity & Access Management, la gestione degli utenti e dei privilegi (nessuno supera il 3%), e scompaiono dalle priorità, anche rispetto alle esigue per-

centuali registrate nelle previsioni dello scorso Rapporto CLUSIT, la sicurezza dei sistemi SCADA, la *network security* e la formazione.
Si è invece collocata tra i principali ambiti di investimento anche la sicurezza dei dispositivi mobili, indicata dall'8% degli intervistati, sebbene con risultati meno rilevanti di quanto era stato previsto dal nostro campione lo scorso anno.

Si potrebbe dire pertanto che nel 2013 le aziende si sono concentrate in quelle aree ritenute maggiormente prioritarie per:

- rilevanza legale;
- impatti verso il business;
- attuare buone pratiche di gestione sicura della IT, anche rinunciando ad investire negli ambiti che già agli inizi dello scorso anno ritenevano di ampio interesse.

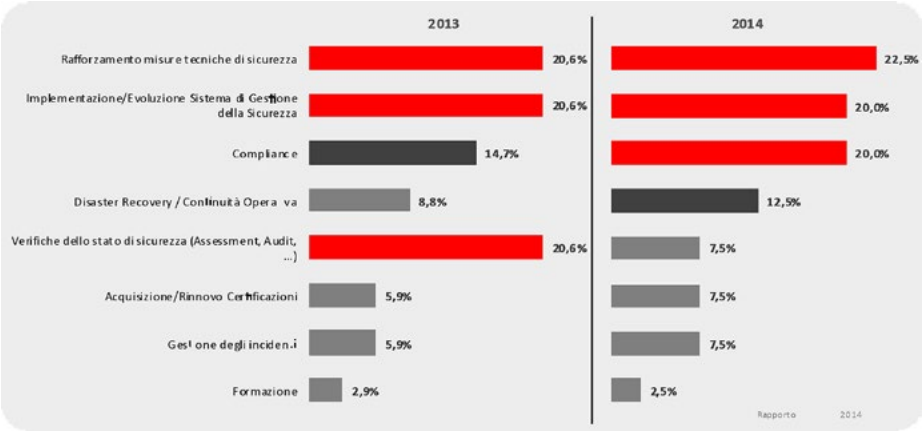
Le previsioni per il 2014 sono caratterizzate da una maggiore distribuzione degli orientamenti nei vari settori di investimento proposti agli intervistati, con l'effetto di ridurre il distacco dei settori "premiati" lo scorso anno. L'incremento degli investimenti nell'area di governance, risk management e audit, e una più omogenea distribuzione della spesa nei vari settori tecnologici, sembra esprimere la volontà di implementare la famosa "catena" delle aree di sicurezza per ridurre il numero di anelli deboli, in particolare andando a toccare anche quelle tematiche che negli anni precedenti sono state scarsamente presidiate.
Anche la conformità alle normative, pur restando saldamente in testa tra i driver del mercato del 2014, non lo fa di misura come avveniva in passato. Va detto che questo è un risultato positivo, perché consolida la flessione del numero di imprese per le quali gli obiettivi normativi sono un inutile onere imposto dal regolatore di turno, mentre cresce il numero di coloro i quali inquadrano tali adeguamenti all'interno di un approccio più ampio di tutela del valore dell'azienda, rappresentato ad esempio dalle iniziative di governance della sicurezza, risk management e audit.
Se la c.d. *mobile security* non ha avuto, nel 2013, i risultati che il mercato si attendeva, questo fatto non sembra tuttavia ridurre le attese riposte in questo settore, che è evidentemente percepito come utile dagli utenti e promettente dai fornitori, tanto da considerarlo il terzo ambito di maggiore investimento per il 2014 (12%, +4% rispetto al 2013). La previsione è giustificata dall'ampliarsi delle minacce verso i device mobili ed ai servizi ad essi dedicati, che i media non hanno mancato di enfatizzare nell'anno passato, nonché dalla sempre più ampia diffusione del c.d. Bring Your Own Device – BYOD, a causa della quale le aziende stanno via via riducendo la propria capacità di mantenere sotto controllo i propri asset informativi.

Si ridimensiona l'orientamento agli investimenti per iniziative di Disaster Recovery/Continuità Operativa, dopo aver superato nel 2013 le aspettative di aziende utenti e fornitori rilevate nella scorsa edizione del Rapporto CLUSIT; il dato si attesta ad un 9% di tutto rispetto (-5% rispetto allo scorso anno), passando quindi dal secondo al quarto posto nella

nostra "classifica", tra le iniziative di maggiore interesse. Questo risultato si può leggere anche alla luce della (ancora) crescente diffusione dei progetti di consolidamento delle infrastrutture e/o di crescita dell'utilizzo di servizi nel cloud da parte delle imprese, interventi che sosterranno nel 2014 i settori della sicurezza nel cloud e nelle infrastrutture virtualizzate. In questo caso, il risultato positivo si deve anche all'offerta, la quale si è notevolmente ampliata, e ha raggiungo un buon livello di maturità in termini di professionalità, prodotti e soluzioni dedicate.
Nell'ambito della sicurezza SCADA si orientano il 5% delle preferenze, dato ancora più significativo se si considera che il nostro campione, negli anni precedenti, dava scarso rilievo a questa tematica. Analizzando i nostri questionari, emerge come il trend di crescita sia più ampio presso i fornitori, che evidentemente vedono in quest'area la chiave di accesso a nuovi clienti o una forma per ampliare il business su quelli consolidati.

La *network security* e la formazione hanno registrato le peggiori performance dal 2012, ma tale risultato non sembra intaccare le attese per il 2014: in questi casi più che di sviluppo dovremmo parlare di una vera e propria "ripresa", o riconquista, delle quote di investimenti tradizionalmente destinati a questi ambiti.
Infine, relativamente alle iniziative che ruotano attorno alla gestione dell'identità e dei privilegi degli utenti, nel 2013 queste hanno mantenuto una quota significativa degli orientamenti di spesa delle aziende utenti. Questo è avvenuto nonostante, in questo settore, non vi siano da qualche tempo novità rilevanti, quanto meno dal punto di vista tecnologico, rispetto ad esempio a quanto sta avvenendo in alcuni degli altri settori elencati nella nostra survey. E' forse con questa motivazione che si spiega un calo delle previsioni nel 2014 (2%, -4% rispetto al 2013).

Focus su iniziative concrete



Per la prima volta, quest'anno abbiamo chiesto alle aziende utenti della sicurezza ICT quali siano state e quali saranno, nel corso del 2014, le iniziative di maggior rilievo o che li hanno maggiormente impegnati nell'ambito della sicurezza ICT.
È opportuno precisare che questo dato non è necessariamente collegato alla spesa in sicurezza, ma costituisce a nostro avviso un indice interessante degli orientamenti e delle priorità delle imprese. A conferma di quanto detto, la compliance, che è la prima voce di spesa nell'ambito della security nel 2013, è stata in realtà solo al quarto posto (14,7%) tra le priorità delle aziende utenti.
In testa alle iniziative a maggior rilievo condotte nel 2013 le aziende posizionano infatti al primo posto, in ex-aequo:

- verifiche dello stato di sicurezza (dai risk assessment ai penetration test);
- attività di implementazione o evoluzione del sistema di gestione della sicurezza;
- rafforzamento delle misure tecniche di sicurezza.

Partendo dall'ultima, potremmo interpretare solo superficialmente questo risultato come effetto dell'oggettiva complessità degli interventi di natura tecnica rispetto ad altre tipologie di iniziative in ambito sicurezza. In tal caso, tuttavia, dovremmo riscontrare un analogo livello di priorità tra i driver di investimento. Quello che possiamo dedurre quindi, anche alla luce del posizionamento al primo posto di questi interventi nel 2014, è l'esigenza delle aziende di attuare misure concretamente in grado di apportare benefici in termini di prevenzione e contrasto alle minacce sempre più crescenti alla sicurezza ICT.
Questa impostazione è confermata anche dal dato delle attività di verifica dello stato di sicurezza, dai risk assessment ai penetration test. Queste attività vanno certamente nella direzione di determinare quali siano gli interventi dove l'azienda deve concentrare i propri

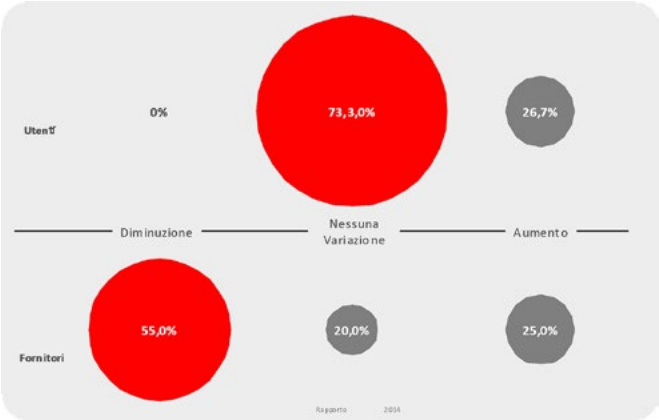
sforzi, siano essi di mantenimento degli standard attuali di sicurezza, o di integrazione/evoluzione dell'esistente con nuove misure. Questa tendenza probabilmente è anche figlia di questi tempi di crisi, che impongono alle aziende di essere capaci di scegliere dove posizionare una coperta sempre più corta, e di dare ragione al business delle motivazioni di tali scelte.
Il terzo ex-aequo in prima posizione, l'implementazione / evoluzione del sistema di gestione della sicurezza, colpisce in particolare a confronto del già citato quarto posto ottenuto dalla conformità, che pure domina nella classifica degli ambiti di investimento. Il dato è confortante perché è indice della volontà di rendere strutturale se non strategico, nell'ambito dell'organizzazione dell'azienda, il processo di sicurezza ICT, indipendentemente dall'obbligo di rispondere a questa o quella normativa.

Le previsioni nel 2014 confermano l'esigenza di concretezza delle aziende, che posizionano di nuovo al primo posto, se possibile in modo più marcato, le attività di rafforzamento delle misure tecniche di sicurezza ICT.
Coerentemente con le previsioni di investimento, per quest'anno la priorità delle iniziative di compliance torna a crescere fino al secondo posto, nell'attesa delle evoluzioni del panorama normativo privacy e per effetto di un insieme di nuove misure introdotte nell'ambito finance. A pari merito resiste tuttavia l'obiettivo di attuare o evolvere il sistema di gestione della sicurezza, in coerenza con la tendenza rilevata nel 2013.
Cresce il numero di aziende che considerano tra i propri obiettivi l'attuazione di strategie di disaster recovery e continuità operativa, da un circa 9% del 2013 al 12,5% nel 2014; questo risultato è di nuovo in linea con le previsioni di investimento delle imprese.
Si riduce in modo significativo il numero delle aziende che daranno priorità alle attività di verifica dello stato della sicurezza, in genere le aziende che avevano definito priorità diverse nel 2013 e che evidentemente vedono nel 2014 l'anno in cui valutare i risultati raggiunti e definire nuove priorità.

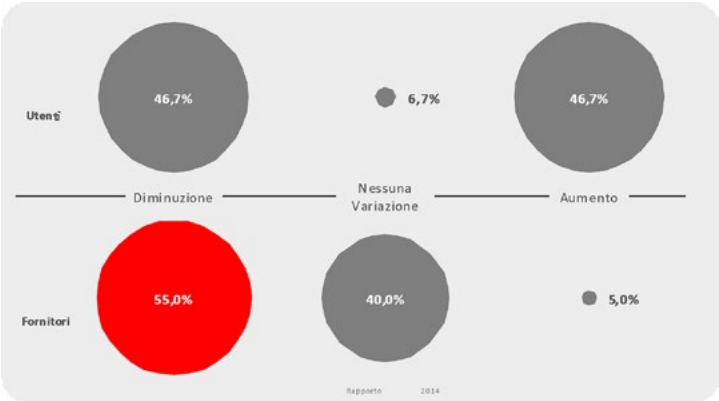
In generale, il 2014 nelle previsioni delle aziende è un anno dove le priorità delle imprese di distribuiscono in modo leggermente più omogeneo su tutte le tipologie di intervento proposte. Cresce infatti, rispetto al 2013, il numero di coloro che considerano iniziative di maggiore rilievo l'acquisizione o il rinnovo di certificazioni e l'implementazione di misure, processi e procedure di gestione degli incidenti informatici (in entrambi i casi, dal 5,9% al 7,5%). Il dato delle iniziative di formazione/awareness è invece in lieve calo, tuttavia in questo caso il dato reale è che un ambito che è praticamente il fanalino di coda degli investimenti possa costituire un obiettivo primario delle aziende. Questo risultato non deve stupire: la formazione può essere svolta, con risultati positivi, anche con investimenti estremamente limitati se comparati con la spesa complessiva ICT, o del solo settore della *security*!

Mercato del lavoro: stabilità o incertezza?

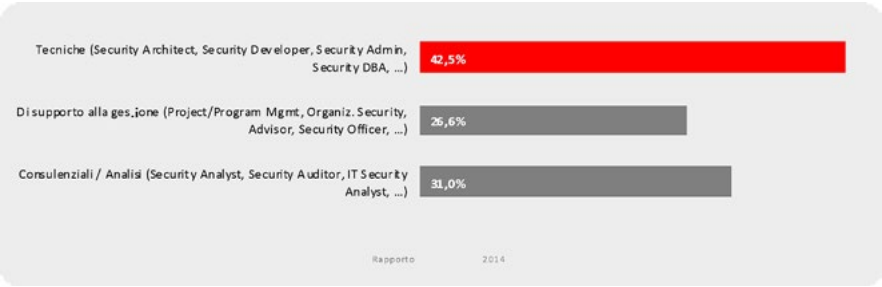
Nel 2013 le aziende utenti dimostrano di avere ancora esigenza di professionalità nel campo della sicurezza ICT, ma l'incertezza generale, la contrazione della crescita e la forte competizione del mercato, hanno avviato un trend leggermente negativo riguardo alle prospettive occupazionali presso i fornitori del settore.



In particolare, le aziende utenti ci restituiscono un quadro positivo se comparato al più ampio scenario nazionale: infatti, la stragrande maggioranza (73,3%) dichiara di aver mantenuto stabile l'occupazione, e per un numero superiore al 25% di esse nel 2013 si è verificato un aumento degli addetti. E' altresì positivo il fatto che nessuna azienda abbia registrato una diminuzione dell'occupazione nel settore della sicurezza ICT.
I fornitori al contrario delineano una situazione meno positiva, nella quale in più del 50% dei casi si registra una diminuzione di occupati nel settore della security, mentre il resto del campione è spaccato tra coloro i quali hanno rilevato un aumento dell'occupazione nel settore, e coloro i quali hanno mantenuto stabile il livello occupazionale.



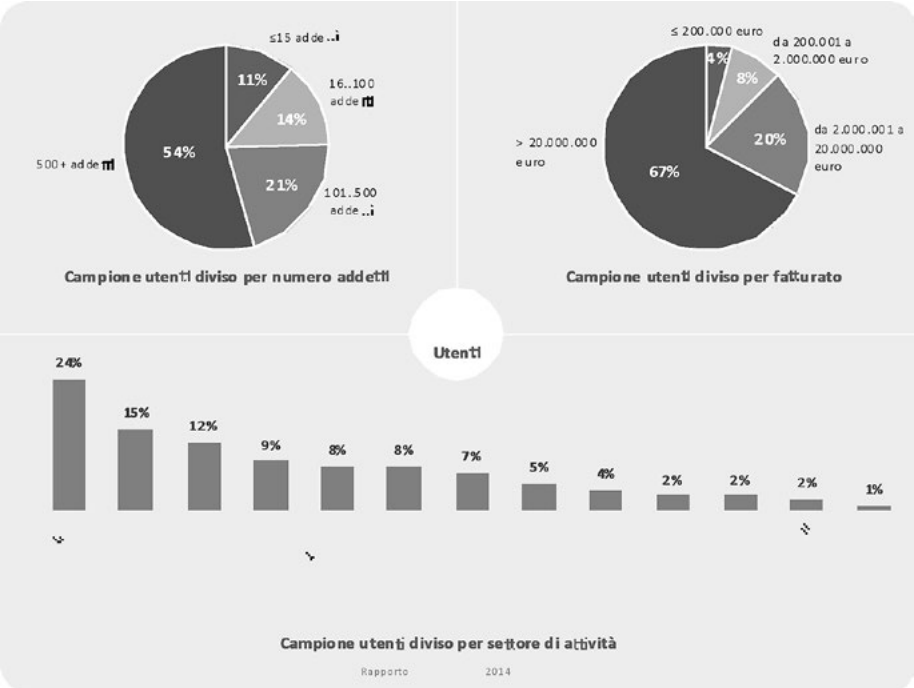
Relativamente al dato previsionale del 2014, contrariamente a quanto avvenuto per altri indicatori, in questo caso è estremamente difficile analizzare le prospettive di aziende utenti e fornitori per definire delle tendenze. E' in qualche modo evidente come il complesso scenario congiunturale renda meno facile fare delle previsioni anche nel breve termine, come emerge dai dati che abbiamo raccolto.
Le previsioni delle aziende utenti per l'anno corrente sono emblematiche: il dato è nettamente spaccato tra coloro i quali vedono nei prossimi mesi una ripresa della domanda di professionalità nel settore della sicurezza, e coloro che presagiscono, al contrario, una contrazione del mercato del lavoro. Solo un'esigua percentuale, il 6,7%, ritiene che non vi saranno variazioni.
È più marcato l'orientamento dei fornitori per il 2014, che confermano il trend di contrazione dello scorso anno, seppure in modo lieve. Questo a causa sia del numero consistente di aziende che intravedono una diminuzione della domanda del mercato del lavoro (55%, stesso dato del 2013), sia perché si riduce il numero di imprese che prevedono per il 2014 un aumento degli addetti nel settore della sicurezza ICT, passando dal 25% del 2013 al 5% attuale.

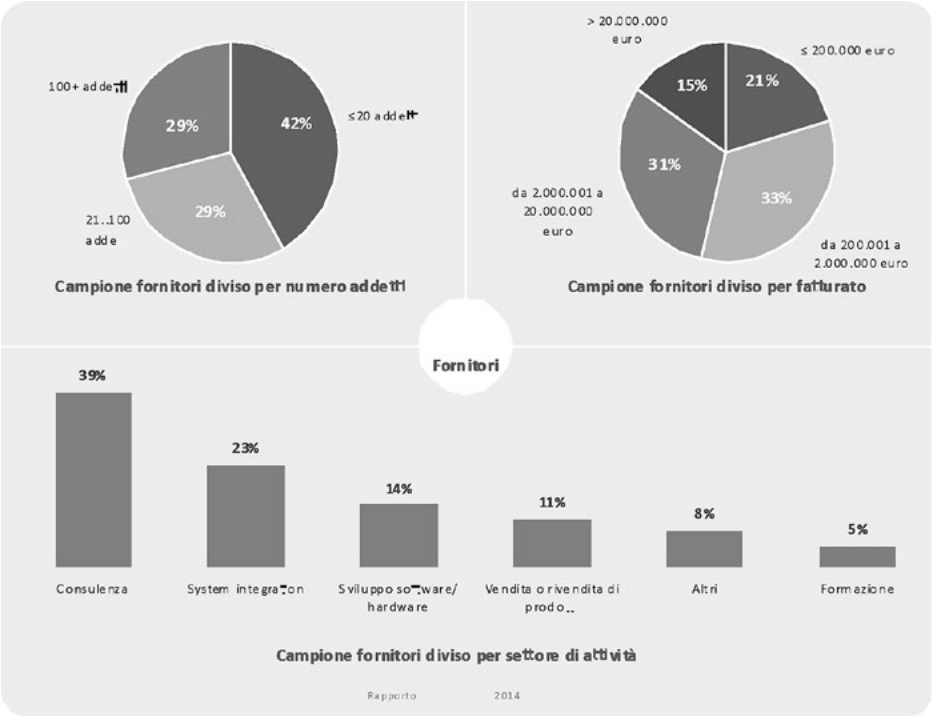


Tra le figure professionali in ambito sicurezza ICT maggiormente richieste, prevalgono quelle tecniche (42,5%,), seguite da quelle consulenziali (31%) e da quelle di supporto alla gestione (26,5%).

Campione

Il campione di indagine è costituito da 438 aziende, di cui 81 fornitori.




100+ addetti
29%
42%
≤20 addetti
29%
21..100 addetti
Campione fornitori diviso per numero addetti
> 20.000.000 euro
≤ 200.000 euro
15%
21%
31%
33%
da 2.000.001 a 20.000.000 euro
da 200.001 a 2.000.000 euro
Campione fornitori diviso per fatturato
Fornitori
39%
23%
14%
11%
8%
5%
Consulenza
System integration
Sviluppo software/ hardware
Vendita o rivendita di prodotti
Altri
Formazione
Campione fornitori diviso per settore di attività
Rapporto 2014

Rapporto Clusit 2014 – FOCUS ON

Questa sezione del Rapporto 2014 è dedicata a delle aree di particolare rilevanza per la sicurezza ICT in Italia.
Abbiamo chiesto ad alcuni dei maggiori esperti italiani, nelle singole materie, di approfondire i seguenti temi:

- Smartphone, Tablet e Social Networks in Azienda;
- La strategia europea per la cybersecurity;
- Lo stato della digital forensics in Italia;
- I controlli interni sui processi ICT in ambito aziendale;
- Security By Design;
- La Security vista dal Management;
- Formazione e Consapevolezza, strumenti indispensabili per la Sicurezza delle Informazioni.

Di Smartphone, Tablet e Social Networks si è già molto scritto nei precedenti Rapporti Clusit, ma qui il fenomeno è analizzato con particolare riguardo all'utilizzo aziendale. La strategia europea è determinante per la sicurezza di tutti gli stati membri ed anche per la strategia italiana in tema di cybercrime. Digital forensics, controlli interni, Security by Design, sono temi di grande rilevanza per la sicurezza delle informazioni in azienda. La security vista dal management ci aiuta a capire il livello di consapevolezza del management delle aziende italiane nei confronti della sicurezza delle informazioni e l'evoluzione dei loro comportamenti. In un paese tra gli ultimi in Europa per livello di informatizzazione e per utilizzo di servizi informatici e della rete, La Formazione nelle scuole, e a tutti i livelli, è uno strumento indispensabile per aumentare consapevolezza e competenze.

Smartphone, Tablet e Social Networks in Azienda

a cura di Alessio Pennasilico

Quando in azienda si parla di Social Network si pensa sempre a qualcosa di competenza dell'IT, da filtrare, o di competenza del Marketing, per promuovere l'immagine ed i prodotti dell'azienda.
Purtroppo questa visione, è evidente ai più, si dimostra miope oramai da qualche anno. I social network, infatti, costituiscono un rischio sia da un punto di vista di immagine (brand reputation) sia da un punto di vista della più classica security (relativamente all'opportunità di preservare la confidenzialità di alcune informazioni).

I social network, infatti, possono mettere a serio rischio la Business Security di una azienda. Se poi si coniuga l'aspetto social network, con la sua imprescindibile altra metà del cielo, i dispositivi mobili, ecco che il rischio si palesa in tutta la sua maestosità.
Non regolamentare, non prevenire, non controllare l'accesso e l'uso di tali strumenti, infatti, può portare non solo a danneggiare l'immagine dell'aziende nei confronti di un pubblico molto vasto, ma addirittura al furto di informazioni aziendali riservate.

L'approccio che d'istinto si sarebbe istintivamente portati ad adottare prevederebbe di filtrare integralmente tutti i social network, cercando di limitare il più possibile l'utilizzo di dispositivi mobili aziendali. Di dispositivi personali, poi, meglio non parlare proprio. Purtroppo questo approccio si dimostra fallimentare sul lungo periodo. Gli utilizzatori, infatti, riterranno i blocchi ingiusti, cercando continuamente di aggirarli. La diffusione di dispositivi mobili, invece, non potrà essere bloccata nei confronti del top-management. Ci si troverà, quindi, di fronte a continui tentativi di violazione delle policy aziendali, di cui qualcuno prima o poi andrà a buon fine, mentre tutte le informazioni aziendali più preziose saranno in viaggio assieme ai dispositivi delle figure apicali. Questo porterà a scontento degli utenti, un falso senso di sicurezza da parte di tutti e ad una discreta quantità di minacce non gestite che rischieranno di creare danni seri al business aziendale, a fronte di un produttività aziendale abbassata dal malcontento.

Per questa ragione si rende necessario comprendere appieno il "fenomeno social" e stabilire una efficace strategia di gestione ed utilizzo. I dispositivi mobili aziendali devono essere una risorsa che permetta di lavorare meglio, non soltanto un rischio. Gli strumenti tecnologici per ottenere questi risultati esistono oramai da tempo sul mercato. Forse quel che manca è la sensibilità al tema e la voglia di affrontare il problema.

Relativamente ai Social Network grande cura va evidentemente prestata nella loro gestione, tenendo presenti aspetti che il Marketing da solo non può gestire, e per questo il CSO do-

vrebbe essere coinvolto nel processo. Non tutti i contenuti, inoltre, sono dannosi o inutili, per cui una buona politica di gestione degli accessi non ai portali, ma ai contenuti, andrebbe stabilita.
Alcuni rischi, infatti, sono facilmente identificabili, come ad esempio la perdita o il furto del dispositivo. In questo caso ci si espone all'accesso in prima battuta ai dati memorizzati sul dispositivo. Dimenticando troppo spesso che sul dispositivo stesso sono memorizzate le credenziali per accedere alla rete aziendale via VPN o via WiFi, permettendo quindi ad un eventuale malintenzionato, o semplice curioso, di accedere a risorse ben più critiche di quelle memorizzate sul dispositivo stesso. Si trascura a volte anche la possibilità di usare i social o la semplice e-mail aziendale configurata sul dispositivo per impersonare il suo possessore, a volte con rischi anche economici rilevanti (si pensi alle truffe che invitano clienti a bonificare del denaro su un conto diverso da quello aziendale o chiedono ad un interno di trasferire del denaro, comunicare credenziali o altro).

Ancora estremamente sottovalutato è invece il rischio "infezione", vale a dire che una applicazione malevola esegua sul device operazioni non volute. Il codice in oggetto può essere contenuto in una applicazione scaricata dallo store di riferimento, essere una "app" di un social, provenire da un sito visitato intenzionalmente (ad esempio cliccando su un link contenuto in una pagina web o in una mail) o inconsapevolmente (dai shortlink ai QR Code). Si è già assistito a campagne basate sull'utilizzo di volantini cartacei che riportano QR Code, ad esempio, che conducono ad un sito malevolo atto ad infettare una particolare release di sistema operativo di un particolare telefono. Fino ai fax che contengono link scritti a mano che si invita a visitare...
Il dispositivo mobile, quindi, va visto oramai come un PC a tutti gli effetti: sia per i rischi che corre, sia per la sua potenza. Un dispositivo mobile può tranquillamente gestire uno scan di rete, un attacco di brute force per indovinare le password, essere usato per inviare spam e phishing. Tutto senza rallentare eccessivamente il dispositivo, quindi senza danneggiare la "user experience" dell'inconsapevole utilizzatore.

Si pensi ad esempio ad un dispositivo infettato durante la navigazione tramite la rete 3G o LTE, che poi inizi a fare scansioni della rete aziendale una volta collegato al wireless aziendale. Questo è uno dei tipici rischi ancora troppo sottovalutati, assieme al fatto che un dispositivo di tal genere possa essere usato come testa di ponte, vale a dire che offra un accesso remoto in VPN ad un attaccante, mentre è collegato alla rete WiFi aziendale, creando così un canale diretto verso la rete corporate, scavalcando il firewall e tutte le misure perimetrali adottate.
E non esiste un marchio o un prodotto esente da rischi: abbiamo già assistito a efficaci dimostrazioni di come tutte le release di tutti i vendor per ogni piattaforma siano incappate in gravi falle di sicurezza o si prestino, con maggiore o minore complessità, ad essere infettate con applicazioni malevole.

Purtroppo il fenomeno "malware per mobile" è ancora così trascurato che la percentuale di dispositivi mobili protetti con l'apposito prodotto antivirus (indipendentemente da marca e modello) è ad oggi risibile. Una azienda che oggi voglia stabilire una corretta e coerente security policy non dovrebbe permettere che questo accada ai suoi dispositivi. Soprattutto osservando i trend di mercato. Con numeri a volte diversi, tutti i produttori di "antivirus per piattaforme mobili" riconoscono lo stesso trend: aumento esponenziale degli strumenti disponibili, delle minacce reali, delle tecniche di attacco, nonché delle intrusioni andate a buon fine. [**Fig. 1**]

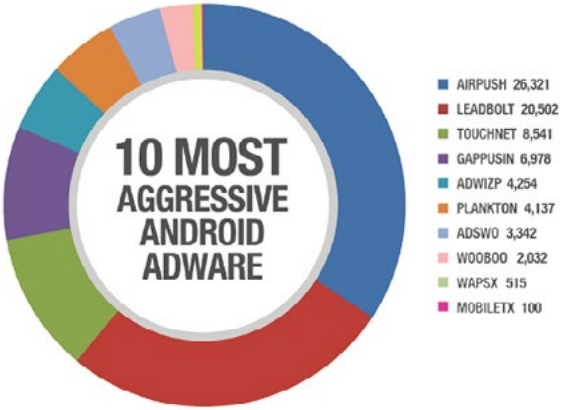


Immagine tratta dal Trend Micro Report for Q3, 2012: Zero-Days, Mobile Malware and Phishing che evidenzia come il fenomeno mobile malware sia in crescita e molto aggressivo.

Se poi l'analisi si dovesse spostare sui rischi degli incidenti sui social il panorama sarebbe ancora più preoccupante.
Abbiamo già assistito in passato ad esempi eclatanti dell'uso di piattaforme social per accedere a dati aziendali rilevanti: si pensi all'articolo "Facebook from a Hacker's perspective" pubblicato da Kevin Finisterre nel 2009 (http://snosoft.blogspot.it/2009/02/facebook-from-hackers-perspective.html). Tramite l'uso intelligente di Facebook si è riusciti ad ottenere un accesso in VPN alla rete di una azienda, con credenziali dai diritti decisamente rilevanti.

Si pensi poi a veri e propri incidenti, come quello che ha dovuto gestire Alpitour lo scorso anno, dove il banale furto di una password ha esposto un brand di primaria rilevanza nazionale a dover gestire un rischio rilevante per i propri clienti, con una possibile perdita economica tutt'altro che trascurabile. Sono finiti gli anni '90, quando se prendevano possesso di un tuo asset si limitavano a farsi beffe delle tue misure di security. Oggi dobbiamo affrontare criminali veri, interessati esclusivamente al denaro, che non usano la pagina in questione per dichiarare la propria superiorità tecnica, ma per infettare il maggior numero di device possibile, cercando di indurre i clienti a cliccare link che portano a siti malevoli.

Questo tipo di attacco è più pericoloso perché non immediatamente evidente, non immediatamente rilevabile e quindi destinato a raccogliere vittime su tempi più lunghi. D'altro canto, considerando lo scenario di oggi, si trattasse di vandali (perché la parola terroristi ad oggi rischia di essere ancora sovradimensionata, ma non troppo) il messaggio non sarebbe più "ha ha io sono più bravo di voi perché vi ho bucati", ma sarebbe "Questa azienda è malvagia, perché viola i seguenti dettami morali/etici/religiosi comportandosi in questo modo non accettabile". Inutile dire che il secondo tipo di messaggio è decisamente più rilevante in termini di perdita di reputation per il brand che dovesse subire tale intrusione, soprattutto su piattaforme dove oramai la frequenza di accesso da parte di possibili clienti rischia di superare quella delle campagne DEM, del blog aziendale o del sito istituzionale.

Il peccato originale sta all'importanza che viene attribuita al "mondo social" che, come già detto, viene visto esclusivamente come rischio di una perdita di tempo da parte dei collaboratori, quindi da filtrare punto. Manca ancora la consapevolezza che quel che avviene in "quel mondo" non è "altro rispetto a quel che avviene nel mondo reale". Non parliamo, infatti, di due realtà distinte ed indipendenti, ma di uno scenario complesso dove le conseguenze di quel che accade sono pervasive.

Se dieci anni fa qualcuno mi avesse raccontato che con un "tweet" si potevano far perdere ingenti quantità di denaro forse avrei sorriso. Temo abbiano sorriso meno coloro che hanno visto sfumare il proprio denaro [**Fig. 2**] quando dopo avere violato l'account di Associated Press qualcuno ha postato una notizia dell'ultimo minuto circa un attentato alla casa bianca [**Fig. 3**].

Per questa ragione diventa necessario prendere coscienza di tutti i rischi che questi strumenti possono creare, al fine di indirizzarli nel modo corretto, con la tecnologia che, per nostra fortuna, già abbiamo a disposizione.

La strategia europea per la cybersecurity

a cura di Corrado Giustozzi

In questi ultimi anni, diverse nazioni o organizzazioni internazionali hanno provveduto a dotarsi di una formale strategia per affrontare in modo sistematico i sempre più importanti temi della cybersecurity. Mancava tuttavia all'appello l'Unione Europea che, pur avendo affrontato più volte la problematica nel recente passato, lo aveva sempre fatto con interventi limitati in ambito e scopo, e quindi più tattici che strategici. Da circa un anno tuttavia questa carenza è stata finalmente colmata: nel febbraio del 2013, infatti, con la promulgazione del tanto atteso documento di impostazione strategica, l'Europa ha espresso la sua visione unitaria sul problema della cybersecurity e delineato le linee guida comuni per il contrasto al cybercrime ed a tutte le altre minacce "*cyber*".

È chiaro che sviluppare una strategia comune per un'organizzazione transnazionale così complessa e peculiare come l'Unione Europea non è un compito facile: occorre infatti sempre tenere presente le specificità di ben ventotto diversi sistemi politici, sociali, giudiziari; e spesso mediare tra gli altrettanti, e forse ancor più differenti tra loro, approcci culturali e filosofici di ciascuno degli Stati membri. Tuttavia, come già la Convenzione di Budapest aveva pionieristicamente sottolineato nel lontano 2001 pur facendo riferimento al solo cybercrime, la transnazionalità delle nuove minacce rende inevitabile il dover raggiungere un forte consenso ed un'attiva collaborazione fra tutti i sistemi-Paese, se si vogliono ottenere risultati efficaci nella prevenzione e nel contrasto al fenomeno.

Nel cyberspazio nessuna nazione è un'isola, e dunque solo adottando strategie comuni e meccanismi di risposta collaborativi e coordinati si possono costruire risposte adeguate ai rischi globali che minacciano le, purtroppo vulnerabili, infrastrutture di comunicazione e di gestione delle informazioni sulle quali si basa il funzionamento della moderna società civile.

Proprio in linea con queste considerazioni, dunque, il documento di strategia comune europea non si limita ad indicare le priorità ed individuare le modalità d'intervento comunitarie, ma fornisce inoltre ai singoli Stati membri indicazioni e linee guida sulle quali allineare operativamente le proprie strategie nazionali.

La strategia definita dall'Europa, inoltre, non risponde solo ad un'astratta esigenza formale, e soprattutto non vuole rimanere un mero buon proponimento "sulla carta": essa pertanto si incastra in una serie di azioni concrete che, iniziate già da tempo, trovano ora un'adeguata sistematizzazione proprio nell'ambito della strategia stessa. Il documento è stato infatti pubblicato solo pochi mesi dopo l'attivazione del CERT-EU, avvenuta ufficialmente a fine 2012, ed è stato accompagnato dalla contestuale presentazione di una importante proposta di direttiva comunitaria per la sicurezza informatica di cui la Commissione raccomanda la pronta adozione da parte del Consiglio e del Parlamento europei. Solo poche settimane più tardi, inoltre, il Parlamento ha rinnovato ad Enisa (l'Agenzia europea per la sicurezza delle reti e delle informazioni) il mandato che era oramai scaduto, dotandola tuttavia nel

contempo di un nuovo e più efficace statuto che ne amplia in modo importante missione e responsabilità: e ciò proprio in vista del ruolo cruciale che essa dovrà giocare nell'implementazione della strategia europea per la cybersecurity.

Pilastri fondanti

Denominata formalmente "An Open, Safe and Secure Cyberspace" (che, nella traduzione ufficiale in italiano, diventa "Uno spazio informatico aperto e sicuro"), la cyberstrategy europea risponde ad una necessità ben radicata da tempo nella consapevolezza dei responsabili sia politici che tecnici dell'Unione, ossia che la sicurezza del cyberspazio comunitario è prerequisito imprescindibile per lo sviluppo dell'Europa. Non a caso il terzo dei sette "Pillars" (pilastri) sui quali si articola l'Agenda Digitale Europea, il documento fondamentale di indirizzo che declina lo sviluppo tecnologico europeo da qui al 2020 attraverso l'implementazione di 101 specifiche "Actions" (azioni), si chiama proprio "Trust & Security". Tale pilastro consta di 17 azioni mirate a rafforzare i prerequisiti fondamentali di sicurezza e fiducia delle infrastrutture tecnologiche e di comunicazione, le quali sono considerate come il più importante strumento per poter ottenere competitività, sostenibilità e progresso sociale ed economico in Europa.
L'aspetto che più caratterizza la strategia europea rispetto alle altre omologhe iniziative proposte da altre nazioni od organizzazioni sovranazionali sta nei principi per così dire più "filosofici" che ne hanno ispirato l'impostazione, e su cui a sua volta essa si poggia: i quali quindi, e non poteva essere altrimenti, si richiamano direttamente ai valori fondanti dell'Unione stessa. È interessante quindi esaminarli brevemente.

In primo luogo viene sancito esplicitamente il principio fondamentale secondo cui i valori fondanti dell'Unione Europea si applicano al mondo digitale tanto quanto a quello fisico; ciò in particolare comporta, come diretto corollario, che le medesime leggi e norme che regolano gli altri aspetti della vita quotidiana dei cittadini europei valgono direttamente anche nel dominio cyber. In altre parole l'UE afferma che non vi sia alcun bisogno di sviluppare nuove leggi e norme specifiche per il cyberspazio: quelle esistenti sono già più che sufficienti a descrivere e regolare la vita, le azioni e le attività on-line, basta applicarle estensivamente al modo giusto.
Il secondo principio fondamentale è quello che traguarda la protezione dei diritti fondamentali, della libertà di espressione, della riservatezza (privacy) degli individui e dei relativi dati personali. Le libertà e i diritti individuali dei cittadini europei, che sono alla base della carta politica dell'UE, vengono dunque riflessi direttamente nei principi che la strategia intende salvaguardare.
Gli altri principi ispiratori riguardano infine le garanzie irrinunciabili per una moderna ed efficace democrazia partecipata, che si basa anche sulla sicurezza di Internet e delle altre infrastrutture ICT: accesso per tutti, una multi-stakeholder governance democratica ed efficiente, e soprattutto la responsabilità condivisa da parte di ciascun attore, istituzionale o no, per garantire la sicurezza della complessa e variegata società digitale.

Ambiti di intervento

Il documento di strategia, dicevamo, espone la visione complessiva ed unitaria dell'Unione europea non solo sul modo migliore di prevenire perturbazioni e attacchi informatici, ma anche su come organizzare ed articolare la risposta: al fine, come recitava l'annuncio ufficiale, di "*promuovere i valori europei di libertà e democrazia e garantire che l'econo*mia *digitale possa svilupparsi in modo sicuro*".

A tal fine sono previste azioni specifiche per rafforzare la resilienza dei sistemi di informazione, ridurre la criminalità informatica e potenziare la politica internazionale dell'UE in materia di sicurezza e di difesa in tale ambito.

Va notato a tal proposito come la nuova strategia riconosca esplicitamente ed onestamente come alcune delle passate iniziative comunitarie a sostegno della sicurezza siano state talvolta condotte in modo tattico e poco coordinato, diciamo "a macchia di leopardo", e spesso senza un chiaro obiettivo in mente. Trasformando tuttavia in opportunità gli errori del passato, la nuova strategia mira anche a recuperare e mettere a fattor comune, inserendole sinergicamente in una visione unitaria, tutte le iniziative sinora già realizzate a livello di strutture o attività.

Per perseguire i propri obiettivi, la cyberstrategia europea articola dunque le sue iniziative specifiche su cinque priorità fondamentali, da cui discendono direttamente altrettante direttrici basilari d'intervento. Esse specificamente sono mirate a:

- conseguire la resilienza informatica;
- ridurre drasticamente la criminalità informatica;
- sviluppare la politica di difesa e le capacità informatiche connesse alla politica di sicurezza e di difesa comune;
- sviluppare le risorse industriali e tecnologiche per la sicurezza informatica;
- istituire una coerente politica internazionale del ciberspazio per l'Unione europea e sostenere i valori fondamentali dell'UE.

Ciascuna di queste cinque direttrici a sua volta raccoglie ed indirizza, declinandole opportunamente, specifiche linee d'azione.

Iniziative specifiche

La principale priorità individuata dal documento di strategia è il conseguimento della *cyber resilience*, ossia la capacità delle reti e dei sistemi di comunicazione di resistere ad attacchi condotti per sabotarli, danneggiarli o impedirne il regolare funzionamento.

In quest'ambito l'Europa si sta muovendo già da diversi anni, e l'iniziativa forse più importante e visibile messa in atto è l'organizzazione periodica di regolari esercitazioni pan-europee nelle quali, simulando svariati realistici scenari di attacco, gli Stati membri e le strutture comunitarie verificano la propria *readiness* e la capacità di fronteggiare le minacce via via presentate. Sino ad oggi, grazie al fattivo supporto di Enisa, già si sono tenute due esercitazioni pan-europee (Cyber Europe 2010 e 2012) ed una esercitazione congiunta EU-USA (Cyber Atlantic 2011). La strategia raccomanda di proseguire attivamente in questa importante pratica, ed infatti è già in corso l'organizzazione della prossima Cyber Europe

2014 alla quale per la prima volta parteciperanno anche i Paesi europei aderenti all'EFTA ma non alla UE. In sottordine alle esercitazioni pan-europee la strategia prevede inoltre che anche gli Stati membri debbano organizzare periodiche esercitazioni nazionali per verificare la "tenuta" agli attacchi delle proprie infrastrutture critiche locali.
Altre due iniziative più tecniche in ambito a questo obiettivo sono il lancio di un progetto pilota per la lotta alle *botnet* (soprattutto quelle localizzate in Europa), e lo studio di fattibilità per un CERT europeo dedicato specificamente alla sicurezza dei sistemi automatici per il controllo industriale (SCADA e simili).
Sul piano legislativo invece la Commissione raccomanda al Parlamento di approvare rapidamente la Direttiva sull'alto livello comune di sicurezza delle reti e delle informazioni (NIS Directive) che, una volta in vigore, obbligherebbe gli Stati membri ad adottare misure tecniche ed organizzative comuni e condivise per innalzare il livello di sicurezza delle infrastrutture nazionali, e migliorare altresì la cooperazione internazionale a livello di *preparedness* e di *information sharing*.
Ulteriori iniziative in ambito riguardano l'innalzamento della consapevolezza delle istituzioni e dei cittadini sui temi della cybersecurity, ad esempio mediante l'istituzione del "mese della cybersecurity" a livello europeo e dei singoli Stati membri, di specifici "campionati di cybersecurity" per gli studenti universitari, dell'insegnamento della cybersecurity nei licei e nelle pubbliche amministrazioni, e anche di un progetto di certificazione volontaria delle competenze di sicurezza informatica progettato sulla falsariga della "Patente europea del computer".
Per quanto riguarda la seconda priorità, ovvero la lotta al cybercrime, oltre a raccomandare a tutti gli Stati membri che non l'abbiano ancora fatto di ratificare al più presto la Convenzione di Budapest, la strategia prevede iniziative soprattutto sul piano dell'armonizzazione a livello europeo delle singole legislazioni nazionali e dei relativi strumenti di contrasto. In particolare il Centro Europeo per il Cybercrime (EC3), recentemente fondato all'interno di Europol, collaborerà con Europol ed Eurojust per supportare gli Stati membri in tale allineamento sia sul piano normativo che su quello tecnico. Inoltre il CEPOL (l'Accademia Europea di Polizia) svilupperà specifici piani di formazione per fornire a tutte le forze di polizia nazionali le adeguate conoscenze e competenze per fronteggiare al meglio la lotta al crimine informatico.
La terza priorità, lo sviluppo di una politica di difesa comune, prevede iniziative specifiche di *cyberdefence* da svilupparsi nell'ambito del framework CSDP (Common Security and Defence Policy) già attivo per le necessità di difesa tradizionale. Ciò prevede una maggiore cooperazione specifica tra strutture civili e militari dell'EU, e ovviamente anche un dialogo operativo con la NATO e gli altri partner internazionali del mondo della difesa.
La quarta priorità indirizza la necessità per l'Europa di sviluppare competenze industriali autonome ed indipendenti in ambito cybersecurity, e conseguentemente l'obiettivo di promuovere un mercato unico europeo per i prodotti e i servizi di cybersecurity. A tale riguardo sono dedicate iniziative che vanno dallo sviluppo di linee guida e *best practice* europee da adottarsi per indirizzare la sicurezza nei settori pubblico e privato, all'introduzione di in-

centivi per favorire l'adozione nelle aziende di strumenti e soluzioni di sicurezza aggiornati ed efficaci. Ma oltre a ciò sono previste iniziative specifiche per rafforzare la competitività delle aziende europee nel settore dei prodotti e servizi di sicurezza, in particolare favorendo la Ricerca e Sviluppo e l'innovazione industriale in tale segmento di mercato; il supporto a tali iniziative sarà fornito mediante il coordinamento con i progetti finanziati già previsti dal vasto programma Horizon 2020.
Infine la quinta priorità indirizza le esigenze di preservare un cyberspazio libero, aperto e sicuro, nel quale valgano i principi fondanti europei di dignità, libertà, democrazia, uguaglianza, così come le norme di legge ed il rispetto dei diritti fondamentali. Questo obiettivo più "alto" e filosofico verrà perseguito mediante iniziative di natura essenzialmente politica, indirizzate allo sviluppo di *policy* comuni e norme di comportamento nel cyberspazio, anche finalizzate alla responsabilizzazione di tutti gli *stakeholder* che insistono su di esso.

Ruoli e responsabilità

Naturalmente il documento prende anche in considerazione il complesso intreccio di ruoli e responsabilità dei vari attori coinvolti nell'attuazione della strategia: un aspetto reso critico dalla peculiare natura dell'Unione, che non è un unico soggetto politico ed amministrativo ma una struttura di governo partecipata la quale mantiene tuttavia intatte le sovranità nazionali dei singoli Stati membri.
La strategia tiene dunque conto di tale situazione, riconoscendo esplicitamente l'esistenza di due livelli di responsabilità cui corrispondono altrettanti ambiti d'azione: quello nazionale, situato al livello interno dei singoli Stati membri, e quello sovranazionale, situato a livello comunitario. E mentre alcune iniziative previste dalla strategia sono naturalmente idonee ad essere portate avanti a livello comunitario, altre per la loro specifica natura non possono che essere demandate ai singoli livelli nazionali.
Così i tre pilasti operativi "verticali" sui cui ricade l'attuazione operativa complessiva della strategia, ossia le autorità ed istituzioni competenti per la sicurezza informatica, le agenzie di *law enforcement* e le agenzie per la Difesa militare, dovranno a loro volta declinare ordinatamente le proprie attività sui due distinti livelli orizzontali, quello comunitario e quello nazionale, secondo una suddivisione di compiti e responsabilità organizzata a matrice secondo lo schema di **Figura 1**.

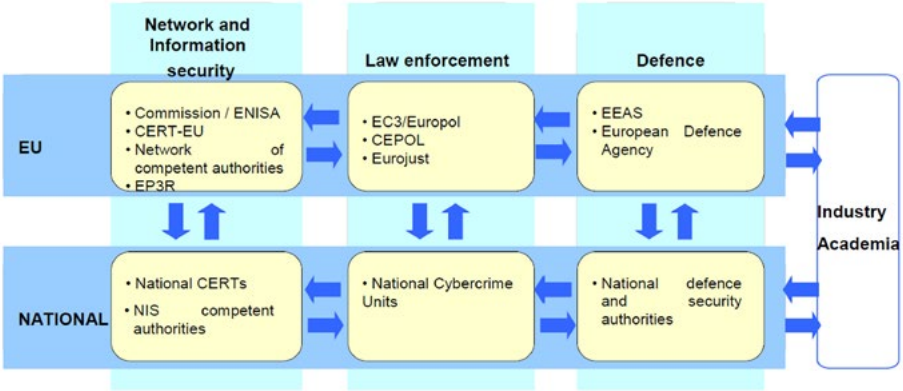


Figura 1: la complessa articolazione europea prevede una ripartizione a matrice di ruoli e responsabilità fra i diversi attori (pilastri verticali), i quali dovranno declinare la propria attività sui livelli (orizzontali) nazionale e comunitario. (Fonte: "Cybersecurity Strategy of the European Union")

In esso sono indicate le istituzioni ed organizzazioni direttamente responsabili delle iniziative, ed i flussi di comunicazioni tra di esse intercorrenti; a latere va sottolineata la presenza dell'industria privata e del mondo accademico, due soggetti non strettamente istituzionali ma evidentemente importantissimi, i quali partecipano attivamente alle iniziative ad entrambi i livelli.

Conclusione

L'Europa è giunta a definire una propria strategia per la sicurezza del cyberspazio dopo molti altri Grandi del pianeta, ma ha finalmente colmato il divario e lo ha fatto in modo efficace. Essa infatti ha consolidato una visione molto pragmatica del problema, orientata soprattutto alla tutela, in linea coi principi fondanti di libertà e democrazia, del cyberspazio come presupposto tecnologico irrinunciabile per lo sviluppo sociale, politico ed economico dell'Unione; individuando a tal fine obiettivi concreti e soprattutto attuabili, ed iniziative chiare e operative per conseguirli.

Certo il percorso futuro non è facile: l'elemento caratterizzante dell'Unione, ossia la straordinaria diversità culturale tra i suoi Stati membri, è anche il vincolo maggiore da superare quando si tratta di definire politiche comuni. È infatti necessario armonizzare tra le molte e differenti visioni, e mettere a fattor comune le situazioni già consolidate; cosa che richiede tempo e sforzi molto maggiori di quelli richiesti a singoli organismi nazionali, dove è evidentemente più facile ad un governo centrale imporre un determinato percorso.

È molto rilevante, a tale riguardo, il forte appello che la strategia rivolge alla collaborazione tra pubblico e privato, la quale viene vista come uno strumento cruciale per il consegui-

mento degli obiettivi individuati. La volontà della Commissione, che non è neanche tanto nascosta tra le righe, è quella di sviluppare un comparto industriale comunitario che, col supporto della ricerca accademica opportunamente incanalata e potenziata, possa essere in grado sia di svincolare il mercato europeo dall'attuale dipendenza commerciale nei confronti di Paesi extraeuropei per quanto riguarda servizi e prodotti di cybersecurity, sia di supportare le istituzioni comunitarie nel conseguimento degli obiettivi di protezione e *cyber resilience* individuati dalla strategia.
Alcuni tasselli operativi cruciali, quali la costituzione della rete europea di CERT nazionali e del CERT europeo, o l'effettuazione di esercitazioni allargate di *preparedness* e *readiness*, sono già efficacemente in atto. Altre iniziative specifiche sono già partite, molte delle quali veicolate sotto il grande ombrello del programma Horizon 2020. Ma il grosso dell'attuazione rimane ancora da fare, ed è quello che deve partire dal basso: tutti gli Stati membri dovranno infatti dare attuazione convinta ed efficace alle indicazioni della strategia declinandole adeguatamente al proprio interno, con la collaborazione delle proprie istituzioni specificamente dedicate alla cybersecurity nazionale, e coordinandosi con le istituzioni europee e degli altri Stati membri.

Lo stato della digital forensics in Italia: accademia, Forze dell'Ordine, magistratura e avvocatura, esperti e aziende

A cura di Giovanni Ziccardi

Premessa

Lo "stato" della digital forensics in Italia si è, negli ultimi anni, evoluto sensibilmente e, fortunatamente, in maniera abbastanza **omogenea**.
Sin dagli anni Duemila, la scienza che studia la corretta identificazione, acquisizione, produzione e, in senso lato, "resistenza" in giudizio della fonte di prova digitale ha vantato anche in Italia uno sviluppo lineare che ha riguardato tutti i settori coinvolti, nessuno escluso: il mondo dell'**accademia** (che si occupa dello studio degli aspetti teorici e procedurali di tali argomenti), le **Forze dell'Ordine** (tramite una riflessione e una attività di formazione avente ad oggetto le migliori modalità pratiche d'investigazione in una società sempre più connessa e complessa), la **magistratura** e **l'avvocatura** (tramite l'analisi di problematiche prettamente giuridiche e correlate al lato pratico/processuale) e il mondo dei **consulenti**, dei tecnici, degli esperti, delle associazioni e delle **aziende** che producono software ed hardware per la digital forensics (soggetti, questi, giustamente più votati a un approccio alla materia tecnico e d'immediata utilità, compresa la formazione nell'utilizzo di tali strumenti, sovente complessi).
Ciò ha portato a uno sviluppo equilibrato del settore, cosa molto utile e apprezzabile in un ambito che viene a toccare, come è noto, i diritti fondamentali dell'individuo.

L'accademia

Il mondo dell'accademia ha cercato di portare avanti la **didattica** e la **formazione** su questi temi sin dai primi anni di studio nelle aulee universitarie e, soprattutto, in tutte le Facoltà, sia **giuridiche** (quindi con insegnamenti volti al futuro avvocato, magistrato o giurista d'impresa) sia nelle Facoltà **scientifiche**, soprattutto informatica e ingegneria, con insegnamenti sovente collegati alle tematiche della sicurezza.
Gli studi accademici, dopo aver definito la digital forensics, hanno cercato di individuare i lati originali della materia all'interno del grande alveo della sicurezza informatica e della scienza informatica in generale.
Sono stati organizzati corsi di perfezionamento post-laurea che permettono, nei programmi attuali, di meglio analizzare singoli aspetti della forensics. Vi era, infatti, fino a qualche anno fa la possibilità di formarsi su una forensics per così dire "generalista", ossia che si occupasse di **tutto**.

Oggi, al contrario, è richiesta maggiore specializzazione, e intere aree della forensics, quali ad esempio l'analisi di dispositivi **mobili**, o di grandi sistemi di server **aziendali**, o del **cloud**,

si stanno pian piano guadagnando un' indipendenza di analisi (una sorta di "autonomia"), dal momento che presentano aspetti del tutto originali e differenti dagli altri comparti, ed è per questo che i corsi di perfezionamento post-laurea mirano a sviscerare temi più specifici quali l'antiforensics, la mobile forensics, il cloud forensics, e così via.
Si noti anche che vi è stata un'estensione, sempre nell'accademia, da un'analisi della forensics come tema legato a doppio filo alle indagini **penali** e, in generale, alla criminalità informatica, al codice penale e al codice di procedura penale, per passare a una forensics nel diritto di **famiglia**, nel diritto **commerciale**, nel diritto del **lavoro** e nel diritto **tributario**, dove i dati sono sempre più trattati digitalmente (si pensi a separazioni e divorzi) in un quadro giuridico però assai differente. Lo spostamento della forensics anche in questo settore comporta l'attenzione necessaria ad altri aspetti del diritto che non sono più soltanto le regole di procedura: penso alla legge sulla **privacy** e alla tutela dei diritti della **personalità**, al segreto della **corrispondenza**, e così via.
L'accademia collabora da qualche anno con associazioni di volontari che, anche in Italia, mantengono viva l'attenzione e la formazione su questi temi.

Le Forze dell'Ordine

Da alcuni decenni anche il mondo delle Forze dell'Ordine, coloro che si trovano "sul campo" a investigare, ha manifestato un interesse concreto al tema.
Rispetto all'approccio accademico, l'attenzione primaria delle Forze dell'Ordine è nei confronti di metodi di investigazione, modelli di indagine e di analisi o best practices.
Questo perché, nella pratica, ciò che serve loro sono le **procedure** da seguire che consentano al contempo di cristallizzare la fonte di prova in modalità **corrette** non contestabili anche in nuovi "ambienti" quali, ad esempio, i social network, i sistemi di messaggistica istantanea e le chat, e che siano rispettose delle regole di procedura.

Accanto a questo approccio, vi è un'attenzione ai nuovi metodi investigativi richiesti da un nuovo ambiente, quello telematico, e alle competenze domandate, soprattutto in un'ottica di **formazione** specifica di agenti con forti conoscenze informatiche. Il problema più grave, in questo caso, è quello del **tempo**, o meglio del tempo/uomo necessario per le investigazioni dei dispositivi in un'era di grandi **masse** di dati e di migliaia di messaggi, immagini, e-mail e conversazioni. In sostanza: una analisi accurata di migliaia di e-mail (e oggi ogni cittadino ha sul suo computer o telefono migliaia di e-mail) richiede **tempo**, ma il personale che opera è sempre lo stesso e in alcuni casi non riesce a gestire con cura più di un certo numero di indagini all'anno. Ciò prospetta un utilizzo intenso di strumenti **automatizzati** (ad esempio software che estraggono e selezionano certi tipi di immagini) che possono creare successivamente non pochi problemi processuali.

La ricerca di un **metodo** è stata facilitata, seppur in senso molto lato, dalle modifiche introdotte dalla Legge n. 48 del 2008, di ratifica della Convenzione sulla criminalità informatica di Budapest, che ha inserito nel codice penale e di procedura penale alcune regole minime,

soprattutto relative alla inalterabilità della fonte di prova, alla ripetibilità delle operazioni e alla copia-clone dei dati originali, che hanno per la prima volta formalizzato un minimo di metodo, anche a garanzia dell'indagato.

Magistrati e avvocati

Il mondo del diritto, composto da magistrati e avvocati, è anch'esso interessato particolarmente al settore, seppur con un approccio, e con un taglio, leggermente differenti.
La magistratura, soprattutto quella deputata a coordinare e svolgere indagini, è molto interessata, ultimamente, alla legittimità o meno di utilizzo di strumenti investigativi **invasivi** quali i **trojan** o **microspie** da installare nei computer da tenere sotto sorveglianza, suscitando non poche polemiche in tal senso. Negli ultimi anni, poi, molti magistrati si sono avvicinati alla computer forensics studiando il nuovo quadro posto dalla **criminalità** informatica, soprattutto con riferimento alle **frodi** (anche internazionali), al riciclaggio del denaro, a nuovi ambienti quali quelli dei social network e all'annoso problema delle intercettazioni telematiche (con attenzione anche a sistemi quali Skype).

Gli avvocati, dal canto loro, sono sempre stati attenti a una forensics che fosse anche **garanzia** dei diritti dell'indagato, soprattutto in tema di **ripetibilità** delle azioni d'indagine compiute, e al **rigore** metodologico con cui vengono effettuate le operazioni. I casi stanno aumentando, e si sta formando una giurisprudenza abbastanza copiosa che consente di individuare alcune linee interpretative precise.
Anche per queste due categorie l'obbligo di **formazione** sta diventando impellente, non essendo più possibile delegare completamente agli esperti la comprensione dei temi indicati.

Consulenti e aziende

Gli esperti, infine, sono anch'essi molto vivaci nel settore, soprattutto in due direzioni: i) la **presenza** nel contesto processuale, con consulenze e testimonianze, e ii) lo sviluppo di **strumenti** software e hardware che possano agevolare determinate procedure.
Circa il primo punto, c'è stato un forte aumento di richieste di competenze tecniche nell'economia processuale sia civile sia penale, dal momento che il diritto sta diventando tutto informatico. Non essendoci un albo di esperti di computer forensics, la formazione viene svolta o tramite percorsi universitari tradizionali, o con alcune **certificazioni** mirate a dare una competenza specifica nel settore.
Al tecnico, sovente, non vengono domandate unicamente consulenze teoriche ma anche vere e proprie **azioni** sui dati o sui dispositivi, tanto da rendere necessario l'allestimento di un piccolo (ma spesso costoso) laboratorio.

Sul secondo punto, è vivace sia la vendita di strumenti di computer forensics software e hardware con relativi corsi di aggiornamento e di utilizzo, sia lo sviluppo di distribuzioni **open source** per il primo intervento o per la gestione di una analisi forense.
Si è assistito a un leggero calo di prezzi dell'hardware, che fino a qualche anno fa era con-

siderato "materiale da iniziati", e a una certa standardizzazione delle procedure utilizzate. Comune è l'utilizzo di diversi apparati o software per raggiungere uno **stesso** obiettivo (ad esempio la copia di un disco) al fine di evitare, in udienza, contestazioni sul metodo utilizzato, o per "rafforzare" l'operazione.

Conclusioni

In un quadro simile e così dinamico, che vede tanti "attori" partecipare, il futuro è sempre incerto, ma alcuni punti sono abbastanza prevedibili.
Il primo è l'**aumento** esponenziale di dati che sta avvenendo, giorno dopo giorno. Milioni di messaggi e di mail scambiate in tutto il mondo, dispositivi portatili che hanno la capienza di memoria di un vero e proprio computer, conversazioni ininterrotte che avvengono ogni minuto. La **quantità** dei dati sarà secondo me il primo problema per le investigazioni, e ciò comporterà la necessità di una selezione e di un mutamento nell'approccio al trattamento dei dati.
Il secondo punto "caldo" è il cloud o, meglio, la delocalizzazione di servizi, risorse e informazioni. Il cloud richiederà un ripensamento dell'azione dell'investigatore che "inseguirà" i dati e nuovi rapporti con le società che li detengono.
Infine gran parte della digital forensics si è già spostata dai computer ai telefonini intelligenti (e tablet) e al mondo del social network, anche in questo caso richiedendo all'interprete e al pratico nuove modalità di approccio e di analisi.

I controlli interni sui processi ICT in ambito aziendale

A cura di Stefano Niccolini e Claudio Telmon

All'interno di un'azienda di dimensioni rilevanti le politiche aziendali sono importanti per comunicare ai collaboratori lo stile imprenditoriale con l'obiettivo di indirizzare motivazione e comportamenti secondo uno stile preciso, caratteristico dell'impresa. Si tratta di indirizzare il buon senso individuale, bene prezioso nelle situazioni eccezionali in cui si devono gestire rischi e non sono precisate procedure o regole.
Il vantaggio della diffusione delle politiche aziendali consiste nella riduzione del rischio di comportamenti "non in linea" in situazioni anomale.
Dalle politiche, in particolare quelle sui rischi aziendali, dovrebbero trarre spunto i regolamenti interni, in primis quelli che descrivono i processi decisionali.

I Controlli Interni, esterni alle strutture produttive, dovrebbero valutare l'osservanza e l'applicazione da parte di queste alle indicazioni dell'impresa, ai fini dell'ottenimento degli obiettivi di business in un quadro di ottimizzazione delle risorse e minimizzazione dei rischi. Particolarmente in realtà complesse, può diventare molto difficile la costruzione di una valutazione affidabile sul tematiche come l'ottimizzazione delle risorse e adeguato trattamento dei rischi.
Le fasi chiave di un buon sistema dei controlli interni possono essere quindi i seguenti.

Definizione delle politiche commerciali e del rischio: è un documento che descrive l'orientamento al business dell'azienda e l'approccio al rischio. Ai principi ivi esposti si riferiscono tutti gli altri documenti che descrivono le attività e i processi aziendali. A quei principi deve ispirarsi chi opera in azienda nei casi in cui si debba operare in assenza di regole specifiche. In sintesi, le politiche sono "il buon senso secondo la nostra azienda".

Attribuzione delle responsabilità: è il primo dei processi di controllo del rischio. Questa fase produce i regolamenti, con l'avviso di escludere da questi la descrizione del come si fa, privilegiando la descrizione degli obiettivi. Nell'attribuzione delle responsabilità si deve considerare anche l'interazione tra i diversi portatori di responsabilità, in modo da chiarire i processi decisionali. Tale azione consente di rilevare i cosiddetti conflitti di interesse e di prevenire situazioni in cui un unico soggetto possa ottenere libertà di azione non coerenti con lo spirito imprenditoriale o in contrasto con norme o leggi vigenti.

Definizione dei processi: il destinatario di una responsabilità che implica lo svolgimento di attività dovrebbe rendere conto sulle modalità di assolvimento di quanto conferito. Questo aspetto non sempre viene pienamente realizzato e si può presentare il caso di responsabili di aree di business che operano in base a procedure definite esternamente all'area. Tale

situazione però tende a svuotare il mandato imprenditoriale all'area operativa, spostando la responsabilità in merito all'efficacia, efficienza e forse anche conformità di quanto svolto esternamente ad essa. Viceversa l'attribuzione all'area operativa dell'onere di definire processi e controlli interni innalza lo spirito imprenditoriale anche se ciò richiede una specifica cautela da parte del vertice aziendale: il sistema dei controlli interni.

Attuazione di un Sistema di Controlli Interni: il Sistema dei Controlli Interni costituisce la fase di chiusura del processo di attribuzione delle deleghe di responsabilità. Il processo infatti dovrebbe fornire indicazioni al vertice aziendale sulla capacità della struttura di operare come previsto, sulla sua potenzialità evolutiva e, in definitiva, sulla capacità di creare valore secondo un approccio fedele al mandato imprenditoriale definito nelle politiche dell'azienda.

Il quadro sopra esposto, necessariamente riassunto e reso essenziale, non include esplicitamente il fattore informatico perché è *ovvio* e *sottinteso*. Ormai l'informatica è nell'azienda, a prescindere da quanto i collaboratori e i dipendenti portano con sé, nei dispositivi mobili personali. Oltretutto, l'informatica permette la registrazione di fatti attinenti al business da cui ricavare informazioni sulla capacità dell'azienda di gestire il rischio in ogni sua forma: economico / finanziario, reputazionale, legale, operativo, ecc. Queste registrazioni sono rilevanti sia dal punto di vista dei controlli interni che della sicurezza.

Tuttavia, un aspetto problematico dell'informatica è il rischio associato al suo utilizzo. Le tecnologie emergenti offrono sempre maggiori possibilità in termini di efficienza dei sistemi di governo e gestione dell'impresa. Cloud, Big Data, Mobile Devices sono tecnologie o prodotti pervasivi e le imprese si trovano a doversi interrogare sull'opportunità di cavalcare la tigre. Ma con quali rischi? Sicurezza e Conformità sono i punti di attenzione attualmente più gettonati.

La valutazione dell'esposizione del business ai rischi è di competenza dei proprietari del business. *Business Owner* implica *Risk Owner*, anche per i rischi IT. Tuttavia la garanzia di una valutazione equilibrata e corretta può essere opportunamente considerata da un soggetto esterno. Si parlerà quindi di Assurance, attività propria dell'Internal Auditing, in particolare dell'ICT Auditing.
Tale funzione è opportuna in realtà medio grandi ed è resa obbligatoria, ad esempio, nel mondo bancario italiano dalle Disposizioni di Vigilanza di Banca d'Italia.
Per essere efficace la funzione di Audit deve essere *indipendente* dalle strutture che vengono sottoposte a valutazione. Tale caratteristica è stata storicamente sempre ben considerata.
Per le realtà più piccole, che non hanno le risorse per realizzare un sistema di controlli interni strutturato, può essere opportuno appoggiarsi a competenze esterne che siano in grado di valutare la capacità del sistema informativo di supportare l'azienda nel raggiungimento dei suoi obiettivi. Per fare questo, dovrà disporre non solo di competenze tecniche informati-

che, ma anche della capacità di comprendere le effettive esigenze del business dell'azienda, e dovrà comunque avere la dovuta indipendenza da chi, internamente all'azienda o fornitore esterno, gestisce effettivamente il sistema informativo.

Nell'ambito dell'audit ICT, la sicurezza riveste un interesse particolare. Dato che l'audit è per sua natura focalizzato principalmente sui processi più critici per l'organizzazione, è chiaro che la possibilità di questi processi di svolgersi correttamente è legata fra l'altro alla garanzia che non siano possibili attività illegittime che possano danneggiare i processi stessi. In effetti, l'ambito della sicurezza è quello in cui alcune forme di audit sono tutto sommato note e relativamente comuni anche fuori dagli ambiti regolamentati come le banche.

Si tratta dei cosiddetti *vulnerability assessment e penetration test* (VA/PT), che rappresentano un'attività molto circoscritta di audit, ma che rendono l'idea di cosa possa essere un audit di sicurezza: un'attività svolta da una terza parte indipendente (anche quando si tratti di una struttura interna). Questa, disponendo di competenze specifiche nell'ambito della sicurezza IT ha lo scopo di verificare se la gestione del sistema informativo sia adeguata, quali siano i punti di miglioramento, e darne visibilità ai vertici dell'organizzazione.
Nel caso del VA/PT però, si tratta di un'attività che si limita a fotografare lo stato corrente di alcuni aspetti limitati della sicurezza di un sistema informativo. I risultati che si ottengono, salvo eccezioni, devono essere inquadrati in un più ampio contesto. Un audit ICT affronta, in generale, un insieme più ampio di problematiche, ad esempio la distribuzione di ruoli e responsabilità, le tematiche contrattuali, la capacità di gestire gli eventuali incidenti, la conformità alle normative (fra le quali naturalmente è particolarmente significativa quella sul trattamento dei dati personali), lo sviluppo e l'acquisizione di codice sicuro, e molti altri. In definitiva si tratta di esprimere una valutazione del rischio di disallineamento tra soluzioni ICT aziendali e necessità di business. L'audit sulla sicurezza ICT, attraverso un programma di verifiche, anche "sul pezzo" (VA/PT), esprime la valutazione precedentemente citata sulla distanza tra le aspettative di protezione dell'azienda e i presidi effettivamente in essere.

La competenza di chi, interno o esterno, svolge l'attività di audit, è fondamentale.I danni che possono essere arrecati ad un'azienda da relazioni di ICT Audit con valutazioni inesatte sono rilevanti. Le competenze di un professionista sono in generale difficilmente comprovabili, e in questo le associazioni hanno un ruolo importante. Nel campo dell'ICT Audit ISACA, che associa oltre 100.000 professionisti ICT in tutto il mondo, si propone come entità certificatrice per i professionisti che svolgono attività di ICT Audit. La certificazione CISA è accordata a professionisti che oltre ad una certa anzianità nel campo dell'Audit, superano un esame scritto di rilevante difficoltà. L'esame verte sulla conoscenza dei sistemi informativi, non soltanto sotto profili tecnici o tecnologici, ma anche sotto il profilo della gestione manageriale. Ad AIEA ad esempio, che è anche capitolo di Milano di ISACA, aderiscono attualmente 484 soci con certificazione CISA.

Quattro sono le linee di attività in ambito ICT che ISACA promuove: la Governance, il Gestione dei Rischi, la Sicurezza e l'Audit. Per ognuna di esse l'associazione pubblica regolarmente documentazione che consente di rimanere al passo con l'evoluzione tecnologica.
A supporto di chi si deve occupare di governare e gestire i sistemi informativi spicca COBIT 5. Si tratta di un framework che aiuta a coniugare le esigenze di business di un'impresa con quelle informatiche, individuando diversi fattori abilitanti: non solo processi ma anche le caratteristiche di ambiente come le persone, la cultura, le competenze.
ISACA eroga tramite i capitoli nazionali corsi di formazione per quei professionisti che intendono ottenere certificazioni di tipo professionale in ciascuno dei quattro ambiti citati, Governance, Gestione dei Rischi, Sicurezza e Audit.

Concludendo, se il ricorso ai sistemi informativi è soluzione che a sua volta apre un ventaglio di problemi, i controlli interni, opportunamente progettati ed eseguiti, consentono di raggiungere con ragionevole certezza gli obiettivi di business.
I controlli, e fra questi anche quelli relativi alla sicurezza, devono possibilmente avere carattere preventivo ma sono disponibili metodologie e profili professionali in grado di riportare in linguaggio comprensibile anche a non informatici fatti e problematiche di taglio anche specialistico.
La professionalità dei soggetti che si occupano di ICT è essere avvalorata dalle certificazioni internazionali che attestano la competenza di chi l'ha conseguita.

Security By Design

A cura di Walter Ginevri e Alessandro Vallega

Tra i professionisti della Sicurezza, e perfino a livello delle istituzioni Europee, si parla spesso di Security by Design, ovvero dell'approccio secondo il quale è bene progettare i prodotti e i servizi informatici pensando alla sicurezza fin dal principio. Secondo gli esperti, si tratta dell'unico modo per contrastare efficacemente le minacce e le frodi che hanno come bersaglio i sistemi informativi e che sono ormai diventate un fenomeno diffuso di criminalità.
Su questo tema, Clusit ha dato vita ad una collaborazione con la principale associazione internazionale di Project Management, ovvero il Project Management Institute (PMI) e, più precisamente, con i suoi rappresentanti del Northern Italy Chapter (PMI-NIC).
Tutto ciò ha permesso di portare a compimento un'indagine rivolta ad una base associativa composta da oltre 1600 project manager del settore privato e pubblico.
Accettando il rischio di vanificare l'effetto sorpresa, possiamo anticipare che le risposte ci inducono ad un certo ottimismo (**Fig. 1**), anche se, come vedremo nel seguito, "non è tutto oro quel che luccica". Infatti a fronte di un'azienda che impone un approccio di Security By Design è ragionevole pensare che tale "design" si attui ottemperando ai requisiti tramite un approccio comune e condiviso da molteplici progetti.

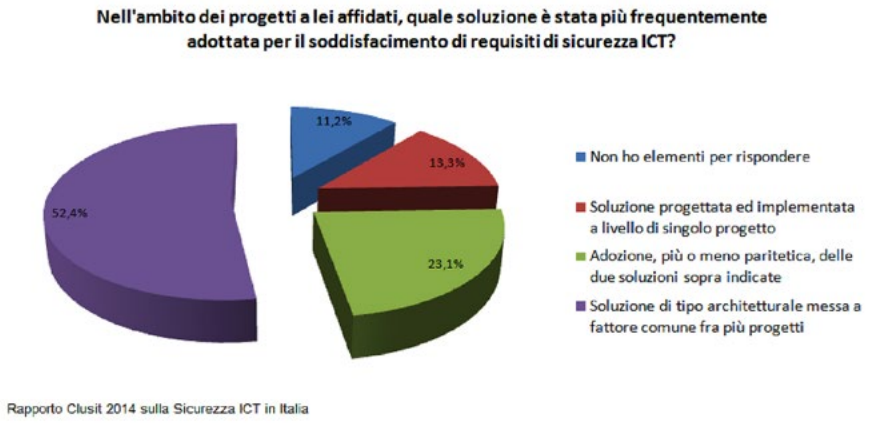


Fig 1: Tipologia di soluzioni di sicurezza

Descrizione del campione

La ricerca è stata condotta nel mese di gennaio 2014 sugli associati PMI-NIC. Vi hanno risposto 283 persone, caratterizzati dal possedere la certificazione professionale di Project

Management Professional. Essi corrispondono a circa un quinto degli associati e vanno rapportati ai 4.500 project manager totali certificati in Italia. Sono quindi un ottimo campione di analisi.
I project manager che hanno risposto al questionario operano su aziende grandi e piccole (per addetti e per fatturato) di ogni settore industriale italiano come riportato nelle figure successive.

Dimensione aziendale	Num. rispondenti
1 - Fino a 15 addetti	19
2 - Da 16 a 100 addetti	29
3 - Da 101 a 500 addetti	56
4 - Oltre 500 addetti	182
	286

Fatturato aziendale	Num. rispondenti
1 - fino a 200k	12
2 - fino a 2.000k	25
3 - fino a 20.000k	61
4 - oltre 20.000k	188
	286

Settore Industriale (scelta multipla)	Num. rispondenti
Informatica	99
Telco	58
Finance	49
Vendor security	42
Utilities	36
Manifatturiero	31
PAL	27
Sanità	20
PAC	15
Commercio	10
Difesa	10
Trasporti	8
GDO	3
Altri	0

Fig 2: Descrizione del campione – Rapporto Clusit 2014 sulla Sicurezza ICT in Italia

Risultanze

Prima di giungere alle conclusioni e ai commenti finali, l'analisi realizzata ci permette di fare diverse considerazioni:
Tutti gli intervistati ritengono che "la presenza di requisiti non funzionali attinenti la sicurezza ICT", ovvero la richiesta di sicurezza nei progetti, sia aumentata (69%) o almeno rimasta invariata (30%) negli ultimi due anni. Quasi nessuno degli intervistati ne riscontra una diminuzione. Questo risultato non costituisce alcuna sorpresa e conferma quello che da più parti già si conosce; infatti i Project Manager e gli esperti di sicurezza, sono testimoni di sempre maggiori richieste dovute all'aumentata sensibilità aziendale ai temi della sicurezza per via degli incidenti di sicurezza molto pubblicizzati sui media e dalle richieste di aderenza a leggi e regolamenti (compliance).

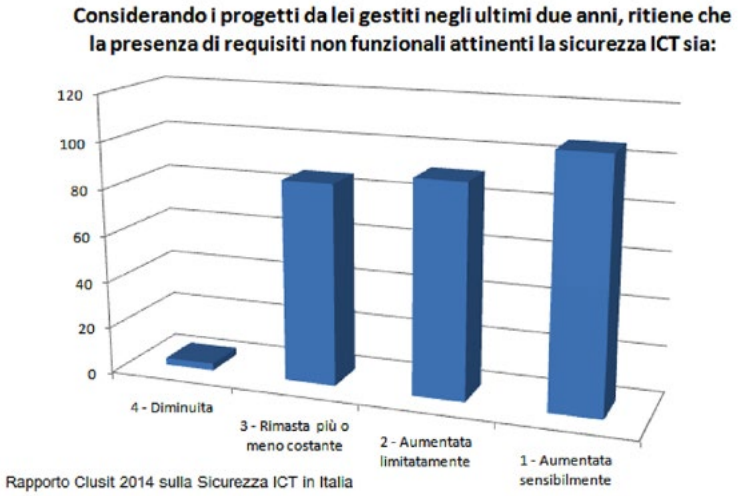


Fig 3: Sensibilità al tema della sicurezza

Il campione, a fronte di una domanda sulle motivazioni aziendali rispetto all'adozione di misure di sicurezza, indica in maniera assolutamente paritetica il rischio (47,7%) e la compliance (48%), ovvero si investe in sicurezza per "l'esigenza di assicurare la compliance rispetto a leggi e normative di sicurezza" e per "l'esigenza di ridurre il rischio di business dovuto a perdita di dati, frodi etc.". La stessa proporzione si riscontra anche separando le grandi aziende dalle piccole e medie, mentre le aziende bancarie sono leggermente maggiormente sensibili al rischio e quelle in ambito telecomunicazione alla compliance. Sempre ininfluente la percentuale di quelli che ritengono si faccia per "l'esigenza di ridurre il rischio di compromettere l'immagine aziendale" (4%); e questo nonostante sia l'Europa sia l'Italia con alcuni provvedimenti per alcuni specifici settori, richiederà o richiede la notifica obbligatoria di eventuali perdite di dati personali alle autorità e alle persone danneggiate (il cosidetto "data breach notification act").

Come già menzionato (**Fig. 1**), più del 50% dei rispondenti si trova più frequentemente ad adottare soluzioni di sicurezza di "tipo architetturale messe a fattor comune fra più progetti". A questi si uniscono un 23% che "adotta in maniera più o meno paritetica le soluzioni messe in comune e quelle a livello di singolo progetto". Tale significativa maggioranza indica che le aziende hanno creato una sovrastruttura di sicurezza alla quale i progetti devono far riferimento, e, come è facile intuire, gli autori di questo report la reputano una buona notizia. E' infatti oneroso e faticoso realizzare la security ogni volta, progetto per progetto. E' sicuramente più efficiente lavorare a livello architetturale. A fronte di un dato certamente positivo, troviamo un 52% che segnala, sia la necessità di "implementare dei requisiti di

sicurezza in corso d'opera" (31%) che quella di dover operare tale intervento "dopo il rilascio del prodotto / servizio" (21%). La nostra interpretazione è che le soluzioni architetturali siano di recente adozione e comunque non sufficienti a coprire tutti i requisiti di sicurezza costringendo, in certi casi, a delle rilavorazioni onerose.
Il 55% dei rispondenti attribuisce al cliente / committente una certa insensibilità rispetto alla sicurezza. Alla domanda "nell'ambito dei progetti a lei affidati, in che misura i tempi e i costi necessari per implementare i requisiti di sicurezza ICT sono stati riconosciuti dal cliente/committente?" il 14% ha risposto "per nulla", il 42% "molto limitatamente", di converso il 44% è invece soddisfatto e un singolo isolato caso, che ci piacerebbe conoscere, ha dichiarato di aver osservato tale riconoscimento "oltre le normali aspettative". A parte le facili battute, su questa tematica si innesta la ricorrente controversia relativa ai cosiddetti "requisiti non funzionali", su cui le specifiche di progetto sono spesso formulate in maniera lacunosa dal committente e, a volte, non chiarite preventivamente e quindi negoziate dal fornitore della soluzione.
In aggiunta a quanto appena argomentato e a parziale scarico di responsabilità del committente, il fattore ritenuto più importante dal Project Manager per "soddisfare i requisiti di sicurezza ICT" è la "disponibilità delle competenze necessarie all'interno del team di progetto" (44%) mentre rimane solo al secondo posto "negoziare tempi e costi adeguati per implementare i requisiti di sicurezza ICT" (28%). A nostro avviso, tale indicazione rappresenta un'ulteriore conferma di quanto sia determinante la capacità di azione collettiva del team e di come il PM possa giocare un ruolo centrale nel "supportare il project team sensibilizzandolo sull'importanza della sicurezza ICT" (23)%. Tale percentuale, se raffrontata con quella riferita alla necessità di "controllare costantemente l'operato del team valutandone i risultati prodotti" (5%) dà la misura di come il "leading by example" sia ritenuto molto più efficace del "leading by control".

Sul tema dell'importanza della formazione specifica di sicurezza per lo stesso Project Manager, quasi il 42% del campione la ritiene "molto importante per ricoprire al meglio il ruolo", il 51% la ritiene "utile ma non indispensabile" e solo il 7% la ritiene non essenziale in quanto essere un tema specialistico. In questo caso, si tratta di un dato più difficile da decifrare e per il quale possiamo azzardare l'ipotesi che presupposti diversi abbiano generato una tale risposta, ovvero: da una parte, quello di chi considera la sensibilità alla sicurezza come un tema più "culturale" su cui il PM può dare un contributo significativo; dall'altra, quella di chi ne vede soprattutto l'aspetto tecnico e quindi la sua estraneità rispetto al ruolo manageriale del PM. Ovviamente, il nostro auspicio che i primi prevalgano sempre più sui secondi.
Il tema della Security by Design non poteva essere affrontato senza andare un po' nel dettaglio di quali effettive misure fossero poi implementate, ma le risposte alla semplice domanda, a risposta multipla con fino a 4 scelte, "nell'ambito dei progetti a lei affidati, quali tipi di soluzioni di sicurezza si è trovato ad implementare?" offrono uno scenario articolato e soggetto a differenti interpretazioni. Proviamo a farlo utilizzando la tabella seguente.
Nell'ultima colonna è riportato quante volte quella specifica misura è stata indicata dai

rispondenti (ad esempio 217 per il controllo accessi); nelle colonne precedenti è riportato il numero totale di altre misure scelte insieme a quella della specifica riga. Per esempio 26 persone hanno scelto un'altra misura oltre al controllo accessi[1].
Il controllo accessi, strong authentication, identity federation, single sign on eccetera, ovvero tutte le tecnologie per assicurarsi dell'identità degli utilizzatori dei sistemi e per restringere la quantità dei dati accedibili si piazza con 217 risposte nettamente al primo posto, praticamente il 75% dei rispondenti ha dichiarato di aver adottato questa misura. Tale numero va però interpretato. Infatti il controllo accessi è ampiamente diffuso in tutti i sistemi, non esiste praticamente più alcuna applicazione che non richieda almeno una coppia di utente e password per permettere l'accesso alle sue funzionalità. Quello che può però cambiare da un punto di vista tecnico è il modo in cui si effettua il processo di autenticazione: la verifica dell'utente viene svolta dentro l'applicazione oppure da del middleware specializzato? In questo secondo caso si potrebbe parlare di Security by Design mentre non nel primo.
Il secondo insieme di misure riguarda la caratteristica della Disponibilità, stiamo parlando del "Backup, ridondanze eccetera" che segue con 160 risposte.
Questa indicazione non ci sorprende: il tema della disponibilità del dato è ormai ben conosciuto dalle aziende e la sua mancanza è immediatamente visibile al top management; di conseguenza negli anni sono stati realizzati diversi investimenti in tale area. Diverso è il caso della Riservatezza che implicherebbe una serie di misure tra le quali la "cifratura del dato a riposo e/o della trasmissione" (92) o dell'Integrità con, per esempio il "logging, auditing, cruscotti e allarmi.." (93). Per queste caratterstiche e le relative misure gli autori si aspettano nel prossimo futuro una crescita di attenzione che speriamo di misurare il prossimo anno (**Fig. 4**).

Conclusioni

Avendo anticipato nelle premesse una visione ottimista circa le prospettive future emerse da questa indagine, non possiamo che ribadire come l'importanza del "Security by Design" sia stata ampiamente riconosciuta dalla popolazione dei project manager coinvolti. Detto questo, vorremmo concludere con delle osservazioni che derivano da una lettura più profonda di alcune delle risposte che sono state date.

In primo luogo, la criticità evidenziata relativamente ai requisiti di sicurezza ci deve sensibilizzare sul fatto che la debolezza e quindi la vulnerabilità di una soluzione deriva molto spesso dalla mancanza di un approccio di tipo "sistemico" per quanto attiene all'identificazione degli stakeholder, al disegno dell'architettura, all'integrazione delle competenze, alla mediazione fra gli interessi in gioco e quindi al rapporto stesso fra cliente e fornitore.

1 Con questa logica salta all'occhio un rispondente che pur avendo indicato "nessuna soluzione" ha però indicato altre due soluzioni (numero 1 in colonna denominata "3"). Questo va essere considerato un errore di chi ha compilato il questionario.

	Numero di misure scelte insieme a quella specifica della riga				
	1	2	3	4	Grand Total
Cifratura del dato a riposo e/o della trasmissione per la riservatezza delle informazioni	0	7	21	64	92
Controllo accessi, strong authentication, identity federation, single sign on ecc. per assicurarsi dell'identità degli utilizzatori e/o per restringere la quantità di dati accedibili	6	26	61	124	217
Code review di sicurezza, vulnerability assessment, penetration testing, controlli di qualità del software ecc. per controllare e prevenire vulnerabilità	0	5	13	51	69
Hardening e patching dei sistemi hardware, sistemi operativi, basi dati e altri componenti software seguendo le raccomandazioni dei vendor	0	4	10	43	57
Logging, auditing, cruscotti, allarmi automatici e presidio umano per evidenziare comportamenti anomali degli utenti e delle applicazioni ecc.	0	7	17	69	93
Backup, ridondanze, sistemi altamente affidabili per garantire la disponibilità del servizio	1	20	54	85	160
Misure tecnologiche e/o organizzative per garantire le buone pratiche della Separazione dei Compiti, Separazione degli ambienti (operativi, rete ecc.), del Minimo Privilegio, del Need to Know, ecc.	0	6	17	53	76
Clausole contrattuali a protezione della propria azienda nei contratti (per rischio e per la compliance)	4	7	29	40	80
Formazione degli utenti utilizzatori e degli utenti amministratori sui temi di sicurezza	0	2	14	27	43
Nessuna soluzione	15	0	1	0	16

Fig 4: Adozione delle misure di sicurezza - Rapporto Clusit 2014 sulla Sicurezza ICT in Italia

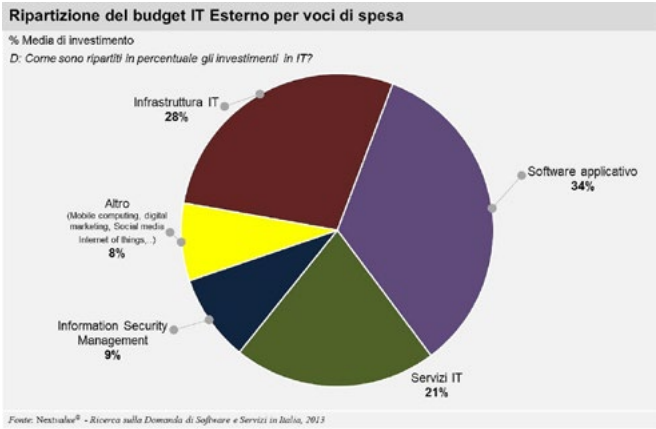
Come sappiamo, rispetto a questo fenomeno non sono certo estranei l'utilizzo spinto dell'outsourcing, la parcellizzazione dei ruoli e delle responsabilità, la compressione dei costi e le rigidità contrattuali che spesso influenzano l'impostazione stessa del piano e dell'organizzazione progettuale.

In secondo luogo, le sottolineature relative alle competenze del team e al ruolo centrale del PM quale elemento di sensibilizzazione sul tema della sicurezza, non fanno che dimostrare come la performance progettuale sia basata su una formula molto semplice, che vede al numeratore il prodotto di due fattori, hard skills e soft skills, rispetto ai quali le buone prassi e soprattutto l'ambiente di lavoro devono contribuire, sia come facilitatori dell'azione collettiva, che come riduttori di complessità".
Ci piace infine ricordare che l'evento organizzato dal PMI-NIC nel febbraio del 2013 in collaborazione con Clusit, ha stabilito il record assoluto di presenze sfiorando i 400 partecipanti. Tutto ciò, al di là delle evidenze statistiche analizzate in questo survey, è comunque di buon auspicio per un futuro in cui le organizzazioni riconoscano al tema della sicurezza ICT tutta l'importanza e l'attenzione che merita.

La Security vista dal Management

A cura di Alfredo Gatti

Siamo in molti a ritenere che al gioco della sicurezza dell'informazione sia molto difficile vincere. Ho avuto modo di tornare su questo argomento in molte occasioni di incontro con "numeri uno" di grandi imprese italiane e loro riporti, tra cui diversi Direttori IT che partecipano alla community CIONET. Nessuno si illude: i "cattivi" dispongono di mezzi e di competenze mai visti finora e nessun business può essere al riparo da rischi se costoro ritengono che valga la pena di attaccarlo. Ciononostante è fondamentale definire una strategia di Information Security Management che includa anche "il che cosa fare prima, durante e dopo" un attacco, oltre che assicurarsi che la propria azienda disponga di difese informatiche aggiornate. Il gioco è quindi più complesso e dal suo esito finale può dipendere la sopravvivenza dello stesso business.

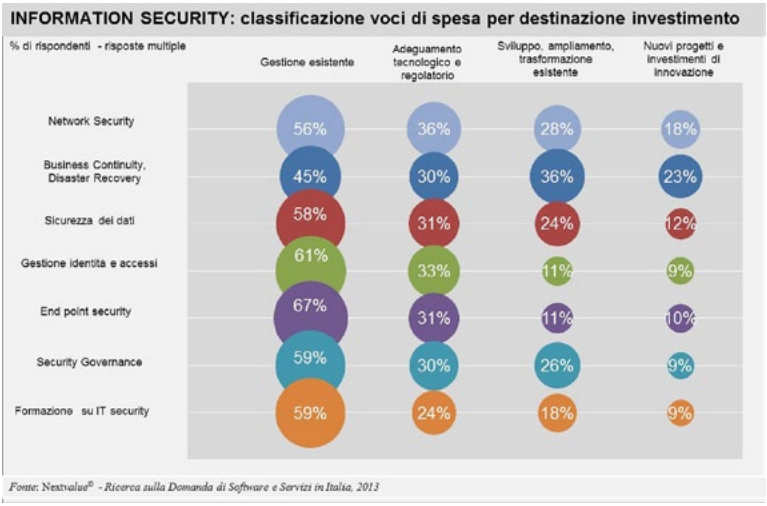


Il primo risultato delle nostre ricerche condotte sui vari panel di decisori al top delle imprese italiane è proprio questo: la comprensione della problematica e dei rischi connessi all'information security management di anno in anno migliora e di pari passo cresce l'attenzione per le strategie di difesa che, peraltro, potrebbero indebolirsi o perdere di smalto a causa dalle ristrettezze di bilancio imposte dal perdurare della crisi economica.

Conseguenza diretta sono alcuni inequivocabili fatti positivi:

- i budget dedicati al rafforzamento e al mantenimento delle difese informatiche si mantengono nell'ordine del 9% dei budget IT complessivamente spesi con fornitori esterni;
- in parecchie organizzazioni, come istituzioni finanziare e telco, questi budget non sono

che la punta di dell'iceberg dieci volte maggiore dedicato alla problematica complessiva;
- CSO e CISO, laddove già presenti, tendono sempre più a rispondere ai primi livelli del management aziendale, pur mantenendo il loro link con la funzione IT.



Purtroppo questi trend positivi avvengono proprio mentre i "cattivi" divengono sempre più minacciosi e le loro tecniche di aggressione divengono sempre più sofisticate e inarrestabili, con la conseguenza di un lungo sciame di danni economici e alla reputazione delle imprese, alla loro stessa capacità di competere. Se i "cattivi" vincono sempre, può ingenerarsi nel management dei "buoni" un certo scetticismo, se non proprio una perdita di fiducia nella capacità di contrastare il cybercrime. Se quest'ultimo continua a generare un fatturato che supera il PIL della Danimarca, forse rimane poco da fare ai "numeri uno" delle grandi imprese. Anche se continuano ad ostentare tranquillità e confidenza, in cuor loro potrebbe diffondersi una certa dose di fatalismo e, in questo caso, il top management diventerebbe parte del problema e non la chiave di volta della sua soluzione.

A distanza di un anno dalla prima pubblicazione del nostro Insight dedicato all'Information Security Management nelle Imprese Top italiane e che tanto interesse ha riscosso da parte di nostri follower, siamo ritornati decisamente sull'argomento riproponendo ai numerosi e qualificati CIO, CISO e CSO del nostro panel la questione dell'impatto della sicurezza dell'informazione sul business delle loro aziende. Con essi stiamo aggiornando la situazione degli investimenti, degli aspetti organizzativi, della gestione del rischio e della compliance e di come il tutto è soggetto a una governance. I loro preziosi feedback sono, ancora una volta, confortanti. Anche se è scontata l'alta probabilità di perdere al gioco della sicurezza, sono i "buoni" che, anche nel nostro Paese, ce la stanno mettendo tutta per cambiare le regole del

gioco e mettere in campo la strategia vincente.
I risultati preliminari della nostra survey confermano che CSO e CISO, pur alle prese con sempre nuove criticità, cercano di coinvolgere sempre di più i primi livelli di management. Il primo gap da colmare è appunto la loro stessa capacità di coinvolgere tutti gli stakeholder e far sì che la sicurezza dell'informazione sia una responsabilità condivisa mentre l'impresa procede nel proprio sviluppo e nei propri programmi di innovazione.
La sicurezza stessa è innovazione e non una battaglia di retroguardia. L'azione della prima linea di management è fondamentale perché il cammino avvenga quanto più possibile senza scossoni o rischi di ribaltamento; in molti sono ben consapevoli che l'approccio tradizionale alla sicurezza informatica è ormai collassato con il progredire delle stesse tecnologie e dei modelli di business. Perfino i timori iniziali correlati ai servizi Cloud stanno sublimando e il grado di fiducia in questi servizi e nei provider che li propongono appare migliore con il crescere dell'accessibilità e delle verifiche sul campo. Nelle migliori piattaforme di Governance, Risk e Compliance (GRC) sono già presenti numerosi building block rassicuranti, anche se alcune aree grigie rimangono in fatto di commistione dei dati e quando sia difficile ottenere dal provider la piena trasparenza sulla protezione e le modalità di manipolazione dei dati stessi.
A mio avviso la sicurezza dell'informazione nel Cloud richiede ancora qualche passo avanti sia da parte dei provider, sia da parte delle aziende loro clienti. Almeno nelle fasi iniziali di adozione di servizi in Cloud occorrerebbe essere pronti a rinunciare a parte dei benefici diretti per reinvestire i risparmi economici ottenuti nel rafforzamento della sicurezza nel nuovo ambiente e familiarizzare con esso.

Un ulteriore aspetto critico, come è noto, ha a che vedere con l'area dell'End User Computing, nel momento in cui la mobility diviene scontata. Per fare un esempio, senza scomodare practice di Bring Your Own, è normale per uno user effettuare azioni di tipo "dropbox" anche per dati e applicazioni aziendali. Gli stessi "numeri uno" lo fanno, assumendo che il loro comportamento da provetti consumatori sia corretto anche per il loro IT. Di certo non è nelle loro priorità scegliere practice di file sync & share corrette o preoccuparsene.
In questo scenario di per sé complesso sta irrompendo anche l'Internet of things, o, meglio, ogni oggetto va in Internet: l'era IoT è abbondantemente cominciata e oggetti ed apparati di ogni sorta acquisiscono capacità di processing che cambiano la loro stessa natura.
Lo stesso concetto di "computing" assume un significato diverso, mentre cambiano le aspettative e gli orizzonti degli utilizzatori attraverso soluzioni e servizi sempre più in tempo reale. Così la sicurezza delle "cose", ma anche degli apparati, degli impianti e delle stesse infrastrutture, amplia esponenzialmente il "perimetro" della situational awareness aziendale. Mutuando questo termine dalle tattiche militari, le organizzazioni più avanzate hanno cominciato a chiamare così la consapevolezza delle capacità di difesa dispiegate.
Che la cyber situational awareness si debba estendere molto oltre i confini dell'organizzazione o della struttura è assodato, pertanto sempre più imprese si consociano in network per mettere a fattor comune conoscenze, capacità, risorse, analisi di big data inerenti la

sicurezza, per sostenersi l'un l'altra e rafforzare la difesa complessiva.
Dominare la cyber situational logic avvalora anche la posizione ed il ruolo del Chief Information Security Officer, in quanto capace di mettere in collegamento minacce prevedibili con oggettive capacità di risposta.
Allorché capiti un incidente, il CISO è (o forse dovrebbe essere) in grado di rispondere a tre domande essenziali: che cosa è accaduto? Perché è potuto accadere? Che cosa facciamo adesso?
Per dare una risposta immediata alle prime due domande, l'organizzazione si basa sulla cognizione della propria posizione di difesa. La risposta alla terza domanda dipende fortemente dalla capacità di reazione che è stata predisposta con anticipo. Il "che cosa facciamo adesso?" è tanto più immediato ed efficace, quanto più la singola impresa avrà mutuato esperienze da altre imprese, puntando a realizzare con esse un sistema condiviso di informazioni, di competenze e di risorse. La cyber situational logic implica questa capacità di delimitare le zone di impatto e la conoscenza a priori delle conseguenze negative di un incidente di per sé probabilmente inevitabile, ma anche e soprattutto quella del what's next.

La questione della sicurezza dell'informazione entra in uno scenario più evoluto, in cui è il business stesso a subire un forte cambiamento per questioni di sicurezza. Come abbiamo ribadito, nessuna organizzazione può ritenersi al 100% al sicuro da aggressioni, per cui è normale che tutte le organizzazioni investano risorse e tempo in modo significativo per accrescere le loro capacità di intercettazione e di pianificazione delle risposte agli attacchi. Il rischio cibernetico è sempre più anche un'idea fissa dei numeri uno in azienda, anche se la sensazione è che siano ancora in molti a confidare forse troppo nelle capacità delle nostre organizzazioni o, peggio, nelle capacità dei partner di venire in nostro soccorso all'ultimo momento.
Questo nuovo scenario è, naturalmente, mutevole ed è inevitabile che anche per l'intera industry della sicurezza si giunga ad uno spartiacque. Al di là degli strumenti e delle practice indotte dall'innovazione tecnologica, anche una maggiore collaborazione tra privato e pubblico dovrebbe ricevere maggiori impulsi, considerato che ormai agenzie, legislatori e policy-maker hanno tutti gli elementi per avviare un circolo virtuoso che va a favore di tutti. In qualche modo, anche informale, le stesse imprese del settore privato già scambiano tra di loro informazioni critiche su minacce, incidenti e workaround. La collaborazione tra pubblico e privato può diventare uno step in più per riequilibrare le forze in campo a sfavore dei "cattivi".

Se la questione non è se e quando saremo attaccati, ma cosa fare dopo: prevenzione e capacità di risposta sono la condizione necessaria. Per vincere tuttavia occorre saper agire dopo l'attacco: i cybercriminali vinceranno molte battaglie, ma saranno sempre più vittorie di Pirro, ce lo auguriamo, quando la maggior parte delle organizzazioni sarà in grado di mitigare le conseguenze delle violazioni inevitabili e predisporre piani efficaci di sopravvivenza. Credo che questa sia la strada in cui crede maggiormente il management, anche quello del-

le imprese italiane e la nuova frontiera è di investire perché questi piani "del dopo" funzionino. Per prima cosa questi piani non dovrebbero essere "generici", ma correlati puntualmente agli specifici accadimenti, mentre le organizzazioni dovrebbero superare la complessità dell'integrazione di questi piani nelle varie unità di business. Spesso le singole unità creano loro piani di risposta ottimizzati, che possono essere utili per trattare con attacchi mirati, ma che non sono così efficaci per la gestione di un incidente attraverso l'intera organizzazione. È il classico approccio "a silos", che inibisce anche la condivisione delle conoscenze e delle best practice, tipicamente identificate in alcune persone che hanno il compito "istituzionale" di conoscere e attuare il piano, perdendo il vantaggio degli automatismi che l'intera community di business dovrebbe possedere.

Una parte fondamentale della strategia è poter disporre di informazioni, mettere a fattor comune le esperienze, aprirsi sull'argomento in situazioni pre-competitive. Il nostro Insight vuole essere uno strumento che serve a questo, perché riporta fedelmente risultati e posizioni di merito utili a tutti gli stakeholder della sicurezza dell'informazione, ma sono soprattutto associazioni come Clusit, i rapporti diretti tra addetti ai lavori, tra le aziende private e le istituzioni pubbliche, che possono fare la differenza in questo momento pur sempre molto critico per la sicurezza dell'informazione.

Formazione e consapevolezza, strumenti indispensabili per la Sicurezza delle Informazioni

a cura di Andrea Rui e Stefano Ramacciotti

Più aumentano l'attenzione e le competenze specifiche nel settore e più aumentano i casi di cybercrime a danno degli utenti. È una sorta di forbice che si apre: da una parte (quella professionale) la consapevolezza aumenta, e dall'altra (quella della gente comune, ben più vasta) diminuisce. Onde invertire questa tendenza è evidente che occorre estendere il nostro *target* di riferimento comprendendo, oltre al mondo degli utenti professionali, anche le categorie che fino ad oggi sono state meno considerate. È per questo motivo che quest'anno dedichiamo uno spazio anche allo stato della formazione in Italia per un utilizzo del Web e delle nuove tecnologie consapevole e sicuro.
Mentre sino a poco tempo fa si viveva in un'era post-industriale, oggi stiamo vivendo in un'epoca "esponenziale", in cui il tempo e la velocità non sono più definiti dai mezzi di trasporto, ma da Internet e dalla velocità del trasferimento delle informazioni. Chi oggi parla di sicurezza in Rete è nato e cresciuto senza telefoni cellulari ed ha avuto il tempo di evolvere con le tecnologie della Rete; tuttavia anche costui oggi fatica a stare dietro all'evoluzione della tecnologia.

Ancora peggiore è la situazione per i cosiddetti "nativi digitali", di coloro che sono nati avendo già un computer in casa e una connessione ad Internet. Ma le cose evolvono così in fretta che adesso anche questa generazione è stata superata: siamo ormai alla generazione dei"*mobile born*", di coloro che non installano sistemi operativi: semplicemente, li usano (sempre che sappiano cosa sono e a cosa servano), e che non installano più applicazioni, ma scaricano "*app*" in quantità. Ma la semplicità della Rete con i suoi servizi, e la promessa di un ingannevole "tutto gratis"[1], sono fattori che portano con sé un uso sempre più inconsapevole di tecnologie che divengono ogni giorno più complesse e potenzialmente subdole. Occorre quindi far comprendere che, qualsiasi sia il servizio che si utilizza e indipendentemente da chi lo fornisce, se il servizio è gratuito, è perché **il prodotto è l'utente stesso**.
Per svariate ragioni, in questi ultimi anni l'attenzione dei media ai problemi della sicurezza della Rete e degli utenti in Rete è andata costantemente crescendo.
Tuttavia è da rilevare che gli sforzi mediatici tendono più a fare allarmismo piuttosto che a sviluppare consapevolezza nei cittadini; è un continuo sentir dire che avvengono frodi e furti d'identità *on-line*, ma quasi mai si tocca il tema di come la gente possa e debba difendersi. Anche quando vengono intervistati i soliti esperti si sentono spesso dire banalità e non si avvia mai un serio programma di informazione per la popolazione.
Da ciò deriva una diffusa mancanza di fiducia in Internet e nelle sue potenzialità, limitando l'*e-Commerce*, l'*home banking* ed il rapporto telematico del cittadino con la Pubblica

[1] "77% of all Apple App Store revenue now comes from gaming, and 92% of this sum is paid using in-app purchases" (http://blog.kaspersky.com/5-signs-of-extortion-in-free-games/)

Amministrazione, contribuendo a favorire quello che viene anche definito digital divide, troppo spesso erroneamente associato soltanto alla disponibilità e all'accessibilità di tecnologie e connettività.

La mancanza di consapevolezza, unita alla diffusa disinformazione e all'allarmismo portano da un lato i cittadini meno digitalizzati, di solito i più anziani, a evolvere (tecnologicamente) ancora più lentamente, e porta i cittadini della Rete (i cosiddetti netizen) a ignorare gli evidenti allarmismi dei più anziani, ritenuti poco credibili, spesso ignorando anche i principi più elementari della prudenza, della discrezione e della riservatezza.
Consideriamo poi l'effetto che tutto ciò ha sull'economia (e in un momento di crisi come questo è un obbligo): alcuni studi evidenziano una stretta correlazione tra aumento della banda e aumento del PIL. La Ericsson, in una ricerca del 2011, dice che:"*Doubling the broadband speed for an economy increases GDP by 0.3%*"[2], ma ci sono autori che si spingono fino a un aumento dell'1% del PIL al raddoppio della banda. Altri studi[3], portano a dire che gli effetti dell'aumento di banda sono meno efficaci nei confronti dei paesi meno inclini ad accettare i cambiamenti (come l'Italia che, a seconda delle statistiche, si ritrova soltanto tra il 50o[4] e il 95o[5] posto nel mondo come capacità della propria rete ADSL).

Origine del Problema

Questo *digital divide*, come si è già detto più culturale che tecnologico, ha le proprie origini in una concomitanza di cause che, combinandosi, amplificano il problema sociale.
Certamente ha contato molto la velocità con cui il mercato ha reso disponibili alle masse strumenti quali *smartphone, tablet* e connettività dalle caratteristiche tanto impensabili che la società e la cultura non hanno fatto in tempo a prepararsi e ad adeguarsi al fenomeno.
Se fino a pochi anni fa chi utilizzava un computer aveva almeno una vaga idea della distinzione tra *hardware*, *software* (sistema operativo e programmi, che dovevano essere installati manualmente), e dati, oggi ci troviamo invece a utilizzare i dispositivi appena estratti dalla confezione (persino la batteria è già carica!), e a creare e comunicare dati senza sapere dove questi risiedano realmente.
Un ulteriore causa è imputabile al totale stravolgimento del *modello di business*: se fino a pochi anni fa i prodotti e i servizi avevano un prezzo, per cui prima di impegnarsi si cercava anche di comprendere cosa si stava acquistando e si facevano confronti, oggi abbiamo accesso ad un'infinità di servizi ed applicazioni a costo zero, o al limite al costo di un caffè.
È importante poi l'aspetto psicologico ove la quantità, e non la qualità, delle applicazioni e dei servizi a nostra disposizione fanno sì che l'irrazionalità della fretta e della curiosità

---

2 http://www.ericsson.com/news/1550083
3 https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/ 85961/UK_Broadband_Impact_Study_-_Literature_Review_-_Final_-_February_2013.pdf
4 International Business Times – http://it.ibtimes.com/articles/46459/20130411/internet-disastro-italia-cinquantesimo-posto-rapporto-innovazione.htm
5 NetIndex.com - http://www.netindex.com/download/allcountries/#

di provare abbiano il sopravvento sulla razionalità del chiedersi che cosa si stia realmente facendo.
Un aspetto certamente fondamentale è il modo di rapportarsi del *netizen*, sia con la tecnologia che con i propri simili, che è radicalmente cambiato. Fino a pochi anni fa vi era una certa ritrosia nell'affidarsi completamente alla tecnologia. Oggi, dove tutte le relazioni sono ormai quasi

sempre mediate da qualche mezzo informatico, i *netizen* non si pongono più nemmeno il problema: una informazione è vera perché lo dice un oggetto da pochi centimetri cubici. Anche le relazioni personali sembrano essere cambiate. Prima le relazioni si consumavano tra gli interessati, e al limite si estendevano a cerchie un po' più allargate attraverso il passaparola o il pettegolezzo, e avevano una durata legata soltanto alla memoria delle persone e alle fotografie fatte stampare a caro prezzo. Oggi, nonostante la Sociologia ci dica che vale ancora il "numero di Dunbar"[6] (circa 150 è "limite cognitivo teorico che concerne il numero di persone con cui un individuo è in grado di mantenere relazioni sociali stabili"), quanti non conoscono ragazzini che si vantano di avere migliaia di "amici" sui più noti *social network*, senza nemmeno sapere quanto tale elevato numero aumenti i loro rischi.
L'immediatezza del rapporto con gli altri ha fatto perdere la possibilità di riflettere e di cambiare idea prima di dire o scrivere qualcosa, e la mediazione telematica ha, di fatto, limitato la possibilità di cogliere le emozioni, l'espressività e la gestualità che sono elementi fondamentali nel relazionarsi.
Lo stesso oblio dei ricordi con cui le civiltà hanno convissuto per millenni è stato completamente scardinato dalla sua funzione sociale, a causa della persistenza della memoria della Rete e della semplicità con cui è possibile accedere a questa incredibile "macchina del tempo universale".

Target di riferimento

Usando il gergo proprio dei pubblicitari, con "*target di riferimento*" vogliamo intendere gli utenti non-professionisti che già utilizzano il digitale. Essendo un insieme di persone troppo vasto per un'efficace opera di sensibilizzazione, appare più opportuno concentrarsi su chi rappresenta il futuro di questo Paese: i ragazzi in età scolare. Ben sapendo che quelli più grandi, delle Superiori, saranno già un gruppo difficile da raggiungere, dato che, in mancanza di informazioni precise, si sono spesso già fatti idee proprie, spesso errate e difficili da eradicare.
Purtroppo, la velocità con cui si succedono le generazioni (non biologiche ma culturali) ha reso completamente impreparate le classi dei genitori, dei nonni e degli insegnanti (per non parlare delle istituzioni), che da sempre hanno svolto un ruolo fondamentale nell'educazione e nella crescita psicologica dei minori. I genitori e i nonni che insegnavano ai bambini il classico: "Non accettare caramelle dagli sconosciuti!" non sono preparati a rimodulare questo insegnamento per la nuova vita sociale in Rete.

---

[6] http://it.wikipedia.org/wiki/Numero_di_Dunbar

Questa inadeguatezza porta quindi a reazioni di totale divieto o completa permissività, non sapendo ove sia quella linea di confine tra il bene e il male, tra la sicurezza ed il pericolo.
Oltre ai ragazzi in età scolare, alle loro famiglie (genitori e nonni), il *target* su cui intervenire è, ovviamente, anche quello del personale didattico (dirigenti scolastici, docenti, tecnici di laboratorio). È il caso di notare che ognuna di queste figure è un portatore di interessi diversi, in relazione al proprio ruolo nell'educazione dei giovani. Pertanto, così come si suddividono i ragazzi in fasce d'età per ottimizzare la loro formazione, è necessario anche prevedere temi ed approcci diversi per le diverse figure.

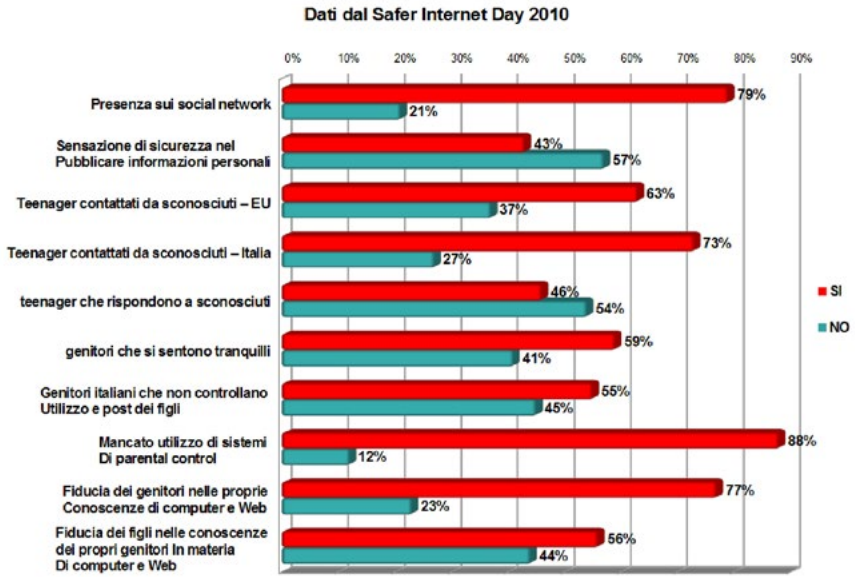
Situazione Attuale

Dal punto di vista della sicurezza, attualmente la scolarizzazione informatica porta benefici minimi, quando non ne aumenta i pericoli a causa della frequente limitata preparazione dei docenti su tematiche di sicurezza delle informazioni. L'approccio generale è più orientato all'insegnamento utilizzando le nuove tecnologie, come le LIM che alla comprensione di come realmente funzioni un sistema informatico. A maggior ragione mancano le competenze per spiegare come funzionino la connettività e le tecnologie mobili.
Esistono naturalmente dei punti di eccellenza: scuole che oltre ad aver scelto lo strumento informatico come mezzo didattico colgono anche l'offerta disponibile per organizzare momenti di informazione e di formazione per studenti, genitori e terza età.
Certamente sfugge a una gestione didattica organizzata e coerente il fatto che i giovani di oggi saranno, tra pochissimi anni, coloro che governeranno l'Italia, la sua società e la sua economia, e che solo il loro grado di comprensione delle tecnologie della Rete e del loro funzionamento farà in modo che il nostro Paese possa di nuovo sedere a pieno titolo al tavolo dei Grandi o essere un mero inseguitore nella competizione per l'innovazione e la crescita nel panorama livello mondiale.
E mentre ancora ci attardiamo a parlare di *smartphone* e *mobile*, la Internet dei PC si sta trasformando nella *Internet of things*, dove persino i nostri orologi (*smartwatch*) e gli occhiali (*SpaceGlasses*) sono divenuti oggetti attivi e costantemente connessi, con notevoli problemi per la *privacy* propria e degli altri.
E purtroppo l'aspetto sociale delle tecnologie della Rete non viene affrontato se non citando come "social" servizi quali *FaceBook*, *Twitter*, *WhatsApp*, etc., invece che il loro impatto e le loro implicazioni sulla vita sociale "reale". Gli stessi provider non aiutano dato che chiamano "amici" quelli che sono al più dei semplici "conoscenti", abbattendo, di fatto, le ultime remore dei più giovani internauti.
È difficile presentare dati aggiornati, in quanto l'unica rilevazione sistematica su scala europea risale ancora al 2010, con il Safer Internet Day, promosso da Insafe; rilevazioni più recenti, come quella IPSOS del 2013[7], si basano su campioni molto più ristretti, e quindi meno significativi; tuttavia dal confronto con i dati del 2011 emerge un leggero miglioramento nella percezione dei pericoli relativi a cyberbullismo e molestie di vario tipo, mentre

[7] http://images.savethechildren.it/IT/f/img_pubblicazioni/img204_b.pdf

peggiora la percezione di quelli relativi a mancanza di relazioni significative, disturbi alimentari e malattie trasmissibili
Telefono Azzurro riporta[8] che circa un quarto degli adolescenti ha trovato on-line pettegolezzi e falsità sul proprio conto o foto imbarazzanti, e di aver ricevuto SMS o MMS a sfondo sessuale.
È anche difficile ottenere dati specifici sui reati sui minori perpetrati attraverso o grazie allo strumento informatico.
La mancanza di una cultura della sicurezza delle proprie informazioni emerge anche dai dati 2012-2013 della Polizia Postale, con 93.815 denunce e 24.000 frodi creditizie perpetrate attraverso il furto d'identità, con un danno complessivo di 195 milioni di Euro.

I dati emergenti dal *Safer Internet Day 2010* riportavano, già allora, un quadro in cui la maggioranza dei giovani ha una importante presenza sui social network, pubblica tranquillamente informazioni molto personali quali il proprio indirizzo, la propria scuola, la foto ed i propri contatti, e soprattutto si sente assolutamente tranquilla nel farlo.



Risultava che quasi i tre quarti dei teenager italiani fossero stati contattati online da sconosciuti (una percentuale peggiore della media europea, attestata intorno ai due terzi), ed emergeva un altro aspetto preoccupante: quasi la metà dei giovani rispondeva, per la curiosità, a persone sconosciute.

8 http://www.azzurro.it/it/news-ed-eventi/area-stampa/statistiche-recenti/88

Un aspetto degno di riflessione è che quasi la metà dei genitori tende a sovrastimare le proprie competenze in materia di computer e di Web e il grado di maturità e prudenza dei propri figli, al punto di non controllare l'utilizzo che i figli fanno della Rete. Purtroppo vi è da dire che spesso non saprebbero nemmeno dove guardare. Da qui la scarsa stima che i figli nutrono nelle competenze dei propri genitori.
Dalla data del sondaggio a oggi i numeri non hanno fatto che amplificarsi grazie all'incremento dell'accesso alla Rete via ADSL e soprattutto al *mobile* e alle reti 3G e 4G.
Ciò ha fatto sì che i giovani di oggi abbiano perso quasi totalmente di vista il concetto di privacy e di come la sua perdita possa condizionare la propria vita presente e futura, e che le attuali generazioni di adulti e le istituzioni, che hanno il compito di educarli e farli crescere in modo sano, abbiano perso la capacità di farglielo comprendere.

Occorre tuttavia evidenziare come le istituzioni stiano iniziando a sviluppare una certa attenzione ai problemi della Rete, come testimonia la recentissima pubblicazione del Codice di Autoregolamentazione contro il Cyberbullismo[9].
A causa di questa situazione di disinformazione diffusa si è andata sviluppando in gruppi di associazioni e professionisti del settore una percezione condivisa della necessità di offrire un proprio contributo, al fine di mitigare gli atteggiamenti sbagliati che le nuove generazioni adottano nell'utilizzo di Internet.
Anche alcune istituzioni e rappresentanti delle istituzioni (Magistrati, Polizia Postale, Difesa, etc.) e aziende private con i propri specialisti in sicurezza informatica e cybercrime organizzano interventi informativi e di sensibilizzazione sul territorio. Tuttavia si tratta di interventi senza un denominatore comune tra loro, ciascuno presentando, interpretando e veicolando il messaggio della sicurezza attraverso il filtro della propria professionalità; questo approccio porta ad una dispersione degli sforzi e alla loro scarsa riutilizzabilità.
Mancando un piano coordinato, non si riesce attualmente a capitalizzare gli sforzi, impedendo quindi di raggiungere e coprire con costanza e uniformità ogni nuovo anno scolastico e tutto il territorio.

Verso quale direzione andare

La rapidissima evoluzione della "*Internet of things*" offre purtroppo pochissimo tempo per l'aggiornamento continuo, e chi dovrebbe sapere ed insegnare si trova invece sempre ad inseguire i giovani, il mercato e la legge.
Per quanto siano i benvenuti, tutti gli sforzi puntuali di professionisti, associazioni ed aziende per elevare le competenze e il grado di consapevolezza di giovani e docenti risultano estemporanei, e non hanno il potere di garantire la diffusione su tutto il territorio e la continuità a tutte le nuove generazioni.
Anche ricerche come quella condotta nel 2010 per il *Safer Internet Day*, se non ripetute e aggiornate con continuità, non possono offrire informazioni sufficienti per adeguare nel

[9] http://www.sviluppoeconomico.gov.it/images/stories/documenti/codice_cyberbullismo_8%20gennaio_2013.pdf

tempo le scelte della politica. Ed è per questo aspetto, che potrebbe essere auspicabile il coinvolgimento del Ministero della Giustizia nel reperire dati aggiornati sui reati specifici che coinvolgono i minori e del Ministero dell'Istruzione.
Occorre pertanto introdurre nel piano dell'offerta formativa per i giovani anche gli argomenti per un utilizzo consapevole dei servizi che la Rete offre, incentivando coloro che partecipano all'educazione dei giovani, fornendo loro la formazione e gli strumenti didattici utili e necessari per svolgere il proprio compito. E questo sia per aumentare la consapevolezza, che per fornire una prima risposta a quanto detto dall'ing. A. Ragosa, Direttore Generale dell'Agenzia per l'Italia Digitale, in occasione del Security Summit 2013 a Roma: «... *già nel corso del 2013 in Europa non saranno occupati un milione di posti di lavoro disponibili legati all'economia digitale perché mancano le competenze sufficienti per ricoprirli*», e specificamente nel settore della sicurezza.

Sono pertanto da sostenere tutti gli interventi finalizzati a "formare i formatori", che potrebbero contribuire a sviluppare le figure professionali mancanti, portando conoscenza nelle scuole e creando parallelamente nuovi posti di lavoro.
Per il conseguimento dell'obiettivo è di fondamentale importanza sfruttare tutte le sinergie disponibili. In questo senso Clusit, con la collaborazione del capitolo italiano di (ISC)[2], ha stabilito un rapporto con il Ministero dell'Istruzione, dell'Università e della Ricerca (MIUR) al fine di affrontare il problema e sviluppare e promuovere gli strumenti didattici necessari.

Gli autori del Rapporto Clusit 2014

Luca Bechelli è consulente indipendente nel campo della sicurezza informatica dal 2000. Con aziende partner svolge consulenza per progetti nazionali ed internazionali su tematiche di Compliance, Security Governance, Risk Management, Data Protection, Privilege Management, Incident Handling e partecipa alla progettazione ed al project management per attività di system integration. Svolge attività di ricerca e sviluppo con aziende nel campo della sicurezza e tramite collaborazioni con enti di ricerca, nell'ambito delle quali ha svolto docenze per master post-laurea. È co-autore di pubblicazioni scientifiche e tecni- co/divulgative. Socio Clusit dal 2001, è membro del Direttivo e del Comitato Tecnico Scientifico dal 2007 ed ha partecipato come docente a numerosi seminari Clusit Education, anche nell'ambito dei Security Summit.

Gianluca Bocci, laureato in Ingegneria nel 1996, certificato CISA, CISM, Lead Auditor ISO/IEC 27001:2005 e ITILv3, ha maturato un'esperienza pluriennale nel settore della Sicurezza Informatica, inizialmente come Security Solution Architect presso multinazionali di rilevanza per lo specifico settore con la conduzione di attività progettuali per Clienti di fascia enterprise e attualmente in Poste Italiane S.p.A. in qualità di Security Professional Master nella funzione corporate "Tutela Aziendale - Sicurezza delle Informazioni" supportando le attività del Computer Emergency Response Team e la realizzazione del Distretto di Cyber Security previsto nell'ambito delle iniziative del Programma Operativo Nazionale (PON).

Raoul "Nobody" Chiesa, 40 anni, torinese, dopo essere stato tra i primi hacker italiani a cavallo tra gli anni '80 e '90, decide nel 1997 di muoversi verso l'Information Security professionale e fonda una delle prime aziende di security consulting «vendor-neutral». Raoul, socio fondatore del CLUSIT, è membro del Comitato Direttivo di ISECOM, CLUSIT, OWASP Italian Chapter, Osservatorio Italiano Privacy (AIP/OPSI); è inoltre uno dei coordinatori del GdL "Cyber World" al CASD/OSN (Centro Alti Studi Difesa, Osservatorio per la Sicurezza Nazionale) presso il Ministero della Difesa.

Nel novembre del 2012 fonda Security Brokers Società Cooperativa per Azioni, un innovativo think-tank composto da professionisti provenienti dal mondo dell'Information Security con esperienza ultradecennale in differenti settori di specializzazione.

Dal 2003 Raoul ha iniziato la sua collaborazione con l'agenzia delle Nazioni Unite "UNICRI" (United Nations Interregional Crime & Justice Research Institute) lavorando al progetto "HPP" (Hacker's Profiling Project); oggi il suo ruolo presso UNICRI è quello di "Special Advisor on Cybercrime Profiling".

Dal 2010 Raoul è membro del PSG (Permanent Stakeholders Group) di ENISA, European Network & Information Security Agency, con mandato sino al 2015.

E' autore di numerose pubblicazioni, cartacee ed on-line, sia all'Italia che all'estero, tra cui: Apogeo Editore, Feltrinelli, McGrawHill, Taylor&Francis Group/CRC Press, Hoepli, Sperling&Kupfler, ed e' ospite in tramissioni televisive nazionali ed estere sin dal 1996.

Davide Del Vecchio, da sempre appassionato di sicurezza informatica, con il soprannome "Dante" ha firmato numerose ricerche nell'ambito della sicurezza informatica. Scrive sporadicamente per Wired ed altre testate ed è tra i fondatori del Centro Hermes per la Trasparenza ed i Diritti Digitali in rete. Ha collaborato con diverse università ed ha partecipato come relatore a parecchi congressi nazionali e internazionali.

Attualmente ricopre il ruolo di responsabile del SOC e dei servizi di sicurezza gestita per i clienti executive di FASTWEB.

Alfredo Gatti è imprenditore, managing partner e fondatore di NEXTVALUE, e managing director di CIOnet Italia. In questo ruolo si dedica ai programmi di ricerca sui temi emergenti e di sviluppo di relazioni con imprenditori e manager del mercato IT e New Media, affiancando i decisori in progetti di sviluppo, innovazione e Merger&Acquisition.
Essi gli riconoscono capacità di visione e manageriali, leadership e competenze, assieme ad un approccio pragmatico e orientato ai risultati ed eticamente sempre corretto.
Queste caratteristiche professionali derivano anche da un importante percorso di management svolto alla guida di team di specialisti e manager di business unit in GTE, Hewlett-Packard e AT&T, in contesti nazionali ed internazionali.
Laureato in Ingegneria Elettronica al Politecnico di Milano, ha arricchito il proprio background di competenze specializzandosi presso l'Insead di Parigi e presso il Cambridge Technology Group di Boston e completando i percorsi di formazione dedicati ai first line manager in At&T e in Hewlett-Packard.
Attivamente impegnato come Consigliere di Assintel, l'Associazione Italiana delle Aziende di Software e Servizi, è autore di numerose pubblicazioni ed articoli di management dell'IT e opinion leader riconosciuto in ambito europeo nell'ambito della diffusione di best practice e di innovazione dell'IT.

Walter Ginevri Dopo la laurea in ingegneria e un decennio speso quale specialista nell'ingegneria del software, ha progressivamente spostato i propri interessi nell'ambito del re-engineering organizzativo e del project management in contesti complessi. Tutto ciò, gli ha permesso di acquisire una consolidata esperienza, sia quale Project Advisor presso gruppi bancari ed industriali, sia quale responsabile della governance di progetti e servizi presso una multinazionale di ICT.
In virtù delle esperienze maturate in settori e in posizioni assai diverse, e soprattutto grazie alle lezioni apprese dai progetti più problematici, ha maturato la convinzione che il project management del 21° secolo debba caratterizzarsi sempre più su tre elementi portanti:
Multidisciplinare, ovvero capace di integrare le discipline scientifiche ed umanistiche
Multiculturale, ovvero capace di cogliere il meglio dalle culture occidentale e orientale
Multimediale, ovvero capace di sfruttare gli strumenti più collaborativi di comunicazione
Su queste basi, svolge l'attività consulenziale presso aziende italiane ed estere, affiancandola a quella di Trainer e Coach con l'obiettivo di trasferire le proprie competenze, unito a

quello di "imparare, disimparare ed imparare di nuovo" (A. Toffler).
Nel 2001 è entrato a far parte della famiglia professionale nel Project Management Institute, al quale dedica una parte significativa del proprio tempo quale volontario del PMI Northern Italy Chapter, di cui è Presidente dal 2011. In tale contesto, si dedica da anni allo studio della teoria della complessità applicata ai progetti, nonché alla diffusione del project management presso la scuola primaria, iniziativa questa che ha portato alla realizzazione di un kit metodologico sperimentato in diversi paesi e oggi disponibile in una dozzina di lingue.

Paolo Giudice è segretario generale del CLUSIT. Negli anni 80 e 90 ha svolto attività di consulenza come esperto di gestione aziendale e rischi finanziari. L'evoluzione del settore IT, che ha messo in evidenza le carenze esistenti in materia di Security, lo ha spinto ad interessarsi alla sicurezza informatica e, nel luglio 2000, con un gruppo di amici, ha fondato il CLUSIT. Dal 2001 al 2008 ha coordinato il Comitato di Programma di Infosecurity Italia e dal 2009 coordina il Comitato Scientifico del Security Summit. Paolo è Partner di C.I.S.C.A. (Critical Infrastructures Security Consultants & Analysts) a Ginevra.

Corrado Giustozzi Consulente e docente di sicurezza delle informazioni, divulgatore scientifico.
Impegnato sui temi della sicurezza informatica sin dal 1985, attualmente si occupa in particolare di: crittografia, steganografia e tecniche di data protection; sicurezza delle informazioni nelle organizzazioni complesse; crimini ad alta tecnologia e loro contrasto; indagini digitali, computer forensics e tecniche di antiforensics; cyberwarfare e cyberterrorismo; rapporti tra tecnologia e diritto (firma digitale, privacy, governance & compliance); aspetti socioculturali di rischio nell'uso delle nuove tecnologie.
È membro del Permanent Stakeholders' Group dell'Agenzia Europea per la Sicurezza delle Reti e delle Informazioni (ENISA). Fa parte del "Expert Roster" della International Telecommunications Union (ITU) e collabora con l'Ufficio delle Nazioni Unite per il Controllo della Droga e la Prevenzione del Crimine (UNODC) su progetti internazionali di contrasto alla cybercriminalità ed al cyberterrorismo
Collabora da oltre quindici anni con il Reparto Indagini Tecniche del Raggruppamento Operativo Speciale dell'Arma dei Carabinieri nello svolgimento di attività investigative e di

contrasto del cybercrime e del cyberterrorismo; fa parte del Comitato Scientifico dell'Unità di Analisi del Crimine Informatico della Polizia delle Telecomunicazioni; è Perito del Tribunale Penale di Roma in materia di criminalità informatica.
Come professore a contratto insegna i temi della sicurezza e del contrasto al cybercrime presso diverse università italiane. Come consulente ha condotto importanti progetti di audit ed assessment di sicurezza logica, e progettato infrastrutture di sicurezza e trust, presso grandi aziende e pubbliche amministrazioni.
Giornalista pubblicista e membro dell'Unione Giornalisti Italiani Scientifici (UGIS), svolge da sempre un'intensa attività di divulgazione culturale sui problemi tecnici, sociali e legali della sicurezza delle informazioni partecipando a trasmissioni televisive e radiofoniche, e tenendo frequentemente conferenze e seminari. Ha al suo attivo oltre mille articoli e quattro libri.

Stefano Niccolini Laurea in Fisica (110/110) Università di Trento 1980.
Dopo una significativa esperienza in ambiente universitario e successivamente in campo industriale, nel 1983 è entrato nel mondo IT bancario, svolgendo attività che hanno spaziato dalla programmazione, all'analisi fino all'organizzazione.
Dal 1999 svolge attività di Internal Auditing, è Associato AIEA dal 2002 e ha conseguito la certificazione CISA nel 2003. Da allora si occupa di ICT Auditing, di Governance e Risk Assessment in ambiente bancario. Le aree di intervento includono le aree di business come gli outsourcer informatici e società erogatrici di servizi.
Ha collaborato con AIEA nella realizzazione di traduzioni di documentazione ISACA, nella realizzazione della pubblicazione "CobiT e ITIL, due framework complementari" (2007).
Dal 2007 al 2012 ha svolto attività per AIEA in qualità di CobiT teacher. È stato membro del Comitato Elettorale dal 2006 fino al settembre del 2012.
A inizio 2013 è stato eletto Presidente di AIEA per il triennio 2013 – 2015.

Alessio L.R. Pennasilico, Security Evangelist di Alba ST, conosciuto nell'hacker underground come -=mayhem=-, è internazionalmente riconosciuto come esperto di sicurezza delle informazioni. Entusiasta cittadino di Internet, si dedica ad aumentare l'altrui percezione delle problematiche legate a sicurezza, privacy ed utilizzo della tecnologia, oltre che a prevenire o respingere attacchi informatici conosciuti o non convenzionali.
Da anni partecipa come relatore ai più blasonati eventi di security italiani ed internazionali. Ha infatti tenuto seminari in tutta Europa ed oltreoceano. Collabora, inoltre, con diverse università ed a diversi progetti di ricerca.
Alessio fa parte del direttivo e del comitato tecnico scientifico di Clusit, del Comitato Direttivo Nazionale dell'Associazione Informatici Professionisti (AIP) e dell'Executive Commitee dell'Osservatorio Privacy & Sicurezza Informatica OPSI-AIP.

Stefano Ramacciotti è stato per sei anni Direttore del Ce.Va. Difesa del II Rep. di SMD; prima ancora, Capo Ufficio Firma Digitale (delegato per la PKI della Difesa e responsabile della Carta Multiservizi della Difesa) e Referente Tecnico della Marina Militare per il CNIPA e, prima ancora, Vice-Direttore del Centro nodale dei sistemi informatici della MM (Maritele Roma). Dopo il master di Sicurezza ICT Avanzato, nel 2008 ha conseguito in Canada i brevetti di Valutatore Common Criteria fino a EAL4. Laureato in "Scienze Marittime e Navali" ha frequentato corsi di "Risk management" e "FIPS 140-2". Contribuisce allo sviluppo di norme internazionali dell'ISO come capo delegazione per i Security Evaluation Criteria (WG3 di ISO/JTC1/SC27). E' CISSP ed è qualificato LA ISO/IEC. E' conferenziere in ambito nazionale ed internazionale su tematiche di sicurezza e autore di articoli specialistici pubblicati su riviste nazionali ed estere. Socio fondatore e membro del Comitato Direttivo di (ISC)2 Italian Chapter è responsabile del GdL di Educazione alla Sicurezza Informatica.

Andrea Rui opera da dieci anni nel mondo dell'IT per il Ministero della Giustizia. In questo periodo si è appassionato alla sicurezza delle informazioni, e si è specializzato nella gestione della qualità e del rischio, della compliance normativa e della business continuity, oltre che della sicurezza delle informazioni nel cloud.
È un entusiasta del mondo del software libero e degli open data e di tutte le loro implicazioni culturali nella società.
Per la sua passione per la sicurezza delle informazioni, ha sposato da diversi anni la causa della divulgazione della cultura della sicurezza in Rete divenendo un evangelist presso i giovani e le scuole, e promuove tali iniziative presso le Istituzioni.
È certificato CISA, BCMP e CCSK, ed è socio Clusit con delega per i rapporti con il Ministero della Giustizia e con il mondo della scuola.
Per il Rapporto Clusit 2014 sulla sicurezza ICT in Italia è co-autore del focus "Formazione e consapevolezza, strumenti indispensabili per la Sicurezza delle Informazioni".

Claudio Telmon è consulente freelance nel campo della sicurezza da quasi quindici anni. Ha gestito il laboratorio di sicurezza del Dipartimento di Informatica dell'Università di Pisa, ed in seguito ha continuato a collaborare con il Dipartimento per attività di didattica e di ricerca, in particolare nel campo della gestione del rischio.
Si è occupato come professionista dei diversi aspetti tecnologici eorganizzativi della sicurezza, lavorando per aziende del settore finanziario, delle telecomunicazioni e per pubbliche amministrazioni.
È membro del comitato direttivo del CLUSIT, con delega per l'Agenda Digitale in ambito sanitario. Nell'ambito delle attività dell'associazione è anche responsabile: dei Progetti Europei, dei Progetti per le PMI, del Premio Tesi.

Alessandro Vallega, in Oracle Italia dal 1997 come Project Manager in ambito ERP e nell'Information Technology dal 1984, è Business Development Manager e si occupa di Governance Risk and Compliance, Database Security ed Identity & Access Management. È il coordinatore della Oracle Community for Security ed è membro del Consiglio Direttivo di Clusit. E' coautore, editor o team leader delle pubblicazioni "ROSI Return on Security Investments: un approccio pratico", "Fascicolo Sanitario Elettronico: il ruolo della tecnologia nella tutela della privacy e della sicurezza", "Privacy nel Cloud: le sfide della tecnologia e la tutela dei dati personali per un'azienda italiana", "Mobile Privacy: adempimenti formali e misure di sicurezza per la compliance dei trattamenti di dati personali in ambito aziendale", "I primi 100 giorni del Responsabile della Sicurezza delle Informazioni (Come affrontare il problema della Sicurezza informatica per gradi)", "La Sicurezza nei Social Media - Guida all'utilizzo sicuro dei Social Media per le aziende del Made in Italy", "Le Frodi nella Rete"

Andrea Zapparoli Manzoni si occupa con passione di ICT Security dal 1997 e di Cyber Crime e Cyber Warfare dal 2003, mettendo a frutto un background multidisciplinare in Scienze Politiche e Computer Science. È Presidente de iDialoghi. È membro del gruppo di lavoro "CyberWorld" nell'ambito dell'Osservatorio per la Sicurezza Nazionale del Centro Militare di Studi Strategici. E' membro del Consiglio Direttivo di Clusit e di Assintel. Ha tenuto per Clusit numerosi seminari e partecipato come speaker alle varie edizioni del Security Summit ed alla realizzazione di white papers (FSE, ROSI v2, SocialMedia) in collaborazione con la Oracle Community for Security. Per il Rapporto Clusit 2014 sulla sicurezza ICT in Italia, ha curato la sezione relativa all'analisi dei principali attacchi a livello internazionale ed ai trend futuri.

Ringraziamenti

Clusit e Security Summit ringraziano gli autori e le organizzazioni e le persone che hanno contribuito alla realizzazione del Rapporto Clusit 2014.

In particolare: A2A, ADS, AIEA, Alba ST, ACE Insurance, Alfa Group, Astrea, Besafe, Bl4ckswan, BSC Consulting, CioNet Italia, Cisco Systems, CLUSIF, Cleis Security, CRAG Partners, CSQA Certificazioni, Di.Fo.B Studio Associato, Eclettica, Electrolux, ENISA, Eris Consulting, Euro Informatica, FASTWEB, Hacktive Security, Hypergrid, IBM, iDialoghi, Infocert, Insiel, Iside, KPMG, KPMG Advisory, McAfee, Mediaservice, MELANI, Neonevis, Networking & Security Consulting, NexSoft, Nextvalue, Oracle, Oracle Community For Security, Project Management Institute - Northern Italy Chapter, Partner Data, Protiviti, Reality Net, Regione Liguria, Ricca Informatica, SafeNet, Security Brokers, Selex ES, Sernet, Shorr-Kan, Trend Micro, VEM Sistemi, Websense, WIND Telecomunicazioni.

E ancora: Pietro Amorusi, Stefano Arduini, Orlando Arena, Iacopo Avegno, Pasquale Baldassarre, Paolo Beatini, Luca Bechelli, Simona Bechelli, Giampiero Bedogna, Pietro Benincasa, Bruno Bernardi, Luca Bertoglio, Gianluca Bocci, Luca Boselli, Danilo Bruschi, Fabio Bucciarelli, Giulio Camagni, Paolo Capozucca, Davide Casale, Aldo Ceccarelli, Francesco Cedrini, Raoul Chiesa, Mauro Cicognini, Corradino Corradi, Paolo Cozzi, Antonio Cucinella, Giovanni Daconto, Paolo Dal Checco, Loris Dal Magro, Fabio Degli Espositi, Giuseppe De Iaco ,Davide Del Vecchio, Massimiliano Destefanis, Gianna Detoni, Cristiano Di Paolo, Mattia Epifani, Cinzia Ercolano, Dino Esposito, Gabriele Faggioli, Mariangela Fagnani, Valentina Falcioni, Andrea Ferrarese, Evelyn Ferraro, Ambrogio Ferretti, Enrico Ferretti, Alessandro Galaverna, Cesare Gallotti, Domenico Garbarino, Alfredo Gatti, Paolo Giardini, Walter Ginevri, Luca Giovannini, Corrado Giustozzi, Marco Goria, Luigi Grilli, Fabio Guasconi, Carlo Guastone, Andrea Guglielmi, Giovanni Hoz, Giuseppe Ingletti, Claudio Jacovelli, Francesco Mazzei, Marco Mella, Riccardo Menichetti, Paola Meroni, Diego Mezzina, Lorenzo Migliorino, Gabriella Molinelli, Roberto Mondonico, Claudio Montechiarini, Maurizio Naitana, Stefano Niccolini, Roberto Obialero, Matteo Olivari, Roberto Pachì, Marco Palazzesi, Giuseppe Palazzini, Enrico Parisini, Paolo Passeri, Michele Pavan, Carlo Pelliccioni, Alessio Pennasilico, Rosario Piazzese, Marco Poggi, Daniele Poma, Franco Prosperi, Stefano Ramacciotti, Sandra Reggio, Stefano Ricca, Nicola Rivezzi, Andrea Rui, Fabio Saulli, Giampaolo Scafuro, Riccardo Scalici, Sofia Scozzari, Paola Sipione, Domencio Solano, Stefano Tagliabue, Gigi Tagliapietra, Marco Tagliavini, Paola Tamburini, Carla Targa, Claudio Telmon, Enzo Maria Tieghi, Stefano Tironi, Francesca Tolimieri, Alessandro Vallega, Marco Venditti, Marco Vernetti, Sylvio Verrecchia, Giacomo Verzeletti, Gaia Vinciguerra Frezza, Francesco Maria Vizzani, Alessandro Volpato, Davide Yachaya, Andrea Zapparoli Manzoni, Giovanni Ziccardi, Patrizia Zocco.

Il Clusit, nato nel 2000 presso il Dipartimento di Informatica dell'Università degli Studi di Milano, è la più numerosa ed autorevole associazione italiana nel campo della sicurezza informatica. Oggi rappresenta oltre 500 organizzazioni, appartenenti a tutti i settori del Sistema-Paese.

Gli obiettivi

- Diffondere la cultura della sicurezza informatica presso le Aziende, la Pubblica Amministrazione e i cittadini.
- Partecipare alla elaborazione di leggi, norme e regolamenti che coinvolgono la sicurezza informatica, sia a livello nazionale che europeo.
- Contribuire alla definizione di percorsi di formazione per la preparazione e la certificazione delle diverse figure professionali operanti nel settore della sicurezza.
- Promuovere l'uso di metodologie e tecnologie che consentano di migliorare il livello di sicurezza delle varie realtà.

Le attività ed i progetti in corso

- Formazione specialistica: i Seminari CLUSIT
- Ricerca e studio: Premio "Innovare la Sicurezza delle Informazioni" per la migliore tesi universitaria – 10a edizione
- Le Conference specialistiche: Security Summit (Milano, Bari, Roma e Verona)
- Produzione di documenti tecnico-scientifici: i Quaderni CLUSIT.
- I Gruppi di Lavoro: con istituzioni, altre associazioni e community.
- Il progetto "Rischio IT e piccola impresa", dedicato alle piccole e micro imprese
- Progetto Scuole: la Formazione sul territorio
- Rapporti Clusit: Rapporto annuale su Cybercrime e incidenti informatici in Italia; analisi del mercato italiano dell'ICT Security; analisi sul mercato del lavoro.

Il ruolo istituzionale

In ambito nazionale, Clusit opera in collaborazione con: Presidenza del Consiglio, numerosi ministeri, Banca d'Italia, Polizia Postale e delle Comunicazioni, Arma dei Carabinieri e Guardia di Finanza, Autorità Garante per la tutela dei dati personali, Autorità per le Garanzie nelle Comunicazioni, Università e Centri di Ricerca, Associazioni Professionali e Associazioni dei Consumatori, Confindustria, Confcommercio e CNA.

I rapporti internazionali

In ambito internazionale, Clusit partecipa a svariate iniziative in collaborazione con: i CERT, i CLUSI, Università e Centri di Ricerca in oltre 20 paesi, Commissione Europea, ENISA (European Network and Information Security Agency), ITU (International Telecommunication Union), OCSE, UNICRI (Agenzia delle Nazioni Unite che si occupa di criminalità e giustizia penale) e le Associazioni Professionali del settore (ASIS, CSA, ISACA, ISC², ISSA, SANS).

Security Summit è il più importante appuntamento italiano per tutti coloro che sono interessati alla sicurezza dei sistemi informatici e della rete e, più in generale, alla sicurezza delle informazioni.
Progettato e costruito per rispondere alle esigenze dei professionals di oggi, Security Summit è un convegno strutturato in momenti di divulgazione, di approfondimento, di formazione e di confronto.

Aperto alle esperienze internazionali e agli stimoli che provengono sia dal mondo imprenditoriale che da quello universitario e della ricerca, il Summit si rivolge ai professionisti della sicurezza e a chi in azienda gestisce i problemi organizzativi o legali e contrattuali dell'Ict Security.
La partecipazione è libera e gratuita, con il solo obbligo dell'iscrizione online.
Il Security Summit è organizzato dal Clusit e da Astrea, agenzia di comunicazione ed organizzatore di eventi di alto profilo contenutistico nel mondo finanziario e dell'Ict.

I docenti e relatori.

Nelle precedenti edizioni del Security Summit sono intervenuti oltre 350 docenti e relatori, rappresentanti delle istituzioni, docenti universitari, uomini d'azienda e professionisti del settore.

I partecipanti

Nel corso delle prime 5 edizioni, il Security Summit è stato frequentato da oltre 8.000 persone e sono stati rilasciati circa 5.000 attestati validi per l'attribuzione di 8.500 crediti formativi (CPE) e 900 diplomi.

L'edizione 2014

La quinta edizione del Security Summit si tiene a Milano dal 18 al 20 marzo, a Bari il 29 maggio, a Roma il 18 e 19 giugno e a Verona il 2 ottobre.

Informazioni

- Agenda e contenuti: info@clusit.it, +39 349 7768 882.
- Altre informazioni: cinzia.ercolano@astrea.pro
- Video riprese e interviste: http://www.youtube.com/user/SecuritySummit
- Foto reportage: http://www.facebook.com/group.php?gid=64807913680&v=photos
- Sito web: http://www.securitysummit.it/

In collaborazione con

Il presente Rapporto
è stato prodotto in occasione del

www.securitysummit.it