Rapporto

2013

sulla sicurezza ICT
in Italia

SECURITY SUMMIT

Rapporto

2013

sulla sicurezza ICT
in Italia

Cardi Editore
galleria San Babila 4
20122 Milano
www.cardieditore.com

Indice

Prefazione

Siamo ben consapevoli dell'impegno che ci siamo assunti nel predisporre il rapporto annuale sulla sicurezza ICT in Italia: impegno di contenuti, di precisione, di informazione.
Un impegno che possiamo onorare grazie alla dedizione dei soci Clusitche rappresentano al più alto livello le varie professionalità che compongono la complessa filiera del mondo della sicurezza informatica.

Già lo scorso anno, con ben due edizioni e una capillare diffusione, abbiamo dato una precisa indicazione al mercato: non è possibile pensare allo sviluppo della società dell'informazione nel nostro Paese senza una piena consapevolezza delle minacce e dei rischi a cui far fronte. Questa nuova edizione è la prova della nostra determinazione.

Ma il compito del Clusitnon è solo quello di svolgere la funzione di "sensore" dei nuovi scenari, ben più importante, crediamo, sia il potenziale di intelligenza e di passione che possiamo mettere a disposizione di chi voglia affrontare con convinzione un tema strategico per il nostro futuro.

Sia a livello nazionale che europeo ci sono positivi segni di una precisa volontà dei governi e delle istituzioni di voler agire concretamente per proteggere le risorse e i sistemi che permettono alle imprese e ai singoli di comunicare e interagire e siamo pronti a dare il nostro contributo di idee e di esperienza.

È vero, c'è molto da fare! Lo diciamo da tempo ed è per questo che abbiamo già cominciato a farlo.

Buona lettura

Gigi Tagliapietra
Presidente Clusit

Introduzione al rapporto

Nel 2012 abbiamo dato vita al primo "Rapporto sulla sicurezza Ict in Italia", seguito da una seconda edizione, in giugno, e da una versione inglese in settembre. L'interesse suscitato (oltre cinquanta articoli su varie testate e alcune decine di migliaia di richieste pervenuteci per richiedere il rapporto), ci ha incoraggiato a continuare ed abbiamo deciso di produrre il Rapporto Clusit con cadenza annuale e, se possibile, con aggiornamenti nel corso dell'anno.
Il Rapporto 2013 inizia con una panoramica degli eventi di cyber-crime e incidenti informatici più significativi del 2012 e con le tendenze per il 2013. Si tratta di un quadro estremamente aggiornato ed esaustivo della situazione globale, con particolare attenzione alla condizione italiana. Abbiamo classificato gli oltre 1.600 attacchi noti del 2011 e 2012, suddivisi per tipologia di attaccanti e di vittime e per tipologia di tecniche d'attacco. Per l'Italia, abbiamo esaminato i 129 attacchi rilevati nel corso del 2012, analizzandone distribuzione e tipologia di attacco.
Segue un contributo della Polizia Postale e delle Comunicazioni, che traccia un quadro molto dettagliato dei fenomeni criminosi a cui si trova confrontata, e fornisce dei dati inediti, quantitativi e qualitativi, su attività investigative e risultati ottenuti nel corso del 2012.
Il Rapporto contiene anche i risultati di una survey che ha coinvolto 207 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.

Il Rapporto fornisce inoltre importanti approfondimenti su una quantità di temi caldi: la sicurezza nel Mobile, nei Socialmedia, nel Cloud; la sicurezza in Sanità e nell'e-Commerce, due temi centrali dell'Agenda Digitale Italiana; completano i Focus On del Rapporto 2013: il nuovo protocollo IPv6 e una serie di riflessioni utili per un corretto salvataggio delle informazioni e la continuità operativa.

Panoramica degli eventi di cyber-crime e incidenti informatici più significativi del 2012 e tendenze per il 2013

Quest'anno, nell'analizzare quanto avvenuto nel 2012 e nei primi mesi del 2013, non possiamo che confermare, purtroppo, le tendenze da noi anticipate nel Rapporto Clusit dell'anno scorso, e rappresentare le crescenti preoccupazioni degli addetti ai lavori a fronte di una situazione che, va detto senza mezzi termini, è in netto peggioramento.

In questo particolare periodo storico, che vede la transizione di oltre un miliardo di persone e, tendenzialmente, della nostra intera civiltà dall'analogico al digitale, dal fisico al cyberspazio, gli attacchi informatici crescono in maniera esponenziale sia come numerosità che come gravità, mentre i difensori incontrano serie difficoltà a mitigare tali rischi, e di conseguenza gli scenari che possiamo ipotizzare per il breve-medio termine non sono affatto confortanti.

In sostanza, ad un anno dal Rapporto 2012 ci troviamo oggi di fronte ad una vera e propria emergenza nella quale nessuno può più ritenersi al sicuro, dove tutti sono in qualche modo ed a vario titolo minacciati, dai singoli cittadini alle PMI fino agli stati nazionali ed alle più grandi imprese del mondo, mentre la frequenza degli incidenti è aumentata del 250% in un solo anno, ed il Cyber Crime è diventato la causa del 54% degli attacchi (era il 36% nel 2012), con una crescita anno su anno del numero di attacchi di oltre il 370%...

Quanto emerge dai dati insomma va ben oltre la preoccupazione che avevamo espresso l'anno scorso, confermando gli scenari "worst case" che avevamo ipotizzato. Riteniamo, senza timore di apparire inutilmente allarmisti, che il tempo delle chiacchiere sia finito e che siamo arrivati al punto in cui è necessario agire, subito e con grande efficacia, come si evince anche dall'analisi dei principali incidenti internazionali e delle tendenze in atto che riportiamo più avanti.

Questo studio, che si riferisce ad un campione di oltre 1.600 incidenti significativi avvenuti negli ultimi 24 mesi, è il risultato di complesse attività di classificazione e correlazione, ed ha richiesto il vaglio di migliaia di fonti aperte, numerose verifiche incrociate tramite attività mirate di

OSInt[1] e, non ultimo, il confronto con le informazioni che emergono dai report di molti Vendor (tra i quali ricordiamo Cisco, IBM, Kaspersky, Mc Afee e Trend Micro).
In questo contesto la nostra sembra una delle poche nazioni a non occuparsi ancora seriamente del fenomeno o, quantomeno, a non voler ancora dare nella pratica il giusto peso alla gravità degli scenari che si prospettano per i mesi e gli anni a venire.
È senz'altro vero che nel testo dell'Agenda Digitale per l'Italia sono previste alcune linee guida anche per quanto riguarda la sicurezza informatica, e che il 23 gennaio scorso il Governo Monti ha annunciato un provvedimento[2] in materia di "sicurezza cibernetica" che, sulla carta, fa ben sperare, ma non è sufficiente.Mancano una adeguata consapevolezza da parte di tutti gli attori interessati, le competenze tecniche, il coinvolgimento delle parti sociali, della scuola, delle istituzioni e della politica, mancano gli investimenti e soprattutto manca la visione prospettica necessaria ad affrontare un problema tanto complesso, che richiede tempi di reazione rapidissimi e soluzioni multidisciplinari, coordinate, sofisticate, a fronte di un assalto continuo, su tutti i fronti, che va avanti 24 ore su 24 e che ormai costa alla nazione miliardi di euro all'anno di danni diretti ed indiretti. Riducendo sostanzialmente queste perdite si potrebbe recuperare quasi un punto di PIL: possiamo permetterci di non farlo?
Il nostro auspicio è che da quest'anno finalmente si proceda con la massima celerità, senza perdere altro tempo prezioso, allineando il nostro Paese agli altri paesi avanzati, per colmare le gravi lacune rappresentate dal non avere ancora, alla data in cui andiamo in stampa, un CERT governativo, né una chiara cyber-strategia di sicurezza nazionale, dotata di organismi, uomini e mezzi adeguati e di un indirizzo politico all'altezza della situazione.
Nella speranza che questo Rapporto Clusit 2013 possa dare un piccolo contributo nell'affrontare le sfide che ci attendono, auguriamo a tutti una buona lettura!

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

[2] http://www.governo.it/Presidenza/Comunicati/dettaglio.asp?d=70337&goback=.gde_4169913_member_207772373

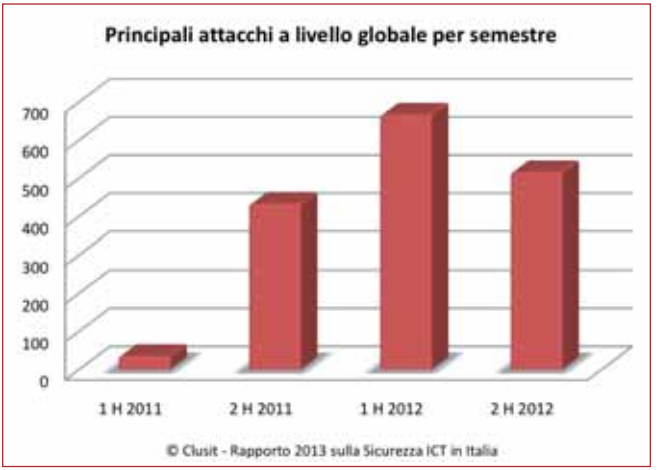
2012: minacce informatiche ai massimi storici

Nel corso del 2011, come abbiamo documentato nel Rapporto Clusit dell'anno scorso[3], il numero complessivo degli attacchi informatici e la loro gravità sono aumentati in modo significativo rispetto agli anni precedenti, prendendo i più alla sprovvista e portandoci ad ipotizzare una ulteriore accelerazione del fenomeno per il 2012, a causa di una lunga serie di motivi strutturali e congiunturali.

Questa (facile) previsione si è avverata, per certi aspetti anche oltre le nostre aspettative, confermando le tendenze emerse dalla nostra analisi dei principali incidenti internazionali noti[4] del 2011 (circa 470) ed anzi mostrando una ulteriore accelerazione.

I quasi 1.200 principali attacchi (tra quelli noti) analizzati per il 2012[5] mostrano che si è trattato di un anno di forte crescita (+254% complessivamente) delle minacce informatiche, in base a tutte le dimensioni interpretative del fenomeno, essendo aumentate, in parallelo, sia la numerosità degli attacchi e la loro sofisticazione sia, di conseguenza, la severità dei danni subiti dalle vittime[6].

Per dare un riferimento numerico (relativamente al nostro campione di 1.652 incidenti noti, che, va ricordato, rappresentano solo la punta dell'iceberg del problema), osserviamo il grafico relativo all'ultimo biennio:



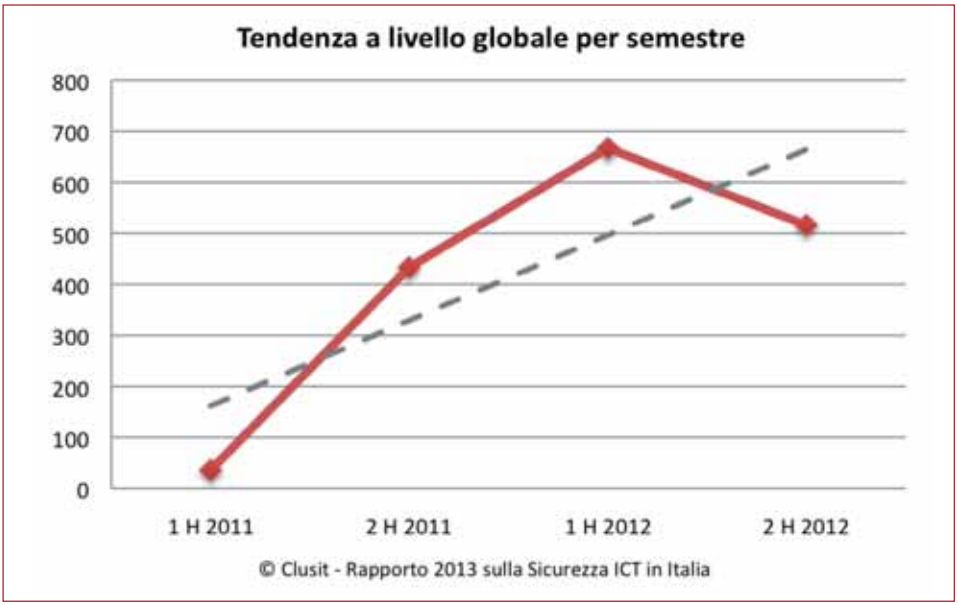
[3] http://milano2012.securitysummit.it/page/rapporto_clusit

[4] http://hackmageddon.com/2011-cyber-attacks-timeline-master-index/

[5] http://hackmageddon.com/2012-cyber-attacks-timeline-master-index/

[6] http://www.ilsole24ore.com/art/tecnologie/2012-09-22/crimini-informatici-italia-costano-110136.shtml

Va premesso che le informazioni in merito agli attacchi che abbiamo analizzato e classificato sono state reperite principalmente da fonti aperte e che, di conseguenza, il loro livello qualitativo (in termini di affidabilità e completezza) nonostante i nostri sforzi di verifica deve essere considerato variabile.
Ciò detto, la crescita tendenziale del numero di attacchi significativi nel corso degli ultimi 24 mesi è chiaramente apprezzabile dal seguente grafico.



Nonostante la flessione nel numero di attacchi significativi divenuti di dominio pubblico nel secondo semestre 2012, dovuta sostanzialmente ad una diminuzione delle azioni dimostrative su larga scala da parte degli Hacktivist (che sono stati duramente colpiti dalle Forze dell'Ordine nel corso dell'anno), la linea di tendenza appare inequivocabile:
I principali effetti dell'aggravamento della situazione avvenuta nel corso dell'anno passato, che vediamo confermati anche in questo primo scorcio di 2013, possono essere sintetizzati come segue:

- Tutti sono ormai diventati potenziali bersagli, per il solo fatto di essere connessi ad Internet. Statisticamente esistono ancora distinzioni tra grandi e piccole imprese, tra differenti settori merceologici, tra privati cittadini e VIP, tra uomini e donne, adulti e bambini, etc, ma le differenze stanno

diminuendo. I differenti gruppi di attaccanti mostrano ancora preferenze rispetto alla tipologia di vittime, ma questo dipende più che altro dal fatto che si stanno sempre più specializzando[7]; d'altra parte però sono diventati talmente numerosi e sfrontati, e la loro azione è ormai talmente pervasiva, da avere di fatto saturato tutto lo spettro delle potenziali vittime. Per questo motivo, e per il fatto che molti utenti utilizzano allo stesso tempo PC fissi o portatili e device mobili, aumentando la propria "superficie di attacco", non esistono più categorie "sicure";

- Le protezioni tradizionali (antivirus, firewall) non sono più sufficienti per bloccare le minacce, che sono sempre più sofisticate e sfuggono alla maggior parte dei sistemi di controllo. In questa fase di transizione verso forme più avanzate di sicurezza informatica, nella quale i difensori sono in netto svantaggio, è dunque particolarmente importante la prevenzione, sotto forma di aumento della consapevolezza e di modifica delle abitudini più pericolose da parte degli utenti;
- Nessuna piattaforma è immune dalle minacce informatiche. Fino ad un paio di anni fa, le minacce si concentravano principalmente sui prodotti Microsoft, data la loro vastissima diffusione sia in ambito enterprise che nel settore privato. Oggi, parallelamente ai cambiamenti in atto nel mercato ICT, gli attacchi informatici avvengono con crescente frequenza (ed alti tassi di successo) anche verso piattaforme meno diffuse (ma in forte ascesa) quali Mac OS X[8], iOs[9], Android[10] e Blackberry[11]. Anzi, sempre più spesso si assiste alla realizzazione di malware multipiattaforma[12], oppure in grado di infettare il PC delle vittime dopo averne infettato lo smartphone[13], e viceversa.

Questa situazione di crescente, endemica pericolosità potrebbe durare anni anche nel caso migliore, ovvero se venissero adottate domani stesso contromisure efficaci, e deve essere tenuta in considerazione da tutti gli

---

7 http://uscyberlabs.com/blog/2012/06/11/tor-black-market-cybercrime-ecosystem/

8 http://threatpost.com/en_us/blogs/new-malware-found-exploiting-mac-os-x-snow-leopard-050212

9 http://www.chmag.in/article/aug2012/apple-ios-vulnerabilities

10 http://www.pcworld.com/article/262321/over_half_of_android_devices_have_unpatched_vulnerabilities_report_says.html

11 http://www.berryreview.com/2012/03/14/webkit-vulnerability-plagues-blackberry-ios-android/

12 http://threatpost.com/en_us/blogs/rise-cross-platform-malware-082412

13 http://www.securelist.com/en/blog/208193760/New_ZitMo_for_Android_and_Blackberry

stakeholders della nostra civiltà tecnologica, non potendo più essere ignorata alla luce dei suoi impatti. Di fatto, come vedremo più avanti, in base alle frequenza stimata gli attacchi informatici sono oggi diventati la prima tipologia di reato della quale un cittadino italiano può essere vittima.
Sfortunatamente in questa fase storica alla velocità di diffusione delle nuove tecnologie informatiche non corrisponde la parallela adozione di misure di sicurezza adeguate (culturali, organizzative e tecnologiche), mentre, d'altra parte, i malintenzionati sono estremamente rapidi nel trarre vantaggio dalle vulnerabilità dei sistemi e dalla mancanza di consapevolezza dei loro utenti.
Oggi tra la scoperta di una vulnerabilità critica, che coinvolge magari centinaia di milioni di sistemi (p.es. una vulnerabilità di Java, o di Acrobat, o di Flash, oppure di una piattaforma web molto diffusa come un Social Network o un sistema di Web Mail) ed il suo sfruttamento da parte di cyber criminali, spie o "cyber warriors" possono passare poche ore, giorni al massimo. In questo contesto la velocità di reazione dei difensori diventa fondamentale, ma pochissimi sono in grado di tenere il passo.
Va inoltre ricordato il costante aumento delle vulnerabilità così dette "0-day", ovvero non conosciute dal produttore e per le quali non esiste una contromisura, le quali alimentano un mercato nero globale da molti milioni di dollari[14] che spinge sempre più "hackers" a cercare di trarne profitti, che possono superare le centinaia di migliaia di dollari per una singola vulnerabilità.

ADOBE READER	$5,000-$30,000
MAC OSX	$20,000-$50,000
ANDROID	$30,000-$60,000
FLASH OR JAVA BROWSER PLUG-INS	$40,000-$100,000
MICROSOFT WORD	$50,000-$100,000
WINDOWS	$60,000-$120,000
FIREFOX OR SAFARI	$60,000-$150,000
CHROME OR INTERNET EXPLORER	$80,000-$200,000
IOS	$100,000-$250,000

Questo fenomeno rappresenta un circolo vizioso, dal momento che una

[14] http://www.forbes.com/sites/andygreenberg/2012/03/23/shopping-for-zero-days-an-price-list-for-hackers-secret-software-exploits/

crescente disponibilità di risorse economiche consente agli attaccanti di sviluppare malware sempre più sofisticati.
Possiamo affermare che il principale problema odierno sia proprio questa crescente discrepanza tra la grande rapidità e disponibilità di mezzi degli attaccanti da una parte e la relativa lentezza di chi cerca di tenervi testa con mezzi scarsi dall'altra, e che sia questo il punto fondamentale da affrontare con urgenza, prima che la situazione peggiori ulteriormente.
A questi fenomeni nel 2012 si è aggiunto, prepotentemente, l'emergere della tematica Cyber Warfare[15], che si configurerà come una delle principali fonti di rischio sistemico, d'ora in avanti.

Quello che nel precedente Rapporto era indicato come un rischio potenziale è diventato nell'arco di pochi mesi un serio problema internazionale, considerato della massima gravità da governi, organizzazioni sovranazionali ed addetti ai lavori, che stanno investendo miliardi in questo ambito.
Tutti i principali attori sulla scena internazionale, Stati Uniti in testa, stanno sviluppando importanti capacità offensive con finalità di deterrenza, ed alcuni minacciano persino di ricorrere a misure cinetiche nel caso di cyber attacchi[16], in un crescendo di dichiarazioni che sanciscono l'inizio di un'era di "cyber guerra fredda" della quale è difficile ipotizzare gli sviluppi, ma che sicuramente nei prossimi anni è destinata a modificare gli equilibri geopolitici mondiali.
È da sottolineare come, in questo come in altri ambiti della sicurezza informatica, il nostro Paese sconti un ritardo di anni, ed una sostanziale mancanza di realizzazioni concrete, esponendosi a rischi significativi, nella sostanziale indifferenza della politica e dei cittadini.
Ma quali sono, in sostanza, le conseguenze pratiche di tutte queste minacce? Per fornire alcuni esempi, anche quest'anno, prima di procedere con l'analisi statistica dei dati disponibili, ci soffermiamo brevemente su alcuni casi particolarmente eclatanti (ed a vario titolo significativi) occorsi durante il 2012.

15 http://mashable.com/2013/01/30/cyber-warfare/
16 http://www.zdnet.com/obama-can-order-pre-emptive-cyber-attack-if-u-s-faces-threat-7000010769/

Casi emblematici

Tra i circa 1.200 attacchi significativi del 2012 che abbiamo analizzato, a puro titolo esemplificativo delle tendenze emerse (ed emergenti) riportiamo di seguito una selezione di dodici casi, non necessariamente tra i più gravi, ma a vario titolo emblematici.

1. "Non usate il nostro prodotto"

Vittima	Attaccante	Tecniche usate
Multinazionale dell'ICT Security	Hacktivist indiani: "YamaTough" del gruppo LoD, altri?	SQLi, Social Engineering, Hacking

Una vicenda singolare, dai contorni ancora poco definiti, che nel suo complesso coinvolge hacktivisti, spie, cyber criminali, governi ed alcune note multinazionali.

A gennaio 2012 un produttore internazionale di soluzioni di sicurezza ammettere di aver subito, nel 2006, un furto di codici sorgenti realizzato da ignoti, precisando che la causa sia stata la compromissione dei server di un proprio partner.

All'origine di questo annuncio un tentativo di ricatto da parte degli hacker antagonisti del gruppo indiano "Lord of Dharmaraja" (LoD), i quali dichiarano di aver compromesso una serie di server governativi sensibili del proprio Paese, e di avervi trovato, tra le altre cose, tali sorgenti (in cambio dei quali chiedono 50.000 USD al produttore).

Insieme a campioni di questi sorgenti, i LoD forniscono altre informazioni "scottanti" (per esempio, forti indizi di compromissione dei sistemi del United States-China Economic and Security Review Commission – USCC, e le "prove" che alcune primarie società occidentali produttrici di telefoni cellulari abbiano inserito delle backdoors nei loro prodotti su richiesta del governo indiano).

Come se non bastasse, dopo una prima serie di comunicati stampa rassicuranti, tesi a minimizzare i rischi per gli utenti, il produttore internazionale di soluzioni di sicurezza invita i propri clienti a non utilizzare il proprio software di accesso remoto (una delle soluzioni di mercato più diffuse al mondo) ed a "disabilitarlo finchè l'azienda non avrà rilasciato le opportune patch di sicurezza"[17].

[17] http://www.symantec.com/connect/sites/default/files/pcAnywhere%20Security%20Recommendations%20WP_01_23_Final.pdf

Un'affermazione coraggiosa e senza precedenti, come ha commentato H.D. Moore, chief architect di Metasploit[18], che ha provocato enorme scalpore nella comunità degli addetti ai lavori, anche perché il furto dei sorgenti risalirebbe ad oltre cinque anni prima (con tutte le implicazioni del caso)[19].

2. "Pronto, chi paga?"

Vittima	Attaccante	Tecniche usate
Decine di migliaia di utenti di telefonia cellulare	Cyber criminali	Ignote

A seguito di indagini svolte dall'U.S. Secret Service, un procuratore generale di New York apre un procedimento contro dodici cyber criminali per aver realizzato una sofisticata frode telefonica, clonando decine di migliaia di telefoni cellulari, per un totale di 250 milioni di dollari di profitti illeciti[20].
In base alle carte processuali risulta che, rubando le informazioni di ignari utenti, i criminali avessero messo in piedi un impressionante mercato nero di chiamate internazionali non tracciabili.
Il coinvolgimento del Department of Homeland Security fa ritenere che, tra i "clienti" di questo servizio, vi fossero anche sospetti di terrorismo.

3. "Il Re è nudo"

Vittima	Attaccante	Tecniche usate
Presidente Siriano Bashar al-Assad	Hacktivisti (Anonymous), ribelli siriani	Insider (talpa), SQLi

Una cellula di oppositori del regime siriano riesce ad ottenere da una talpa le credenziali delle caselle email private utilizzate dal Presidente Assad e da sua moglie Asma, e può monitorare tutte le loro conversazioni per oltre 9 mesi.
Quando, nella primavera del 2012, una cellula di Hacktivst del gruppo Anonymous riesce indipendentemente a compromettere il sito web del Ministero degli Interni siriano[21], tra le molte informazioni sottratte entra in possesso anche di 80 account di posta utilizzati da fedelissimi del regime, incluse quelle del Presidente e della moglie.

---

[18] http://www.reuters.com/article/2012/01/25/us-symantec-hacking-idUSTRE80O1UY20120125
[19] http://www.infosecisland.com/blogview/20505-Remote-Attack-Code-for-Symantecs-pcAnywhere-in-the-Wild.html
[20] http://blog.dhs.gov/2012/02/secret-service-investigates.html
[21] http://www.guardian.co.uk/world/2012/mar/14/how-assad-emails-came-light

Solo quando il contenuto di migliaia di email (incluse molta corrispondenza decisamente compromettente) viene reso pubblico da Anonymous tramite Wikileaks, le comunicazioni tramite queste caselle di posta cessano di colpo.

4. "Compliance ok, sicurezza ko"

Vittima	Attaccante	Tecniche usate
1,5 milioni di utenti di carta di credito	Gang cyber criminale del centro america	Ignote (social engineering, hacking?)

Per quanto anche in questo caso le informazioni siano frammentarie e contraddittorie[22], è assodato che una società americana deputata alla gestione di transazioni con carta di credito sia stata attaccata da una gang di cyber criminali.
Per questo motivo le principali carte di credito hanno immediatamente radiato tale società dalla lista dei gestori affidabili. Inevitabilmente questo ha avuto importanti ripercussioni sul titolo azionario della società.
L'attacco, realizzato a partire dalla compromissione dei terminali di una importante compagnia di taxi di New York, ha causato la perdita di informazioni relativamente a 1,5 milioni di carte di credito, prima che il sistema anti-frode in essere rilevasse anomalie.
A seguito di questo incidente, oltre ad aver subito una sensibile riduzione degli utili, la società ha dovuto ottenere una nuova certificazione PCI-DSS, e recentemente è stata condannata ad un risarcimento di 94 milioni di dollari (essendo assicurata contro queste evenienze per "soli" 30 milioni USD)[23].

5. "Furto di identità su scala nazionale"

Vittima	Attaccante	Tecniche usate
9 milioni di cittadini greci	Cyber criminale	social engineering, hacking

La polizia greca ha arrestato un 35enne di Atene[24] con l'accusa di aver rubato i dati personali di oltre due terzi della popolazione greca, ovvero circa nove milioni di profili su un totale di undici milioni di cittadini.
Tali profili, oltre al nome, al sesso ed all'età, comprendevano il numero di

[22] http://www.scmagazine.com/visa-confirms-processor-credit-card-breach/article/234478/
[23] http://www.scmagazine.com/global-payments-now-expects-to-pay-94m-for-breach-costs/article/275832
[24] http://news.yahoo.com/man-arrested-athens-over-id-theft-most-greek-171450741.html

previdenza sociale, la targa di eventuali veicoli, etc.
L'uomo è stato individuato perché cercava di vendere tali dati su Internet. Non è chiaro se avesse uno o più complici all'interno dell'amministrazione ellenica.

6. "Operazione High Roller"

Vittima	Attaccante	Tecniche usate
Numero imprecisato di aziende europee ed americane	Cyber crime organizzato	social engineering, phishing, hacking

Una gang di cyber criminali di notevoli capacità tecniche ha potuto sottrarre oltre 78 milioni di dollari dai conti di numerose aziende[25], infiltrando i computer aziendali in dotazione al personale amministrativo, preventivamente individuato tramite i Social Network e fatto oggetto di email mirate di phishing con malware quali Zeus e SpyEye, per catturare le credenziali dei conti bancari, distribuiti su oltre 60 diversi istituti di credito.
Gli esperti che hanno analizzato le modalità dell'attacco[26] lo descrivono come estremamente sofisticato ed altamente automatizzato, in grado di superare protezioni avanzate quali one time password e sistemi di autenticazione a due livelli.

7. "La banda della firma digitale"

Vittima	Attaccante	Tecniche usate
Imprenditore italiano	Truffatori "evoluti"	Richiesta di smart card a nome della vittima

La truffa è stata scoperta dal GAT (il Nucleo speciale frodi telematiche della Guardia di finanza). Tre truffatori si sono impadroniti delle credenziali dell'azienda di un ignaro imprenditore, impersonandolo e facendosi rilasciare una smartcard a lui intestata, tramite un Commercialista ed una società di servizi che sono risultati, a loro volta, vittime del raggiro.
Ottenuta la smart card a nome del truffato, hanno proceduto ad una cessione di quote, registrandola regolarmente tramite i sistemi informatici della Camera di Commercio e scippando di fatto l'azienda al legittimo proprietario.
Citando dalla cronaca: «la banda della firma digitale - spiegano gli investi-

[25] http://blogs.wsj.com/cio/2012/06/26/operation-high-roller-targets-corporate-bank-accounts/
[26] http://www.mcafee.com/us/resources/reports/rp-operation-high-roller.pdf

gatori - ha operato in barba alle tanto decantate misure di sicurezza e alla invulnerabilità della soluzione tecnologica per l'autenticazione della sottoscrizione degli atti pubblici»[27].

8. “Operation Enlightenment”

Vittima	Attaccante	Tecniche usate
Numerose organizzazioni ed aziende, principalmente USA	Cyber Espionage	Malware, hacking

Una delle operazioni di spionaggio internazionale più importanti emerse nel corso del 2012. Scoperta casualmente (così come Flame, Shady Rat, Rocra ed altri casi simili) da alcuni ricercatori, che indagavano su un singolo caso di compromissione[28], si è presto dimostrata essere una campagna di intelligence su scala planetaria, condotta con metodo e determinazione da attaccanti presumibilmente legati ad interessi dell'estremo oriente.
Tra i bersagli, molto diversi tra loro, organizzazioni governative europee ed americane appartenenti a molti settori, società high tech, studi legali, società di pubbliche relazioni, think tanks, etc[29].
Un aspetto rilevante di questa operazione è che gli attaccanti, pur avendo utilizzato tecniche di hacking poco sofisticate, per certi aspetti anche banali, sono riusciti ad infiltrare decine di organizzazioni, alcune delle quali sensibili, senza destare alcun allarme, per un periodo di molti mesi.

9. “Milioni di account compromessi”

Vittima	Attaccante	Tecniche usate
Numerosi Social Network e siti web	Cyber crime organizzato	SQLi, hacking

Nel corso dell'anno sono state numerose, oltre che eclatanti, le compromissioni che hanno portato al furto di milioni di passwords e di account da Social Networks e da siti web ad alto traffico.
In un caso la società vittima ha richiesto a tutti i suoi 28 milioni di utenti di cambiare password[30].

---

[27] http://www.ilsole24ore.com/art/notizie/2012-03-26/rubano-firma-digitale-intestano-181133.shtml
[28] http://www.cybersquared.com/project-enlightenment-a-modern-cyber-espionage-case-study/
[29] http://w.infosecisland.com/blogview/21195-Project-Enlightenment-Attacks-Reminiscent-of-Shady-Rat.html
[30] http://nakedsecurity.sophos.com/2012/07/11/formspring-hacked-28-million-users-told-to-change-their-passwords

In un altro caso sono state compromesse le credenziali di circa 6,5 milioni di utenti di un famoso Social Network professionale[31].
Una nota piattaforma di microblogging invece, a seguito di un diffuso attacco ai suoi utenti mirato a comprometterne le credenziali, nel dubbio ha resettato un gran numero di account, scusandosi poi con i propri utilizzatori per il disagio[32].
Infine diversi importanti fornitori di servizi di Web Mail e di chat, a causa di vulnerabilità nei loro sistemi di password reset[33], hanno reso possibile a malintenzionati di accedere a qualsiasi account dei loro utenti, senza dover nemmeno compromettere le relative credenziali.

10. "Cyber crime as a service"

Vittima	Attaccante	Tecniche usate
Un numero imprecisato di società a livello globale	Cyber crime organizzato	SQLi, phishing, social engineering, hacking

Tra i molti esempi possibili della sofisticazione raggiunta dai cyber criminali, questo non è certamente il più preoccupante, ma spicca per professionalità ed organizzazione del gruppo che gestisce l'attività illecita.
Un sito web (raggiungibile tramite TOR) offre a prezzi modici l'accesso a tempo ad oltre 17.000 sistemi, compromessi tramite il loro servizio RDP (Remote Desktop) esposto su Internet[34].
Con pochi dollari è possibile acquistare l'accesso al sistema vittima, ed avere così la possibilità di penetrare, oltre al sistema, anche la rete che lo ospita.
Le macchine compromesse possono essere ricercate per range di IP pubblici, il che rende estremamente agevole individuare una macchina compromessa all'interno della rete di una specifica organizzazione o azienda.
Nel caso il sistema compromesso venga disattivato o messo in sicurezza durante il periodo di accesso concordato, è possibile inviare un ticket ai cyber criminali che provvederanno a sostituirlo con un altro.

[31] http://en.wikipedia.org/wiki/2012_LinkedIn_hack
[32] http://mashable.com/2012/11/08/twitter-hack-password-reset-call/
[33] http://techlogon.com/2012/04/29/hotmail-accounts-hacked-no-matter-how-strong-the-password/
[34] https://krebsonsecurity.com/2012/10/service-sells-access-to-fortune-500-firms/

11. “Man in the Router”

Vittima	Attaccante	Tecniche usate
4,5 milioni di utenti ADSL brasiliani	Cyber crime organizzato	social engineering, hacking

Sfruttando una banale vulnerabilità di numerosi modelli di router forniti da ISP brasiliani, una banda di cyber criminali è riuscita ad accedere alle credenziali di accesso della loro interfaccia web, ed a modificare gli indirizzi dei server DNS nella loro configurazione[35].
In questo modo, utilizzando server DNS malevoli sparsi per il mondo (oltre 40), i cyber criminali hanno potuto redirigere la navigazione degli utenti a loro piacere, spingendoli a scaricare malware ed a visitare siti appositamente realizzati per sembrare Google, Gmail, Facebook etc, in modo da rubarne le credenziali.
Inoltre i cyber criminali hanno modificato le password di accesso ai router compromessi, rendendo più difficoltoso (e quindi costoso) il loro ripristino.
A febbraio 2013, milioni di router risultano ancora compromessi.

12. “Social Botnet”

Vittima	Attaccante	Tecniche usate
11 milioni di utenti di Social Nerwork	Cyber crime organizzato	social engineering, malware

Questa vicenda, pur essendo una delle più rilevanti del 2012, è sostanzialmente passata sotto silenzio.
L'FBI, con il supporto di uno dei principali Social Network al mondo, ha arrestato 10 sospetti, di sette diverse nazionalità, nell'ambito di una complessa indagine in merito ad una delle botnet più grandi mai scoperte[36].
Gli utenti, presi di mira tramite il Social Network dal malware denominato Yahos (derivato dal malware alla base della famigerata botnet Butterfly, smantellata nel 2011), erano vittime di furti di identità e di credenziali bancarie.
L'FBI stima che le perdite totali causate da questa botnet, composta da 11 milioni di macchine infette, siano state nell'ordine degli 850 milioni di dollari[37].

---

35 http://www.securelist.com/en/blog/208193852/The_tale_of_one_thousand_and_one_DSL_modems
36 http://www.zdnet.com/facebook-helps-fbi-smash-global-11-million-strong-botnet-7000008671/
37 http://www.fbi.gov/news/pressrel/press-releases/fbi-international-law-enforcement-disrupt-international-organized-cyber-crime-ring-related-to-butterfly-botnet

Classificazione dei principali incidenti internazionali noti

Di seguito i criteri di classificazione che abbiamo adottato (necessariamente di alto livello, data la frequente mancanza di informazioni dettagliate sugli incidenti) e le relative consistenze numeriche rispetto al totale.
Abbiamo segnalato in arancio gli incrementi percentuali rispetto al 2011 che risultano essere superiori alla media generale, i quali evidenziano con buona approssimazione le principali tendenze in atto.

ATTACCANTI PER TIPOLOGIA	2011	2012	Totale	Incremento
Cybercrime	170	633	803	372,35%
Unknown	148	110	258	-25,68%
Hacktivism	114	368	482	322,81%
Espionage / Sabotage	23	29	52	126,09%
Cyber warfare	14	43	57	307,14%
TOTALE	**469**	**1.183**	**1.652**	**252,24%**

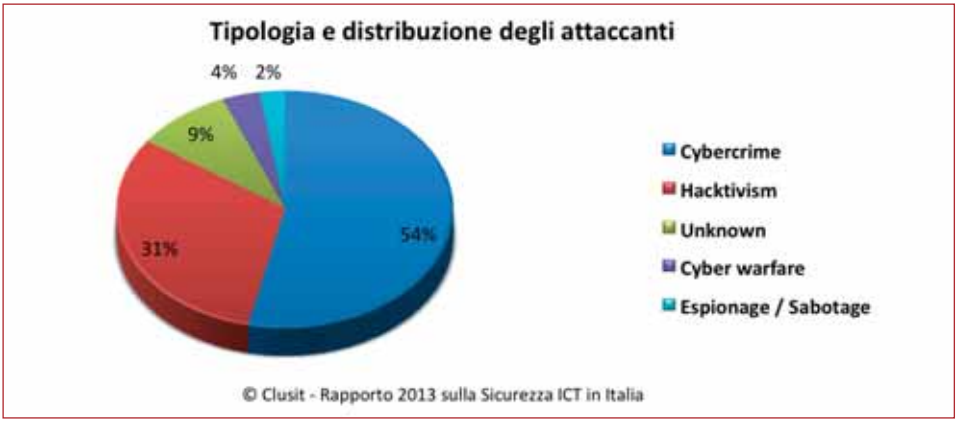
VITTIME PER TIPOLOGIA	2011	2012	Totale	Incremento
Institutions: Gov - Mil - LEAs - Intelligence	153	374	527	244,44%
Others	97	194	291	200,00%
Industry: Entertainment / News	76	175	251	230,26%
Industry: Online Services / Cloud	15	136	151	906,67%
Institutions: Research - Education	26	104	130	400,00%
Industry: Banking / Finance	17	59	76	347,06%
Industry: Software / Hardware Vendor	27	59	86	218,52%
Industry: Telco	11	19	30	172,73%
Gov. Contractors / Consulting	18	15	33	-16,67%
Industry: Security Industry:	17	14	31	-17,65%
Religion	0	14	14	1400,00%
Industry: Health	10	11	21	110,00%
Industry: Chemical / Medical	2	9	11	450,00%
TOTALE	**469**	**1.183**	**1.652**	**252,24**

TECNICHE DI ATTACCO PER TIPOLOGIA	2011	2012	Totale	Incremento
SQL Injection[38]	197	435	632	220,81%
Unknown / APT	73	294	367	402,74%
DDoS[39]	27	165	192	611,11%
Known Vulnerabilities / Misconfigurations	107	142	249	132,71%
Malware	34	61	95	179,41%
Account Cracking	10	41	51	410,00%
Phishing / Social Engineering	10	21	31	210,00%
Multiple Techniques	6	13	19	216,67%
0-day[40]	5	8	13	160,00%
Phone Hacking	0	3	3	300,00%
TOTALE	**469**	**1.183**	**1.652**	**252,24%**

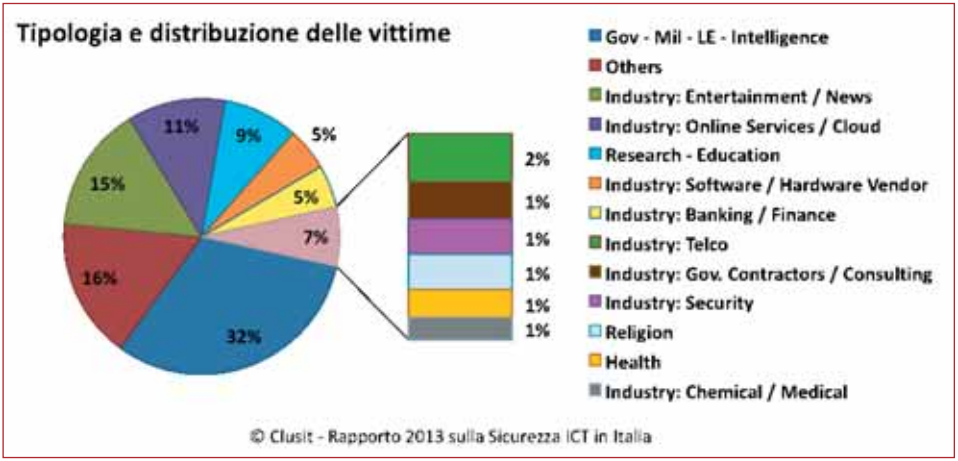
© Clusit - Rapporto 2013 sulla Sicurezza ICT in Italia

[38] http://it.wikipedia.org/wiki/SQL_injection
[39] http://it.wikipedia.org/wiki/DDOS
[40] http://it.wikipedia.org/wiki/0-day

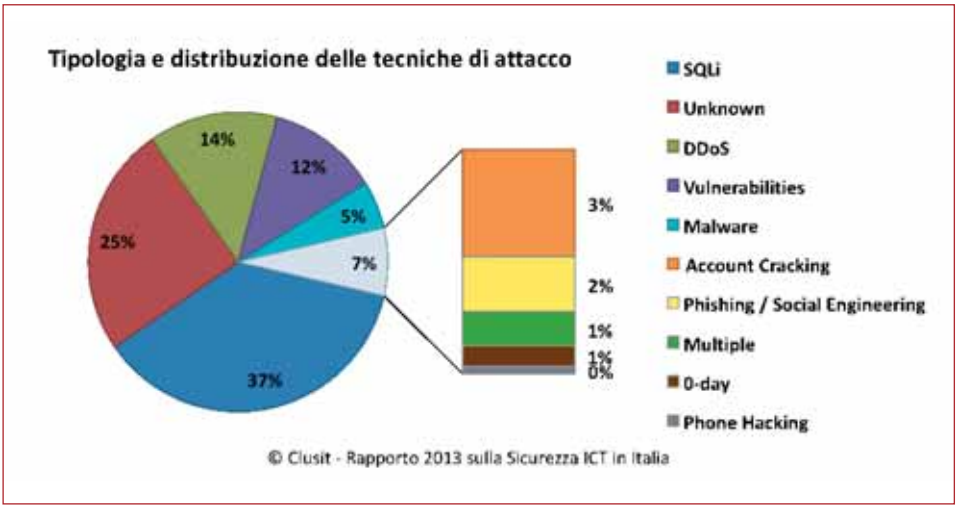
Possiamo visualizzare sinteticamente i dati relativi all'analisi dei 1.183 attacchi noti del 2012 come segue:



Da notare come il Cyber Crime superi ormai il 50% del totale (dal 36% del 2011 al 54% del 2012).

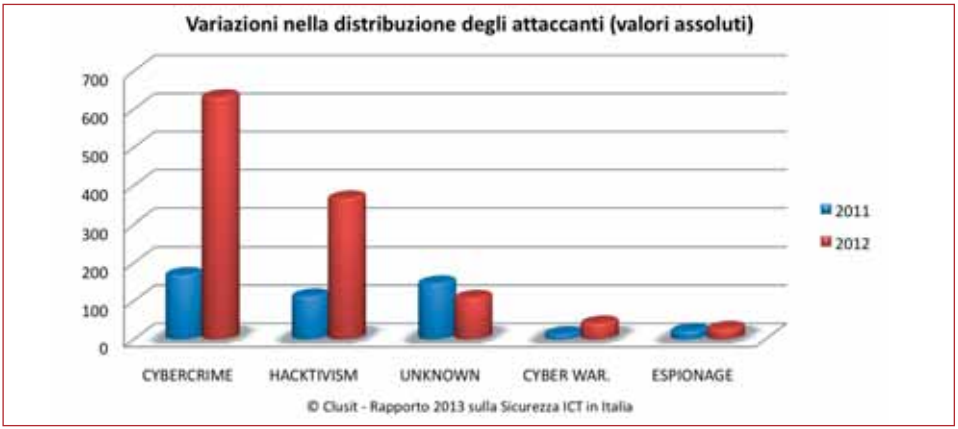


Per quanto riguarda la distribuzione delle vittime, diminuiscono leggermente gli attacchi verso enti governativi, ma aumentano quelli contro l'industria dello spettacolo, i servizi web e le istituzioni scolastiche.
Infine nel 2012, per quanto riguarda la classificazione degli attacchi in base alle tecniche utilizzate dagli attaccanti, spicca il notevole incremento della categoria DDoS, mentre si confermano sempre molto utilizzate le tecniche di SQL Injection, lo sfruttamento di vulnerabilità note e l'utilizzo di malware.

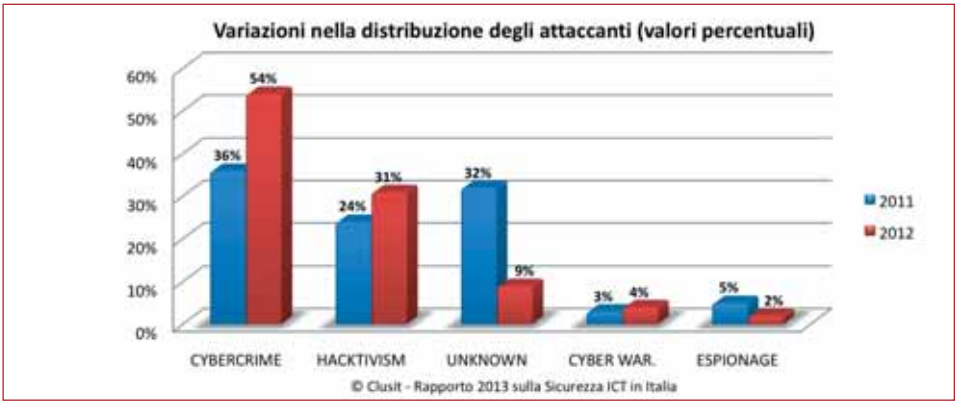


Nella maggior parte dei casi gli attacchi sono stati realizzati con tecniche ben conosciute, sfruttando cioè la mancanza di patch, misconfigurazioni, falle organizzative, la mancanza di awareness da parte degli utenti etc, ovvero tutte vulnerabilità che potrebbero e dovrebbero essere mitigate, se non eliminate, con una certa facilità, mentre anche quest'anno rappresentano il 68% del totale. Da questo grafico appare evidente come i difensori abbiano ampi margini di miglioramento.

Nel confrontare i dati del 2012 con quelli del 2011, cominciamo con l'analizzare l'incremento in valore assoluto delle diverse categorie di attaccanti, che mostrano quanto abbiamo anticipato nel capitolo precedente.

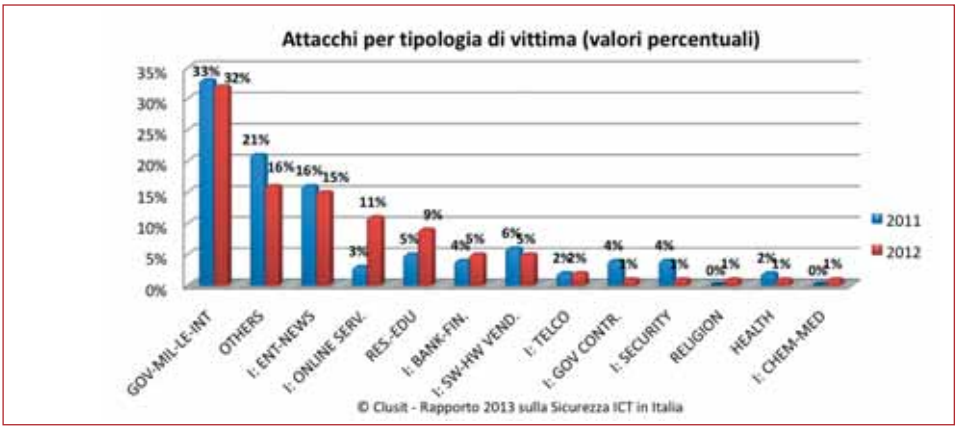


Si evidenzia nettamente l'incremento di incidenti dovuti al cyber crime, un aumento meno marcato di quelli dovuti agli hacktivist, una diminuzione degli attacchi realizzati da ignoti, un leggero aumento degli attacchi legati ad attività di cyber warfare ed una leggera diminuzione dei casi noti di cyber espionage.
Normalizzando i valori assoluti e calcolando le percentuali relative a ciascuna categoria di attaccanti nei due anni considerati, la situazione appare ancora più chiaramente:

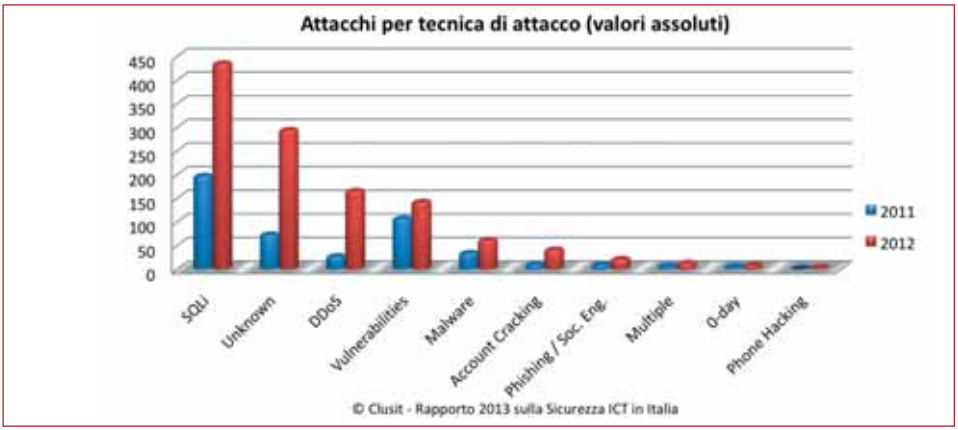


La crescita percentuale dei casi noti di cyber crime è molto significativa. Da un lato sottolinea il fatto che gli autori ormai non si preoccupano nemmeno più di nascondere le proprie tracce, dall'altro, come dimostra anche la netta diminuzione di autori ignoti, fa supporre che sia in atto un miglioramento nella capacità dei difensori di individuare i responsabili, il che è senz'altro positivo.
Spostando l'attenzione alla classificazione in valori assoluti degli attacchi per tipologia di vittima emergono fenomeni interessanti:

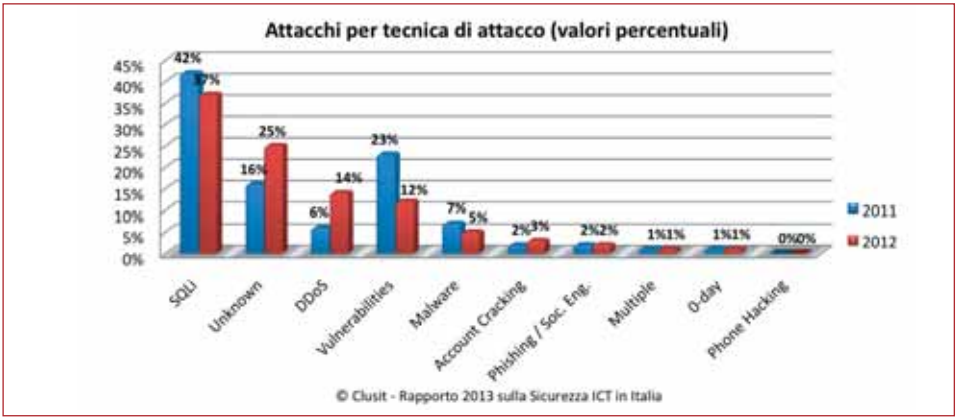
Nonostante il settore Governativo mantenga il non invidiabile primato di essere il bersaglio più frequentemente colpito all'interno del nostro campione, è il settore Online Service e Cloud (che include i Social Networks) a mostrare i tassi di crescita maggiori degli attacchi (+900%).
Confrontando le percentuali sul totale di ciascuno degli anni considerati emergono altri dati significativi:



Rispetto al 2011 si nota un sostanziale incremento degli attacchi non solo contro i Servizi Online, ma anche contro istituzioni scolastiche e finanziarie, mentre le altre categorie rimangono pressoché invariate, con l'esclusione del comparto denominato "altri", che mostra una riduzione.
Per quanto riguarda infine la classificazione degli incidenti in base alle tecniche di attacco, si evidenzia chiaramente l'aumento di alcuni tipi di minacce:



In valore assoluto continuano a prevalere le tecniche di SQL Injection (il che non depone a favore dei difensori, come dicevamo più sopra), ma aumentano sensibilmente anche gli attacchi di tipo Distributed Denial of Service e quelli realizzati con tecniche ignote (tipicamente tramite le così dette APT[41]), oltre a quelli realizzati tramite lo sfruttamento di vulnerabilità note (per mancanza di patching) e di malware.
Confrontando le percentuali sul totale di ciascuno degli anni considerati emergono chiaramente i trend che i difensori dovrebbero tenere in maggiore considerazione:



Le tipologie di minacce che mostrano i maggiori tassi di crescita sono i DDoS e le tecniche ignote / APT (a questo proposito, in alcuni casi questo incremento può statisticamente essere dovuto anche alla reticenza degli investigatori nel rivelare le tecniche utilizzate dagli attaccanti, nel tentativo di ridurne la diffusione e gli inevitabili fenomeni di emulazione).

[41] http://en.wikipedia.org/wiki/Advanced_persistent_threat

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

Mentre in Italia il 2011 da un punto di vista di sicurezza informatica è stato caratterizzato dalla predominanza di minacce di matrice attivista (Anonymous ed i suoi emulatori), anche nel nostro Paese nel corso del 2012 il peso e la frequenza di questi eventi è progressivamente diminuito.
Grazie alla minore frequenza di azioni eclatanti da parte degli antagonisti digitali, hanno trovato maggiore spazio sui media le azioni della criminalità informatica, rendendo (finalmente) visibile, anche al di fuori della comunità degli addetti ai lavori, la maggiore fonte di rischio per imprese, cittadini e pubblica amministrazione, alla quale tutti indistintamente sono quotidianamente esposti.
Volendo identificare i fattori che nel corso del 2012 hanno maggiormente influenzato il panorama italiano, è possibile affermare che:

- Da un punto di vista tecnologico, il 2012 ha visto il consolidamento del trend già avviato nel 2011, relativo all'aumento dell'accesso dei servizi online da dispositivi mobili. A dicembre 2012, in Italia vi erano 38.4 milioni di utenti nella fascia 11-74 anni con accesso continuo ad Internet, e quasi 20 milioni in grado di connettersi con uno *smartphone* o *tablet*[42]. Se si considera che nel 60.4% dei casi l'attività più citata dagli utenti mobili consiste nella navigazione su Internet, e che quasi 5 milioni di utenti hanno scaricato almeno una volta una applicazione, se ne deduce la crescente familiarità verso questi dispositivi. Purtroppo, come dimostrato dalla famigerata operazione Eurograbber[43], anche i criminali informatici si stanno adattando alle abitudini degli utenti.
- Da un punto di vista sociale, il 2012 ha accentuato il clima di sfiducia nei confronti della classe politica, sfiducia ulteriormente acuita dal difficile contesto economico attuale e dai conseguenti sacrifici a cui il nostro paese è stato sottoposto. A questo inasprimento del clima sociale non è tuttavia corrisposto un aumento proporzionale delle azioni di protesta digitale da parte degli attivisti italiani come accaduto nel corso dell'anno precedente. Il 2012 è stato da questo punto di vista un anno a due facce: se

[42] Dati AUDIWEB TRENDS - Settembre 2012 Dati cuulati cicli 1°+2°+3°+4° del 2012
[43] http://punto-informatico.it/3665862/PI/News/eurograbber-zeus-contro-banche-europee.aspx

nel corso della prima metà dell'anno si sono registrate azioni di protesta isolate (e a volte contraddittorie), tuttavia queste sono andate progressivamente scemando nel corso dell'anno e sono state, come impatto e come frequenza, ben lontane dagli eventi dell'estate 2012. Probabilmente a questa diminuzione hanno contribuito le azioni delle forze dell'ordine (che hanno mostrato come sia difficile mantenere l'anonimato, soprattutto per chi si improvvisa attivista digitale), ma anche la crescente sensibilità dei possibili obiettivi che hanno innalzato il livello di attenzione.

- Per contro, nel corso del 2012 è sorta la consapevolezza che il nostro paese non è immune a complesse operazioni di crimine e spionaggio informatico, operazioni che in alcuni casi (sarebbe il caso di dire finalmente) "si sono meritate" le prime pagine delle principali testate quotidiane[44]. E anche se per la stampa nostrana fa ancora più rumore il blog di Beppe Grillo attaccato dagli Anonymous, piuttosto che il bottino stimato di 36 milioni di euro (di cui 16 milioni in Italia) sottratto dai criminali alla base dell'operazione Eurograbber, questo sintomo è significativo di una presa di coscienza sui rischi derivanti dall'eccessiva esposizione della nostra identità digitale, e delle sue appendici, ai rischi di Internet. In effetti, per un cittadino, vedersi svuotare il conto in banca dai criminali, ha un impatto ben maggiore che l'impossibilità accedere per qualche ora al sito del proprio politico di riferimento.

Gennaio-Marzo 2012

Il 2012 si è aperto in continuità con l'anno precedente. Nel primo trimestre dell'anno l'attività di *hacktivism* ha preso vigore, sulla scia delle proteste che hanno caratterizzato il tentativo di far approvare dapprima le leggi SOPA e PIPA (gli attacchi hanno raggiunto l'apice tra il 19 e 20 gennaio quando l'FBI ha sigillato i server di MegaUpload), ed in seguito alla sottoscrizione dell'ACTA da parte di 22 membri dell'Unione Europea. Com'era prevedibile, in Italia sono finite sotto il mirino virtuale degli *hacktivisti* le organizzazioni accusate di difendere il vecchio modello di *copyright* (SIAE, copyright.it), piuttosto che il sito del Ministero della Giustizia[45],

[44] http://www.corriere.it/tecnologia/12_dicembre_06/hacker-maxi-furto-da-conti-online-banche-europee_0e8cd008-3f82-11e2-823e-1add3ba819e8.shtml

[45] http://cylaw.info/?p=72

come forma di protesta contro il cammino parlamentare della proposta legge Fava (bocciata poi dalla Camera il successivo 1 Febbraio), la declinazione italiana dell'ACTA.
Nel mese di marzo, in concomitanza con l'acuirsi dell'instabilità politica e traendo spunto da alcuni eventi di cronaca (ad esempio gli incidenti occorsi nel cantiere TAV in Val di Susa), si è assistito ad una nuova impennata degli eventi che hanno colpito realtà appartenenti al settore di infrastrutture e trasporti ed energia. Nel vortice di marzo è finito anche lo Stato del Vaticano che ha subito alcune azioni clamorose: il sito istituzionale è stato vittima di ben quattro attacchi DDoS tra il 7 ed il 22 marzo[46], e di altre azioni minori verso siti collegati, anche a causa di una intervista un po' avventata di un partner di sicurezza della Santa Sede che sulle pagine del New York Times aveva dichiarato di aver profilato e sventato, tra luglio e agosto 2011, un presunto tentativo di attacco degli Anonymous.
Sebbene non direttamente connesso con il panorama Italiano, il 6 marzo 2012 accade un evento che è destinato ad avere ripercussioni notevoli nel corso dell'anno per il filone di attivismo digitale: la stampa americana rivela che Hector Xavier Monsegur, più noto come Sabu, il famigerato leader del collettivo LulzSec (protagonista delle principali azioni di "protesta digitale" del 2011 emulate da molti proseliti improvvisati anche nel nostro Paese), agisce da informatore dell'FBI dal 7 giugno 2011[47]. Come è facilmente prevedibile, nella rete dell'FBI finiscono ben presto tutti i rimanenti membri del gruppo. Tuttavia l'operazione ha ripercussioni ben più ampie in quanto cadono preda delle forze dell'ordine molti altri *hacktivisti* che da giugno 2011 continuavano inconsapevolmente ad agire sospinti dallo spirito di emulazione. L'operazione getta nello sconforto la comunità attivista in generale, e rafforza la consapevolezza che l'anonimato digitale è un concetto molto fragile anche per chi agisce dall'altra parte della barricata. Per avere una idea dell'impatto di questo gesto si consideri il fatto che lo stesso Sabu, a detta degli stessi attivisti italiani, è sospettato di avere servito sul piatto degli Anonymous italiani la polpetta avvelenata del CNAIPIC[48], il celebre attacco alla polizia informatica italiana avvenuto a luglio 2011.

---

46 http://anon-news.blogspot.it/2012/03/vaticanva-4-0-benedictomexicomx-tango_22.html
47 http://www.foxnews.com/tech/2012/03/06/exclusive-unmasking-worlds-most-wanted-hacker/
48 http://inchieste.repubblica.it/it/repubblica/il-venerdi/2012/03/21/news/intervista_anonymous-31956238/

Ma il Cyber Crime non è solo *hacktivism*. È interessante notare il fatto che le truffe informatiche di grandi dimensioni cominciano a conquistarsi le prime pagine dei quotidiani. Alla fine di gennaio i militari di Bari sgominano una banda internazionale, attiva anche in Italia, dedita alla clonazione di carte di credito utilizzando tecniche di *phishing*[49]. Il danno registrato nel nostro paese è stato circa di un milione di euro.
Alle mire degli hacker nostrani non sfugge nemmeno l'INPS, vittima di una violazione del database interno che consente a una organizzazione criminale di creare false posizioni previdenziali, per un danno stimato all'erario di circa 1.8 milioni di euro[50]. Anche quest'ultimo evento dimostra come la mancanza di misure di sicurezza interne possa avere ripercussioni molto serie per lo Stato e per i cittadini, ripercussioni rese ancora più gravi dalla delicata congiuntura attuale.

Aprile-Giugno 2012
La scia dell'onda attivista si è estesa anche al secondo trimestre del 2012. Soprattutto all'inizio di Aprile, i cannoni virtuali degli attivisti hanno continuato a tenere sotto tiro diversi siti istituzionali o appartenenti ad entità direttamente o indirettamente legate alle note vicende in Val di Susa.
L'evento che ha caratterizzato questo trimestre, più per il folklore che per l'effettivo impatto dell'attacco informatico accade invece l'8 giugno. In questo giorno una cellula autonoma appartenente al locale capitolo degli Anonymous "dedica" le proprie attenzioni verso il sito del comico Beppe Grillo che diviene oggetto di un attacco di tipo *Distributed Denial Of Service*[51]. Il sito è reso irraggiungibile per circa un giorno, ma soprattutto l'azione, tra successive rivendicazioni e smentite in perfetto stile Italiano, genera una spaccatura all'interno degli Anonymous che attribuiscono la paternità dell'attacco ad un sottogruppo, in seguito disconosciuto, specializzato nell'utilizzo di Botnet[52]. In compenso l'attacco ottiene il suo scopo, per gli

[49] http://bari.repubblica.it/cronaca/2012/01/31/foto/carte_di_credito_clonate_online_sgonimata_banda_internazionale-29082918/1/
[50] http://palermo.repubblica.it/cronaca/2012/03/07/news/false_pensioni_su_computer_inps_scoperta_la_truffa_sei_arrestati-31080894/
[51] http://www.corriere.it/cronache/12_giugno_08/anonymous-attacca-il-sito-di-beppe-grillo_e56c295a-b1a9-11e1-ba93-c93b078addf8.shtml
[52] http://www.anon-news.blogspot.it/2012/06/anonops-ircpower2allcom-italy.html

attaccanti e, paradossalmente anche per la vittima, occupando per qualche giorno le prime pagine dei media nazionali.
Sempre a giugno si è invece registrato un picco sul fronte attivista esterno dovuto ad una incursione in Italia del collettivo TeamShell che ha preso di mira alcuni domini.gov (un anticipo del clamoroso attacco ad alcuni atenei mondiali effettuato ad ottobre). Da notare, l'11 giugno, un curioso precedente: per la prima volta una squadra di calcio di Serie A diviene oggetto di un attacco hacker. Il triste primato spetta all'Udinese Calcio, il cui sito istituzionale viene violato[53]. Non è un evento particolarmente significativo come impatto, ma sicuramente sintomatico del fatto che nessuno à al sicuro.
Nello stesso periodo è importante notare, sebbene la vera natura dell'evento sia ancora tutt'altro che chiara, un presunto attacco informatico alle VLT di SNAI che sarebbe la causa di vincite anomale avvenute il 16 aprile 2012[54], vincite che hanno coinvolto 3.000 dispositivi in tutto il territorio nazionale. Proprio per la natura anomala delle vincite il concessionario di Stato ha stabilito di non riconoscere i pagamenti ai vincitori. Vero o presunto che sia l'evento, è un fatto che il settore del gaming rischia di diventare una preda succulenta per i malintenzionati.
Ugualmente importante uno dei rari casi in cui una primaria banca nazionale è finita nelle pagine di cronaca a causa di un furto informatico che ha portato alla sottrazione illecita da parte dei criminali di 400.000 euro appartenenti al deposito del locale Ordine Degli Avvocati[55].

Luglio-Settembre 2012

L'estate del 2012 non ha sicuramente ripetuto la frequenza di attacchi registrati nell'anno precedente, quando bastava aprire le pagine o bacheche di qualsiasi social network per trovare il termine di derivazione militare "tango down" (utilizzato dagli Hacktivist per indicare il successo di un attacco informatico verso un determinato obiettivo) ai primi posti tra i *top trend* di discussione. In realtà il mese di luglio ha mostrato invece una sostanziale calma apparente.

---

53 http://hackmageddon.com/2012/06/11/the-first-serie-a-team-hacked/

54 http://www3.lastampa.it/cronache/sezioni/articolo/lstp/450787/

55 http://corrieredelveneto.corriere.it/veneto/notizie/cronaca/2012/25-maggio-2012/padova-hacker-azione-ripulito-conto-avvocati-201339305138.shtml

Il trend discendente è continuato ad agosto, con l'eccezione di alcuni sporadici eventi di matrice attivista sulla scia dalla nota vicenda relativa alla questione delle acciaierie Ilva di Taranto. Ne hanno fatto le spese la stessa Ilva, oggetto di attacchi informatici e di pubblicazioni illecite di dati[56] protrattesi per tutto il mese, ma anche il Comune di Taranto oggetto di *Defacement*[57].
Tra il serio e il faceto nel mese di agosto è finito sotto le mire degli attivisti informatici appartenenti al collettivo Anonymous anche il maratoneta Alex Schwazer, come conseguenza della sua ammissione di aver fatto uso di doping[58]. Sullo stesso fronte, a Settembre gli Anonymous si sono resi protagonisti di un ulteriore gesto clamoroso, pubblicando oltre 2 Gb di documenti privati ed email appartenenti ad un sacerdote accusato di pedofilia[59].
Tutte azioni, le precedenti, che dimostrano lo stretto legame tra attivismo informatico e cronaca, anche quando i fronti di rivendicazione sono estremamente eterogenei tra loro.
Di matrice completamente diversa (e forse di impatto più serio), l'attacco che ha coinvolto un noto produttore mondiale di elettronica di consumo, dal cui sito Italiano sono state sottratte le credenziali di oltre 8.000 ignari clienti[60]. Importante notare a settembre qualche attacco sporadico a banche Italiane e un nuovo blackout, questa volta privo di rivendicazione, al blog di Beppe Grillo.

Ottobre-Dicembre 2012

L'ultima parte dell'anno si è aperta con un attacco a tre Università di Roma. Alcuni domini sono infatti finiti all'interno dell'operazione Project West Wind, condotta dal collettivo GhostShell, in cui sono state pubblicate su internet 120.000 credenziali appartenenti ad alcuni atenei di livello mondiale (tra cui Harvard, Cambridge, Tokio e, per l'appunto, Roma)[61]. Nel caso specifico, ai 3 atenei impattati nel nostro paese sono state sottratte circa 350 credenziali per un valore più simbolico che pratico.
Il 23 ottobre è invece finita sotto attacco nuovamente la polizia (dopo il con-

56 http://www.anon-news.blogspot.it/2012/08/ilva-taranto-we-do-not-forgive-we-do.html
57 http://hackmageddon.com/2012/08/10/defacement-tarantina-style/
58 http://www.tomshw.it/cont/news/anonymous-ammonisce-il-dopato-schwazer-con-un-defacing/39103/1.html
59 http://thehackernews.com/2012/09/anonymous-dump-25-gb-data-from-email-of.html
60 http://www.cyberwarnews.info/2012/09/23/asus-italy-hacked-site-defaced-thousands-of-client-details-leaked/
61 http://www.theregister.co.uk/2012/10/02/university_hacking_ghostshell/

troverso episodio del 25 luglio 2011) che ha subito la sottrazione illecita da parte degli attivisti (con conseguente pubblicazione) di circa 3.500 documenti privati[62]. La polizia ha ammesso l'incursione illecita[63], minimizzando l'accaduto, e scatenando, come prevedibile la reazione degli Anonymous.
Nel corso dello stesso periodo si è registrato un presunto attacco a Telecom Italia da parte degli stessi attivisti digitali. Questi ultimi hanno dichiarato di avere rilevato nei server della compagnia, circa 3.000 (??) vulnerabilità che hanno consentito l'accesso illecito a oltre 30.000 credenziali[64]. Poiché all'annuncio non sono seguiti ulteriori dettagli (se non la pubblicazione di una manciata di credenziali) permangono molte perplessità sulla effettiva veridicità dell'attacco, a conferma che la reputazione delle fonti continua ad essere il problema più serio per l'attribuzione di responsabilità degli attacchi informatici.
Da un punto di vista globale, l'evento più importante dell'ultimo trimestre dell'anno è stato la scoperta dell'operazione Eurograbber (citata in precedenza), una colossale operazione criminale condotta nei confronti di 30.000 conti correnti europei che ha sottratto agli ignari correntisti oltre 36 milioni di Euro con prelievi illeciti, ai singoli malcapitati, variabili tra i 500 e 250.000 euro. L'operazione, condotta con l'ennesima variante per piattaforme mobile del malware Zeus (ZitMo), è partita proprio dal nostro Paese, che si è meritato il triste primato di risultare quello maggiormente colpito, ed ha coinvolto in Italia 16 istituti bancari, 11.893 utenti, portando infine alla sottrazione illecita di oltre 16 milioni ai nostri connazionali (con una media di quasi 1.380 euro a vittima)[65].
Da menzionare, più per la peculiarità dell'attacco che per il suo effetto, un caso di attacco *Denial Of Service* effettuato dalle pagine di Facebook contro la bacheca di un noto cantante imbrattata di insulti. Sicuramente un modo originale (e piuttosto pericoloso in quanto replicabile e difficilmente contrastabile) di esprimere il proprio dissenso in fatto di gusti musicali.[66]

---

62 http://anon-news.blogspot.in/2012/10/antisecita-polizia-italiana-owned.html
63 http://www.adnkronos.com/IGN/News/CyberNews/Internet-Dipartimento-Ps-Anonymous-non-ha-violato-server_313821291195.html
64 http://news.softpedia.com/news/Telecom-Italia-Hacked-by-Anonymous-30-000-Credential-Sets-Stolen-304712.shtml
65 https://www.checkpoint.com/products/downloads/whitepapers/Eurograbber_White_Paper.pdf
66 ttp://bologna.repubblica.it/cronaca/2012/12/24/news/pagina_facebook_di_vasco_irraggiungibile_dopo_l_attacco-49385443/

Uno sguardo al 2013

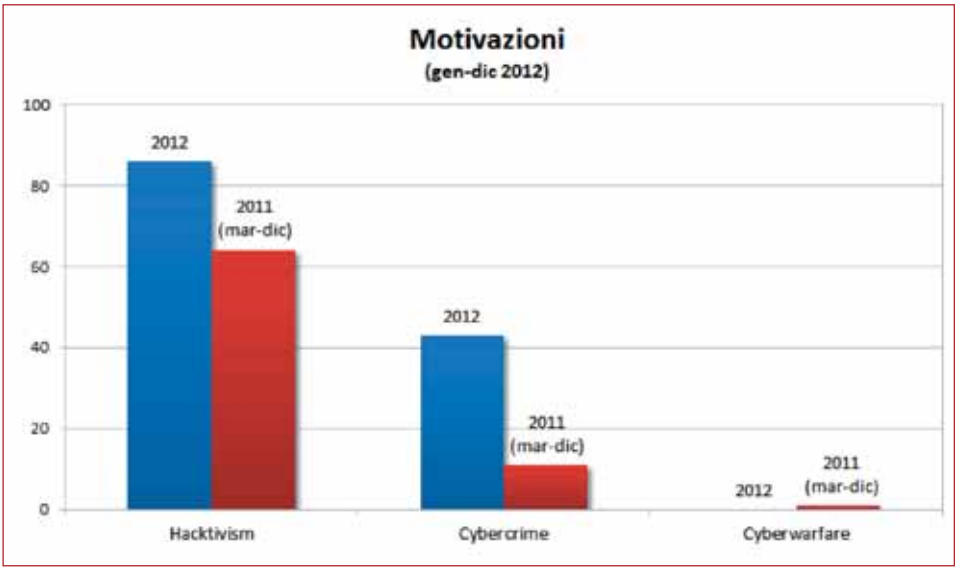
Se il buongiorno si vede dal mattino, il 2013 non promette bene. All'inizio di gennaio una nota azienda di sicurezza ha difatti rivelato l'operazione "Red October", una articolata campagna di spionaggio attiva da oltre 5 anni nei confronti di governi, ambasciate, istituzioni di ricerca e commercio ed aziende appartenenti a diversi settori[67]. Anche in questo caso il nostro Paese figura nella lista degli obiettivi, con 5 non precisate entità colpite dall'attacco. Parallelamente, il numero di attacchi (furti di identità, di denaro, phishing, etc) è in costante aumento.

Analisi della distribuzione e tipologia degli attacchi

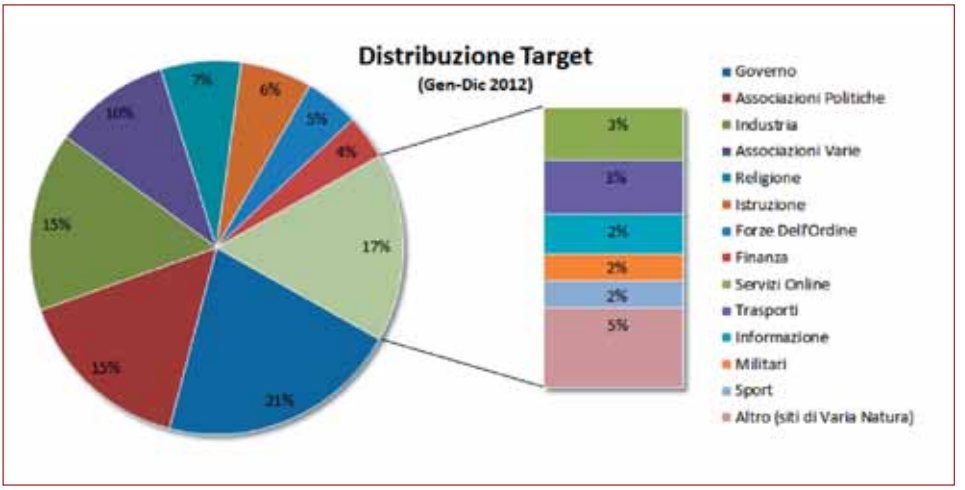
Si vuole proporre nel presente paragrafo un'analisi degli attacchi all'interno di un campione di 129 eventi. Il campione, che non pretende di essere esaustivo dato che si riferisce solo ad eventi divenuti di pubblico dominio, include gli attacchi attuati contro entità del nostro Paese che sono stati rilevati direttamente (perché hanno trovato spazio sui media) o indirettamente (poiché i dati sottratti sono stati pubblicati su social network, online repository come Pastebin, etc.).

Dei 129 attacchi rilevati nel periodo Gennaio-Dicembre 2012, 86, corrispondenti al 67%, risultano essere di matrice *hacktivistica*. In 43 casi, corrispondenti al 33%, si sono riscontrate motivazioni riconducibili al Cyber Crime. È interessante confrontare questo dato con il campione relativo a 10 mesi del 2011 (marzo-dicembre), dove queste percentuali si attestavano rispettivamente all'84 e 14%. Anche per l'Italia quindi nel campione analizzato nel corso del 2012 si è dimostrato un incremento degli attacchi motivati da Cyber Crime ed un calo degli eventi riconducibili a natura *hacktivistica*.

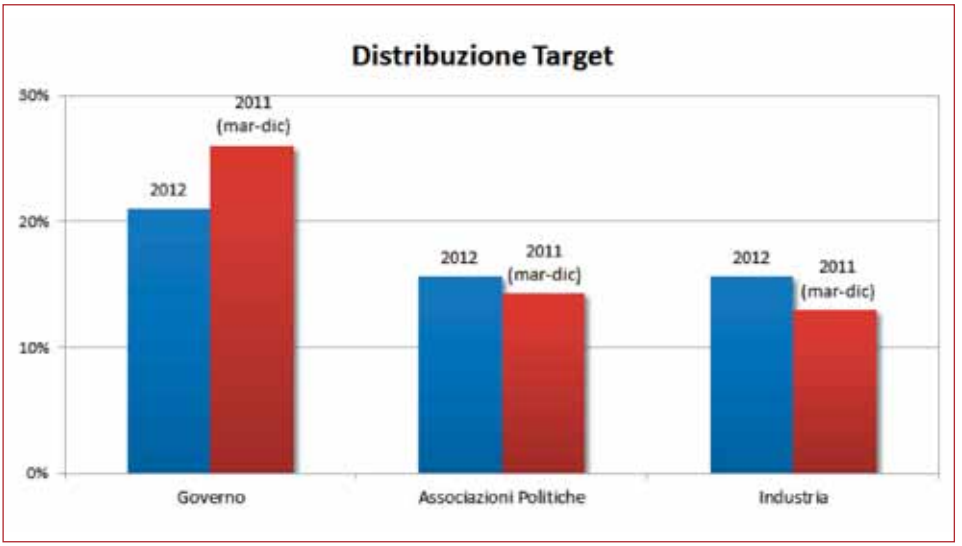
[67] http://www.securelist.com/en/blog/785/The_Red_October_Campaign_An_Advanced_Cyber_Espionage_Network_Targeting_Diplomatic_and_Government_Agencies



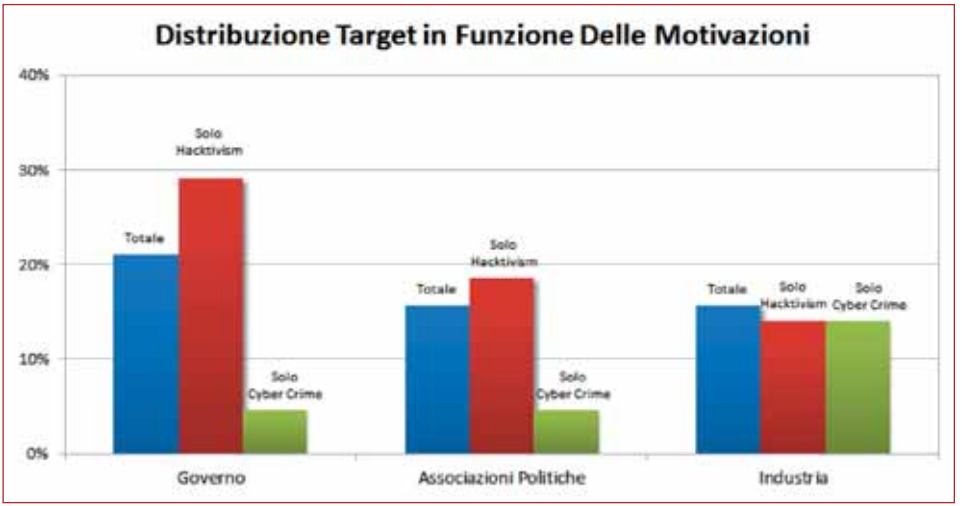
Per quanto riguarda la distribuzione degli obiettivi, il campione analizzato mostra una preferenza degli attaccanti per il settore governativo, immediatamente seguito da associazioni politiche e industria.



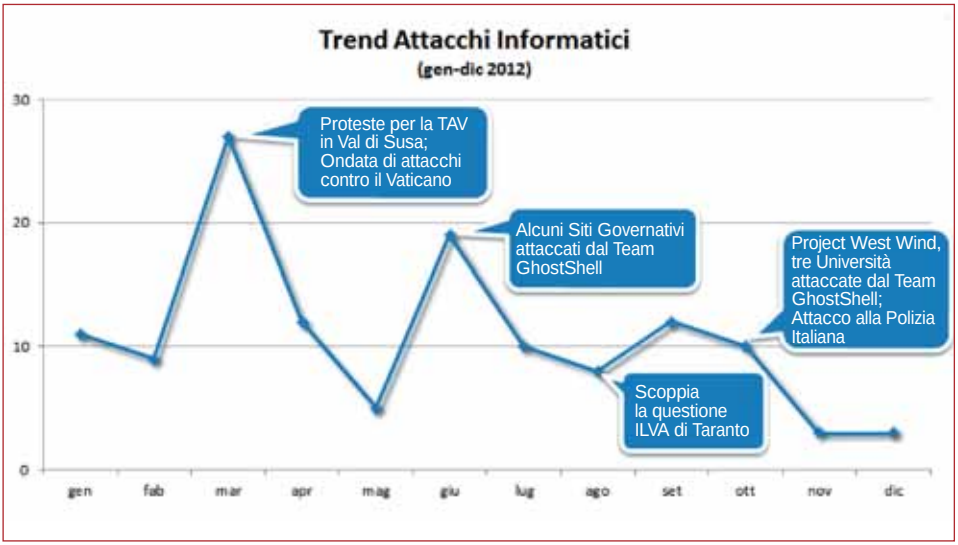
Sommando i primi due settori, si nota come quasi un attacco su tre ha preso di mira istituzioni governative o associazioni politiche. Di nuovo è interessante confrontare questi risultati con quelli dell'anno precedente (10 mesi).



Da cui si nota un lieve calo percentuale degli obiettivi governativi parzialmente ridistribuitosi tra Associazioni Politiche e Industria. Questo è probabilmente dovuto alla minore incidenza degli attacchi imputabili a matrice attivista. Se difatti si esaminano le percentuali in base alla motivazione, si deduce che gli attivisti preferiscono di gran lunga gli obiettivi governativi, la cui incidenza sale al 29% (quasi un attacco su tre) se si estrapolano dal campione i soli attacchi riconducibili ad attivismo informatico.



L'analisi del trend mostra invece un anno a due facce, influenzato dall'andamento dell'attivismo (i cui attacchi hanno tipicamente trovato maggiore spazio nei media). Nel primo trimestre dell'anno vi è stata la maggiore concentrazione di attacchi, dovuta ad alcuni eventi socio-politici avvenuti in Italia, in particolare le proteste in Val di Susa contro la TAV. Il picco del mese del marzo è in parte dovuto ad una serie di attacchi senza precedenti contro istituzioni religiose.
A giugno si è invece registrato un picco dovuto all'incursione del collettivo Ghostshell in Italia: un assaggio della loro operazione Project WestWind che ha trovato pieno compimento nel mese di ottobre. Da luglio in poi la frequenza degli attacchi è andata progressivamente scemando, raggiungendo i valori minimi a novembre e dicembre.



Sicurezza e tutela della propria identità

Aldilà delle statistiche relative agli attacchi, nella precedente edizione del Rapporto chi scrive si augurava un nuovo approccio relativamente al tema della sicurezza dei dati e delle infrastrutture informatiche, indicando come principale fattore di rischio la volatilità del dato, la crescente adozione dei dispositivi mobili e la superficialità di alcuni comportamenti da parte degli utenti (e delle organizzazioni). Questi fattori costituiscono un'esca molto allettante per i criminali e necessitano, oltre che di adeguate contromisure

tecnologiche, di un nuovo approccio da parte degli utenti e delle organizzazioni in termini di normative, tecnologie e cultura.
Purtroppo, ad un anno di distanza, non ci sentiamo di dire che quell'auspicabile processo di sensibilizzazione e consapevolezza degli utenti si sia verificato.
Si sta invece delineando una pericolosa tendenza tra le giovani generazioni (e non solo), che stanno crescendo con un concetto di privacy totalmente nuovo e diverso dalle generazioni precedenti. Un concetto che li espone maggiormente alle minacce virtuali.
Questo fatto è in parte imputabile alla cosiddetta "virtualizzazione dei rapporti sociali": poter vedere una persona in viso, consente di valutare in tempo reale le sue reazioni, e di adattare conseguentemente il proprio comportamento. Non vedere chi (o cosa) ci sta di fronte porta ad atteggiamenti superficiali di cui non è possibile valutare in tempo reale le conseguenze.
La traduzione pratica di questo trend, è che si assiste oramai alla condivisione di una quantità eccessiva di informazioni personali senza avere piena consapevolezza delle implicazioni pratiche. I dati sono facile preda per bulli e stalker digitali, nonché per i criminali che possono ottenere dai social network o da altre informazioni inconsapevolmente condivise (ad esempio le coordinate di una fotografia) indicazioni utili per portare a termine eventuali azioni illecite in ambito virtuale e reale. Per di più non sono solo i malintenzionati a trarne vantaggio: anche per un ipotetico datore di lavoro è fin troppo facile scavare nei dettagli personali di un candidato tra motori di ricerca e social network.
Purtroppo esporre superficialmente informazioni nell'ambito della sfera virtuale, può avere conseguenze drammatiche: non sono mancati nel 2012 (e già all'inizio del 2013) casi di adolescenti che si sono tolti la vita in seguito ad episodi di Cyber Bullismo manifestatisi sulle bacheche dei Social Network. E anche se non è corretto additare la responsabilità di simili eventi interamente ai Social Network, può accadere, come dimostrato dalla cronaca, che l'esposizione incontrollata e superficiale di dettagli personali, da parte di se stessi o di altri, contribuisca ad acuire disagi pre-esistenti (soprattutto nelle fasce di età "difficili").

Le minacce più temibili sono quelle invisibili

Sul fronte del *cybercrime*, ha destato molto rumore tra gli ambienti specializzati e non solo, la statistica di una nota azienda informatica che ha posto nel 2012 l'Italia al nono posto a livello globale per la diffusione di malware e soprattutto al primo posto in Europa (quarto posto a livello mondiale) come numero di PC infettati e controllati da hacker (le cosiddette botnet)[68].

Addirittura Roma, nella poco invidiabile classifica relativa alla diffusione di bot, si è guadagnata il secondo gradino del podio (con 60.000 macchine compromesse stimate a maggio 2012) dietro Taipei[69]. A pareggiare la storica rivalità tra Roma e Milano ci ha pensato la stessa società informatica che colloca Milano al primo posto in Italia (settimo in Europa) per gli illeciti informatici[70].

Con simili premesse, operazioni massive come la già citata Eurograbber non stupiscono affatto. Una operazione criminale di scala così ampia ha dimostrato come l'amore degli Italiani per i dispositivi mobili, e la crescente attitudine a compiere operazioni on-line, siano fattori ben noti (e redditizi) per i criminali informatici, e nel contempo devastanti per le vittime.

Il lato negativo della questione risiede nel fatto che simili attacchi basano molta della loro efficacia sui sopra citati comportamenti superficiali degli utenti (che cliccano su link sospetti senza pensarci due volte).

Se si vuole cogliere un lato positivo in questa vicenda, esso risiede nel fatto che l'evento in questione ha trovato spazio nelle principali testate nazionali. Poiché è praticamente impossibile che le vittime (o gli istituti coinvolti) "pubblicizzino" analoghi accadimenti, è auspicabile che dalla crescente copertura dedicata dai media a simili eventi, che toccano profondamente la sensibilità (e le tasche) dei cittadini, parta quel movimento di sensibilizzazione necessario ad instaurare la prima forma di difesa della propria identità digitale costituita dall'accortezza e dalla diffidenza. Soprattutto nel caso delle minacce di ultima generazione, dove le tradizionali tecnologie non possono garantire piena difesa, questi fattori sono fondamentali. Questo

---

68 http://www.repubblica.it/economia/affari-e-finanza/2012/05/07/news/malware_litalia_al_nono_posto_ma_la_prima_per_le_reti_bot-34591291

69 http://roma.repubblica.it/cronaca/2012/05/02/news/roma_al_secondo_posto_al_mondo_per_computer_infetti-34341309/

70 http://milano.repubblica.it/cronaca/2012/03/10/news/truffe_virus_e_mail_moleste_milano_capitale_dei_reati_online-31273712/

vale doppiamente per noi Italiani che, secondo uno studio di Cambridge, non siamo nemmeno aiutati dalla lingua: l'Italiano difatti risulta essere la seconda lingua al mondo (dopo l'Indonesiano) più vulnerabile ad attacchi di identificazione della password basati su dizionario[71].
Non è un caso che, per contrastare questo crescente fenomeno, ed in generale tutti i reati commessi via Web, l'Europa abbia istituito l'European CyberCrime Center (EC3)[72], un centro di controllo composto da 43 esperti di sicurezza che si occuperanno di presidiare la rete per difendere gli interessi degli utenti (privati o pubbliche istituzioni) e sgominare associazioni criminali operanti sulla rete.
Su scala nazionale, anche se tardivamente (e con qualche anno di ritardo rispetto ai principali Paesi europei) qualcosa si sta muovendo. Il 23 gennaio 2013, il Presidente Del Consiglio Mario Monti ha posto la firma del primo decreto per la nascita di "un'architettura di sicurezza cibernetica nazionale e di protezione delle infrastrutture critiche" e per la conseguente istituzione di un Centro di Coordinamento nazionale (CERT). Alla luce delle operazioni di spionaggio massive che hanno toccato anche il nostro Paese, la scelta è più che mai opportuna. L'augurio degli addetti ai lavori è che la strategia non rimanga solo sulla carta, ma trovi piena applicazione per difendere il nostro Paese nel "cyberspazio", che è a tutti gli effetti ormai considerato il 5° Dominio di Combattimento (dopo terra, mare, aria e spazio) dai principali Paesi avanzati.

Quanto costano davvero gli incidenti informatici in Italia?

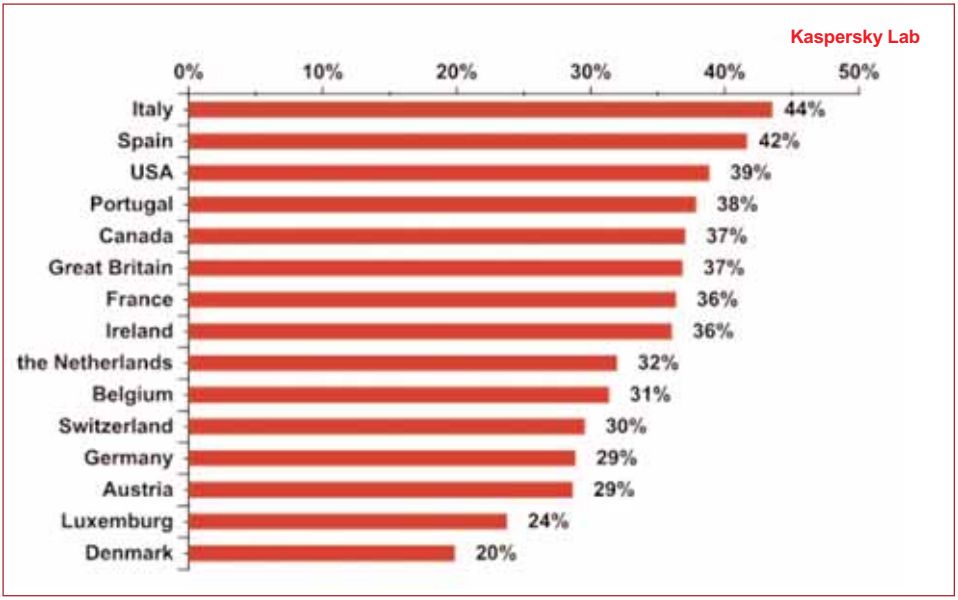
In breve, non lo sappiamo, e siamo costretti a ragionare per analogia con altre nazioni. Per fare un esempio, una ricerca dell'ottobre 2012[73] stima che le perdite dovute al cyber crime in Olanda siano di circa 10 miliardi di euro all'anno.
In Italia non sono disponibili statistiche ufficiali in merito ai danni economici provocati dagli incidenti informatici, sia per la "difficoltà culturale" nel riconoscere di aver subito un incidente da parte delle vittime che per la

[71] http://www.cl.cam.ac.uk/~jcb82/doc/B12-IEEESP-analyzing_70M_anonymized_passwords.pdf
[72] http://www.corriere.it/tecnologia/cyber-cultura/13_gennaio_15/cyberpolizia-unione-europea-malware_927bfbec-5eee-11e2-8d79-cb6cdb3edff8.shtml
[73] www.cyberwarzone.com/cyberwarfare/cybercrime-costs-netherlands-10-billion-euros-year

riluttanza generalizzata a denunciare l'accaduto (anche perché non esiste ancora un obbligo di legge specifico in materia per i soggetti giuridici. A livello Europeo è in via di presentazione una direttiva in merito[74]).
Per quanto riguarda i costi provocati dal Cybercrime esistono però dati parziali, provenienti da aziende private del settore. Secondo un'indagine pubblicata a settembre 2012[75], gli ultimi dati indicano che l'anno scorso dalle tasche dei cittadini italiani sono spariti 2,45 miliardi di euro, con 8,9 milioni di individui che nell'anno sono rimasti vittima di crimini informatici. È importante rilevare che questo numero corrisponde a circa un terzo degli utenti Internet attivi in Italia nel 2012[76].
La situazione non cambia molto in ambito aziendale. Il Ponemon Institute ha condotto nel 2011 una indagine (pubblicata nel 2012), finalizzata ad evidenziare il costo medio nel nostro Paese relativo alla compromissione di un record contenente dati personali[77]. Il risultato è stato eloquente: per ogni compromissione di un record personale un'azienda spende in Italia 78 euro tra indagini, notifiche, spese legali e costi legati all'interruzione del business.
A rinforzare il concetto che la sicurezza non è solo protezione del dato da fattori esterni ma anche, e soprattutto, da fattori interni (che hanno natura principalmente culturale), lo stesso studio ha evidenziato che la prima causa per la perdita di informazioni personali (39%) non è costituita da attacchi criminali, ma da negligenza ed errori umani.
Anche per quanto riguarda lo spionaggio industriale non esistono dati ufficiali, ma solo "sensazioni" colte dal mercato ed alcune case histories (rigorosamente protette da NDA e non pubbliche). Il bersaglio principale sono le nostre PMI ad alto valore aggiunto, che stanno subendo una significativa emorragia di proprietà intellettuale, senza nemmeno accorgersene, da parte di cyber-vampiri di ogni nazionalità. Così il nostro know-how, il nostro design, i nostri brevetti finiscono nelle mani dei competitor, con danni incalcolabili (e che nessuno calcola). Le aziende chiudono anche per questo, al giorno d'oggi.
Sempre in tema di scarsa cultura della sicurezza informatica i nostri giova-

74 http://www.reuters.com/article/2012/12/17/us-eu-cybersecurity-idUSBRE8BG0Z220121217
75 http://www.symantec.com/it/it/about/news/release/article.jsp?prid=20121004_01
76 http://www.webmaori.com/blog/utenti-internet-in-italia-maggio-2012.html
77 http://www.symantec.com/content/en/us/about/media/pdfs/b-ponemon-2011-cost-of-data-breach-italy.en-us.pdf

ni, i famigerati "nativi digitali", in media non sanno nulla di ICT Security, pur essendo quasi tutti rigorosamente dotati di smartphone di ordinanza, sempre connessi sui Social Network e quindi esposti ad ogni genere di minaccia. La scuola in questo contesto dovrebbe senz'altro fare di più.
E gli adulti, in quanto a scarsa consapevolezza, non sono da meno. Per esempio negli approvvigionamenti di prodotti e servizi ICT, di norma né la PA né le aziende private tengono conto degli aspetti di Information Security, sia per quanto riguarda i contratti che per quanto riguarda il contenuto di quello che acquistano. Di conseguenza finiscono per comprare prodotti e servizi intrinsecamente insicuri, oppure per implementarli e configurarli in modo insicuro, senza alcuna garanzia né tutela in caso di incidenti.
Forse per questo in 2 giorni qualsiasi del gennaio 2013 sono stati "defacciati" da script kids di ogni parte del mondo (turchi, filippini, pakistani, brasiliani…) i siti di 70 Comuni italiani[78]. Oppure, come emerge da una recente ricerca[79], è per questo motivo che il 44% dei PC italiani vengono attaccati da malware durante la navigazione in Internet, contro il 20% di quelli danesi.



78 http://www.en3py.net/italian/blog/26/oltre-70-siti-it-nell-elenco-zone-h-di-ieri-e-oggi.php
79 http://www.securelist.com/en/analysis/204792244/The_geography_of_cybercrime_Western_Europe_and_North_America

A parità di sistema operativo e di minacce informatiche, che sono sostanzialmente uguali per tutti, che cosa causa il raddoppio del tasso di rischio dei PC italiani rispetto alle loro controparti del nord Europa? Da un lato la mancanza di policies di sicurezza (o il loro sistematico aggiramento) e di sistemi tecnologici per la loro imposizione, e dall'altro la mancanza di cultura degli utenti.
Così, mentre i reati informatici aumentano in modo esponenziale, le nostre Forze dell'Ordine cercano di fare il possibile, sopportando stoicamente una carenza cronica di uomini e mezzi che non è più tollerabile in un Paese tecnologicamente avanzato.
Come abbiamo scritto anche l'anno scorso nel primo Rapporto Clusit sulla Sicurezza ICT in Italia, tutto questo ha un costo importante e troppo spesso sottovalutato. Nel frattempo, nonostante il varo della tanto sospirata Agenda Digitale Italiana, che sulla carta include una serie di importanti Linee di Azione sulla Cyber Security[80], in Italia negli ultimi 12 mesi dal punto di vista della sicurezza informatica applicata non è cambiato nulla di sostanziale, il che, dati i trend in atto, significa aver perso parecchio terreno.
Dobbiamo sperare che il recente decreto del Governo Monti[81], l'Agenda Digitale Europea, ed in particolare la recente pubblicazione della Cyber Strategy Europea[82], che include una proposta di Direttiva in materia di Network Information Security, possano fare da "traino" per l'Italia, imponendoci di affrontare con maggiore consapevolezza, coordinamento ed efficacia i problemi derivanti dalla crescente insicurezza informatica.
L'alternativa è consegnare il nostro Paese (le sue imprese, le sue Istituzioni ed i suoi cittadini) nelle mani di cyber criminali, spie e potenze ostili, lasciando che diventi un Far West digitale, condizione dalla quale sarebbe poi difficilissimo uscire e che avrebbe un impatto tremendo sull'economia interna, sugli investimenti stranieri e sulla qualità della vita dei nostri cittadini.

80 http://www.agenda-digitale.it/agenda_digitale/index.php/strategia-italiana/cabina-di-regia/74-infrastrutture-e-sicurezza
81 http://www.governo.it/Presidenza/Comunicati/dettaglio.asp?d=70337
82 http://ec.europa.eu/digital-agenda

BIBLIOGRAFIA

Oltre alle fonti già citate in questa «Panoramica degli eventi di cyber-crime e incidenti informatici più significativi del 2012 e tendenze per il 2013», segnaliamo altri Report e Survey che abbiamo preso in considerazione.

[1] Ranking Global Cybercrime - John Barham
http://www.securitymanagement.com/article/ranking-global-cybercrime

[2] Cisco 2013 Annual Security Report - Cisco
http://www.cisco.com/en/US/prod/vpndevc/annual_security_report.html

[3] Panorama de la Cyber-Crminalité – Clusif
https://www.clusif.asso.fr/fr/production/ouvrages/type.asp?id=CYBER%2DCRIMINALITE

[4] Building Business Resilience, A research program sponsored by IBM, Final survey results, 2011 – Economist Intelligence Unit

[5] Appropriate security measures for smart grids, Guidelines to assess the sophistication of security measures implementation, 2012 - ENISA
http://www.enisa.europa.eu/activities/Resilience-and-CIIP/critical-infrastructure-and-services/smart-grids-and-smart-metering/appropriate-security-measures-for-smart-grids/at_download/fullReport

[6] Baseline Capabilities of National/Governmental CERTs, Updated Recommendations 2012 - ENISA
http://www.enisa.europa.eu/activities/cert/support/files/updated-recommendations-2012/at_download/fullReport

[7] Critical Cloud Computing, A CIIP perspective on cloud computing services, 2012 -ENISA
http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/critical-cloud-computing/at_download/fullReport

[8] Cyber Europe 2012, Risultanze fondamentali e raccomandazioni - ENISA
http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cyber-crisis-cooperation/cyber-europe/cyber-europe-2012/cyber-europe-2012-key-findings-report-1

[9] Deployment of Baseline Capabilities of National/Governmental CERTs - ENISA
http://www.enisa.europa.eu/activities/cert/support/files/status-report-2012/at_download/fullReport

[10] ENISA Threat Landscape, Responding to the Evolving Threat Environment, 2012 - ENISA
https://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/ENISA_Threat_Landscape/at_download/fullReport

[11] Give and Take, Good Practice Guide for Addressing Network and Information Security Aspects of Cybercrime - ENISA
http://www.enisa.europa.eu/activities/cert/support/fight-against-cybercrime/good-practice-guide-for-addressing-network-and-information-security-aspects-of-cybercrime/at_download/fullReport

[12] Proactive Detection of Security Incidents, Honeypots, 2012 - ENISA
http://www.enisa.europa.eu/activities/cert/support/proactive-detection-of-security-incidents-II-honey pots/at_download/fullReport

[13] Proposal for a “Directive of the European Parliament and of the Council” concerning measures to ensure a high common level of network and information security across the Union, 2013 - European Commision
http://ec.europa.eu/information_society/newsroom/cf//document.cfm?doc_id=1666

[14] Finding a strategic voice, Insights from the 2012 IBM Chief Information Security Officer Assessment - IBM
http://www.ibm.com/smarterplanet/us/en/business_resilience_management/article/security_essentials.html

[15] Reputational risk and IT - IBM
http://www-935.ibm.com/services/multimedia/2012_Representational_Risk_Study.pdf

[16] X-Force Report 2012 - IBM
http://www-03.ibm.com/press/us/en/pressrelease/38915.wss

[17] Global IT Security Risks: 2012 - Kaspersky
http://www.kaspersky.com/downloads/pdf/kaspersky_global_it-security-risks-survey_report_eng_final.pdf

[18] Data Loss Barometer - KPMG
http://www.kpmg.com/UK/en/IssuesAndInsights/ArticlesPublications/Documents/PDF/Advisory/data-loss-barometer-2012.pdf

[19] Publish and be Damned - KPMG
http://www.kpmg.com/uk/en/services/advisory/risk-consulting/services/tech-risk/documents/forbes-survey-publish-be-damned.pdf

[20] Rapporti semestrali - MELANI
http://www.melani.admin.ch/dokumentation/00123/00124/01526/index.html?lang=it

[21] Android Under Siege: Popularity Comes at a Price – Trend Micro
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/reports/rpt-3q-2012-security-roundup-android-under-siege-popularity-comes-at-a-price.pdf

[22] Detecting APT activity with network traffic analysis - Trend Micro
http://www.trendmicro.com/cloud-content/us/pdfs/security-intelligence/white-papers/wp-detecting-apt-activity-with-network-traffic-analysis.pdf

[23] Minacce alla sicurezza delle aziende, lo stile di vita digitale e il cloud, Previsioni Trend Micro per il 2013 e oltre – Trend Micro
http://www.trendmicro.it/media/misc/2013-predictions-security-threats-it.pdf

[24] Verifica di Sicurezza del 2°T 2012, Sono grossi affari... e la cosa si sta facendo personale – Trend Micro
http://www.trendmicro.it/media/misc/big-business-is-getting-personal-report-it.pdf

[25] Global Risks 2013: Digital Wildfires in a Hyperconnected World - World Economic Forum
http://reports.weforum.org/global-risks-2013/risk-case-1/digital-wildfires-in-a-hyperconnected-world/#read

[26] Fraud Management & Security – ZeroUno & NetConsulting (in partnership con Attachmate)
http://www.attachmate.it/Info/Luminet/thankyou-feb2013.htm

La Polizia Postale e delle Comunicazioni e il contrasto al cybercrime

In questo contributo, la Polizia Postale e delle Comunicazioni descrive i fenomeni criminosi a cui si è trovata confrontata e fornisce dei dati inediti, quantitativi e qualitativi, su attività investigative e risultati ottenuti nel corso del 2012.

Pedopornografia On-Line

L'impegno del Servizio Polizia Postale e delle Comunicazioni nel contrasto alla pedopornografia in rete e alle connesse forme di devianza si appalesa ogni giorno più complesso sia per la continua evoluzione delle tecnologie utilizzate per l'occultamento e la diffusione di immagini di abuso sessuale sui minori, sia per le nuove frontiere di rischio che si profilano per le nuove generazioni sempre più diffusamente proiettate nei contesti dei social network.

L'attività di contrasto è coordinata a livello centrale dal Centro Nazionale per il Contrasto alla Pedopornografia On-line (C.N.C.P.O.) con il supporto operativo dei Compartimenti regionali.

Fino alla fine di novembre 2012 la Specialità ha arrestato complessivamente 78 persone e ne ha denunciate 327 per reati connessi alla produzione e diffusione on-line di materiale pedopornografico.

Di grande rilievo il numero (27) dei minori vittime di abusi sessuali identificati a testimonianza del forte impegno della Polizia, non concentrato solamente nel mero aspetto repressivo, ma diretto anche ad individuare le reali vittime di questa grave fenomenologia criminosa che alimentano uno squallido mercato su scala mondiale.

L'individuazione delle giovani vittime consente infatti di sottrarle ad ignobili vessazioni per avviarle nel contempo sui più appropriati percorsi di assistenza.

Tra le più significative iniziative in ambito di prevenzione e di investigazione è in fase di avanzata realizzazione un progetto di collaborazione con il Dipartimento di Informatica ed Applicazione dell'Università di Salerno finalizzato all'identificazione degli autori delle immagini pedopornografiche attraverso l'analisi delle tracce digitali rilevate nei congegni di videoripresa.

Di rilievo anche il numero (37) delle vittime di adescamento on-line individuate in linea con la recentissima formulazione normativa in materia.
I dati evidenziano un oggettivo consistente incremento dell'attività come emerge chiaramente dal raffronto con il numero degli arrestati (49) e delle vittime identificate (12) nel corso dell'intero anno 2011.

ATTIVITÀ	2011	2012*
ARRESTI	49	**78**
DENUNCE	777	**327**
IDENTIFICAZIONE MINORI VITTIME DI ABUSI	12	**27**
IDENTIFICAZIONE MINORI ADESCATI	-	**37**
* dati aggiornati al 30 Novembre 2012		

Attività di prevenzione
Il monitoraggio di oltre 24.610 siti sospetti ha consentito l'individuazione di 461 spazi web con contenuti pedopornografici, ospitati presso server stranieri.
I siti sono stati successivamente inseriti nella apposita black-list per impedirne l'accesso dall'Italia.

ATTIVITÀ	2011	2012*
SITI MONITORATI	21.199	**24.610**
NUOVI SITI INSERITI IN BLACK LIST	365	**461**
TOTALE SITI IN BLACK LIST	1.062	**1.486**
* dati aggiornati al 30 Novembre 2012		

Di seguito i dati di sintesi delle operazioni di maggior rilievo nell'anno in corso.

- Il Compartimento di Torino, unitamente al Centro Nazionale per il Contrasto alla Pedopornografia On-line con il coordinamento della Procura Distrettuale di quel capoluogo, ha condotto un'operazione sottoco-

pertura che ha portato all'arresto di 8 persone e alla denuncia di altre 22 per detenzione e divulgazione in rete di materiale pedopornografico.
L'attività investigativa ha inoltre permesso di identificare un diretto autore degli abusi, tre minori vittime e di verificare che quattro degli arrestati producevano direttamente il materiale con contenuti pedopornografici destinato alla rete.
Gli operatori della Specialità si sono introdotti all'interno di comunità virtuali pedofile che condividevano materiale pedopornografico accreditandosi all'interno di luoghi virtuali di scambio individuandone in tal modo i frequentatori.
Lo stesso Compartimento ha inoltre individuato 28 spazi web con contenuti pedopornografici.

- Il Compartimento di Catania, con il coordinamento della Procura Distrettuale di quel capoluogo, ha condotto un'operazione in tre fasi, anche con il ricorso ad attività sottocopertura, che ha portato all'arresto di 8 persone, alla denuncia di altre 112 per detenzione e divulgazione in rete di materiale pedopornografico nonchè all'identificazione di un minore vittima di abusi sessuali. Le indagini, che hanno avuto origine attraverso le segnalazioni di utenti della rete e di associazioni impegnate nella tutela dell'infanzia, sono state incentrate sullo sviluppo di tracce informatiche che hanno consentito all'individuazione di soggetti che condividevano file pedopornografici in rete.
Lo stesso Compartimento ha inoltre individuato 247 spazi web con contenuti pedopornografici.

- Il Compartimento di Genova, con il coordinamento della Procura Distrettuale di quel capoluogo, ha condotto un'operazione sottocopertura che ha consentito l'arresto in flagranza di 5 persone mentre condividevano in rete materiale pedopornografico.
Lo stesso Compartimento ha inoltre individuato 7 spazi web con contenuti pedopornografici.

- Il Compartimento di Reggio Calabria, con il coordinamento della Procura Distrettuale di quel capoluogo, ha svolto un'operazione, anche con ricorso ad attività sottocopertura, che ha portato all'arresto di 5 persone e alla denuncia di altre 73 per detenzione e divulgazione di materiale pedopornografico in rete.

Lo stesso Compartimento ha inoltre individuato 2 spazi web con contenuti pedopornografici.

- Il Compartimento di Firenze, con il coordinamento della Procura Distrettuale di quel capoluogo, ha condotto un'operazione, con ricorso ad attività sottocopertura, che ha portato all'arresto di 3 persone e alla denuncia di altre 18 per detenzione e divulgazione di materiale pedopornografico. Gli operatori di Polizia si sono infiltrati all'interno di comunità virtuali di scambio acquisendo le informazioni necessarie riuscendo così ad individuare i responsabili delle attività illecite.
Il predetto Compartimento ha inoltre individuato 45 spazi web con contenuti pedopornografici.

- Il Compartimento di Venezia, con il coordinamento della Procura Distrettuale di quel capoluogo, sulla scorta di una segnalazione pervenuta dalla polizia statunitense, ha denunciato 9 persone per detenzione di materiale pedopornografico. Le indagini hanno consentito di far luce sulla completa filiera di vendita di immagini ritraenti abusi su minori attraverso siti di e-commerce, le cui rimesse venivano poi trasferite in Russia.
Lo stesso Compartimento ha inoltre individuato 13 spazi web con contenuti pedopornografici.

- La Sezione di Salerno, con il coordinamento della Procura Distrettuale di quel capoluogo, ha arrestato 8 persone e denunciato altre 2 per associazione per delinquere finalizzata alla detenzione di materiale pedopornografico. Le indagini hanno riguardato casi di condivisione di copiosissimo materiale attraverso reti anonimizzate.

- La Sezione di Cremona, con il coordinamento della competente Procura Distrettuale, sviluppando alcuni spunti forniti dalla Polizia tedesca in due distinte operazioni, ha arrestato 2 persone e ne ha denunciate altre 22 per detenzione e divulgazione di materiale pedopornografico in rete.
I rimanenti spazi web con contenuti pedopornografici sono stati individuati dagli altri Compartimenti come di seguito riportato:
n° 46 dal Compartimento di Trento
n° 12 dal Compartimento di Trieste - Sezione di Udine

n° 9 dal Compartimento di Ancona
n° 9 dal Compartimento di Pescara
n° 7 dal Compartimento di Milano - Sezione di Bergamo
n° 6 dal Compartimento di Roma
n° 5 dal Compartimento di Cagliari - Sezione di Nuoro
n° 4 dal Compartimento di Perugia
n° 4 dal Compartimento di Napoli
n° 4 dal Compartimento di Bari - Sezione di Foggia
n° 2 dal Compartimento di Palermo
n° 1 dal Compartimento di Milano

Tutela delle infrastrutture critiche informatizzate

Nel settore della protezione delle Infrastrutture Critiche informatizzate di interesse nazionale, nel 2012 il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche, nell'ambito dell'attività di prevenzione e contrasto, ha gestito complessivamente 286 eventi in danno di infrastrutture critiche informatizzate di interesse nazionale (private e istituzionali).
In particolare la Sala Operativa del CNAIPIC, oltre a gestire:

- 136 attacchi informatici di tipo DDOS ovvero defacement, nei confronti di servizi internet relativi a siti istituzionali e infrastrutture critiche informatizzate di interesse nazionale;
- 61 intrusioni e accessi abusivi a sistemi informatici relativi ad infrastrutture critiche ovvero banche dati istituzionali;
- 51 compromissioni di credenziali di autenticazione sui sistemi informatici di infrastrutture critiche, realizzate tramite virus informatici e botnet, ha diramato anche 38 allert per vulnerabilità riscontrate su sistemi informatici/telematici.

Tra le attività investigative condotte dal Centro si segnala la conclusione, con l'arresto di una persona, di una complessa indagine coordinata dalla Procura Distrettuale di Roma, relativa ad una serie di accessi abusivi a sistemi informatici e connessa apprensione e successiva vendita di credenziali di autenticazione alla banca dati dell'Agenzia delle Entrate.
Nel corso dell'anno è stata incrementata significativamente l'attività di partenariato pubblico - privato, istituzionalmente prevista, che ha portato alla stipula di quattro nuove convenzioni rispettivamente con le società Enel, H3G, Finmeccanica, Atac.

Gravi fenomeni criminali in danno dei sistemi/servizi di monetica e di Home Banking

La costante e continua evoluzione delle aggressioni ai sistemi di pagamento elettronico e dei servizi di home banking ha reso necessario l'affinamento di adeguate strategie di prevenzione e di repressione.

Degno di rilievo, in tal senso, un protocollo d'intesa tra la Polizia Postale e delle Comunicazioni e i principali istituti di credito, le società di emissione delle carte elettroniche di pagamento, gli intermediari e i fornitori delle infrastrutture telematiche a supporto delle transazioni finanziarie elettroniche.

Il progetto, finanziato dalla Commissione Europea e ispirato a realizzare le più utili sinergie tra i settori pubblico e privato, è incentrato nell'avvio di innovative procedure di condivisione di dati per il rilevamento precoce di situazioni sospette.

In merito è già in fase di sperimentazione ed avrà piena operatività nel primo semestre 2013, una piattaforma informatica di analisi sviluppata nell'ambito del progetto europeo OF2CEN – On line Fraud Cyber Centre and Expert Network, che vedrà collegati tutti gli istituti convenzionati con il Servizio Polizia Postale e delle Comunicazioni e le sue ramificazioni periferiche.

Importanti i risultati dell'attività investigativa.

Nell'anno in corso la Specialità ha arrestato complessivamente 150 persone e ne ha denunciate 4.876 per reati in danno dei servizi/sistemi di monetica e di home banking.

ATTIVITÀ	2011	2012*
ARRESTI	96	**150**
DENUNCE	5.264	**4.876**

* dati aggiornati al 30 Novembre 2012

Nel mese di maggio il Compartimento di Perugia, con il coordinamento della Procura Distrettuale di quel capoluogo, ha arrestato 11 cittadini nigeriani componenti un'organizzazione criminale transnazionale dedita alla massiva sottrazione e al successivo illecito utilizzo di codici di carte di credito.

Nel mese di giugno il Compartimento di Milano, con il coordinamento della Procura Distrettuale di quel capoluogo, ha arrestato in Italia e all'este-

ro 45 persone componenti di un'organizzazione criminale italo-rumena, dedita a frodi informatiche seriali in danno di sistemi di home-banking.
Nel mese di luglio, lo stesso Compartimento, sempre con il con il coordinamento della Procura Distrettuale di quel capoluogo, ha arrestato in Italia e all'estero 21 persone componenti di un'organizzazione criminale rumena responsabile di illecita sottrazione e successivo utilizzo di codici di carte bancomat.
Nel mese di settembre il Compartimento di Bologna, con il coordinamento della Procura Distrettuale di quel capoluogo, ha arrestato 4 persone denunciandone altre 50, componenti di una organizzazione criminale italio-rumena dedita ad attività fraudolente in danno di sistemi di home-banking.
Nel mese di dicembre il Servizio Polizia Postale e delle Comunicazioni unitamente al Compartimento di Pescara e alla Questura di Teramo, nell'ambito di una più ampia operazione interforze coordinata dalla Procura Distrettuale dell'Aquila, ha arrestato 50 persone componenti un'organizzazione criminale transnazionale dedita alla clonazione e all'illecito utilizzo di di carte di pagamento elettronico.

Uso di Internet per finalità discriminatorie ed eversive

Nel mese di novembre il Servizio Polizia Postale e delle Comunicazioni e la DIGOS della Questura di Roma, con l'ausilio dei Compartimenti della Specialità e di varie Questure italiane, con il coordinamento della Procura Distrettuale di Roma, ha arrestato 4 persone denunciandone altre 17, componenti un'articolata organizzazione criminale dedita alla diffusione online di contenuti ispirati all'odio razziale e all'istigazione, sempre attraverso la rete, a commettere atti discriminatori razziali.

La pirateria satellitare

DIRITTO D'AUTORE (CARD-SHARING)

Nell'ambito dei reati commessi nel campo del diffuso fenomeno della pirateria satellitare, mirata a violare i sistemi di criptazione delle cosiddette trasmissioni televisive ad accesso condizionato, il Servizio Polizia Postale e delle Comunicazioni, direttamente o tramite i Compartimenti, ha svolto complesse attività investigative sul fenomeno del cd. card sharing (illecita condivisione informatica di un unico abbonamento tra più utenti).
Di particolare rilievo, in tal senso, l'attività del Compartimento di Catania

che, con il coordinamento della Procura Distrettuale di quel capoluogo, ha denunciato 177 persone per truffa informatica e violazione della normativa a tutela del diritto d'autore.

Truffe On-Line

Le nuove frontiere dell'innovazione tecnologica hanno, come noto, consentito da un lato il moltiplicarsi delle opportunità di fruire di tutta una serie di servizi attraverso la rete, dall'altro la diffusione di crimini in danno degli utenti.
Di seguito i dati di sintesi delle operazioni di maggior rilievo svolte nell'anno in corso:
Il Compartimento di Reggio Calabria, con il coordinamento della Procura Distrettuale di quel capoluogo, ha arrestato 13 persone e ne ha denunciate 43 per associazione per delinquere finalizzata alla realizzazione di truffe in danno di società finanziarie ed istituti di credito.
Il Compartimento di Pescara, con il coordinamento della Procura Distrettuale di quel capoluogo, ha arrestato 9 persone componenti di un sodalizio criminale che, svolgendo truffaldine attività di brokeraggio nelle procedure di iscrizione ai campionati di calcio, produceva e procurava, attraverso l'utilizzo del mezzo informatico, falsi titoli fidejussori apparentemente rilasciati da noti istituti di credito.

Illeciti nel settore dei Social Network

ILLECITI CONSUMATI SULLA PIATTAFORMA FACEBOOK

Nel corso dell'anno significative sono state le attività di rimozione di "falsi profili" o di "gruppi" e "post" dai contenuti minatori o diffamatori e di identificazione dei responsabili.

- Phishing di account facebook

Il Servizio Polizia Postale e delle Comunicazioni, a seguito di articolate indagini, ha denunciato alla Procura della Repubblica di Roma 2 cittadini rumeni che, clonata la pagina web del noto social network, avevano carpito le credenziali di oltre trenta utenti accedendo indebitamente ai rispettivi profili Facebook sottraendo crediti maturati tramite giochi d'azzardo on-line.

- Estorsioni a sfondo sessuale

Il Compartimento di Genova ha svolto articolate indagini sul fenomeno arrestando in flagranza di reato un cittadino tunisino.
Le vittime venivano contattate da avvenenti donne su canali di chat, invi-

tate a intrattenere comunicazioni erotiche tramite webcam e successivamente ricattate con richieste di denaro in cambio della rimozione dei video abusivamente registrati.

Le campagne educative della Polizia Postale e delle Comunicazioni

I progetti educativi avviati dalla Polizia Postale e delle Comunicazioni nel corso del 2012 hanno coinvolto studenti, genitori ed insegnanti attraverso iniziative ed eventi su tutto il territorio nazionale come di seguito riportato:

Progetto "Buono a Sapersi", che ha coinvolto oltre 450.000 studenti attraverso incontri mensili negli istituti di 100 capoluoghi di provincia sul tema della sicurezza on-line.

Progetto "Web in cattedra", finalizzato alla formazione dei docenti sui rischi e pericoli della rete.

"Internet Safer day", giornata mondiale sulla sicurezza informatica che ha visto il coinvolgimento in un'unica giornata di oltre 50mila studenti, insegnanti e genitori sul territorio nazionale.

Progetto "Non perdere la bussola", frutto della collaborazione tra la Polizia Postale e delle Comunicazioni, Google e YouTube. Originariamente destinato agli studenti delle scuole medie inferiori e superiori, esteso poi ad un numero sempre più ampio di utenti, compresi genitori e insegnanti, si è rivelato uno strumento fondamentale per stimolare un utilizzo responsabile e sicuro degli strumenti informatici.

Progetto "In strada come in rete", rivolto ai ragazzi tra i 10 e i 14 anni delle scuole medie di primo grado della Provincia di Roma, ai loro genitori e agli insegnanti con l'obiettivo di evidenziare i rischi cui si espongono i giovani sia sulla strada "reale" che in rete.

"Giochi Online – rischi e pericoli", iniziativa rivolta ai ragazzi tra i 15 e i 18 anni, ai loro genitori e agli insegnanti delle scuole medie superiori sul territorio nazionale, con l'obiettivo di sensibilizzare sui rischi e i pericoli connessi alla pratica del gioco on line.

Investimenti: il mercato è cresciuto nel 2012 e continuerà a crescere nel 2013

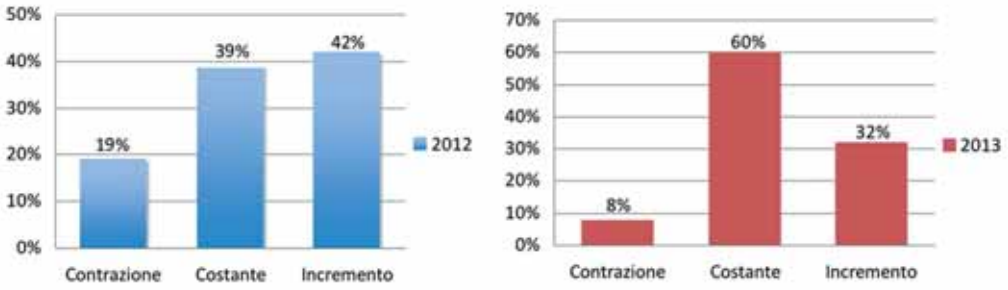
Nonostante la crisi economica che colpisce tutti i settori dell'economia, il mercato dell'Ict security mantiene un andamento positivo stabile e va in controtendenza rispetto al resto. È un segnale incoraggiante sia per le aziende che operano nel settore, sia per il mondo delle aziende utenti, sia per il Paese in generale che vede crescere e diffondersi la consapevolezza sulla criticità della difesa dei dati e sull'importanza di investimenti qualificati per proteggere i sistemi che li ospitano. La nuova edizione del nostro Rapporto mette a confronto in questo capitolo i dati a consuntivo che emergono dalle interviste effettuate a oltre 200 aziende, equamente suddivise tra offerta e domanda, con le previsioni per il 2013 che queste stesse aziende hanno formulato. Ne esce un quadro dinamico, positivo, con molte conferme e qualche piccola novità.

Il mercato continua ad investire

Nel 2012 le aziende che hanno incrementato i loro investimenti in tecnologia sono state il 42% del campione, seguite da una percentuale del 39% che invece ha mantenuto costanti gli investimenti. Ma nello stesso anno la crisi ha colpito duro sul mercato, perché il 19% degli intervistati ha dichiarato una contrazione dei suoi investimenti. Il saldo finale è però positivo con una crescita a consuntivo del 23%, percentuale "da sogno" rispetto ad altri settori.

La stessa positiva visione rimane anche per il 2013 nelle intenzioni degli intervistati. Mentre cresce il numero di coloro che dichiarano stabilità di investimenti (60%) e cala la percentuale di chi incrementa (32%), crolla la percentuale di chi prevede una contrazione: sono solo l'8%. Anche in questo caso la crescita del mercato, al netto tra contrazione e incremento, è decisamente positiva: + 24%

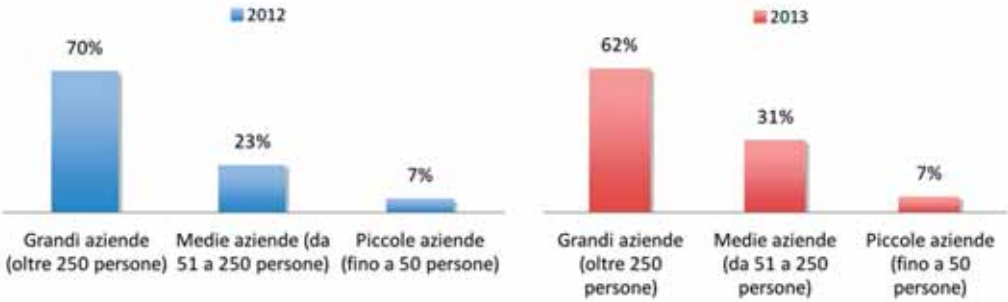
Investimenti nella sicurezza ICT nel 2012 e stima per il 1013



Cresce la sensibilità presso le medie aziende

A tirare la volata negli investimenti sono, come è ovvio aspettarsi, soprattutto le grandi aziende per le quali ormai non c'è più possibilità di fare business senza una seria politica di investimenti in sicurezza. Ben il 70% delle grandi aziende nel 2012 ha investito in Ict security. Meno presente è questa consapevolezza nel mondo delle medie e delle piccole imprese, ma il 2013 dovrebbe presentare un quadro di interessante evoluzione.

Propensione agli investimenti secondo dimensione delle aziende



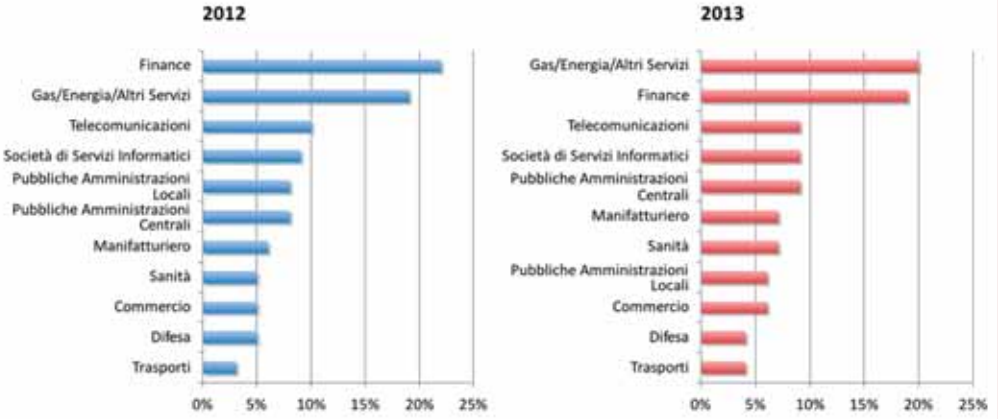
Dovrebbe crescere infatti, e questo dovrebbe essere motivo di consolazione e di stimolo a predisporre nuovi sistemi di offerta da parte dei vendors, la propensione agli investimenti presso le aziende che abbiamo chiamato di media dimensione, quelle tra 51 e 250 addetti, che costituiscono la struttura portante della nostra economia nazionale. Nel 2012 solo il 23%, meno di un quarto, si è dimostrato propenso all'investimento. Nel 2013

questa percentuale dovrebbe crescere a quasi un terzo (31%) del totale. È il segnale più evidente che, pur nella prudenza che il momento richiede, ci sono aziende consapevoli del rischio informatico decise a percorrere la strada dell'innovazione per crescere e per difendersi. C'è da chiedersi se il sistema di offerta del nostro mercato è, a questo punto, calibrato correttamente su questa emergente richiesta: sistemi di distribuzione, sistemi di pricing, sistemi di assistenza post vendita sono in grado di gestire un potenziale ampio parco di clienti più piccoli, meno strutturati sul piano delle competenze, meno concentrati in poche, canoniche aree territoriali?

Servizi e utility protagonisti

La nostra indagine ha correlato anche la propensione agli investimenti con il settore di attività rivelando che il futuro non presenterà sostanziali cambiamenti rispetto al 2012. Nel 2012 il settore che si è dichiarato più interessato agli investimenti è stato quello "finance" e la cosa non deve destare sorpresa. L'apertura delle banche e delle compagnie assicurative al rapporto diretto con il cliente sul web o addirittura sui social network, impone politiche di Ict security con un profilo molto più alto di quanto non sia necessario quando il perimetro di controllo è limitato alla propria rete proprietaria. A seguire, ma con un distacco molto ridotto, il mondo delle utility e dei servizi.

Propensione agli investimenti per settore di attività

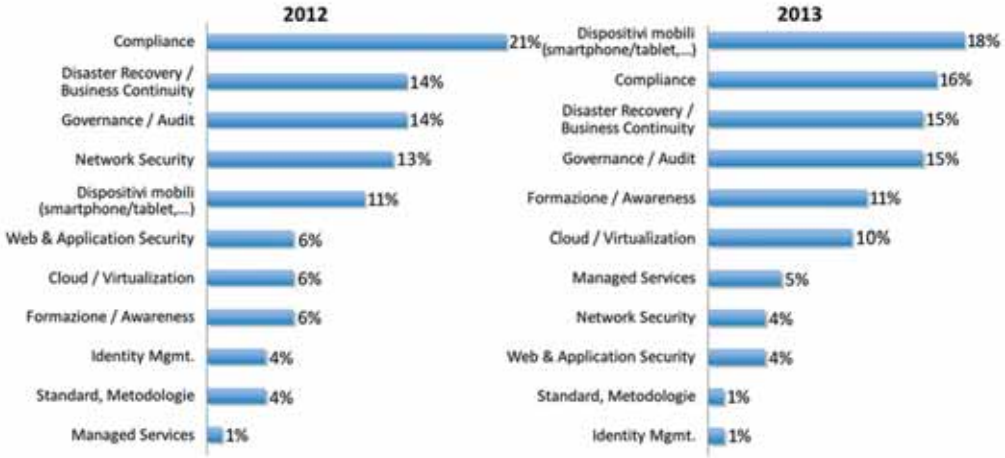


Nel 2013 le posizioni si rovesciano e al primo posto c'è invece il mondo dei servizi e delle utility. Che rappresenta ben il 20% delle aziende interessate agli investimenti. Gas, Energia e Altri servizi primeggiano in testa alla classifica seguite a ruota da Finance e Telecomunicazioni. Anche nel comparto "servizi" è in atto quella rivoluzione nel rapporto tra fornitore e clienti di cui abbiamo parlato per il finance e anche in questo caso il perimetro di "difesa" e protezione si allarga e dunque vanno ridisegnate, a tutti i livelli, nuove politiche di security.
Nel resto della classifica c'è una sostanziale stabilità, con variazioni minime tra quanto è accaduto nel 2012 e quanto si prevede per il 2013. Tra i big spender eccellono telecomunicazioni e società di servizi informatici, mentre PA Centrale e Locale e Manifatturiero rimangono a metà classifica. Fanalini di coda il mondo dei trasporti, della difesa e del commercio.

L'avanzata dei mobile devices

In quali ambiti prevedono di investire le aziende che abbiamo coinvolto nella nostra indagine? Anche in questo caso una piccola rivoluzione ci sorprende nella classifica delle scelte dei nostri interlocutori. Al primo posto balza sorprendentemente il mondo del "mobile business", scavalcando di colpo gli ambiti tradizionali di investimento. Il 18% dei nostri interlocutori prevede infatti investimenti indirizzati alla security dei dispositivi mobili. È il segnale non tanto di una moda, quanto di un profondo cambiamento nella struttura operativa, organizzativa e relazionale delle aziende. Un cambiamento che, anche in questo caso, richiede al mondo dei vendors un rapido adeguamento nella struttura di servizio. Perché un conto è pianificare la security di utenze che stanno in aree controllate, e che rispondono a policy aziendali ben definite, altro è invece progettare adeguamenti su dispositivi che sono per definizione "fuori" dall'azienda, in mano a persone inesperte dal punto di vista tecnico e con caratteristiche d'uso che spesso creano pericolose commistioni tra funzioni professionali e funzioni private.
Gli investimenti in compliance e in disaster recovery e business continuity che tradizionalmente costituiscono l'ambito privilegiato di investimento in security passano così al secondo e terzo posto nelle priorità, con una piccola riduzione di peso relativo: dal 35% di peso complessivo nel 2012 si scende al 31%. Ma un altro interessante segnale, a proposito dei due cambiamenti evidenziati, è rappresentato dalla importante crescita degli investimenti in for-

Sviluppo del mercato/ambiti di investimento



mazione: quasi un raddoppio della percentuale. Sono stati un modesto 6% nel 2012, raggiungeranno un significativo 11% nel 2013, specchio di una accresciuta sensibilità sul tema e sulla necessità del coinvolgimento degli utenti finali in tutte le politiche di ict security.

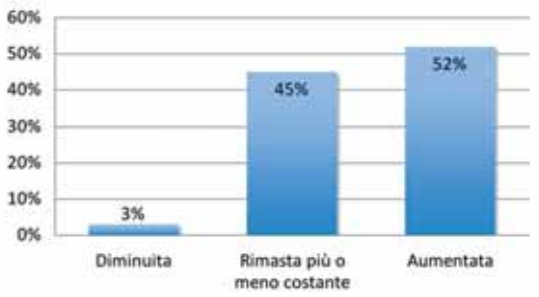
Visoni differenti per il cloud

Tra vendors e aziende utenti nei diversi aspetti che abbiamo finora esaminato ci sono sostanziali identità di vedute e mentre nella scorsa edizione del Rapporto era possibile sottolineare importanti differenze di visione, per il 2013 le posizioni sui diversi temi sono sostanzialmente allineate. Tranne che, significativo caso, proprio nell'ambito delle previsioni di investimento in un particolare, emergente settore: il cloud computing e più in generale l'atteggiamento verso la virtualization. Per i vendors l'apertura verso un nuovo, diverso paradigma organizzativo e tecnologico è al primo posto tra le priorità dell'anno in corso. Per le aziende utenti al contrario il cloud si trova agli ultimi posti tra le priorità, tanto che la media degli interessi totalizza il 10% delle attenzioni, piazzando questa area a metà classifica. Ancora meno rilevanti, e questo è un segnale, ci pare, di arretratezza progettuale, i servizi più innovativi: managed services, network security, identity management che si piazza addirittura all'ultimo posto della speciale graduatoria con un modestissimo 1% delle intenzioni di investimento.

Aumenta la sensibilità sulla security

Il tema della Ict Security rimane, nel percepito dei nostri intervistati, sempre un tema "caldo", al primo posto tra quelli che coinvolgono le aziende. Per il 52% dei nostri prospect infatti nell'ultimo anno la sensibilità sul tema è addirittura aumentata, mentre un consistente 45% dichiara di avere mantenuto la stessa, costante attenzione.

Sensibilizzazione delle aziende al tema della sicurezza informatica

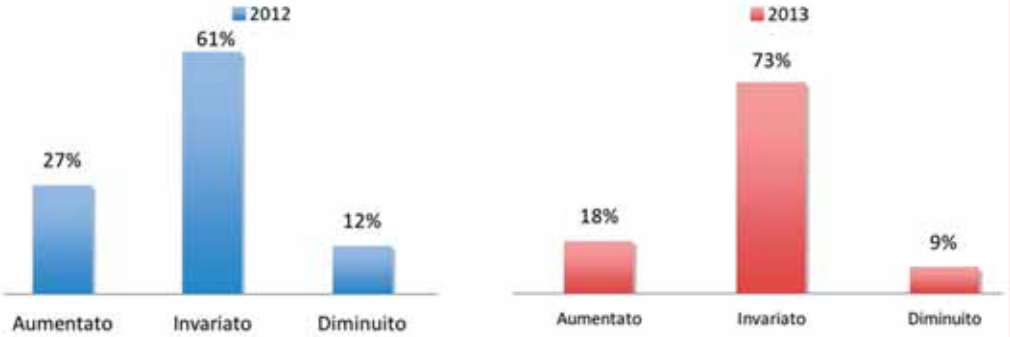


Stuzzicante, sul piano della curiosità, una sparuta pattuglia di intervistati che dichiara di vivere una sensibilità diminuita: sono per fortuna solo il 3%.

Mercato del lavoro: stabilità

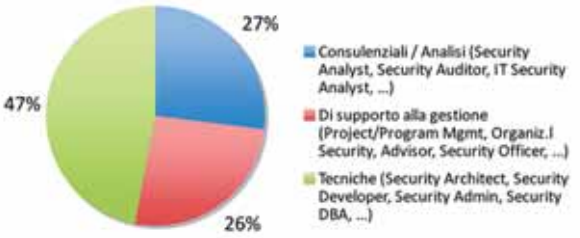
Nel mercato del lavoro specializzato si riflette quell'andamento di crescita che già avevamo individuato a proposito degli investimenti, anche se il 2013 dovrebbe però presentare un rallentamento della crescita occupazionale. Nel 2012 le aziende che hanno continuato ad assumere specialisti sono state più di un quarto del campione, con una percentuale del 27%, a fronte di aziende che invece hanno diminuito gli occupati: 12%.

Andamento del mercato del lavoro - Numero delle persone che si occupano di sicurezza informatica in azienda



Il 61% del nostro campione ha mantenuto stabile l'occupazione.
Nel 2013 le aziende che rimarranno stabili aumentano sensibilmente, saranno il 73%, incidendo sia sulla percentuale delle aziende che prevedono una riduzione (9%) sia su quelle che prevedono un aumento (18%). Il saldo occupazionale, che nel 2012 è stato positivo (15%), nel 2013 dovrebbe continuare a rimanere positivo, ma ridursi a + 9%.

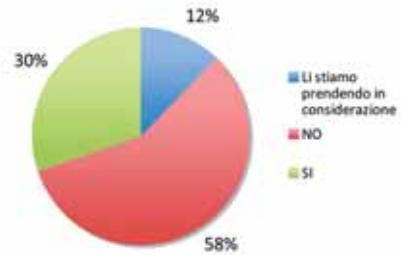
Figure professionali richieste



Prevalgono, tra le figure professionali richieste, quelle a forte contenuto tecnico: Security Architect, Security Developer, Security Admin, Security DBA, per esempio che rappresentano ben il 47% delle nuove figure professionali richieste. In equilibrio invece le altre due famiglie di figure professionali addette al settore: quelle consulenziali (27%) e quelle di supporto alla gestione (26%).

Outsourcing: poco interessate

Abbiamo chiesto alle aziende se utilizzano servizi di outsourcing per la gestione della sicurezza



A conforto delle prospettive occupazionali, nel Rapporto abbiamo anche indagato sulla propensione all'outsourcing per la gestione delle sicurezza. La pratica è ancora molto poco diffusa, tanto che solo il 30% degli intervistati risponde positivamente, mentre quasi una percentuale doppia, il 58%, esclude categoricamente il progetto. Ridotta al 12% invece la percentuale delle aziende che stanno iniziando a considerare questa strada.

Irrilevanti le azioni normative sulla privacy

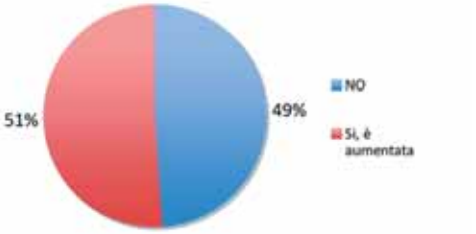
Negli ultimi anni il legislatore ha apportato numerose semplificazioni alle prescrizioni della normativa sulla tutela dei dati personali. Abbiamo chiesto alle aziende quale impatto hanno avuto questi cambiamenti. Ben il 75% degli intervistati ritiene che semplificazioni e riduzione degli oneri derivanti dalla conformità non abbiano comportato vantaggi significativi per le aziende. Nemmeno un quarto degli intervistati ritiene che ci sia stato un vantaggio economico o organizzativo.

Sotto attacco, ma i budget non cambiano

Le strategie di difesa, di protezione e di completezza si confrontano ovviamente con le minacce che provengono dall'interno dell'azienda o dall'esterno. In particolare salgono spesso alla ribalta della cronaca tutte le notizie che riguardano attacchi più o meno criminali contro il patrimonio dati delle aziende. Le minacce contribuiscono a far crescere l'attenzione verso i temi della Ict Security, ci siamo chiesti?

Politiche di privacy e giustificabili cautele impediscono di avere un quadro corretto e completo delle reali minacce che le aziende subiscono quotidianamente, ma i criminali hanno trovato aziende preparate a fronteggiarle, visto che ben il 49% del totale dichiara che l'attacco subito non ha modificato la sensibilità sul tema, riconoscendo dunque alle proprie attuali politiche di protezione una qualità difensiva già adeguata alla guerra in corso. Per il 51% del campione, viceversa, la concretezza degli attacchi subiti ha spinto ad una maggiore attenzione. Il dato incoerente a questo proposito è che a fronte della consistente diffusione degli attacchi, non crescono i

In conseguenza degli attacchi subiti, è cambiata l'attenzione dell'azienda per la sicurezza informatica?



A seguito degli attacchi subiti, avete preso delle contromisure?

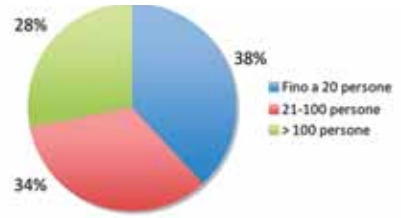
budget dedicati alla difesa. Solo il 25% del campione dichiara che gli attacchi hanno influito sui livelli di investimento previsti, mentre il 75% non ha modificato il budget pianificato.

Le azioni di miglioramento hanno riguardato iniziative di carattere tecnologico (50%), di carattere organizzativo o di processo (33%), o miste (8%). Solo l'8% non ha modificato la propria policy dopo gli attacchi.

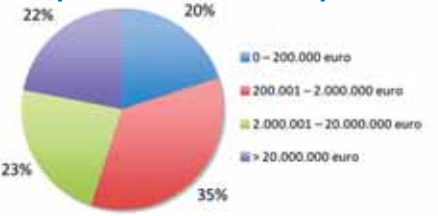
Il campione

Il campione di indagine era costituito da 207 aziende, di cui 99 aziende utenti.

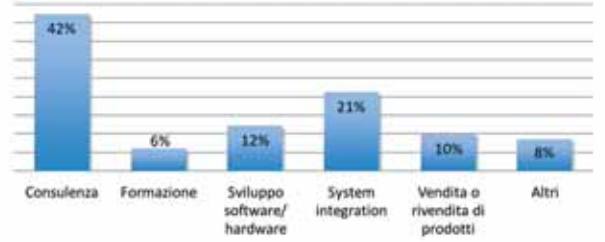
Campione vendors suddiviso per n° addetti



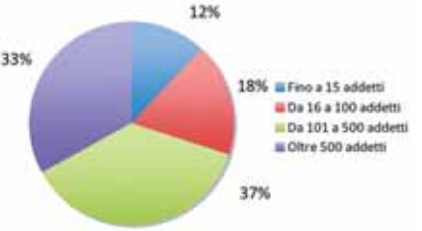
Campione vendors suddiviso per fatturato



Campione vendors suddiviso per tipologia di offerta



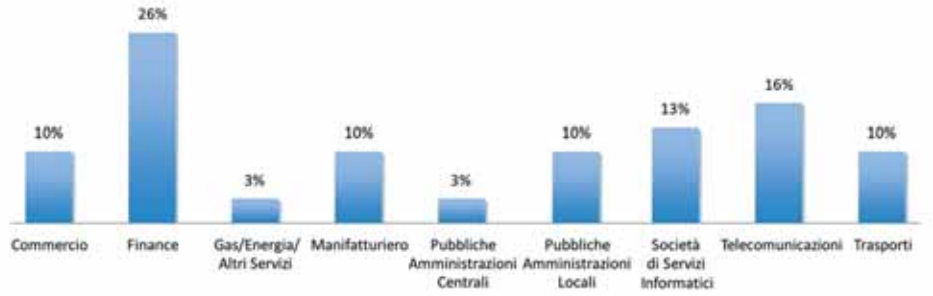
Campione utenti suddiviso per n° addetti



Campione utenti suddiviso per fatturato

Settore di attività

Campione utenti suddiviso per settore di attività



Questa sezione del Rapporto 2013 è dedicata all'approfondimento di alcune 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:

- Mobile Security;
- Social Media Security;
- Cloud Security;
- Sicurezza in Sanità;
- E-Commerce;
- Il protocollo IPv6;
- Il salvataggio delle informazioni e la continuità di servizio.

I primi tre argomenti erano già stati trattati nel Rapporto Clusit 2012, ma si tratta di tematiche sempre di grande attualità e in continuo sviluppo, e necessitavano quindi di un aggiornamento.
La Sanità è uno dei temi centrali dell'Agenda Digitale Europea e Italiana, e per il settore sanitario e in particolare quello ospedaliero, la sicurezza delle informazioni è un'esigenza imprescindibile.
L'e-Commerce è un altro punto fondamentale dell'Agenda Digitale, e potrebbe contribuire in modo significativo alla crescita del PIL; la sicurezza e l'affidabilità delle transazioni sono fattori indispensabili per il suo sviluppo.
Completano i Focus On del Rapporto 2013: cosa cambia, col passaggio al nuovo protocollo IPv6; una serie di riflessioni utili per un corretto salvataggio delle informazioni e la continuità operativa.

Mobile Security

a cura di *Antonio Ieranò*

Dove eravamo rimasti?

Nel Rapporto Clusit 2012 avevamo presentato il 2011 come un anno di transizione dove il Mobile Computing e le relative problematiche di sicurezza stavano emergendo. Le previsioni fatte in quella sede, puntualmente avveratesi, prevedevano, dati i trend, un ulteriore aggravarsi della situazione.

Purtroppo la cronica mancanza di statistiche ufficiali inerenti la sicurezza informatica nel nostro paese ci aveva obbligato a derivare lo status effettivo della sicurezza attraverso una analisi "indiretta".

Rispetto all'anno precedente, il 2012 ha visto crescere consapevolezza nei confronti delle problematiche di Mobile Security e una maggiore offerta in termini di soluzioni e prodotti. Appaiono finalmente anche le prime statistiche di efficacia dei prodotti di sicurezza per mobile (si veda in merito la tabella AVTest presentata più avanti) ma manca ancora una produzione significativa di statistiche italiane sugli incidenti di sicurezza e il mondo mobile in particolare è ancora terra vergine.

Quest'anno, nel fare il punto sullo status della Mobile Security negli ultimi 12 mesi, cercherò di rappresentare un modello di analisi dello stato di esposizione dei rischi basato sull'uso e distribuzione di questi strumenti mobili per poter essere usato come baseline per pianificare correttamente investimenti e risorse sulla sicurezza.

Il 2012 in numeri

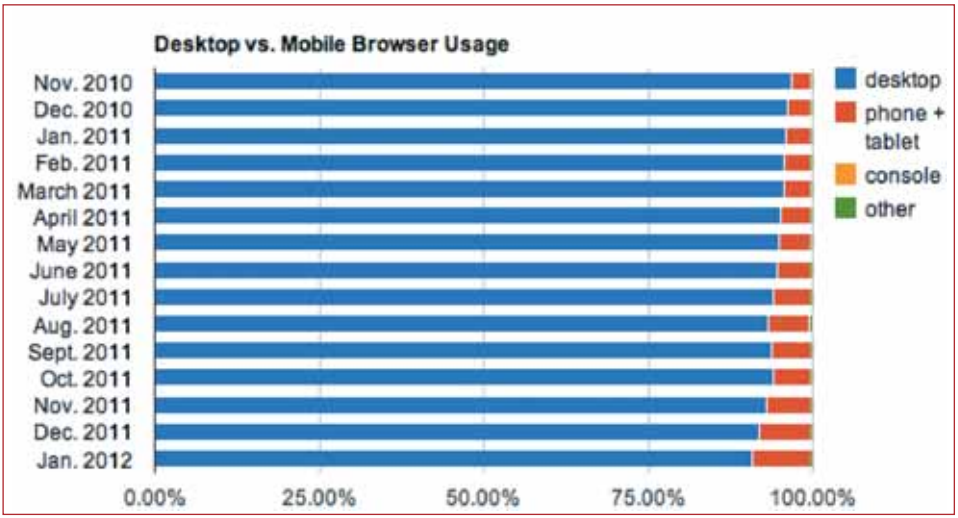
L'anno appena passato è stato segnato principalmente dalla crisi economica che ha pesantemente impattato sugli investimenti delle aziende nella security, e la mobile security non ha mostrato un comportamento diverso.

ANDAMENTO MERCATO ICT IN ITALIA – Risultati III trimestre

	IIIQ 2011		IIIQ 2012	
	Spesa End User	Variazione su anno precedente	Spesa End User	Variazione su anno precedente
	Milioni di Euro	%	Milioni di Euro	%
Hardware	1.493,6	-8,6%	1.429,0	-4,3%
Software	840,0	0,5%	844,1	0,5%
Servizi di sviluppo	977,5	-1,4%	952,3	-2,6%
Servizi di gestione	1.249,8	-3,7%	1.209,8	-2,8%
Totale IT	**4.560,9**	**-4,1%**	**4.435,2**	**-2,8%**
TLC fissa	3.918,7	-4,6%	3.756,5	-4,1%
TLC mobile	5.411,1	-1,6%	5.318,3	-1,7%
Totale TLC	**9.329,8**	**-2,9%**	**9.074,8**	**-2,7%**
Totale ICT	**13.890,7**	**-3,3%**	**13.510,0**	**-2,7%**

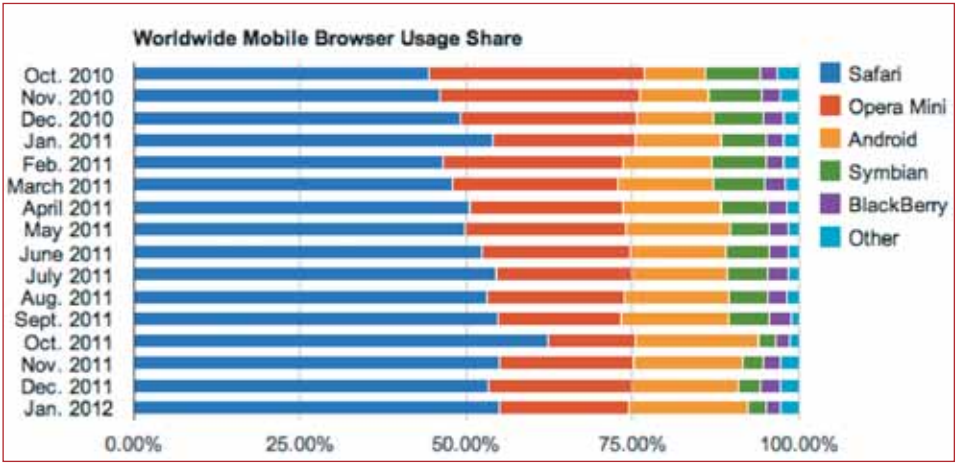
Fonte: SIRMI SPA – Ottobre 2012

Le predizioni di aumento di uso e di rischi fatte nel 2011 sono state fondamentalmente rispettate, e a livello worldwide la presenza di device mobili è in costante aumento, ad esempio se si guardano le statistiche di uso dei browser si evince come le versioni mobile stiano guadagnando terreno a fronte di un calo di quelle desktop.



Net Applications' statistics show the increasing use of tablets and phones for Web browsing.
(Credit: Net Applications)
From <http://news.cnet.com/8301-30685_3-57369393-264/ie-fends-off-rivals-but-absent-from-mobile-battlefield/>

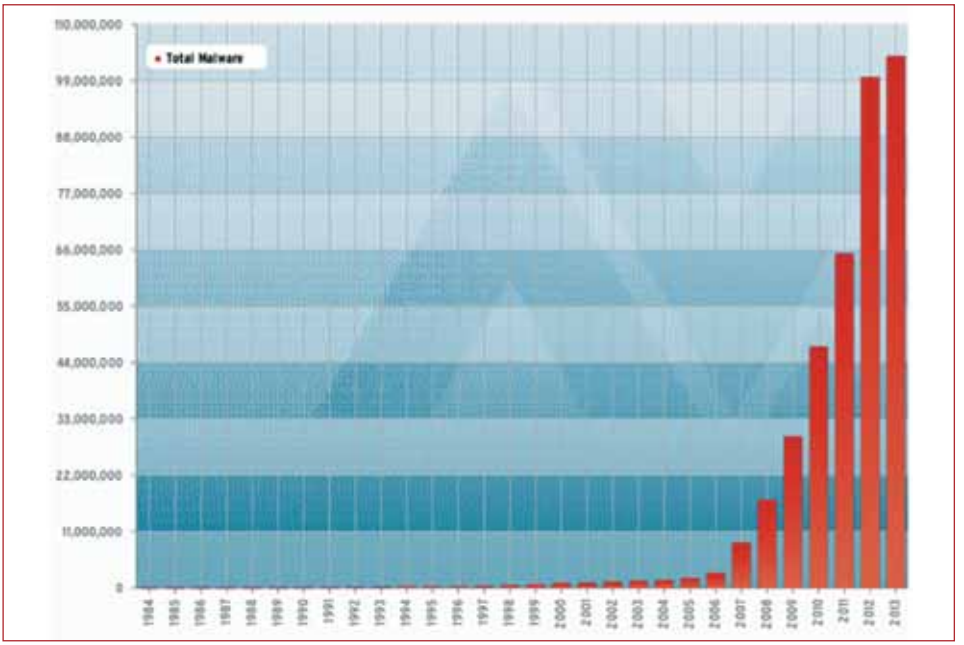
E se poi guardiamo direttamente alle versioni mobile dei browser si vede come il mercato sia chiaramente orientato.



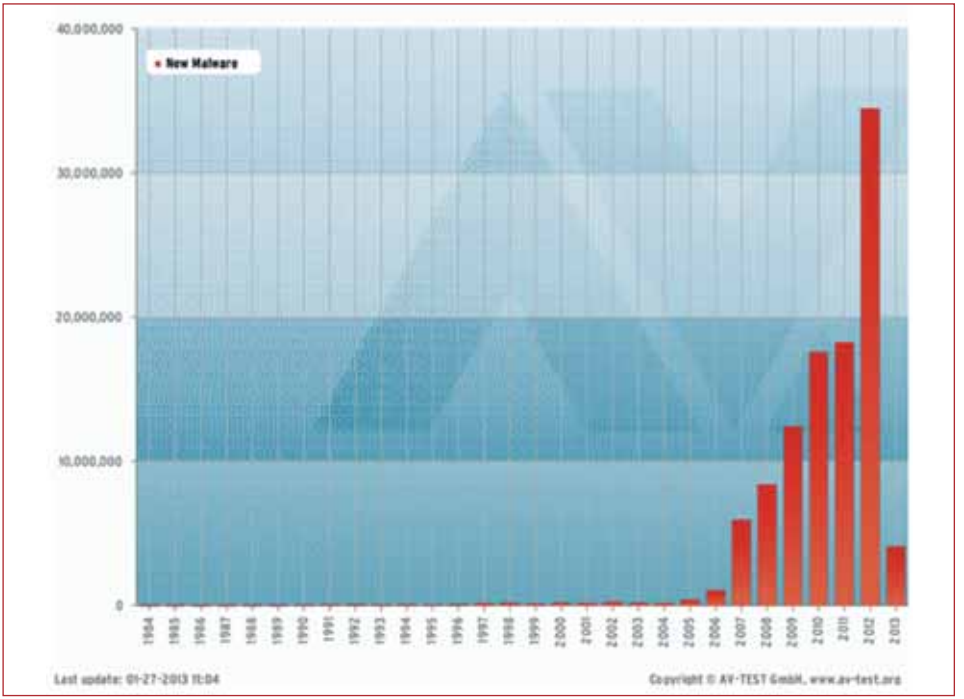
Net Applications' statistics for browser usage on mobile devices.
(Credit: Net Applications)
From <http://news.cnet.com/8301-30685_3-57369393-264/ie-fends-off-rivals-but-absent-from-mobile-battlefield/>

Queste statistiche sono destinate a spostarsi sempre più sul lato Mobile visto il successo e la penetrazione dei nuovi tablet che introducono anche nuovi browser (si pensi a chrome per android o explorer 10 per la piattaforma windows 8)

A fronte di una certa immobilità in termini di investimenti di protezione, vi sono stati trend in crescita in termini di uso, penetrazione ed aumento dei rischi legati all'uso di device mobili capaci di navigare su internet, basta vedere, ad esempio, le statistiche inerenti la crescita di malware (fonte AV test)

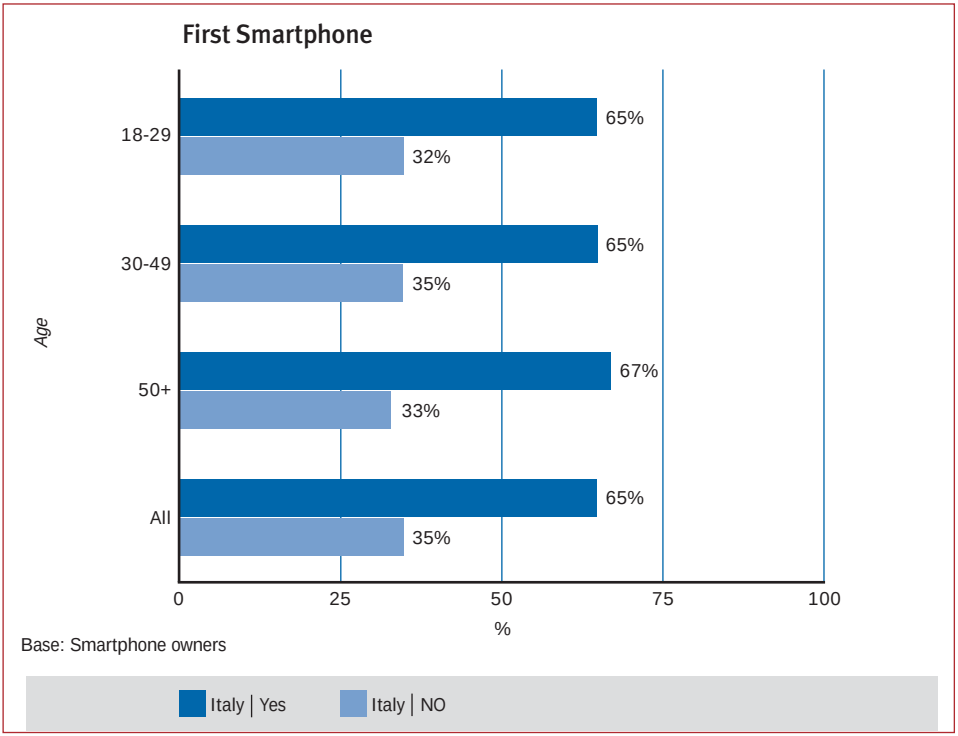


E i nuovi malware:



Si noti come il 2012 abbia rappresentato una impennata impressionate sia in termini di volumi che di novità, e come il 2013 ne stia ricalcando le orme.

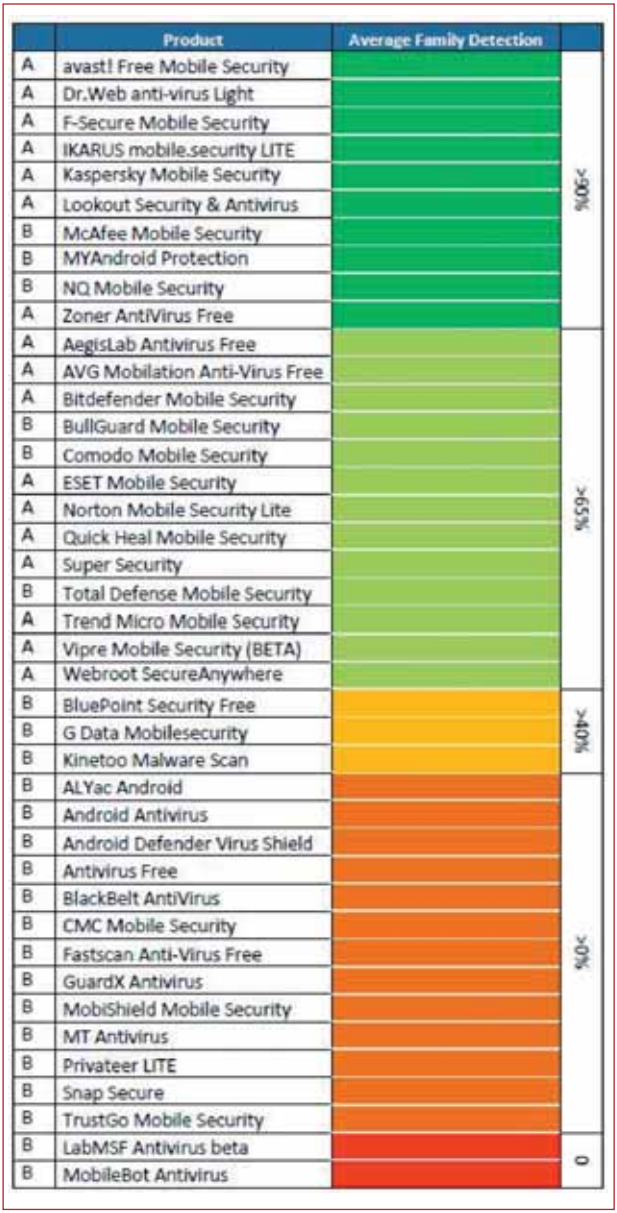
Ed in Italia?
Nello specifico italiano abbiamo una forte crescita nell'uso di smart device:



Il 55% degli utenti di smart device ha acquistato il primo telefono\tablet nel 2012, un tasso di crescita impressionante, se consideriamo anche il periodo di crisi economica.

Dal fronte dei vendor è aumentata l'offerta, concentrando l'interesse principalmente su tre aree:

- La mobile security intesa come introduzione di software antivirus\anti-malware sul device, su cui l'offerta è in costante crescita, basta vedere le statistiche avtest in merito per farsi una idea.



	Product	Average Family Detection	
A	avast! Free Mobile Security		>90%
A	Dr.Web anti-virus Light		
A	F-Secure Mobile Security		
A	IKARUS mobile.security LITE		
A	Kaspersky Mobile Security		
A	Lookout Security & Antivirus		
B	McAfee Mobile Security		
B	MYAndroid Protection		
B	NQ Mobile Security		
A	Zoner AntiVirus Free		
A	AegisLab Antivirus Free		>65%
A	AVG Mobilation Anti-Virus Free		
A	Bitdefender Mobile Security		
B	BullGuard Mobile Security		
B	Comodo Mobile Security		
A	ESET Mobile Security		
A	Norton Mobile Security Lite		
A	Quick Heal Mobile Security		
A	Super Security		
B	Total Defense Mobile Security		
A	Trend Micro Mobile Security		
A	Vipre Mobile Security (BETA)		
A	Webroot SecureAnywhere		
B	BluePoint Security Free		>10%
B	G Data Mobilesecurity		
B	Kinetoo Malware Scan		
B	ALYac Android		>0%
B	Android Antivirus		
B	Android Defender Virus Shield		
B	Antivirus Free		
B	BlackBelt AntiVirus		
B	CMC Mobile Security		
B	Fastscan Anti-Virus Free		
B	GuardX Antivirus		
B	MobiShield Mobile Security		
B	MT Antivirus		
B	Privateer LITE		
B	Snap Secure		
B	TrustGo Mobile Security		
B	LabMSF Antivirus beta		0
B	MobileBot Antivirus		

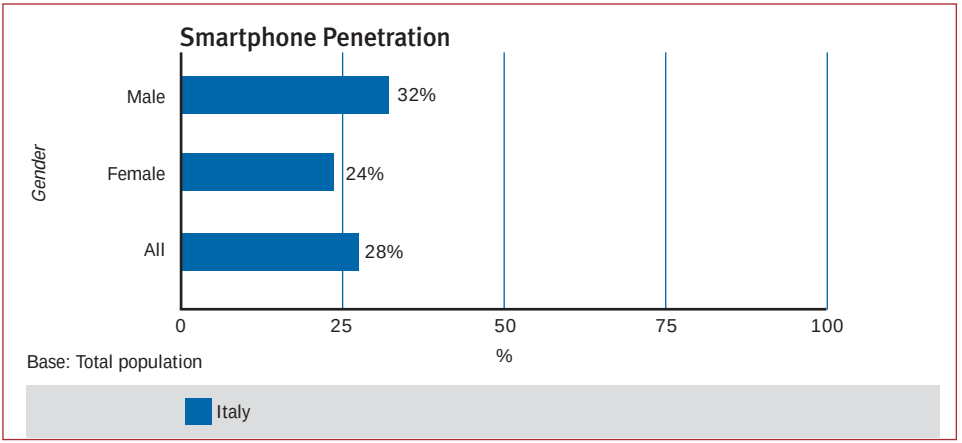
- Il management di device mobili con diverse soluzioni del tipo BYOD che affrontano la questione sotto diversi aspetti: dall'approccio network centrico di Cisco ISE alla piattaforma di gestione mobile multiplatform di MobileIron.

- Un focus su DLP e content analisys di ciò che viene visitato\trasmesso con questi device come ad esempio la soluzione Websense® TRITON™ Mobile Security.

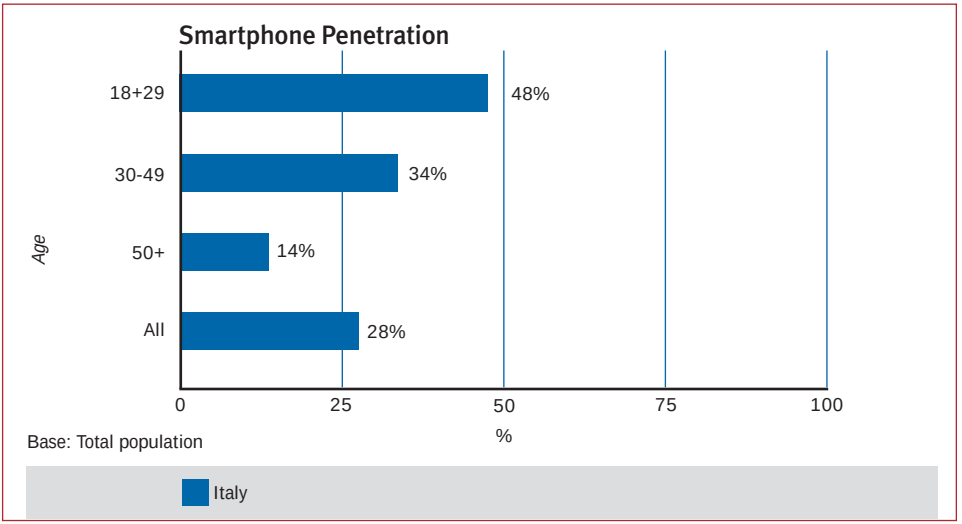
Distribuzione Italiana di smart device

Vediamo quindi come si è evoluto il parco degli utenti mobile in Italia con alcune statistiche di uso su cui è possibile fare considerazioni importanti inerenti la mobile security:

Dalle statistiche (sorgente dati: http://www.thinkwithgoogle.com/mobileplanet) troviamo che la penetrazione di smarthphone e tablet sulla base totale della popolazione è oramai del 28% con una sensibile differenziazione tra uomini e donne.



Se analizziamo questa ripartizione in termini di fasce di età notiamo come questa presenza sia significativa nelle fasce lavorative, e che abbia una distribuzione abbastanza importante anche in quelle fasce di età (over 50) dove vi è una maggiore presenza di senior Manager.



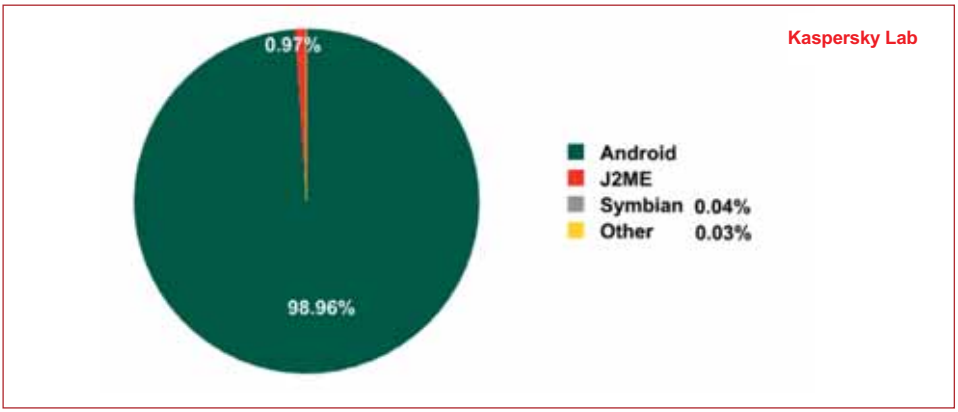
Questa indicazione è concorde con le analisi degli anni precedenti (vedi Rapporto Clusit 2012) dove l'uso di "Smart Device" da parte del management aveva forzato l'introduzione in azienda delle problematiche di mobile security.

Oramai la presenza di questi device è pervasiva in tutte le fasce lavorative, comportando un maggiore impatto aziendale nei confronti della sicurezza.

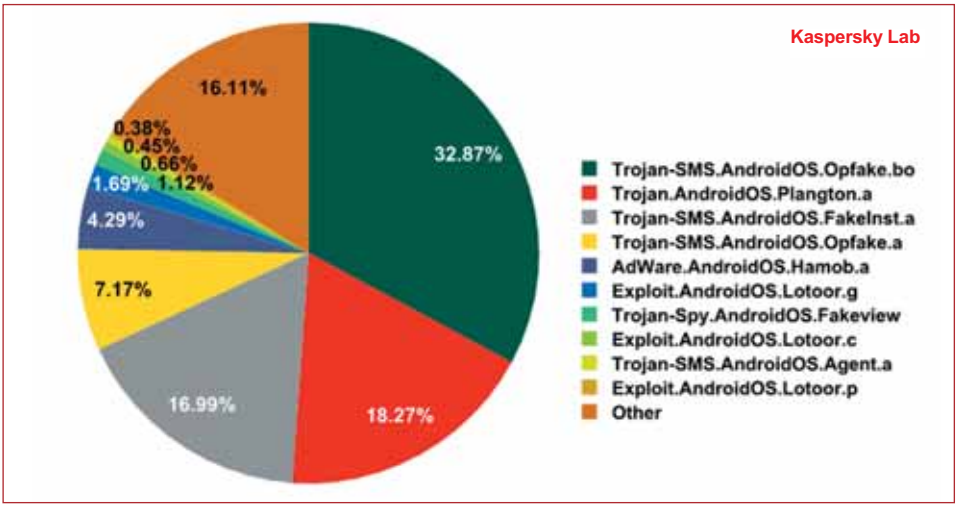
Il Mobile Malware nel 2012

In termini di uso è interessante notare come vi sia una relazione diretta tra le statistiche di distribuzione di virus e malware sulle diverse piattaforme mobili e la distribuzione dei device sulla popolazione:

Secondo le analisi (fonte Kaspersky) il vincitore del poco ambito premio di piattaforma più colpita è stato Android:



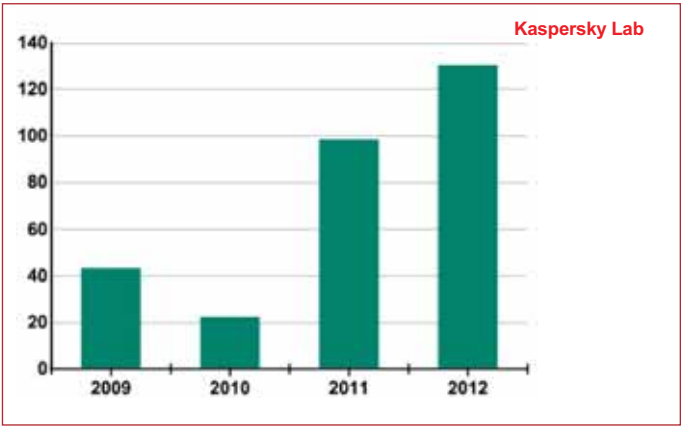
Con una certa prevalenza di trojan su altri attacchi:



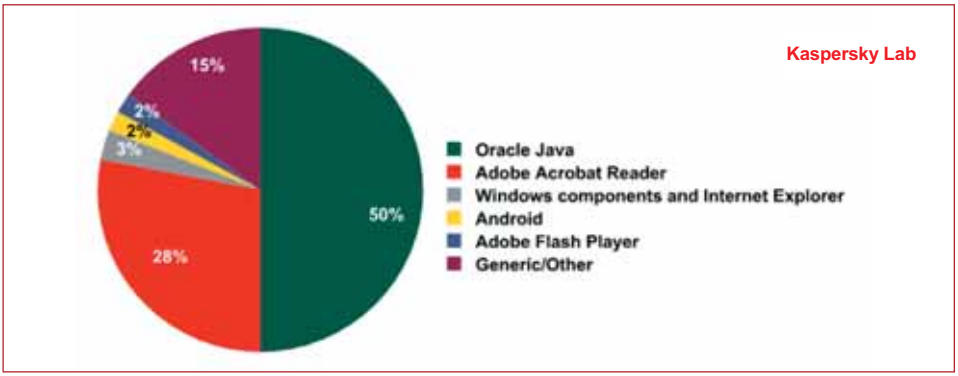
La cosa non dovrebbe essere una sorpresa dato il grande successo della piattaforma di Google che ha, oramai, largamente superato quella di Apple in termini di diffusione. Da un punto di vista tecnico questo sensibile maggior attacco su Android è dovuto proprio alla sua diffusione piuttosto che a "debolezze" intrinseche della piattaforma.

Ma Android non è stato l'unico target, attacchi del tipo Zeus in the Mobile o SpyEye in the mobile (ZitMo e SpitMo) si sono presentati anche sulle altre piattaforme.
Nella immagine vediamo due classici esempi di interfacce di applicazioni infette ZitMo e Spitmo

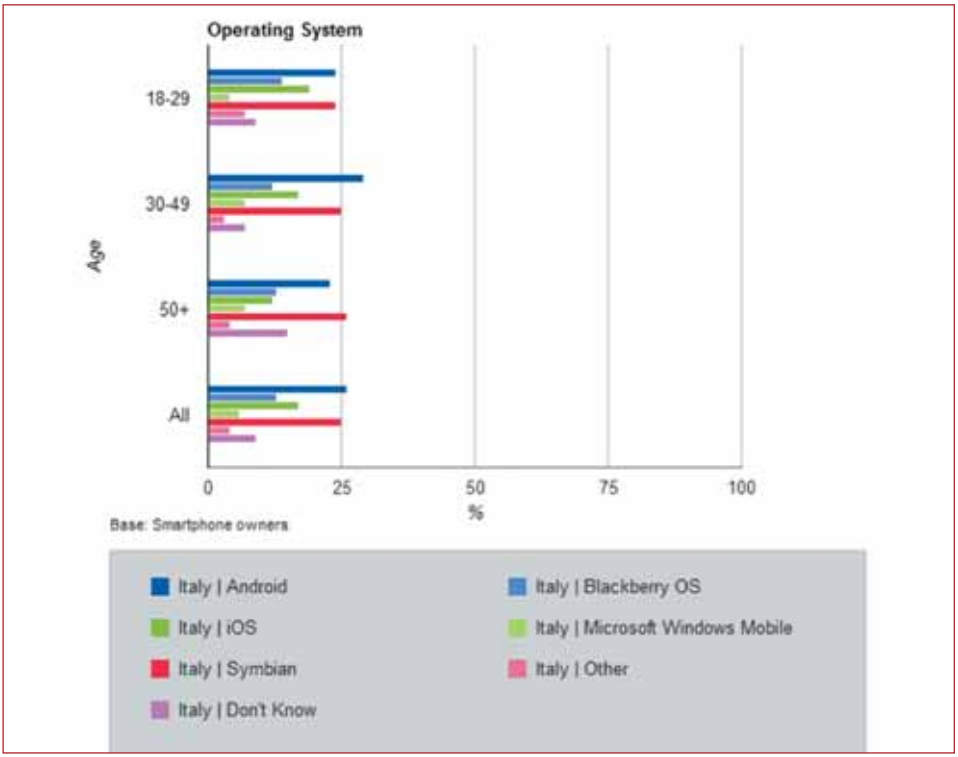
Anche Apple ha visto una crescita di attacchi sulla sua piattaforma mobile. Per averne una idea basta guardare, ad esempio, il numero di nuove signature dedicate da Kaspersky alla piattaforme della casa della mela:



Come poi non dimenticare gli attacchi sviluppati per Java, che è trasversale a quasi tutte le piattaforme mobile e non e che ha totalizzato un buon 50% di tutti gli attacchi registrati:



Relazioniamo questi dati alla distribuzione italiana di OS che vediamo di seguito (sorgente dati: http://www.thinkwithgoogle.com/mobileplanet):

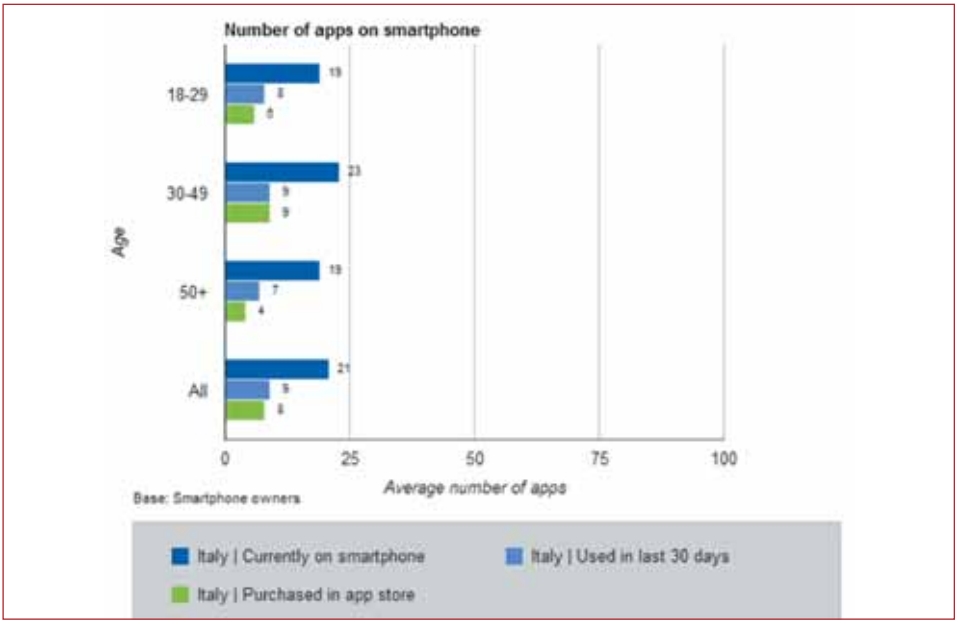


Risulta chiaro come anche in italia Android sia una presenza importante (in media leggermente superiore al 25%), maggiore in termini numerici di

Apple, ma come vi sia ancora una pesante presenza di altri sistemi più "tradizionali".
Questa distribuzione comporta qualche problema in termini di gestione della sicurezza dei device aziendali (BYOD) in quanto, quando sono presenti sistemi di gestione dei device mobili, le aziende sono ancora ancorate a meccanismi proprietari (si pensi, ad esempio, alla soluzione RIM).

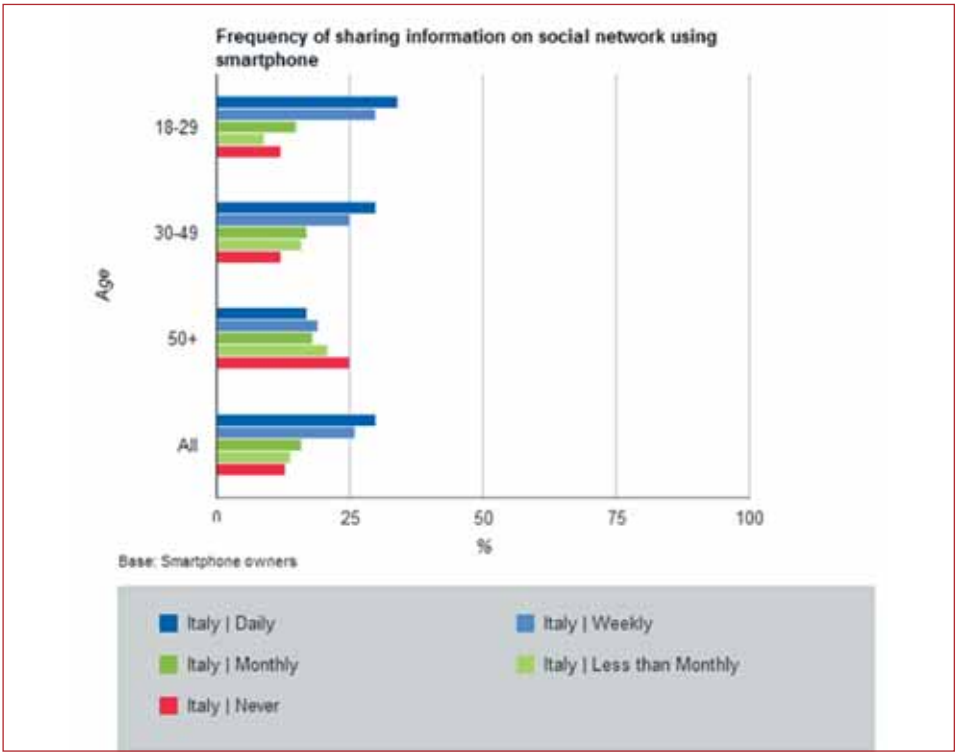
Lo spostamento verso soluzioni "Multivendor" è ancora lento, anche se il mercato inizia ad offrire un vasto parco di prodotti.
Curiosamente mentre Android dilaga alcuni vendor affrontano prima il mondo Apple. Del resto la piattaforma Apple è stata la prima a sfondare le barriere aziendali con soluzioni "smart" e da questo punto di vista rimane la grande incognita di che successo avranno i device windows 8 che riuniscono telefonia, tablet e pc in un solo ambiente di sviluppo.

Uso degli Smart Device
Dalle analisi risulta chiaro che l'uso che si fa dei device mobili e le applicazioni che si scaricano sono punti focali di attacco di malware o hacking. Vediamo quindi la fotografia della situazione Italiana del 2012:



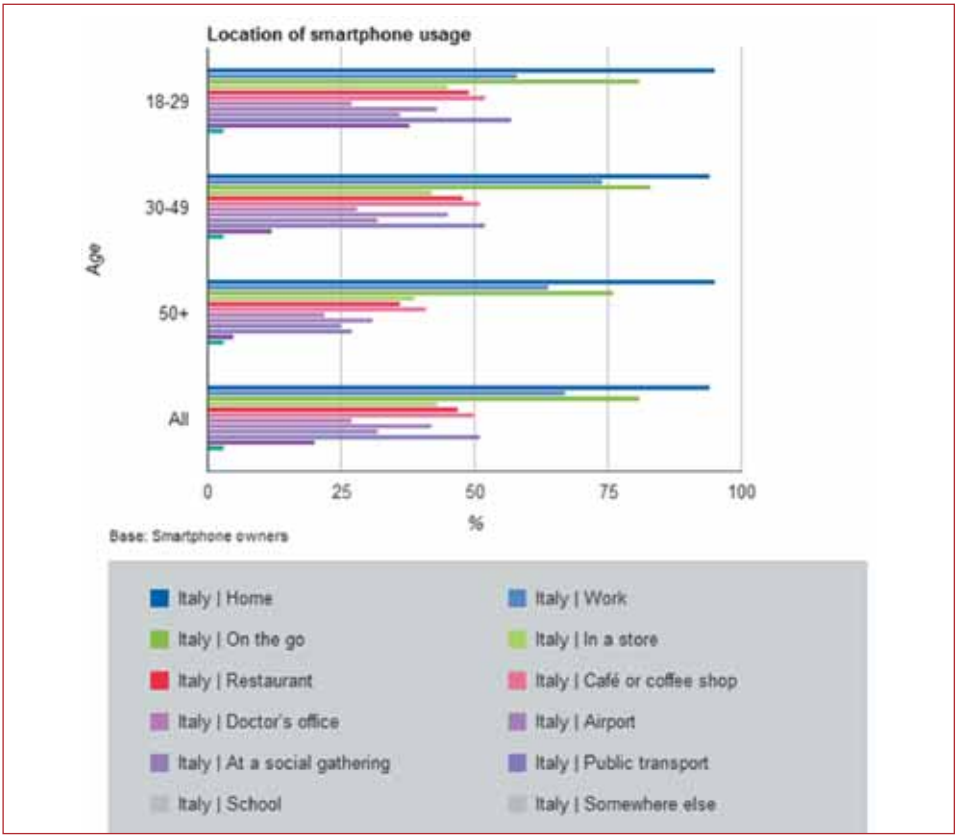
Senza sensibili differenze tra le varie fasce di età, risulta chiaro come il numero di applicazioni scaricate è abbastanza alto. Va poi considerato che la maggior parte di queste applicazioni (particolarmente sulla piattaforma "android") è di tipo gratuito, cosa che espone a maggiori rischi di sicurezza. Il rapporto tra le applicazioni comprate e scaricate gratuitamente in Italia è circa di 1 a 3.

Anche l'uso di social engineering attraverso i social network o il deployment di applicazioni "infette" risulta particolarmente fruttuoso negli smart device per almeno due motivi: la poca diffusione di strumenti di difesa a bordo del device e la maggiore disattenzione degli utenti nei confronti di questi strumenti.



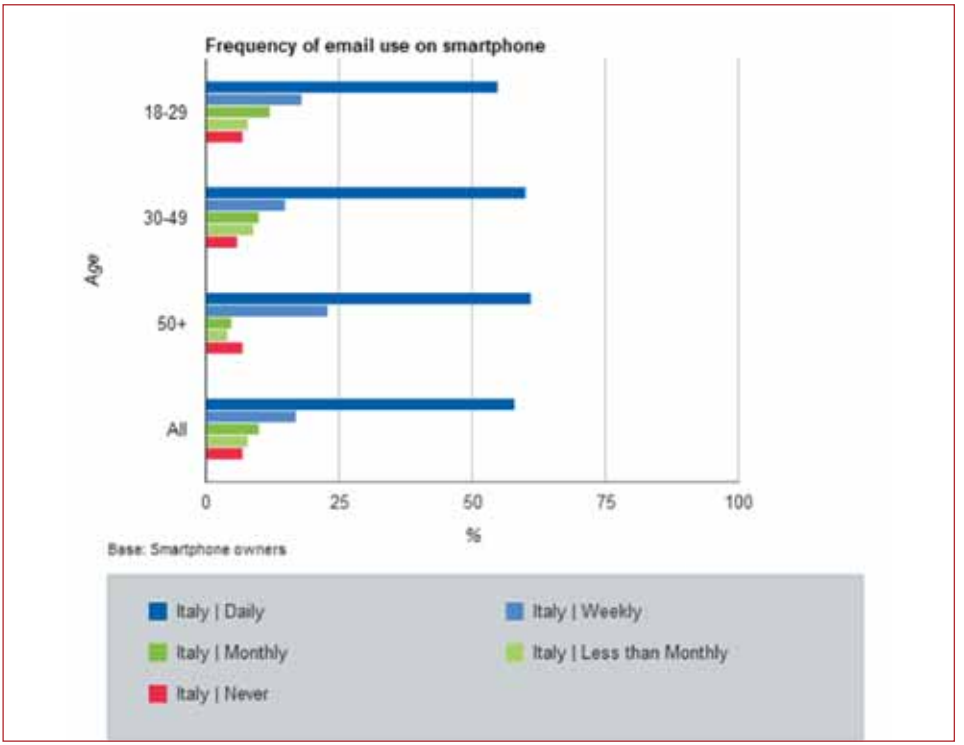
L'uso giornaliero di social media è abbastanza omogeneo in tutte le fasce di età e supera il 25%.
Lo schermo di dimensioni minori, l'uso promiscuo (personale e lavorati-

vo), e le diverse attività e luoghi ove si possono usare questi strumenti aumenta sensibilmente la superficie di attacco in termini di sicurezza.



Possiamo notare come l'accesso italiano presenti una altissima percentuale (>60%) di utenti che utilizzano lo smarthphone sia a casa che al lavoro e, se incrociamo questi dati con le statistiche di scambio di informazioni sui social network, risulta evidente come vi sia una pesante esposizione in Italia a rischi di Social Engineering e perdita di dati.

Un altro elemento evidente di questo rischio espositivo è l'uso di questi device per accedere alla posta elettronica. Il 60% degli utenti accede alla propria posta giornalmente da tablet e smarthphone utilizzando quindi un ambiente virtualmente non protetto.



Accedere alla posta da questi device comporta oggettive maggiori difficoltà nel riconoscere, ad esempio, phishing o target attaks. Solo per fare un esempio: quanti leggono gli header di una mail ricevuta sul telefono?

Estensione della superficie di attacco italiana

Dai dati presentati risulta evidente come la superficie di attacco, intesa come l'insieme delle situazioni che possono generare rischi in termini di sicurezza, si sia drammaticamente allargata sul mercato italiano, senza che vi sia stata una equivalente presa di coscienza da parte dei gestori IT, in parte per mancanza di visione tattica e strategica, in parte per la pesante riduzione degli investimenti dovuta al momento congiunturale economico.

Le ragioni di questo allargamento risiedono nell'impressionane aumento dell'uso di smart device e del loro uso promisquo ed ubiquo ed in una certa inerzia degli utilizzatori.

Pensieri finali

Concludendo si può dire che anche il 2012 sia stato, dal punto di vista della Mobile Security, un Annus Horribilis e che a fronte di una crescente esposizione non vi è stata una coerente copertura da parte delle aziende. Purtroppo le basi non sono positive neanche per il 2013 ed è facile aspettarsi un ulteriore allargamento della forbice tra ciò che occorrerebbe implementare per ridurre la superficie di esposizione ai rischi e gli investimenti di sicurezza.

Social Media Security

a cura di *Andrea Zapparoli Manzoni*

I Social Media sono uno dei temi emergenti anche in ambito Security. Nella edizione precedente del Rapporto (2012) avevamo già affrontato questo tema, focalizzandoci sulle quattro dimensioni fondamentali del problema, dimensioni che rimangono a tuttora di rilevante interesse:

1. I Social Networks sono intrinsecamente basati su un (prevalentemente infondato) senso di fiducia tra i propri membri;
2. I metodi di autenticazione sono carenti e l'identità degli utenti non è accertabile (né accertata);
3. Gli attacchi sono condotti per lo più a livello semantico, tramite tecniche di social engineering e messaggi ingannevoli, ben al di là delle possibilità di rilevamento da parte delle difese tradizionali;
4. La diffusione di smart phones personali e la crescente tendenza verso la consumerization dell'IT aziendale a causa del fenomeno del BYOD (che implica un dual use di questi terminali), unita al fatto che ormai il 50% delle connessioni ai Social Network avviene tramite mobile, rende le difese tradizionali inapplicabili, o le vanifica sostanzialmente.

Di conseguenza al giorno d'oggi un'organizzazione che utilizzi i Social Networks sia verso l'esterno che, a maggior ragione, al proprio interno, si espone immediatamente ed inevitabilmente ad un ampio spettro di rischi in termini di reputazione e di responsabilità verso terzi (altri utenti, clienti e partner), ad attività di Open Source Intelligence da parte di competitors e malintenzionati (per esempio spammers e cybercriminali), oltre a rischiare la perdita di dati sensibili (ai sensi della normativa sulla privacy, o di business), di credenziali di accesso (per esempio bancarie, o della posta elettronica)[1] e naturalmente la compromissione (hijacking) dei propri account sui social network[2], se non dei propri sistemi informatici.

Oggi non esiste un ambito nel quale da un lato le attività malevole abbiano maggiore probabilità di successo ed i rischi siano minori per i malintenzionati, e dall'altro gli errori umani possano propagarsi con maggiore velocità, dei Social Network.

[1] http://www.infosecisland.com/blogview/8592-Social-Media-is-a-Criminals-Playground.html

[2] http://news.cnet.com/8301-27080_3-20104165-245/nbc-news-twitter-account-hacked/

Nel corso del 2012 questo insieme di concause ha determinato un aumento significativo degli incidenti avvenuti a causa dell'utilizzo (o del non utilizzo, che genera furti di identità) dei Social Network, a fronte del fatto che non sono stati mitigati in modo adeguato i rischi, e che contestualmente le minacce (in base al nostro campione di incidenti) sono aumentate del 900% in un anno.
Ciò nonostante ancora oggi dobbiamo constatare che i progetti aziendali orientati all'utilizzo dei Social Media (anche di grandi aziende) sono guidati e gestiti esclusivamente dalle funzioni di business e dal marketing, mentre il coinvolgimento dei sistemi informativi rimane minimo, e la sicurezza non viene ancora chiamata in causa per svolgere quelle attività sistematiche di prevenzione che, come è facilmente comprensibile, sono molto più efficaci di quelle reattive post incidente (anche per la mancanza cronica di competenze in materia di Crisis Management, disciplina praticamente sconosciuta nel nostro Paese).

2012: L'anno dell'affermazione globale dei Social Network

A livello globale, il 2012 è stato l'anno dell'affermazione dei Social Network quali piattaforme privilegiate di diffusione e scambio di informazioni via Internet (a qualsiasi titolo e per qualsiasi finalità) non solo per miliardi di persone, ma anche per molti milioni di imprese, enti ed Istituzioni.
È stato l'anno in cui, in ogni pubblicità, è comparsa la frase "seguici su Facebook", ed anche quello che ha visto Twitter diventare un punto di riferimento (a torto o a ragione) per tastare il polso agli umori ed alle tendenze di pensiero della gente, in ogni ambito. La stessa campagna elettorale in corso in questi giorni è ormai svolta in parte tramite i Social Network, con tutte le conseguenze del caso[3].
Oltre ad essere diventati un punto di riferimento universale, i Social Network nel loro complesso sono ulteriormente cresciuti, sia in termini di utenza che per quanto riguarda il numero delle piattaforme disponibili.
Tra i Social Network generalisti Facebook ha raggiunto il miliardo di profili (corrispondenti a circa 800 milioni di utenti reali, escludendo i profili fake ed i bot[4]), Google+ è cresciuto a sua volta, LinkedIn e Twitter hanno

[3] http://social.cybion.it/elezioni-2013-monitorare-i-social-media/
[4] http://sm-and-s.org/?p=167

superato i 200 milioni di iscritti nel mondo, e tra gli utenti di questi Social Network figurano circa l'80% degli utenti abituali di internet del nostro Paese, ovvero oltre 22 milioni di italiani.
Si sono anche affermati nuovi modelli di Social Networking, da Pinterest a Tumblr, da Badoo (che in Italia è la seconda piattaforma più utilizzata[5]) a Last.fm, ciascuno deputato a "coprire" una specifica nicchia ecologica all'interno di un panorama in continua espansione, all'interno del quale gli utenti ormai trascorrono 1 minuto ogni 3 di navigazione Internet.
Questa prepotente affermazione però non ha coinciso con una presa di coscienza da parte degli utenti, né con l'adozione di particolari forme di protezione da parte delle piattaforme Social (per esempio, applicando sistemi di autenticazione forte all'accesso, o monitorando i propri network per bloccare le minacce alla fonte[6]).
Nel corso dell'anno le stesse piattaforme Social sono state vittime di importanti attacchi, che hanno causato il furto delle credenziali di milioni di utenti.
L'unione di questi due macro-trend ha posto le basi per un aumento impressionante di incidenti.

L'insostenibile leggerezza dei Social Network

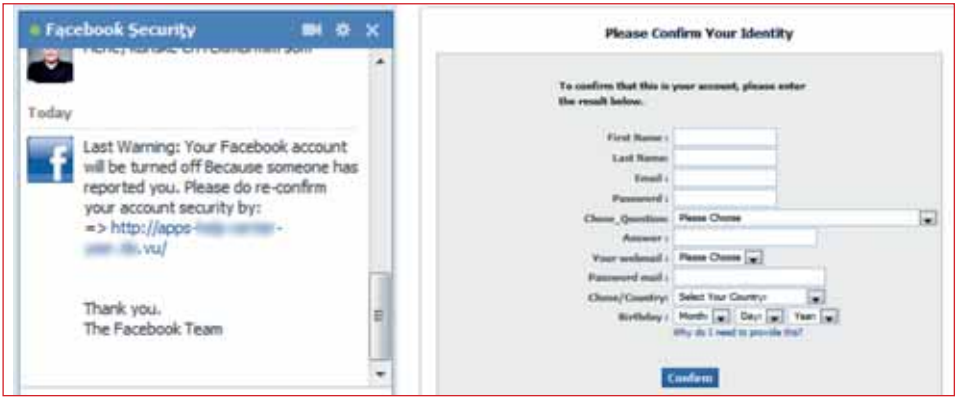
Nonostante questo tumultuoso sviluppo i Social Network continuano ad essere utilizzati in modo superficiale da tutte le tipologie di utenti, dal top manager al politico, dalle agenzie di comunicazione ai media, dagli utenti finali alle imprese ed alle istituzioni, indifferentemente.
Gli utenti sembrano non preoccuparsi delle possibili conseguenze in termini di perdita di dati personali, stalking, cyber bullismo, furti di identità, frodi di ogni genere, spionaggio ed attacchi da parte di cyber criminali, nonostante nel nostro Paese nel 2012 il 40% degli utenti adulti di Internet siano stati raggiunti da qualche forma di minaccia informatica[7], circa la metà delle quali veicolate tramite Social Network.
In particolare risulta incomprensibile l'atteggiamento di molti genitori, che consentono ai propri figli minorenni, spesso anche minori di 14 anni,

5 http://vincos.it/world-map-of-social-networks/
6 http://www.forbes.com/sites/jodywestby/2012/03/14/social-media-companies-contribute-to-cybercrime/
7 http://www.symantec.com/it/it/about/news/release/article.jsp?prid=20121004_01

di trascorrere quotidianamente ore sui Social Network[8], esponendosi ad ogni sorta di minaccia con la più totale mancanza di consapevolezza.
Allo stesso modo desta preoccupazione l'adozione spesso improvvisata dei Social Network da parte delle nostre PMI e di molte Pubbliche Amministrazioni, che si espongono a gravi rischi di compromissione dei propri sistemi e di furto di dati sensibili lanciandosi senza protezioni di sorta in quella che è diventata una vera e propria "jungla" digitale.

Infine, la mancanza di linee guida e di normative specifiche lascia margini di discrezionalità troppo vasti e non supporta chi si occupa di Social Business Security, dato che la mancanza di oneri specifici porta molte organizzazioni a sottovalutare i rischi, assumendo un atteggiamento attendista che aumenta in modo eccessivo l'esposizione ai rischi.
Purtroppo è sufficiente ricevere un'email di questo tipo, e cliccare sul contenuto, per essere compromessi da malware quali Citadel[9], Zeroaccess[10], o Black Hole[11] e diventare vittime di ogni genere di abusi.
Allo stesso modo, ciascun link pubblicato sulla bacheca di Facebook (o in un Tweet) da un presunto "amico" può condurre allo stesso risultato.

8 www.datamanager.it/news/indagine-eu-kids-online-cosa-fanno-i-nostri-bambini-online-44020.html
9 http://www.darkreading.com/threat-intelligence/167901121/security/attacks-breaches/240009308/citadel-trojan-gets-more-customer-friendly.html
10 http://nakedsecurity.sophos.com/zeroaccess2/
11 http://en.wikipedia.org/wiki/Blackhole_exploit_kit



Quando si legge che lo spam tradizionale nel 2012 è diminuito[12] di oltre il 50%, bisogna ricordare che non è scomparso, ha solo cambiato modalità di diffusione migrando sui Social Network, tramite i quali vengono inviati miliardi di messaggi malevoli come quelli riportati, in molte centinaia di varianti (spesso sfruttando l'attualità[13]), che colpiscono milioni di persone ogni giorno[14].

Scenari futuri e possibili contromisure

In base ai dati raccolti dalla recente ricerca "Social Media Effectiveness Use Assessment" svolta da SNID del Politecnico di Milano[15], in Italia la penetrazione dei Social Network in ambito aziendale è circa del 50% (con punte del 70% in alcune aree geografiche come la Lombardia), ed è destinata ad aumentare ulteriormente nel corso di quest'anno.

Gli scenari futuri, in un mondo nel quale si scambieranno 134 exabyte di dati via Internet entro il 2017[16] (134 volte il volume di traffico IP fisso o mobile che esisteva nel 2000), principalmente tramite device mobili, costantemente connessi ad alta velocità ad Internet ed in particolare ai sempre più numerosi Social Network ed a piattaforme Cloud, sono affascinanti e preoccupanti al tempo stesso.

---

12 http://www.datamanager.it/news/spam-diminuzione-siamo-tornati-5-anni-fa-43649.html

13 http://www.scmagazine.com/spam-floods-twitter-after-pope-resigns/article/280118/

14 http://www.securelist.com/en/blog/208193325/Facebook_Security_Phishing_Attack_In_The_Wild

15 http://www.slideshare.net/AndreaAlbanese/risultati-ricerca-ssocial-media-effectiveness-use-assessment-snid-20112012

16 http://www.repubblica.it/tecnologia/2013/02/17/news/2017_pi_connessioni_che_persone-52858092/?rss

Due miliardi di persone saranno collegate ai Social tramite "app" in esecuzione sui loro smartphone e tablets, e scambieranno trilioni di immagini, messaggi e video per lavoro ed a fini ricreativi. Se i trend attuali non saranno in qualche modo invertiti, tutto questo sviluppo porterà inevitabilmente ad un ulteriore aumento degli incidenti, con conseguenze sempre più gravi. Il malware si sta già adattando per infettare sistemi mobili[17], ed è recente la notizia di una botnet cinese composta da un milione di smartphone[18], che prefigura quello che potrebbe accadere, su scala ancora più vasta, nei prossimi anni.

Risulta dunque di fondamentale importanza adottare un insieme di processi e strumenti di analisi e moderazione in tempo reale della conversazione, di monitoraggio contro gli attacchi basati sul malware, di tutela legale, di formazione continua del personale, di prevenzione delle minacce e di gestione degli incidenti, sia per ottimizzare il ROI dei Social Media che per evitare danni economici o d'immagine (anche importanti e complessi da sanare), o per rimediare ove si siano già verificati. In questo genere di attività i tempi di reazione, data la natura virale ed istantanea dei Social Media, sono fondamentali, e richiedono competenze specifiche e cambiamenti organizzativi mirati, che non si possono improvvisare.

Occorre implementare quanto prima dei processi specifici di Social Business Security, realizzata in un'ottica di Risk Management e di prevenzione, al fine di proteggere gli asset informatici (infrastrutture, dati) e quelli immateriali, non meno importanti (reputazione, brand, proprietà intellettuale), senza dimenticare gli importanti profili di compliance e di tutela legale necessariamente implicati dall'uso dei Social.

Per quanto riguarda gli utenti finali, iniziano ad essere realizzate iniziative di sensibilizzazione (lodevole quella del Garante per la Privacy[19]), ma è necessario fare molto di più, cominciando dalle scuole di ogni grado, per creare il giusto livello di consapevolezza tra i giovani ed i giovanissimi, che sono e sempre più saranno i principali utenti dei Social Network.

---

17 http://thehackernews.com/2012/01/another-malware-from-android-market.html

18 http://ntdtv.org/en/news/china/2013-01-16/over-a-million-chinese-smartphones-infected-with-trojan-horse-malware.html

19 http://www.garanteprivacy.it/connettilatesta

Cloud Security

a cura di *Matteo Cavallini*

Nel corso del 2012 il fenomeno del cloud computing è entrato nella fase di maturità in molti mercati del mondo e ha consolidato le relazioni con altre tendenze dominanti dell'information Technology quali ad esempio il mobile.

Dal punto di vista del mercato, hanno inoltre acquisito una notevole importanza le soluzioni di sicurezza erogate in modalità cloud (Security as a Service - SecaaS), con un marcato incremento della numerosità dei prodotti offerti e delle tipologie di servizi. In questo specifico campo, oltre agli ormai consolidati prodotti per la email security, web security e antivirus, si sono sviluppati consistenti offerte nel campo dell'Identity and Access Management, del SIEM e del Data Loss Prevention. Ciò è anche dovuto al fatto che, a livello dimensionale, i dati prodotti da questi sistemi di sicurezza in termini di log e eventi è in costante aumento e che, di conseguenza, la capacità di governare il fenomeno Big Data è ormai percepita come un abilitatore per riuscire a esprimere delle reali capacità di sicurezza.
È quindi naturale che si sia sviluppato (e che probabilmente continuerà a svilupparsi) uno specifico settore del mercato del cloud dedicato a queste esigenze.

Uno sguardo agli incidenti del 2012

Dal punto di vista dei data breach, i servizi cloud non hanno avuto un'attenzione maggiore rispetto ai servizi erogati o gestiti in modo tradizionale. Gli episodi che si sono verificati sulle grandi cloud pubbliche rientrano nella media e non hanno costituito una particolare fonte di preoccupazione e attenzione da parte dei provider e dei consumer.

Uno degli argomenti caldi per quanto riguarda gli incidenti nel mondo cloud è, invece, rimasto quello legato al tema della disponibilità dei servizi. Le ragioni di tanta attenzione risiedono fondamentalmente nella totale passività in cui sono costretti i Consumer in caso di incidente e nella supposta resilienza intrinseca delle infrastrutture cloud che viene puntualmente smentita ad ogni incidente. Da questo punto di vista, gli incidenti

che più hanno fatto eco sono quelli che hanno colpito Amazon; probabilmente perché Amazon è una grande realtà nel mondo dei Cloud Provider di tipo IaaS e ha clienti tra i principali soggetti del mondo dell'IT. Nel corso del 2012, ci sono state alcune brevi interruzioni nell'erogazione dei servizi erogati da Amazon, soprattutto in alcuni datacenter americani. Queste interruzioni del servizio si sono però riflesse su grandi realtà del calibro di Netflix, Instagram e Pinterest, contribuendo così ad attrarre l'attenzione dei media e sottolineando l'esigenza, anche per i Cloud Consumer di piccolo e medio calibro, di dotarsi di contromisure specifiche a garanzia della continuità del servizio.

Gli Stati Uniti e la Federal Cloud Strategy

Gli Stati Uniti hanno elaborato una complessa strategia per diffondere il cloud computing all'interno delle agenzie federali. Questa strategia si compone di varie componenti tra cui il programma "Federal Risk and Authorization Management Program" (FedRAMP[1]) gestito dalla GSA che è finalizzato ad aumentare l'efficienza e la velocità nell'acquisizione di soluzioni cloud senza comprometterne la sicurezza. La General Service Administration si era imposta di iniziare a rilasciare certificazioni per i Cloud Provider entro la fine del 2012 ma ha incontrato numerose difficoltà che ne hanno rallentato il percorso e complicato l'iter, per cui la prima certificazione è stata emessa soltanto il 26 dicembre! A conferma delle difficoltà di questo percorso, nonostante la vivacità del mercato cloud negli Stati Uniti, a Febbraio 2013 risultano ancora solo 2 certificazioni emesse. Tutto ciò, quindi, mette in mostra quanto sia effettivamente complicato riuscire a realizzare degli approcci che coniughino il mantenimento dell'efficacia ed efficienza dei servizi cloud con la garanzia e la sicurezza richieste dagli enti pubblici e dalle pubbliche amministrazioni.

[1] www.fedramp.gov

Uno sguardo all'Europa

L'attenzione che la Commissione Europea dedica al tema cloud, soprattutto in chiave sicurezza, è ormai ampiamente nota. Il costante impegno della Vice Presidente Kroes su questi temi è fonte di continue iniziative sia a livello europeo sia, a cascata, a livello nazionale. Interessante, da questo punto di vista, la gara che è stata bandita per lo sviluppo di progetti sul tema "Governmental Clouds & Incident Reporting"[2]. Questa gara è stata divisa in due lotti, il primo dei quali si occupa di incident reporting in ambito cloud e punta all'estensione ai Cloud Provider di quanto previsto dall'Articolo 13a (risk assessment, risk treatment e data breach notification) della direttiva sulle telecomunicazioni. Il secondo lotto punta, invece, alla definizione di un insieme di linee guida per rendere più sicure le infrastrutture dei Cloud Provider al fine di facilitare la sottoscrizione di servizi da parte del settore pubblico.

Da segnalare, inoltre, la pubblicazione da parte di ENISA del documento "Procure Secure"[3] che costituisce uno dei primi esempi di guide per il monitoraggio dei livelli di servizio per le componenti di sicurezza nei contratti cloud. In particolare, tra gli altri, vengono ad essere analizzati i seguenti importanti parametri: incident response, conformità tecnica e gestione delle vulnerabilità, isolamento dei dati, gestione dei log e forensic. Un importante contributo, quindi, per consentire il trasferimento sicuro sul cloud anche delle parti "core" delle infrastrutture IT.

La situazione in Italia

A livello italiano, tra le varie iniziative interessanti, vale la pena di sottolineare la pubblicazione, a maggio 2012, delle "Raccomandazioni e proposte sull'utilizzo del cloud computing nella Pubblica Amministrazione"[4] da parte di DigitPA. Questo documento riporta una serie di analisi e considerazioni in merito a: le opportunità e i rischi del cloud nella PA, le condizioni per il successo di una iniziativa cloud e le raccomandazioni in senso stretto. Questo documento è il frutto degli sforzi di un gruppo di lavoro

2 http://www.enisa.europa.eu/procurement/cloud-security-governmental-clouds-incident-reporting

3 http://www.enisa.europa.eu/activities/Resilience-and-CIIP/cloud-computing/procure-secure-a-guide-to-monitoring-of-security-service-levels-in-cloud-contracts

4 http://www.digitpa.gov.it/notizie/uso-del-cloud-computing-nella-pa

molto ampio, costituito dai principali attori nel campo della consulenza e dei player del mondo IT, da diverse Amministrazioni Pubbliche, da alcune aziende statali, da alcune Università e da Istituti di ricerca. Il Gruppo di lavoro è stato coordinato da DigitPA con il contributo, per gli aspetti di sicurezza, di Cloud Security Alliance - EMEA.
Parallelamente alla pubblicazione di questo documento, a livello legislativo, è iniziato un percorso che ha portato a definire gli obiettivi dell'Agenda Digitale Italiana e a costituire l'Agenzia per l'Italia Digitale, con la soppressione di DigitPA. Il cloud, in questo scenario, è visto come un argomento di assoluta centralità, che può svolgere un ruolo di abilitatore anche per altri obiettivi dell'Agenda Digitale Italiana, quali l'uso degli open data, le smart cities e l'e-health. L'Agenzia è, ad inizio 2013, ancora in una fase di start-up e, probabilmente, necessita del varo del prossimo governo per avere la necessaria sponsorship e diventare pienamente operativa. Quando però l'Italia disporrà di questo nuovo strumento per l'innovazione, potrà essere nella condizione di riuscire a colmare il ritardo accumulato nel tempo e realizzare una strategia compiuta che attui l'Agenda Digitale, riuscendo a raggiungere quegli obiettivi che tanto sono richiesti da cittadini, imprese e Pubbliche Amministrazioni italiane per riuscire a mettere in pratica i risparmi e l'efficientamento di cui il Paese ha estremo bisogno.

Infine, a completamento del quadro italiano, è da segnalare che il capitolo italiano di Cloud Security Alliance ha pubblicato un paio di ricerche in ambito cloud, la prima dal titolo "Portabilità, Interoperabilità e Sicurezza Applicativa nel Cloud"[5] svolta in collaborazione con OWASP-Italy e la seconda dal titolo "Standard Contrattuali per il Cloud Computing"[6].

Alcune nuove sfide

Con l'accresciuta maturità dei servizi cloud, si è anche "alzato il tiro" delle possibili applicazioni del cloud computing. Le due maggiori sfide che stanno per essere raccolte in questo campo sono: il cloud nelle applicazioni militari e il cloud per le infrastrutture critiche.

---

5 http://cloudsecurityalliance.it/wp-content/uploads/2012/12/CSA_Italy_Portabilita_Interoperabilita_e_Sicurezza_Applicativa_v1.pdf
6 http://cloudsecurityalliance.it/wp-content/uploads/2012/12/Studio-Standard-Contrattuali-per-il-Cloud-Computing-DEC-2012-IT.pdf

Dal punto di vista delle applicazioni militari del cloud computing, l'esercito americano, come era lecito aspettarsi, è all'avanguardia, esprimendo delle posizioni di cauta apertura e di interesse. Sostanzialmente, viene riconosciuto al cloud la capacità di ottenere grandi vantaggi in termini di efficienza, risparmi e flessibilità, oltre alla ineguagliata efficacia nel trattare le grandi moli di dati che caratterizzano le applicazioni più spinte. L'esercito americano, infatti, riconosce al cyberspace un'importanza pari a quella che ha avuto nel recente passato lo spazio aereo. Per questi motivi, la Cyber Superiority viene vista come un obiettivo primario da raggiungere quanto prima. Il cloud computing viene quindi considerato una componente molto rilevante nel quadro delle iniziative per il raggiungimento di questo strategico obiettivo, anche se viene riconosciuta l'esigenza di migliorarne la sicurezza a tutti i livelli: dal "data layer" al "compute layer" passando per il "display layer" (ossia il livello nel quale i dati interagiscono con gli operatori).

Analoghe valutazioni possono essere svolte anche nel campo del cloud per le infrastrutture critiche. L'Europa, in questo caso, ha un ruolo preminente, come anche dimostrato dalla iniziativa di ENISA che ha pubblicato un interessante studio dal titolo: "Critical Cloud Computing. CIIP Perspective on Cloud Computing"[7]. In questo studio vengono analizzati proprio gli aspetti più importanti nella valutazione dell'adozione di servizi cloud da parte di gestori di infrastrutture critiche. In particolare sono valutati gli aspetti dell'analisi del rischio, della gestione degli incidenti, del monitoraggio, del governo dei servizi e della sicurezza in generale.

Conclusioni

Il mondo del cloud computing è ancora in una fase fortemente propulsiva in cui, da parte dei Provider, si elaborano nuove nicchie di mercato nel tentativo di allargare la base dei potenziali consumer che possono essere serviti. Dal punto di vista dei consumer, invece, c'è la presa d'atto che questo tipo di servizi cominciano a diventare essenziali per la moderna gestione delle infrastrutture IT. In questo scenario, i governi cercano di trovare il modo per far entrare in campo anche il mercato della Amministrazione

[7] https://resilience.enisa.europa.eu/cloud-security-and-resilience/critical-cloud-computing/view

Pubblica, al fine di farlo avvicinare alle capacità esecutive tipiche del settore privato e, in ultima analisi, per contribuire al rilancio dell'economia attraverso la creazione delle migliori condizioni per il rilancio delle imprese. L'auspicio è che l'Italia ritrovi la forza e la chiarezza di visione necessarie per riuscire ad eliminare il ritardo accumulato in questo settore così determinante per la crescita del Paese.

Sicurezza in sanità

a cura di *Stefano Cremonesi* e *Claudio Telmon*

Il contesto della Sanità presenta delle peculiarità che devono essere ben comprese per poter trattare in modo efficace il tema della sicurezza delle informazioni. Nel contesto della Sanità infatti, ed in particolare in quello ospedaliero che lo rappresenta in misura maggiore, il "core-business" aziendale consiste principalmente nel trattamento diagnostico-terapeutico delle persone. Questa attività ha due aspetti importanti, che condizionano l'intera organizzazione:

- errori e fallimenti possono comportare danni a persone che possono arrivare fino alla morte dei pazienti (safety);
- in molti contesti, l'emergenza è tutt'altro che un'eccezione: rallentamenti delle attività, dovuti magari a processi autorizzativi nell'accesso alle informazioni, non sono accettabili;
- il tema della sicurezza e quello della tutela dei dati personali hanno forti sovrapposizioni, dato che la gran parte dei dati più critici trattati rientra fra quelli definiti sensibili dalla normativa;
- esiste comunque una cultura di attenzione all'integrità e alla riservatezza delle informazioni che non si è sviluppata solo in seguito all'introduzione della normativa stessa, ma che, seppure con le sue particolarità, risale a molto tempo prima.

Per comprendere il tema della sicurezza IT nella Sanità è utile approfondire meglio i punti sopra elencati.
L'obiettivo principale della Sanità è la tutela della salute delle persone e, nel caso di un ospedale, principalmente curare pazienti affetti da malattie allo stadio acuto. Questa attività pone dei vincoli di efficienza e temporali molto importanti a tutte le attività svolte. L'esigenza di evitare errori è massima: per questo, concetti come processo e protocollo sono molto più acquisiti e connaturati che nella maggior parte di altri contesti, e questo non solo nel trattamento delle informazioni. Si pensi ad esempio alla necessità di associare in modo certo le diagnosi e le terapie ai pazienti o alle conseguenze drammatiche che errori in quest'area hanno avuto in alcuni casi anche riportati dalla stampa. A questo si sovrappone il tema delle urgenze e delle emergenze. Per questo, l'attenzione è prima di tutto

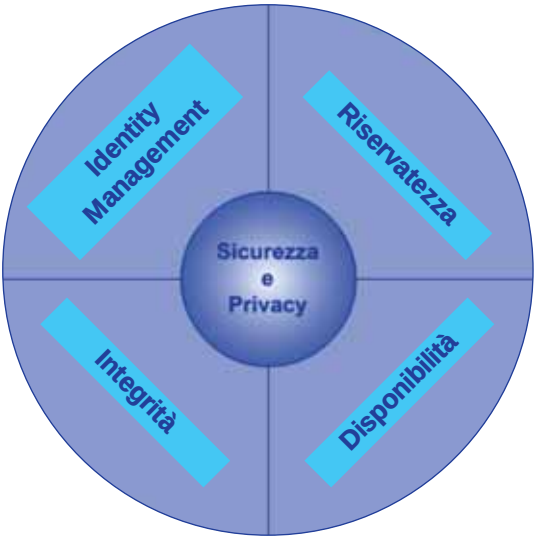
alla disponibilità e integrità delle informazioni.
Il tema della riservatezza ha anch'esso una sua particolarità. Da un punto di vista culturale, il medico tenderebbe a condividere con relativa facilità le informazioni con i colleghi, quando questo sia utile dal punto di vista dell'efficacia ed efficienza delle proprie attività, fidando anche nella deontologia dei colleghi. I dati sensibili tenderebbero quindi a circolare con relativa facilità fra i professionisti coinvolti nelle attività di cura. Viceversa, esiste una barriera molto più forte fra la struttura e il mondo esterno, nei confronti del quale i dati verrebbero maggiormente tutelati. Da molto prima che venissero emanate norme per la tutela dei dati personali infatti, la malattia è considerata una faccenda "privata". La rilevanza di questa riservatezza del resto è testimoniata anche dall'abbondanza di normativa specifica per il trattamento di dati sanitari.

Questa cultura, che si riflette anche in parte nell'organizzazione tradizionale dei processi delle strutture ospedaliere, contrasta però per certi versi con i requisiti posti dalla conformità alla normativa sul trattamento dei dati personali, su alcuni punti critici:

- la normativa impone un controllo in generale molto più granulare riguardo all'accesso ai dati; questo comporta una maggiore complessità, se non delle difficoltà, nel gestire l'aggiunta o rimozione di soggetti autorizzati, ad esempio in contesti come il pronto soccorso;
- la normativa attribuisce al paziente il controllo su chi può accedere ai dati: seppure questo non contrasti con le pratiche dell'ambiente sanitario, tenerne conto impone nei fatti una maggiore complessità nel controllo degli accessi.

Tutto questo suggerisce l'importanza di un approccio complessivo alle problematiche della sicurezza informatica in sanità che cerchiamo di approfondire nei paragrafi seguenti.
Sicurezza e Privacy, intendendo con quest'ultimo termine il trattamento dei dati personali conforme ai principi che sottendono alla relativa normativa, rappresentano qui due aspetti, solo apparentemente antitetici, che devono essere governati "ex ante" in quanto la loro pianificazione può determinare impatti considerevoli nel disegno e nella gestione del sistema informativo aziendale.
La criticità che oggi si evidenzia in misura sempre maggiore consiste nell'equi-

librare un utilizzo esteso e pervasivo delle tecnologie informatiche in azienda con i necessari requisiti di privacy e sicurezza che sono richiesti sia dagli utilizzatori del sistema informativo aziendale sia, e in particolare, dai clienti.
Per questi motivi una governance complessiva di tali aspetti richiede un approccio di tipo globale e sistemico, sinteticamente rappresentato nella figura seguente. Globale in quanto appare necessario presidiare contemporaneamente e congiuntamente diverse variabili tra loro interdipendenti, Sistemico in quanto diverse di queste variabili possono determinare impatti sul business aziendale in generale e richiedono interventi tecnologici, organizzativi, di formazione e change management.



Il sistema di Identity and Access Management (IAM) nel contesto della gestione della sicurezza in ambito sanitario ha un ruolo particolarmente importante. Soluzioni ICT nell'area clinica che utilizzino un Clinical Data Repository, che consente una ricomposizione longitudinale nel tempo di tutte le informazioni clinico-assistenziali di un cittadino, richiedono che tali informazioni siano fruibili solo al cittadino (o alle persone da lui autorizzate) e ai team medico-infermieristici che sono coinvolti nel processo di cura dello stesso.
Ne consegue che l'utilizzo di ICT in sanità richiede specifiche attenzioni alle problematiche legate all'accesso al sistema, in considerazione del fatto che il Sistema Informativo di un'azienda sanitaria è costituito da un vasto insieme di risorse (funzionalità applicative, dati, documenti) che devono

poter essere accedute solo da soggetti riconosciuti ed autorizzati.
Ciò implica adottare soluzioni di IAM per l'intero sistema informativo composte da:

- un sistema di autenticazione ovvero un sistema centralizzato volto ad accertare l'identità degli utenti che accedono al sistema;
- un sistema di autorizzazione ovvero un sistema centralizzato in grado di garantire che solo gli utenti aventi le abilitazioni necessarie possano utilizzare una specifica funzione o dati disponibili nel sistema.

È inoltre opportuno sottolineare che l'operatività del personale comporta spesso accessi da postazioni diverse ed a più applicazioni, generalmente con tempi molto stretti. In questo contesto, sono particolarmente interessanti sia tecnologie di Single Sign On (SSO), sia l'utilizzo di autenticazione basata su "qualcosa che si ha" (ad esempio, una Carta Nazonale dei Servizi, CNS) o "qualcosa che si è", in modo da rendere più semplice e veloce l'accesso.

È utile anche considerare le problematiche associate al Fascicolo Sanitario Elettronico (FSE). Il FSE raccoglie idealmente tutte le informazioni e i documenti relativi allo stato di salute di un cittadino. Nella pratica, il FSE può essere un punto di accesso ad informazioni contenute in realtà in più CCE gestite autonomamente da diverse strutture sanitarie. Si pone quindi naturalmente il tema di sistemi di controllo accessi federati o, eventualmente, controllati centralmente a livello regionale. Anche qui, sia le soluzioni che il relativo livello di maturità non sono uniformi. Nella stessa logica, data la relativa facilità di circolazione o quantomeno di accesso alle informazioni fra le diverse strutture, si pone il problema di garantire livelli uniformi di sicurezza fra le diverse strutture. Il tema è complesso, e può trovare anche in questo caso una soluzione almeno parziale in sistemi federati.

Il valore legale dei documenti prodotti e delle informazioni gestite in generale rappresenta un aspetto di notevole rilevanza in ambito sanitario. Oltre alle numerose indicazioni di legge, è utile sottolineare come, proprio per la natura dell'attività svolta, sia utile e spesso necessario poter garantire l'integrità e l'origine dei dati, per tutelare le diverse parti in causa: aziende, personale e pazienti.In tale contesto l'adozione della firma elettronica, nelle sue declinazioni avanzata, qualificata e digitale) e del processo di conservazione digitale integrano il tema dell'integrità affermando i principi di

autenticità vale a dire la certezza dell'origine del documento oggetto di firma digitale, di *non ripudio* inteso come la prevenzione del disconoscimento di un documento da parte dell'autore dello stesso, di *opponibilità a terzi* attraverso l'apposizione della marcatura temporale che certifica la validità verso terzi di un documento firmato digitalmente.[1]

Quello della sanità è in effetti il contesto in cui per prime si sono sperimentate e poi introdotte in modo anche diffuso varie forme di firma elettronica (l'unico altro contesto di utilizzo diffuso è in effetti la smart card legata ai rapporti fra aziende e Camere di Commercio). Sempre nel contesto della sanità hanno trovato il loro utilizzo principale le Carte Nazionali dei Servizi, anche per l'accesso da parte dei cittadini a servizi online, compreso l'accesso ai referti.

Il tema della disponibilità ha conseguenze importanti dal punto di vista delle architetture e dei sistemi utilizzati nell'area clinica[2]. Si possono evidenziare alcuni casi importanti dal punto di vista del rischio:

1) disponibilità dei dati in presenza di guasti informatici; l'utilizzo di ICT in sanità richiede un'oggettiva attenzione a misure di business continuity sia nelle componenti della server farm sia nella infrastruttura di rete locale e geografica;

2) disponibilità dei dati a lungo termine; tematica fortemente interconnessa alla conservazione sostitutiva dei documenti.

3) disponibilità dei dati in occasione di eventi catastrofici, in una logica di business continuity: non solo l'ospedale deve essere in grado di mantenere la propria operatività, per la quale questi dati sono essenziali, ma deve essere anche in grado di fornirli rapidamente ad altre strutture/organismi coinvolti nello stesso contesto di emergenza.

In effetti, le strutture sanitarie non solo sono classificate fra le infrastrutture critiche, ma sono certamente fra quelle che, in caso di calamità, possono essere impegnate oltre il normale. Le strutture sanitarie pubbliche, come le altre pubbliche amministrazioni, sono sottoposte alle indicazioni dell'articolo 50 bis del Codice dell'Amministrazione Digitale. Devono quindi defi-

---

[1] Questo tema è stato approfondito in particolare dal Gruppo di Lavoro AISIS sulla Cartella Clinica Elettronica, http://www.aisis.it/it/workgroup/gruppo-di-lavoro-sulla-cartella-clinica-elettronica/c79c0409-de54-4efc-8066-e03621d32183

[2] Anche questo tema è stato ulteriormente approfondito in particolare dal Gruppo di Lavoro AISIS sulla Cartella Clinica Elettronica

nire un piano di continuità operativa e, come parte di questo, un piano di disaster recovery. Seppure la definizione del piano sia relativamente diffusa fra le strutture pubbliche, ma comunque in modo variabile sul territorio, l'implementazione di questi piani è molto meno diffusa. Nell'area della continuità operativa si percepisce anzi una sottostima del problema evidenziando che malgrado alcune aree di processo prevedano una attività 24x7, i sistemi di disaster recovery siano sostanzialmente inesistenti. Con una certa frequenza anche gli investimenti nella realizzazione di adeguate server farm e nella ridondanza delle reti locali e geografiche sono limitati.La percezione di un rischio limitato, non solo in termini di continuità operativa ma anche di minacce più specificamente di sicurezza, è però un problema diffuso, che insieme all'elevata attenzione all'operatività, può in qualche caso ridurre più del dovuto l'attenzione al tema della sicurezza.

Di seguito viene evidenziato l'impatto stimato delle variabili sinteticamente descritte sulle macro-aree dei processi aziendali.

Possibili impatti	Identity Management e SSO	Riservatezza	Integrità	Continuità
Area Accoglienza (ADT, PS, CUP)	++	++	+++	+++
Area Clinica (Reparti e Ambulatori)	+++	+++	+++	+++
Area Diagnostica (Lis, AP, Ris-Pacs, CardioPacs)	+++	+++	+++	+++
Area Amministrativa	++	+	+++	+
Area Intranet-Internet	++	+	+++	+
Area Direzionale-BI	++	++	+++	++

Fonte: AISIS

Dalla lettura della tabella si evince che alcune variabili di sicurezza costituiscono criticità rilevante in alcune aree di processo: ad esempio, la continuità operativa è fondamentale per l'area clinica mentre costituisce una minor criticità nell'area amministrativa. Al contrario alcune variabili, ad esempio l'integrità, rappresentano una criticità per tutte le aree operative.
La valutazione degli impatti può consentire una pianificazione degli interventi di pianificazione o di remediation in materia di sicurezza.
Nella tabella seguente vengono invece sinteticamente elencati i rischi possibili derivanti dalla non attivazione di sistemi di sicurezza per tipologia di macro-area.

Possibili rischi	Identity Management e SSO	Riservatezza	Integrità	Continuità
Area Accoglienza (ADT, PS, CUP)	Accesso non autorizzato a dati amministrativi (ad es. esenzioni) o clinici (ad es. Patologie ricovero)	Accesso e/o utilizzo non autorizzato di dati amministrativi e clinici ivi compresi dati contabili dei clienti a pagamento	Accesso, modifica, e/o utilizzo non autorizzato di dati amministrativi e clinici ivi compresi dati contabili dei clienti a pagamento	Nell'area Cup e PS non possibili interruzioni di servizio oltre a 1 ora
Area Clinica (Reparti e Ambulatori)	Accesso non autorizzato a dati clinici	Accesso e/o utilizzo non autorizzato di dati clinici	Accesso, modifica, e/o utilizzo non autorizzato di dati clinici	Nell'area Cup e PS non possibili interruzioni di servizio oltre 30'
Area Diagnostica (Lis, AP, Ris-Pacs, CardioPacs)	Accesso non autorizzato a dati clinici	Accesso e/o utilizzo non autorizzato di dati clinici	Accesso, modifica, e/o utilizzo non autorizzato di dati clinici	Nell'area Cup e PS non possibili interruzioni di servizio oltre 30'
Area Amministrativa	Accesso non autorizzato a dati amministrativo-contabili	Accesso e/o utilizzo non autorizzato a dati amministrativo-contabili	Accesso, modifica, e/o utilizzo non autorizzato di dati amministrativo-contabili	
Area Intranet-Internet	Accesso non autorizzato a dati clinici in caso di aree dedicate al download di referti	Accesso e/o Utilizzo non autorizzato a dati clinici in caso di aree dedicate al download di referti	Accesso, modifica, e/o utilizzo non autorizzato di dati clinici	
Area Direzionale-BI	Accesso non autorizzato a dati amministrativo-contabili	Accesso e/o utilizzo non autorizzato a dati amministrativo-contabili	Accesso, modifica, e/o utilizzo non autorizzato di dati amministrativo-contabili	

Fonte: AISIS

Alcuni rischi sono tali da compromettere in modo significativo le attività di alcune aree operative. Ad es. nell'area clinica il problema della disponibilità è talmente critico per cui vanno pianificate soluzioni che consentano che un eventuale downtime dei sistemi non possa portarsi oltre ad un'ora. Le soluzioni tecnologiche di sicurezza in senso lato non sembrano essere particolarmente diffuse nel contesto sanitario italiano. Probabilmente il budget destinato dalla Aziende Sanitarie all'ICT (che nel rapporto 2012 dell'Osservatorio ICT del Politecnico di Milano è stimato in 1,1% della

spesa sanitaria) non consente investimenti nell'area della sicurezza nemmeno quando questa è dovuta in termini di conformità normativa.
Nell'area della gestione delle identità e della riservatezza, se da un lato si ritiene siano abbastanza diffuse soluzioni legate alla sicurezza perimetrale (firewall, antivirus, antispamming, antiphising, internet filtering…) dall'altro appaiono poco diffuse soluzioni di IDM e SSO. Nell'area dell'integrità l'adozione in diverse regioni della firma digitale sulla documentazione clinica inizia a rappresentare una concreta soluzione del problema anche se rimane sostanzialmente irrisolta la problematica inerente la separazione dei dati anagrafici da quelli sensibili o la cifratura dei db che li contengono entrambi.

Da ultimo si ritiene opportuno evidenziare due ulteriori criticità in materia di sicurezza in sanità. La prima è quella delle apparecchiature biomedicali, che condividono con contesti più tradizionalmente SCADA molte problematiche di sicurezza. Si tratta di apparecchiature concepite per operare in un ambiente isolato, non pensate per la sicurezza e spesso gestiti al di fuori della normale gestione IT (ad esempio, solo dal fornitore ed al solo scopo di manutenzione ordinaria e straordinaria). Questi apparati sono sempre più spesso connessi invece in rete, con problematiche analoghe a quelle dei sistemi SCADA industriali[3].
La seconda riguarda il tema della telemedicina, telediagnostica e teleassistenza. Si tratta ancora per lo più di attività pilota e/o sperimentali, che come tali tendono a considerare secondario il tema della sicurezza rispetto a quelli tipicamente centrali per queste sperimentazioni, come quello della disponibilità e continuità del servizio. Con la diffusione di questi servizi tuttavia, il tema della sicurezza dovrà essere affrontato in modo organico anche in questi ambiti. In tale contesto possono essere ricomprese anche le attività dei medici di base che in misura sempre maggiore richiedono una connessione con tali sistemi o con i sistemi informativi delle aziende ospedaliere.
La sempre maggiore integrazione delle loro attività anche dal punto di vista informatico (si pensi ad esempio a certificati e ricette online, al downlaod di documentazione clinica.), determina una sempre più rilevante attenzione alla sicurezza di queste postazioni di lavoro.

[3] http://www.darkreading.com/vulnerability-management/167901026/security/attacks-breaches/240146474/security-researchers-expose-bug-in-medical-system-used-with-x-ray-machines-other-devices.html.html

E-Commerce

a cura di *Fabio Guasconi*

1. Quadro generale

In un momento di congiuntura economica non certo brillante come quello attuale, il mercato dell'e-commerce continua a rappresentare in tutto il mondo una delle poche isole felici in cui la crescita in valori percentuali si può ancora misurare con numeri a doppia cifra. Secondo un rapporto pubblicato dal Politecnico di Milano, tra i più conservativi in termini numerici, il volume d'affari ad esso collegato nel nostro Paese è infatti cresciuto nel solo 2012 del 19% rispetto all'anno precedente. La suddivisione merceologica vede in testa il settore del turismo, seguito da abbigliamento, assicurazioni ed elettronica di consumo, come visivamente riportato nel seguente estratto dello stesso studio del Politecnico di Milano. Di particolare rilevanza il fatto che il mercato Italiano è da sempre più orientato alla vendita di servizi che a quella di prodotti, in controtendenza rispetto al resto del mondo.

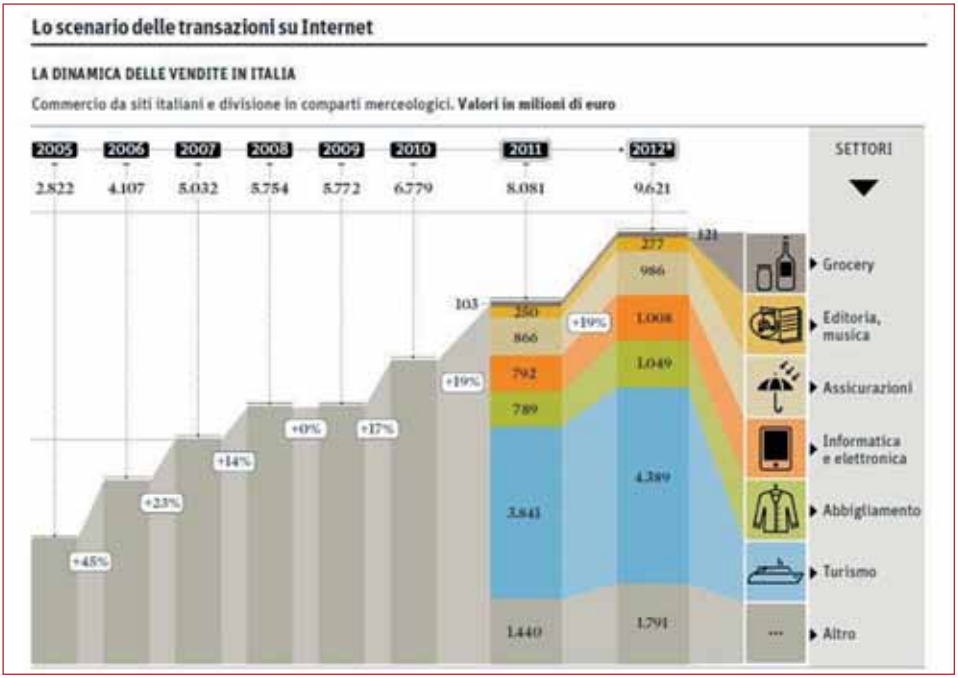


Figura 1 - Mercato dell'e-commerce in Italia,
cortesia dell'Osservatorio eCommerce B2c Netcomm-School of Management del Politecnico di Milano

Esistono branche innovative dell'e-commerce in cui la crescita è ancora più spinta: gli acquisti effettuati attraverso dispositivi mobile (ormai noti come m-commerce) stanno tenendo un incremento prossimo al 50% grazie anche all'endemica diffusione di dispositivi smart-phones o dei tablet, e potrebbero crescere fino a rappresentare 1/4 degli acquisti totali nel 2017.

Allargando la prospettiva alle performance degli altri Paesi europei diventa evidente quanto il fenomeno sia lontano dall'essere locale: sempre secondo il Politecnico di Milano, Germania e Francia hanno avuto una crescita entrambe del 12% rispetto al 2011 e il Regno Unito, da sempre peso massimo del settore, dell'11%. La maggiore crescita dell'Italia è purtroppo imputabile non ad un'eccellenza nel settore, ma ad un ritardo considerevole accumulato nel tempo. Il valore del mercato italiano dell'e-commerce è infatti pari a poco più di 1/6 di quello inglese e alla metà di quello francese, come evidenziato dal diagramma seguente.

L'Italia, secondo diverse analisi effettuate in merito, deve gran parte di questo ritardo a una serie di fattori bloccanti che portano meno della metà della popolazione ad acquistare su internet rispetto alla media europea. Tra questi fattori i principali sono riconosciuti essere:

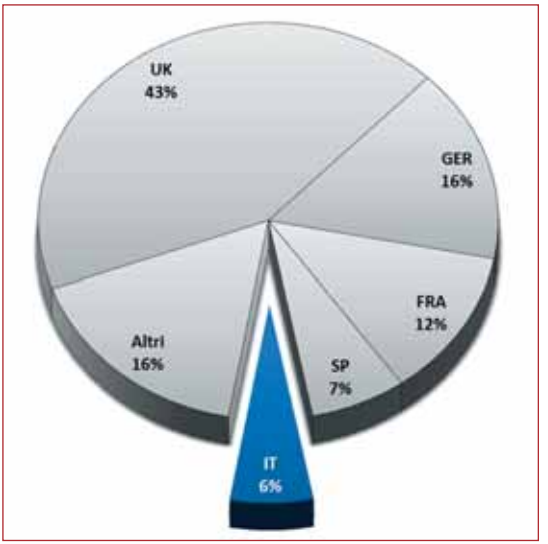


Figura 2 - Suddivisione del mercato dell'e-commerce in Europa, 2012

- la penetrazione di internet e delle comunicazioni ad essa legate è al di sotto della media europea;
- vi sono barriere normative che zavorrano la competitività del canale;
- gli strumenti di pagamento elettronici sono ancora scarsamente diffusi e utilizzati;
- un terzo dei venditori nazionali vende esclusivamente sul mercato nazionale;

- la propensione all'acquisto online e la cultura informatica della popolazione sono limitate;
- la barriera linguistica che penalizza acquisti in altri Paesi è consistente.

Partendo da questi presupposti, e considerando le numerose opportunità derivanti dalla crescita dell'e-commerce (nel Regno Unito l'internet economy vale oltre il 7% del PIL rispetto al 2% in Italia), questo è stato incluso come uno degli elementi di maggiore interesse nell'Agenda Digitale italiana e alcune iniziative di interesse sono state già intraprese nel corso dell'ultimo anno. Ciò non toglie che la strada sia ancora lunga e che alcuni dei fattori bloccanti sopra riportati siano di complessa risoluzione ma è altresì corretto sottolineare anche l'esistenza di opportunità per il nostro Paese, che vanta la seconda posizione per contratti di telefonia cellulare in Europa e di conseguenza, adeguandosi all'ampia crescita del mercato degli smartphones e dei tablet (rispettivamente del 45% e del 96% nel 2012), sta sviluppando un potenziale notevole per una seconda crescita digitale legata al mobile.

2. Sicurezza?

Sorprende che il 60% di chi non acquista online indichi la sicurezza tra gli ostacoli principali, ma sorprende ancora più che nella stessa Agenda Digitale italiana questo elemento, messo in evidenza, sia liquidato come un falso problema.

Se infatti da una parte è vero che la percentuale di frodi sull'e-commerce è in lenta, ma costante riduzione da anni (dal 2011 risulta in calo da uno 0,17% a uno 0,12% delle transazioni e rispetto al 2001 gli esercenti hanno ridotto di un terzo le perdite), la forte crescita del numero di acquisti e del loro volume corroborata dai numeri precedenti e l'aumento progressivo dei canali tecnologici che si possono utilizzare sono tendenze che non possono permettere di abbassare la guardia.

L'esperienza maturata in questi anni dagli esperti sulla sicurezza insegna infatti che l'interesse degli attaccanti si concentra dove si trova il maggior valore: così è per lo sviluppo dei malware, dove certe piattaforme sono preferite ad altre, altrettanto sta avvenendo per il commercio elettronico

effettuato tramite navigazione web tradizionale e, appena inizieranno ad essere impiegati in modo consistente, lo stesso avverrà sugli strumenti mobile e sui canali come l'NFC (pagamenti contactless).

Il fenomeno ormai comunemente definito sotto il nome di Cybercrime diventa sempre più vasto e in grado di operare su ampia scala, mettendo in cantiere veri e propri progetti di complessità precedentemente sconosciuta e condividendo informazioni con una base a bassa competenza, ma numerosa. Nel 2012, oltre alla violazione di altri giganti dei pagamenti online come la russa ChronoPay, si è assistito alla diffusione dei primi malware in grado di trasferirsi dai personal computer ai dispositivi mobile per attaccare i sistemi che utilizzano codici di sicurezza inviati via SMS; sono stati registrati casi di QR code autoadesivi che, applicati sopra a quelli veri di annunci fisici, rimandano a siti contraffatti e diversi siti di commercio elettronico sono stati bersagliati da una molteplicità di micro-frodi, il tutto mentre i primi arresti di cybercriminali hanno fatto notizia anche nel nostro paese, come nel caso di Ali Hassan.
È inoltre sempre cronaca recente la sentenza pronunciata contro Sony in Inghilterra per non aver protetto adeguatamente i dati dei propri clienti memorizzati sulla PlayStation Network nel 2011.
Meno noti e orientati alla truffa ma ugualmente significativi sono i contesti in cui l'e-Commerce viene utilizzato per aggirare restrizioni alla vendita di determinati prodotti, quali ad esempio medicinali o, in modo ancora più grave e legato alla tradizionale criminalità organizzata, droghe, armi e altro.

Figura 3 – Alcune headlines sulla sicurezza dell'e-commerce nel 2012

In questo contesto le truffe sui canali tradizionali, quali la contraffazione di un POS di un distributore di carburante, di uno sportello per il prelievo

bancario o l'immissione sul mercato di un lotto di banconote false, coinvolgono un numero circoscritto di soggetti e quindi generano meno clamore rispetto ai 77 milioni di vittime per il caso di Sony, ma sono molto più probabili di quest'ultimo, creando un maggiore, ma falso senso di sicurezza verso le transazioni fatte di persona, che troppo spesso si pensa di poter essere in grado di smascherare facilmente.

Da molti anni stanno venendo peraltro effettuati sforzi considerevoli per migliorare il livello di sicurezza dei sistemi e delle applicazioni utilizzate nell'e-commerce. Una delle prime piattaforme utilizzate per questa finalità è stata eBay che ha acquisito il famoso servizio di pagamento online PayPal già dal 2002, che oggi è leader delle transazioni online in Italia. Nei prossimi anni non mancheranno le novità nel settore, a partire da MyBank che si baserà sul sistema europeo di pagamenti per passare a Square che si presenta come un piccolo oggetto quadrato da collegare al proprio dispositivo mobile, mettendolo in grado di accettare pagamenti con carta. Tutti i servizi e i prodotti di questo tipo cercano costantemente di rendere al tempo stesso più sicuro e più facile il processo di acquisto online e sono sottoposti a una serie crescente di regole imposte da più parti, tra cui in primis:

- le misure per la protezione dei dati personali di cui al d.lgs 196/2003 e le altre norme ad esso collegate;
- gli standard del PCI Council che si applicano a chi elabora dati delle carte di pagamento dei principali marchi (VISA, MasterCard, American Express, Discover Network, JCB) ora corredati anche da una guida specifica sull'E-commerce;
- la Direttiva 2007/64/CE relativa ai servizi di pagamento nel mercato interno;
- la Direttiva 2009/110/CE concernente l'avvio, l'esercizio e la vigilanza prudenziale dell'attività degli istituti di moneta elettronica.

La riforma delle leggi per la protezione dei dati personali, attualmente in discussione in sede europea, avrà l'opportunità di fissare nuove importanti garanzie per gli utenti dei servizi di e-commerce che, si spera, potranno contribuire ad imporre un livello minimo di sicurezza osservato da tutti gli operatori del settore, ad oggi non sempre così strettamente controllati sugli obblighi normativi sopra riportati. Uno dei temi centrali in questo

senso è l'introduzione dell'obbligo di notifica al pubblico delle violazioni subite da parte di un'entità che tratta dati personali, in caso non si siano adottati sistemi avanzati di protezione dei dati. Questo obbligo è già stato introdotto nella maggioranza degli stati USA e per le aziende di telecomunicazioni che operano in Europa, ma i gestori di negozi online non ne sono al momento soggetti. Per quanto possa sembrare semplice da un punto di vista concettuale, in pratica non è assolutamente banale già solo individuare che una violazione informatica è avvenuta, specie per le entità di più contenuta dimensione.

Ciò nonostante, se chi vende online osservasse correttamente anche solo i seguenti principi, comunemente individuati dagli esperti come di fondamentale importanza, si potrebbe incrementare considerevolmente il livello di sicurezza del mercato (riducendo significativamente il numero di violazioni):
1) adozione di configurazioni sicure (*hardening*) dei sistemi;
2) inserimento della sicurezza nei requisiti di progettazione e nell'implementazione del software;
3) implementazione di sistemi di protezione e controllo automatici;
4) aggiornamento costante di tutti i sistemi;
5) verifica periodica dei rischi esistenti;
6) organizzazione della gestione della sicurezza.

Oltre a questi elementi mandatori sono stati sviluppati nel tempo una serie di accorgimenti funzionali a ridurre le frodi, alcuni di successo come i meccanismi antifrode "risk-based" e altri meno, come quelli di antifrode con regole statiche, alcuni che hanno un impatto sull'utente finale come il 3D Secure delle carte di pagamento e altri del tutto trasparenti ad essi quali la tokenizzazione dei numeri di carta memorizzati sui sistemi informativi del fornitore.

L'anello mancante della catena finora descritta è però la cultura informatica e sulla sicurezza degli stessi utenti finali che, oltretutto, decretano il successo o la caduta dell'e-commerce in generale e degli strumenti in esso impiegati in particolare. La maggior parte delle frodi non sfrutta delle vul-

nerabilità dirette degli strumenti quanto piuttosto un loro uso improprio da parte di chi ha un minore livello di consapevolezza sulla sicurezza. ENISA, l'agenzia europea per la sicurezza delle reti e delle informazioni, è il principale soggetto che si è impegnato nel sensibilizzare gli utenti finali attraverso iniziative mirate e istituendo, lo scorso ottobre, il primo "*European Cyber Security Month*", incentrato sulle principali regole da osservare per mantenere un buon livello di sicurezza nel cyberspace.

Figura 4 – Slogan e logo del Cyber Security Month organizzato da ENISA

Le campagne di consapevolezza indirizzate agli utenti finali che verticalizzino la sicurezza e l'informatica intorno al tema dell'e-Commerce dovrebbero essere parte integrante della strategia per il suo rilancio nel nostro Paese, e percepite a ragion veduta sia come elemento di lotta preventiva alla criminalità sia come importante volano per creare quella fiducia che ancora manca agli italiani per abbracciare le opportunità offerte dall'e-Commerce.

BIBLIOGRAFIA

IL SOLE 24 ORE, E-commerce: acquisti per 11 miliardi di euro nel 2012
http://opendatablog.ilsole24ore.com/2012/10/e-commerce-acquisti-per-11-miliardi-di-euro-nel-2012/#axzz2JG3bp4oM

EUROSTAT, Internet use in households and by individuals 2012 - Issue number 50/2012
http://epp.eurostat.ec.europa.eu/cache/ITY_OFFPUB/KS-SF-12-050/EN/KS-SF-12-050-EN.PDF

PCI DSS 2.0 eCommerce Guidelines
https://www.pcisecuritystandards.org/pdfs/PCI_DSS_v2_eCommerce_Guidelines.pdf

ENISA Cyber Security Month
http://www.enisa.europa.eu/activities/cert/security-month

500K Credit Cards Stolen in Australian Point-of-Sale Hack
http://www.wired.com/threatlevel/2012/08/500k-credit-cards-stolen/

Caso Sony, “Clienti poco protetti dagli hacker”
http://www.corriere.it/tecnologia/videogiochi/13_gennaio_25/sony-multa-playstation-network_262d1d26-66ce-11e2-95de-416ea2b54ab7.shtml

Russian e-Payment Giant ChronoPay Hacked
http://krebsonsecurity.com/2010/12/russian-e-payment-giant-chronopay-hacked/

Fbi e Polizia postale, caccia all'uomo Arrestato a Milano un cybercriminale
http://www.corriere.it/cronache/12_giugno_26/arrestato-a-milano-cybercriminale_525e4038-bfc0-11e1-8089-c2ba404235e2.shtml

That square QR barcode on the poster? Check it's not a sticker
http://www.theregister.co.uk/2012/12/10/qr_code_sticker_scam/

PCI Council
http://www.pcisecuritystandards.org/

IPv6 è già qui, non è più una novità all'orizzonte

a cura di *Marco Misitano*

Di IPv6 si sente parlare da tanto, circa dal 2000. Una transizione imminente, un nuovo anno duemila, un'apocalisse annunciata, nel fatidico momento della fine degli indirizzi IP, di quel protocollo IP che come dice il nome Internet Protocol, sta alla base del funzionamento di Internet, della stragrande maggioranza delle reti aziendali, pubbliche e private di ogni sorta e dimensione, dalle piccole reti casalinghe ai backbone mondiali.
In termini di transizione alla nuova versione del protocollo IP - la v6 appunto - è accaduto di più negli ultimi ventiquattro mesi che nella decina d'anni precedente.

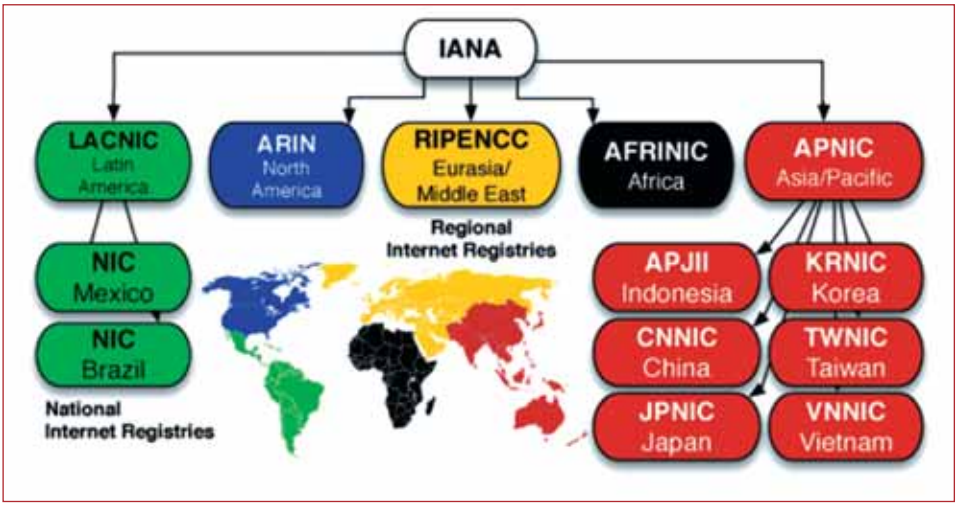
Perché adesso e non prima?

IPv6 ha visto la luce alla fine degli anni '90. Subito dopo il 2000 tutti gli attori dell'ecosistema ICT erano a conoscenza del nuovo protocollo e della necessità di intervenire. Aziende, service provider, operatori mobili, content provider, enti governativi, produttori di dispositivi e infine anche utenti: nessuno si è distinto per una particolare sensibilità al problema. Le aziende hanno atteso dagli ISP un'azione in questo senso, trasferendo il problema e ritenendo di poter tranquillamente sopravvivere con tecniche di Network Address Translation (NAT) e condivisione degli indirizzi IP.
Gli internet service provider, vista la scarsità di richieste, non hanno ritenuto di dover attivamente offrire ai propri clienti (sia residenziali, sia business) connettività con il nuovo protocollo, anche per la quasi totale mancanza di contenuti fruibili in IPv6.
Allo stesso tempo governi e il settore pubblico in generale, hanno preso tempo, aspettando di vedere quali passi avrebbero fatto altri attori. All'interno di questo settore solo le reti di ricerca hanno implementato IPv6 prima di altri, seppur in maniera disuniforme nel mondo.
In questo panorama, i content provider - ci si riferisce ai grandi produttori di contenuti globali come Google/Youtube, Facebook, Yahoo! e simili - non hanno certo brillato, aspettando un'infrastruttura di rete, dispositivi e di conseguenza domanda per contenuti e servizi in IPv6.
Dal canto loro i produttori di dispositivi solo di recente hanno adottato il nuovo protocollo sui propri prodotti, grazie al supporto da parte dei siste-

mi operativi; a oggi, infatti, le più recenti versioni dei sistemi operativi di Apple, Google, Linux, Microsoft supportano IPv6 in modo nativo, e così di conseguenza i dispositivi che li ospitano.
Insomma un circolo vizioso durato oltre un decennio che non ha certo giovato all'innovazione e alla transizione verso IPv6. A onor del vero il motivo principale di questo immobilismo è stata l'assenza di benefici e incentivi ad adottare IPv6.
In questa situazione, in cui tutti aspettavano che qualcun altro facesse il primo passo, mentre il mondo intero si intratteneva stimando il momento più o meno esatto in cui sarebbero di fatto terminati gli indirizzi IP, sono accadute, a partire dal 2011 alcuni eventi, che hanno drasticamente cambiato il panorama e smosso le acque da lungo tempo immobili. Val la pena menzionare questi driver.

Driver #1: gli indirizzi IPv4 sono terminati.
Il 3 febbraio del 2011, IANA[1], l'ente che assegna gli indirizzi IP a livello mondiale, dichiara di avere allocato tutti quelli restanti agli enti regionali. Poco dopo APNIC[2] l'ente regionale asiatico termina i propri, e lo scorso settembre 2012 anche RIPE[3], l'ente che rilascia indirizzi IP a Europa, Medio Oriente e Russia passa alla più restrittiva policy di allocazione finale per gli ultimi, pochi, indirizzi restanti. Dallo scorso settembre dunque anche per l'area europea non sono più assegnati indirizzi IPv4 ai richiedenti, salvo i casi in cui il richiedente abbia già un piano d'indirizzamento IPv6. In ogni caso la massima allocazione ammonta a 1024 indirizzi, una quantità assolutamente insignificante[4]. Le aree rossa e gialla nella figura hanno dunque terminato gli indirizzi IPv4. L'area nord americana - in blu - seguirà a breve, terminando gli indirizzi IPv4 da un momento all'altro.
Questo significa che - a oggi - nessuna nuova attività che richieda una rilevante presenza internet o uno spazio d'indirizzamento relativamente ampio può pensare di partire con IPv4.

1 Internet Society - www.internetsociety.org
2 IANA - www.iana.org
3 APNIC - www.apnic.net
4 RIPE - www.ripe.net



Driver #2: World IPv6 Launch

Sempre nel 2011, all'inizio di giugno si è tenuto il World IPv6 Day, organizzato e coordinato da Internet Society[5]. Per un periodo di ventiquattro ore i principali attori del web fra produttori di contenuti, ISP e aziende, hanno abilitato IPv6 sui loro siti web principali. Il risultato, molto positivo, ha dimostrato che IPv6 funziona, non solo in laboratorio ma anche in un ambiente eterogeneo e globale come Internet. L'esperimento è andato così bene che si è deciso di ripeterlo l'anno successivo, nel 2012, senza però il periodo fisso delle ventiquattro ore. Il 6 giugno 2012 è stato il World IPv6 Launch, iniziativa alla quale hanno partecipato centinaia fra siti web, content provider, aziende, service provider e produttori di apparecchiature per home networking. I partecipanti sono stati invitati a lasciare attivo IPv6 sui propri siti web, gli ISP a offrire connettività IPv6 ai propri nuovi clienti, i produttori di networking a offrire funzionalità IPv6 out of the box sui prodotti venduti.

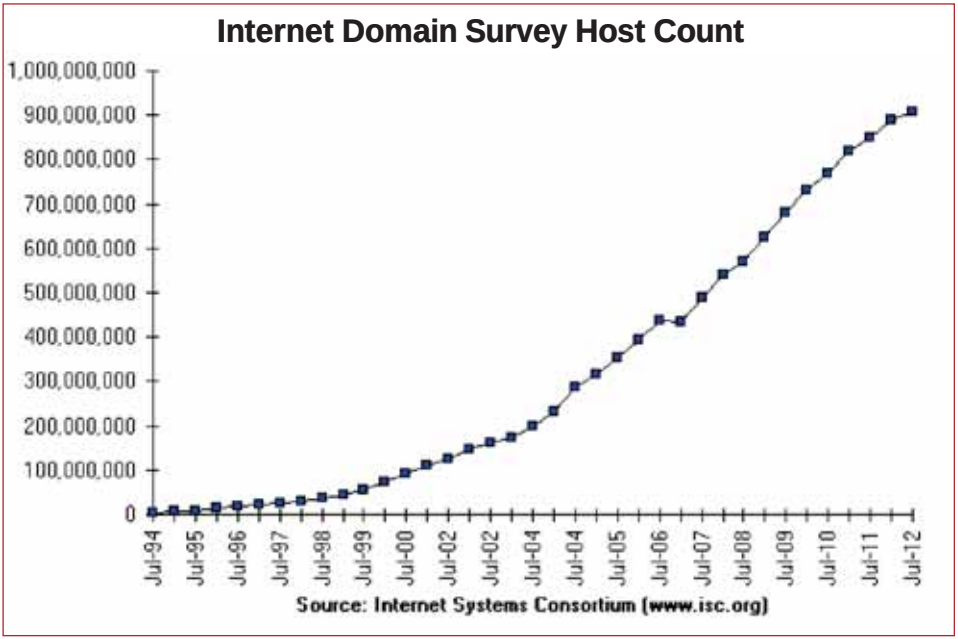
Il 6 giugno 2012 la numerosissima partecipazione all'iniziativa ha segnato dunque un enorme passo in avanti nella disponibilità di contenuti fruibili in IPv6, e nella disponibilità del nuovo protocollo anche fra la clientela residenziale.

---

[5] RIPE NCC Begins to Allocate IPv4 Address Space From the Last /8 - http://www.ripe.net/internet-coordination/news/announcements/ripe-ncc-begins-to-allocate-ipv4-address-space-from-the-last-8

Driver #3: Esplosione della popolazione di Internet

Il limite principale di IPv4 è lo spazio d'indirizzamento, ovvero il non poter indirizzare più di circa 4.3 miliardi di endpoint. La straordinaria crescita del numero degli utenti internet nell'ultimo decennio sicuramente è stata uno dei fattori che ha contribuito all'urgenza di un più vasto spazio d'indirizzamento.

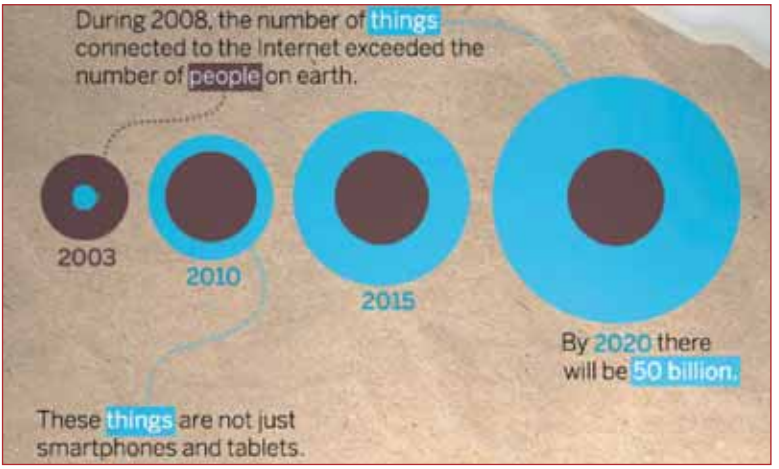


Driver #4: Internet of Things

Il già di per se significativo numero di persone che nell'ultimo decennio ha iniziato a utilizzare Internet, è comunque nulla in confronto al numero di oggetti che si collegano alla rete e fra loro. Basta pensare a smart TV, stampanti, automobili, contatori elettrici, sensori, consolle videogame, media player, smartphone per citare i più popolari in ambito consumer. Quello che va sotto il nome di Internet of Things è una rivoluzione in atto e di spettro ancora più ampio, e dal 2008 il numero degli oggetti collegati fra loro e a Internet attraverso il protocollo IP ha superato l'attuale popolazione terrestre[6]. Si tratta di sensori o dei più disparati oggetti, che possono

[6] dato ed infografica completa da cui è estratta la figura: http://blogs.cisco.com/news/the-internet-of-things-infographic/

avere applicazioni dalle più banali alle più sofisticate. Dall'adeguare l'orario di una sveglia in base al luogo e ora di un appuntamento, prendendo in considerazione la strada da fare, il traffico, se si debba fare o meno benzina durante il tragitto o se mezzi pubblici necessari sono in ritardo; fino all'applicazione di tag intelligenti per il monitoraggio a distanza dei pazienti per prevenire malattie cardiovascolari. Le applicazioni sono infinite, cosìcome i potenziali modelli di business, e tutto questo ha bisogno di uno spazio d'indirizzamento che IPv4 semplicemente non è in grado di offrire.



Driver #5: il web diventa mobile, i telefoni smart.
È in evidenza a tutti la popolarità che nuovi dispositivi come tablet e smartphone stanno guadagnando. La cosa va di pari passo con un uso del web che avviene sempre di più tramite dispositivi mobili[7]. Chi oggi ha un telefono mobile tradizionale molto probabilmente si convertirà a uno smartphone. E da parte loro gli operatori mobili promettono sempre migliori performances, con l'imminente arrivo della 4G/LTE, che nelle specifiche richiede l'IPv6 per il funzionamento del servizio voce, un altro elemento che aumenterà la presenza del nuovo protocollo.
Queste sono alcune delle inarrestabili tendenze che fanno si che la situazione stagnante di cui sopra, con tutti che aspettano tutti, si stia sgretolando sempre più rapidamente.
In totale è stimato che nell'area europea nel 2016 ci saranno due miliardi

[7] www.slideshare.net/kleinerperkins/2012-kpcb-internet-trends-yearend-update

di dispositivi fissi e mobile con IPv6, una significativa crescita se confrontata con i "soli" 125 del 2011[8].

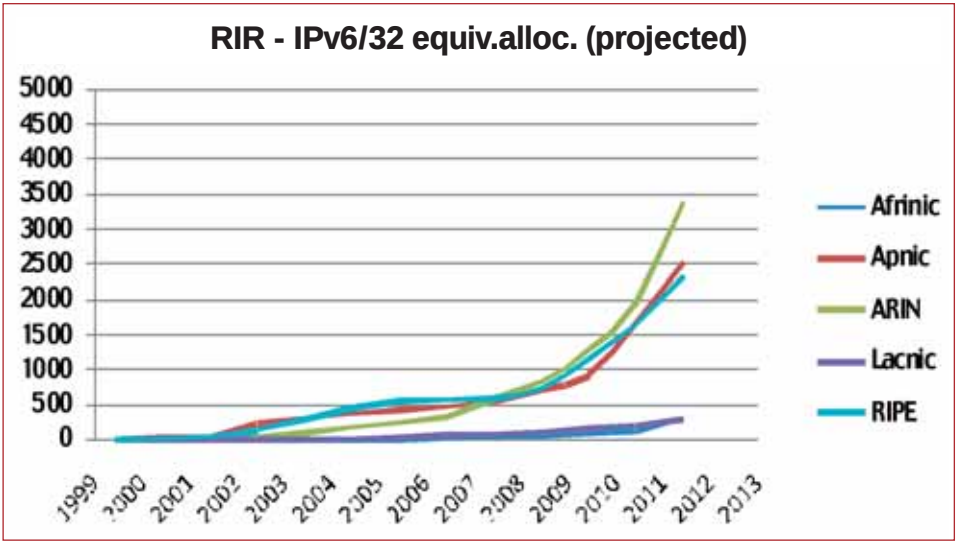
Dalle tendenze ai dati di fatto

Semplificando al massimo, un'azienda che decide di adottare il nuovo protocollo passerà attraverso quattro fasi:

Analizziamo alcuni indicatori che seguono queste quattro fasi per renderci conto di quale sia effettivamente lo stato dell'adozione di IPv6:

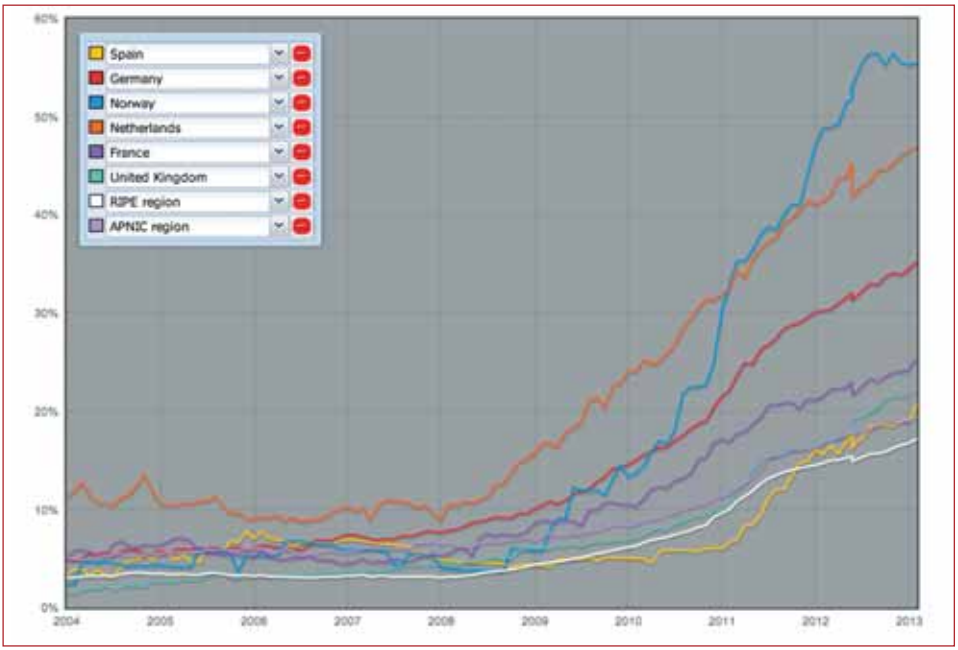
Fase 1 - Assegnazione Indirizzi IPv6 (fonte: RIR)

Dal 2009 si osserva una fortissima accelerazione di allocazione di indirizzi v6 a utilizzatori finali nelle zone più sviluppate del pianeta - RIPE, APNIC e ARIN ovvero Europa, Asia, Nord America e Medio Oriente. Non si tratta ancora di effettivo utilizzo, ma di un'iniziale preparazione ad adottare il nuovo protocollo.



[8] www.cisco.com/web/solutions/sp/vni/vni_forecast_highlights/index.html

Fase 2 - Raggiungibilità in IPv6 (fonte: RIPE)
Crescenti anche le percentuali di coloro i quali annunciano la propria rete (Autonomous System per la precisione) come raggiungibile in IPv6 alla tabella di routing globale. Nella figura[9] si nota come alcuni Paesi europei siano molto avanti in questo senso, mentre l'Italia (azzurro) si mantiene nella media di tutta la zona RIPE (bianco). A partire dal 2009 anche in questo caso si ha una tendenza significativamente in aumento. Chi pubblicizza le proprie reti come raggiungibili in IPv6 alla tabella di routing globale è ad un passo dall'utilizzo effettivo.



Fase 3 – Attivazione IPv6 sui dispositivi (fonte: Cisco)
Il passo successivo da fare è attivare IPv6 sui propri dispositivi: Indirizzi IPv6 sulle interfacce, ACL, protocolli di routing e altre funzionalità legate al nuovo protocollo. Tramite il monitoraggio di dispositivi in uso presso alcune migliaia di clienti, Cisco ha visibilità di quanti abbiano attivato funzionalità IPv6. Anche in questo caso, dal 2011 si vede un'impennata nell'attivazione, indice dell'utilizzo in produzione di IPv6.

[9] http://v6asns.ripe.net/v/6?s=ES;s=DE;s=NO;s=NL;s=FR;s=GB;s=_RIR_RIPE_NCC;s=_RIR_APNIC

Fase 4 – Utilizzo effettivo (fonte: Google)

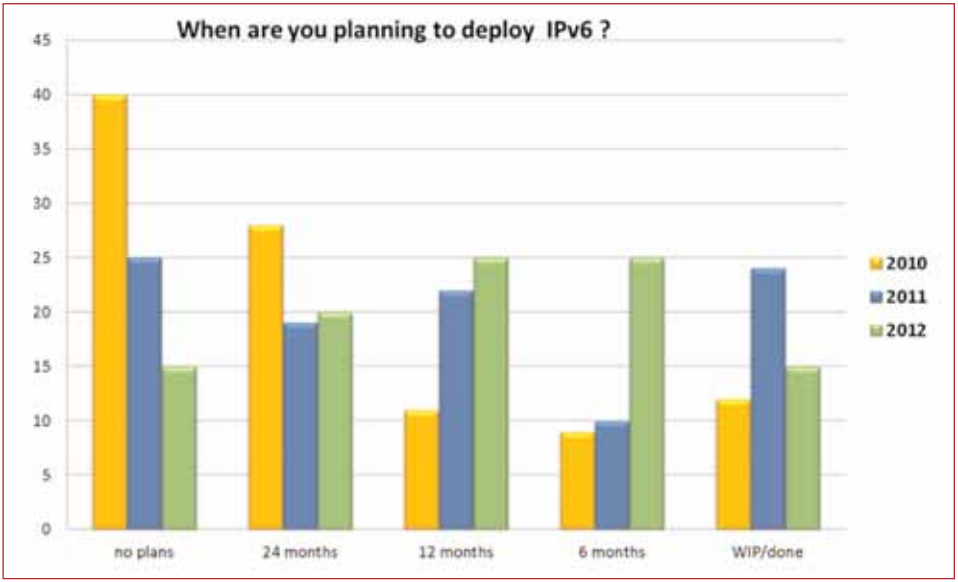
L'ultima fase è quella dell'effettivo utilizzo, e questo grafico di Google[10] mostra come alla fine del 2012 il traffico IPv6 - misurato con il numero di ricerche fatte su Google provenienti da terminali IPv6 - abbia sfondato la barriera dell'1%. Se in assoluto è un numero piccolo, in prospettiva è un'enorme crescita, di circa il 2500% rispetto a cinque anni prima[11].

[10] www.google.com/intl/en/ipv6/statistics.html

[11] blogs.cisco.com/news/ipv6-deployment-threshold-reached/

Traendo le conclusioni, non c'è motivo per cui tutti o qualcuno di questi indicatori registri un'inversione di tendenza nei prossimi mesi o anni.
IPv6 è una realtà. I dispositivi che utilizziamo lo supportano. Una buona parte delle nostre reti è abilitata, molti ISP lo offrono già e moltissimi sono in procinto di farlo. L'imminente connettività 4G porterà IPv6 sulle reti degli operatori mobili e sui nostri smartphone, prestissimo. La maggior parte dei contenuti a cui accediamo, social network (es. Facebook), o servizi erogati da content provider mondiali (es. Youtube/Google), sono accessibili già oggi con il nuovo protocollo. IPv6 è già arrivato.
L'industria non ha dubbi che IPv6 sia la strada da percorrere. Non ci sono altre soluzioni, non esistono strade alternative per permettere l'esplosione di Internet, una nuova ondata d'innovazione, Internet of Things e chissà quanto altro ci aspetta nel breve futuro. Che IPv6 sia il futuro è opinione unanimemente condivisa. Network Address Translation (NAT), Carrier Grade NAT (CGN) e Address Sharing non sono soluzioni che possono durare per sempre e soprattutto, presto, man mano che i vecchi indirizzi IPv4 saranno sempre più scarsi, queste tecniche introdurranno sempre più problemi e sempre meno benefici.

Che cosa fanno gli utilizzatori finali?



Cisco l'ha chiesto a un campione rappresentativo dei propri clienti: se nel 2010, quattro su dieci hanno dichiarato di non avere nessun piano d'implementazione, la percentuale dei "non faccio nulla" cala al 15% nel 2012, indice del fatto che il restante 85% si sta comunque muovendo seppur con strategie e tempistiche differenti. Sempre nel 2012 uno su due dichiara di aver deciso di implementare il nuovo protocollo nei prossimi sei o dodici mesi.
Altre statistiche circa l'adozione a livello mondiale da parte di utenti residenziali, aziende e altro sono disponibili all'URL http://6lab.cisco.com/stats

Che cosa significa implementare IPv6?

Innanzitutto c'è da ricordare un elemento fondamentale: IPv4 ed IPv6 non sono compatibili fra loro. Non si parlano, non c'è comunicazione. Una risorsa disponibile in v4 non può essere fruita da un utilizzatore che utilizza esclusivamente v6 (e viceversa, naturalmente) a meno di una conversione, che generalmente va a sfavore della qualità.
Quando si parla di implementare IPv6 nella stragrande maggioranza dei casi si parla di affiancare il nuovo protocollo al già esistente IPv4, sulla stessa infrastruttura, sugli stessi dispositivi che quindi invece di processare e instradare traffico IPv4, faranno lo stesso per entrambi i protocolli. Esattamente quello che succede già oggi sui PC di ultima generazione (Windows 7 di default utilizza entrambi i protocolli, e lo stesso per Mac OS X a partire da v10.3), che sulle schede di rete hanno attivi entrambi gli stack IP, sia v4 sia v6. Per questo motivo si parla di implementazione "Dual Stack", e in linea di massima processare entrambi i protocolli NON crea un problema di performances degli apparati.
Non occorre quindi ricostruire da zero le reti, anche perché la stragrande maggioranza dei produttori (di apparati di rete come di personal computer e altri dispositivi) offre supporto IPv6 già da molto tempo.
Per un'azienda una strategia può essere quella di determinare quali apparati sono in grado di supportare le funzionalità necessarie e fino a quale punto e stabilire una strategia d'implementazione; questa può essere implementare prima IPv6 sulla propria presenza Internet e in seguito espandere il nuovo protocollo fin sulla rete interna, piuttosto che partire dalla rete interna per poi espandere il dual stack fino alla periferia della rete. Il primo approccio, quello di partire dalla presenza internet è il più

popolare: è rapido, economico, limitato come impatto e risolve il problema più sentito, in altre parole quello di affacciarsi a internet ed essere raggiungibili sia da chi utilizza il nuovo protocollo sia da chi non ha ancora fatto la transizione.

E la sicurezza?

Un mito da sfatare è che IPv6 è intrinsecamente più sicuro di IPv4 perché incorpora funzionalità di sicurezza e cifratura. Non è così, anzi potremmo addirittura prendere in considerazione il fatto che IPv6 è molto più giovane come protocollo, e di conseguenza in linea di massima c'è meno esperienza. Abbiamo comunque una grande opportunità: applicare a IPv6 tutte quelle lezioni circa la sicurezza che abbiamo imparato in oltre trent'anni di reti IP. Finora le reti sono state costruite senza pensare alla sicurezza e solo in seguito ci si è resi conto di determinati elementi che andavano presi in considerazione, e che quindi sono stati "rattoppati". Con IPv6 abbiamo la possibilità di implementare reti pensando prima alla sicurezza, in altre parole a tutto quello che già conosciamo in materia. Questo non è un elemento da sottovalutare.

Un'altra falsa credenza è che avendo IPsec integrato IPv6 garantisca la segretezza dei dati trasportati. Anche questo è un mito da sfatare: è vero, IPv6 ha IPsec integrato, ma l'uso è facoltativo, e va valutato su quali segmenti val la pena abilitarlo – introdurre IPsec su una LAN comporterebbe enormi problemi di gestione e di complessità, impedendo ai firewall un corretto funzionamento o impedendo la gestione della Quality of Service, creando più problemi che benefici. IPsec, anche in ambito IPv6 andrà implementato per attraversare quei segmenti di infrastrutture pubbliche o condivise.

Altre considerazioni di sicurezza restano sostanzialmente invariate, come la valenza di ACL, Firewall ed IPS, tecnologie che comunque vanno adeguate al nuovo protocollo, in altre parole le policy di sicurezza vanno adattate per offrire le stesse funzionalità anche in IPv6.

Attacchi di tipo applicativo come Virus, Worm o altro malware simile restano invariati su un'infrastruttura IPv6. Essi sono indipendenti dallo stack v4 o v6, di conseguenza resta anche invariata la valenza di tecnologia di filtraggio email, antivirus e antimalware in genere.

È da notare come una subnet IPv6 abbia una quantità molto maggiore di

indirizzi IP (sono 2^64), quindi quegli attacchi basati sulla scansione della subnet nella speranza di individuare obiettivi da attaccare teoricamente verrebbero meno perché per una scansione di 2^64 host ci vorrebbe un tempo enormemente lungo. Attenzione, l'attacco resta valido, sono solo le tecniche di scansione che cambieranno, sfruttando DNS, DynDNS, indirizzamenti facili da ricordare (CAFE, F00D, BEBE, …) che ragionevolmente sarebbero privilegiati, e altre tecniche. L'assunto secondo il quale "la subnet è così estesa che non è possibile farne la scansione e individuare gli obiettivi" è una strategia miope.
Altri attacchi, Man-In-The-Middle, attacchi applicativi, sniffing, Rogue Devices, Flooding, restano invariati come efficacia e possono essere mitigati allo stesso modo in IPv4 come in IPv6.
Val la pena ricordare che le infrastrutture di rete sono costruite strato su strato. Il protocollo IP opera al livello 3, indipendentemente dalla versione 4 o 6. Tutti quegli attacchi che operano al livello 2, quindi a un livello inferiore e che mirano a compromettere i livelli superiori vanno mitigati esattamente come prima e con funzionalità apposite. Per questo motivo Cisco ha introdotto First Hop Security (FHS) una famiglia di funzionalità di sicurezza che indirizzano il Link Layer (livello 2) pensate appositamente per IPv6. Queste assicurano la solidità e sicurezza dell'infrastruttura di rete fin dalle fondamenta.
La sicurezza delle reti è un argomento complesso, e la sua applicazione in un ambito nuovo come l'IPv6 non fa che aumentarne la apparente complessità. Lo stesso è già accaduto, e chi scrive se n'è occupato in passato, per le reti Wireless, una novità di una decina d'anni fa e per la Voce su IP successivamente, che per molto tempo ha monopolizzato l'attenzione degli esperti di sicurezza e che oggi è tranquillamente utilizzata da tantissimi. Lo stesso sarà per IPv6 e questa breve monografia vuole solo fare luce e chiarezza su quella che dev'essere la priorità in questo momento: in altre parole fare dell'IPv6 una priorità.
Chi desidera già da subito approfondire gli aspetti di sicurezza dell'IPv6 idealmente dovrebbe farlo in maniera funzionale a una prossima implementazione, dopo aver stabilito una strategia di adozione, facendo dei test in laboratorio o in segmenti limitati della propria infrastruttura di rete, traendo lezioni e conclusioni da questi e naturalmente prendendo in considerazione gli aspetti di sicurezza, in maniera pervasiva. Una più autorevo-

le ed istituzionale esposizione dell'argomento IPv6 Security è offerta nell'esaustiva pubblicazione "IPv6 Security" di Vyncke-Hogg[12], i cui principi fondamentali sono riportati in un intervento di uno degli autori le cui slide sono pubblicamente disponibili[13].

[12] www.amazon.com/IPv6-Security-Scott-Hogg/dp/1587055945

[13] www.slideshare.net/IKTNorge/eric-vyncke-ipv6-security-in-general

Il salvataggio delle informazioni e la continuità di servizio

a cura di *Alessio Pennasilico* e *Davide Del Vecchio*

In Italia esiste una legge, la cosiddetta legge Privacy, tecnicamente il D.Lgs. 196/2003 che prescrive diversi obblighi in egual modo alle aziende ed ai professionisti, che in qualche modo trattano dati che riguardano terzi. Lo scopo di questa legge è, ovviamente, tutelare il soggetto più debole, che deve vedere gestiti i suoi dati in modo adeguato.

Nell'"Art. 34. Trattamenti con strumenti elettronici", alla lettera f) si legge la necessità di effettuare l'"adozione di procedure per la custodia di copie di sicurezza, il ripristino della disponibilità dei dati e dei sistemi;".

Questa misura viene spesso interpretata come esigenza di eseguire una copia di sicurezza, fare backup. Leggendo, invece, la legge ed i suoi allegati si evince che lo scopo è quello di porre chi tratta i dati altrui in grado di poter continuare a trattare correttamente quei dati in caso di incidente.

Basti immaginare, infatti, quale danno verrebbe arrecato ad un'azienda il cui commercialista cancellasse erroneamente i dati, ad un paziente il cui medico subisse la rottura del disco sul quale conserva le informazioni che lo riguardano, ad un cliente il cui avvocato cancellasse erroneamente i file con gli atti di un procedimento.

Questi sono solo alcuni degli scenari che si possono dipingere, ovviamente, senza voler coinvolgere la classica multinazionale con decine o centinaia di server e database.

Il guasto di un supporto magnetico, la perdita di un supporto rimovibile quale un DVD o una chiavetta USB, l'erronea cancellazione o sovrascrittura di un file sono eventi tanto banali, quanto frequenti, che possono mettere a serio rischio la continuità operativa di un professionista o di una azienda e danneggiare, a volte irreparabilmente, chi quei dati li aveva affidati aspettandosi che venissero trattati secondo canoni ben precisi.

Si pensi, per restare nell'esempio precedente, ad un avvocato che accidentalmente perdesse l'unica copia di un atto che sarebbe stato necessario depositare il giorno seguente. Il valore di un dato è, spesso, legato al momento specifico in cui tale dato deve essere disponibile.

Risulta piuttosto sorprendente, nel 2013, rilevare che ancora molte aziende non hanno un piano per il corretto ripristino dei dati e dell'operatività aziendale. Ancora più curioso il fatto che spesso il motivo che spinge a

rivedere le politiche di gestione dei dati sia legato al volersi adeguare ad una norma, come il già citato D.Lgs. 196/2003, e non al voler tutelare il proprio business.
Che differenza corre, quindi, tra l'effettuare i salvataggi ed il predisporre un piano di ripristino dell'operatività?

Quali parametri vengono troppo spesso ignorati?
Innanzitutto salvare i dati su un supporto rimovibile, quale può essere un nastro o un disco USB non è sempre sinonimo di poter ripristinare quel dato.
Quanti verificano che ciò che si aveva intenzione di salvare, sia stato effettivamente salvato in maniera corretta? Quanti, tra quelli che verificano, lo fanno in modo regolare?

Immagine di un IBM 726, uno dei supporti di backup del 1952.[1]

Dando per certa la presenza delle informazioni volute sul supporto scelto, quanti prendono in considerazione gli strumenti necessari per poter poi accedere a quei dati? Se è stato, ad esempio, salvato un database, per poterlo leggere, in caso di rottura del computer o del server, servirà un altro computer o server con lo stesso programma, nella stessa versione, in grado di importare quelle informazioni e renderle di nuovo disponibili. A volte la lettura del file in sè potrebbe richiedere pochi minuti, ma ripristinare il contesto adatto per rendere i dati presenti in quel file usufruibili, potrebbe richiedere alcuni giorni di attesa e di lavoro.

[1] Immagine riprodotta per cortesia di IBM e reperibile all'indirizzo http://www.flickr.com/photos/ibm_media/7203083974/ rilasciata con licenza Creative Commons]

Nell'Allegato B del D.Lgs. 196/2003, inoltre, vi sono persino delle indicazioni in merito alla frequenza con cui bisognerebbe effettuare i salvataggi ed ai tempi di ripristino che devono essere garantiti. L'art. 18, infatti, recita che "Sono impartite istruzioni organizzative e tecniche che prevedono il salvataggio dei dati con frequenza almeno settimanale.", mentre l'art. 23 sottolinea che devono essere "adottate idonee misure per garantire il ripristino dell'accesso ai dati in caso di danneggiamento degli stessi o degli strumenti elettronici, in tempi certi compatibili con i diritti degli interessati e non superiori a sette giorni.". Non avere una copia di quei dati, quindi, ma garantirne l'accesso in tempi certi: questo tecnicamente viene raccontato da un parametro che si chiama RTO, Recovery Time Objective, vale a dire il tempo necessario a tornare operativi. Purtroppo si rileva troppo spesso la totale assenza non solo del porsi questa domanda ma anche nell'organizzazione del proprio piano di salvataggio.
L'altro parametro troppo spesso ignorato è l'RPO, il Recovery Point Objective cioè quanto vecchi, al massimo, potranno essere i dati ripristinati. Risulta evidente, infatti, che un piano che permetta di tornare operativi in pochi minuti, ma con informazioni aggiornate a diversi anni prima, sia tutt'altro che efficiente o desiderabile.

Quale è la criticità dei supporti di salvataggio?

Sempre sul campo è possibile osservare come troppo spesso la sicurezza dei supporti contenenti i salvataggi venga totalmente ignorata. Il server che contiene tutti i file viene protetto con firewall, antivirus, IDS, IPS e diverse altre misure. Contemporaneamnete il supporto che contiene le stesse informazioni giace dimenticato su una mensola di uno scaffale del corridoio, dove chiunque può transitare, ospiti compresi e dove chiunque potrebbe asportarlo senza che nessuno se ne accorga. I supporti vanno protetti, adottando le idonee misure di protezione fisica, affinché nessuno possa accedere a quei dati nella loro copia di salvataggio, tanto utile per un attaccante quanto l'originale sui server.
Troppo spesso, poi, si notano altri comportamenti errati: supporti per il salvataggio nella stessa stanza dei server, quando non addirittura appoggiati sul server stesso. Risulta evidente, in questi casi, che un piccolo incendio, una perdita d'acqua, ad esempio, potrebbero compromettere contemporaneamente sia il server che gestisce i dati che la copia di sicurezza.

Per questa ragione è consigliabile tenere sempre una copia del backup "off-site", vale a dire all'esterno dell'azienda. I più organizzati utilizzano società specializzate per il trasporto dei supporti, contenuti in appositi contenitori sigillati e non facilmente apribili da chi non possiede le chiavi, che conservano poi tali contenitori in equivalenti delle cassette di sicurezza. Troppo spesso invece la soluzione "fai da te" si traduce nel conservare, senza alcun accorgimento tale copia a casa di uno dei dipendenti o del titolare dell'azienda, mettendo quindi a rischio, di nuovo, la sicurezza fisica del supporto e delle informazioni in esso contenute.
Altri preferiscono, invece, affittare degli spazi in strutture terze ove conservare la copia dei dati per preservare l'integrità delle informazioni anche in caso di incendi più gravi o terremoti.

Quale supporto per i miei salvataggi?

Se tradizionalmente, infatti, le copie di sicurezza venivano effettuate su nastri magnetici, oggi le alternative sono molteplici: nastri, CD e DVD, dischi USB, storage proprietari o condivisi in datacenter di Internet Service Provider, fino a soluzioni cloud-based.
Anche in questo caso è bene porsi diverse domande prima di scegliere la soluzione adatta.
Dove sto salvando i miei dati? Con che grado di riservatezza? Come potrò accedervi in caso di necessità, per poterli nuovamente utilizzare?
Non è raro, infatti, scoprire che è stata adottata la buona pratica di utilizzare uno spazio cloud per conservare i salvataggi, abbinando l'uso dell'encryption delle informazioni per proteggerne la riservatezza e confidenzialità. Salvo scoprire poi che la chiave per accedere alle informazioni è conservata in singola copia sui server aziendali, con il risultato che in caso di disastro e con i server aziendali resi inutilizzabili, tali dati saranno protetti non solo da occhi indiscreti, ma anche dal legittimo proprietario che non sarà più in possesso delle chiavi per poterli decifrare.

Lo scenario in Italia

Una ricerca di F-Secure ha dimostrato come al 41% degli intervistati, almeno una volta, è capitato di perdere dati importanti.
La stessa ricerca mostra come solo il 50% del campione esegue regolar-

mente un backup dei propri dati e la tendenza, purtroppo, cambia di poco se si guarda al settore delle piccole e medie imprese italiane.
Between, in un recente studio sul segmento SME italiano, evidenzia come oltre il 30% delle aziende effettui raramente (meno di una volta al mese) copie di sicurezza dei propri dati; solo il 12% esegue un backup giornaliero. Inoltre (fonte: Acronis) solo il 53% dei professionisti IT di piccole e medie imprese ha fiducia nella propria strategia di ripristino dopo un'eventuale emergenza. I restanti intervistati prefigurano invece lunghi tempi di fermo e la mancanza di procedure certe per il ripristino dei dati e delle applicazioni. Questo significa che oltre il 95% delle SME italiane non ha la certezza di

Fonte: ICT Monitor Business 2012 di Between

poter recuperare in modo efficace i dati del giorno prima.
Quasi la metà (45%) degli intervistati ha individuato nella carenza di budget e risorse IT i maggiori ostacoli, mentre un quarto delle persone ha dichiarato di non avere l'appoggio del proprio team dirigenziale.
Il 2012 ha rafforzato ulteriormente un trend iniziato dal 2010: i primi tagli per contenere i costi e fronteggiare la crisi economica partono dall'ICT. Nel 2010 il 60% delle aziende SME dichiarava di voler ridurre la spesa economica per telecomunicazioni ed informatica, nel 2012, il numero delle

aziende che dichiara di voler ridurre la spesa (o addirittura, rimandarla a tempi migliori) è salita ad oltre l'80%.
In questo contesto il prezzo resta una variabile critica, senza però rischiare su soluzioni che promettono forti risparmi, ma con un incertezza sul brand e sulla specializzazione di prodotto.
Gli ultimi trend mostrano come il 66% delle aziende sta valutando in modo positivo la possibilità di dotarsi di un sistema di backup basato su piattaforma cloud che permetta di assicurare i dati delegando l'onere di gestione ad un fornitore dal brand solido.

Conclusioni

Le tecnologie per poter effettuare delle efficaci copie di sicurezza delle informazioni gestite, utilizzabili in tempi rapidi, esistono. Dai backup su supporti rimovibili, alle repliche di macchine virtuali su scala geografica o "in the cloud" esistono decine di strategie adatte a proteggere uno degli asset fondamentali di ogni azienda moderna, sia essa una microimpresa, una PMI o una multinazionale: le informazioni.
I costi giocano di certo un ruolo fondamentale nella scelta della strategia adatta, tuttavia troppo spesso vengono ignorate le reali esigenze di business a favore di soluzioni che risultano adatte solo a fronte di una analisi superficiale e tesa a soddisfare una legge o una policy aziendale e non le reali necessità dell'azienda.
Da molti anni si auspica una maggiore consapevolezza ed una più puntuale gestione di questo tema, tuttavia non si sono rilevati sul campo grandi cambiamenti, se non nella maggior quantità di prodotti disponibili.
Probabilmente, per migliorare questa situazione, più che all'adozione di diverse tecnologie bisognerebbe puntare ad una maggiore consapevolezza di cosa va protetto e come, per poi scegliere, tra le tante possibilità, non solo il prodotto, ma anche il processo organizzativo adatto.

Gli autori del Rapporto Clusit 2013

Luca Bechelli è consulente indipendente nel campo della sicurezza informatica dal 2000, da alcuni anni è docente del Master in Tecnologie Internet del Dipartimento di Ingegneria dell'Università di Pisa per la parte di esercitazione del corso di sicurezza informatica. Con aziende partner svolge consulenza per progetti nazionali ed internazionali su tematiche di 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 R&D con aziende nel campo della sicurezza e tramite collaborazioni con enti di ricerca. È co-autore di pubblicazioni scientifiche e tecnico/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.

Matteo Cavallini lavora nel campo della sicurezza informatica da oltre 15 anni per aziende private ed enti governativi. Attualmente è il Responsabile dell'Area Security di Consip e il Responsabile della Struttura Operativa dell'Unità Locale di Sicurezza MEF/Consip, il CERT interno del Ministero dell'Economia e di Consip.
Dal 2010 è il referente delle attività di Consip nel campo della cloud security e, a luglio 2011, Consip ha pubblicato il suo studio dal titolo: "Cloud Security: una sfida per il futuro". Cavallini è anche Vice Presidente della Cloud Security Alliance - Italy Chapter ed è membro del direttivo di AIPSI.
Precedentemente, ha lavorato al progetto GovCERT.it (ora CERT_SPC) presso il CNIPA e come responsabile della sicurezza perimetrale in Consip. Sempre presso il CNIPA ha svolto il ruolo di esperto senior di sicurezza della Commissione di Collaudo dei servizi di sicurezza del Sistema Pubblico di Connettività. Dal 2000 al 2004 è stato IT Security Project Manager in Consip realizzando alcuni dei progetti più critici dal punto di vista della sicurezza informatica.

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 @ Mediaservice.net, un'azienda 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).
Nel novembre del 2012 fonda, insieme ad un gruppo di professionisti senior, Security Brokers.
Dal 2003 Raoul ha iniziato la sua collaborazione con l'agenzia delle Nazioni Unite “UNICRI”, lavorando al progetto “HPP” (Hackers Profiling Project); oggi il suo ruolo presso UNICRI è quello di “Senior Advisoron Cybercrime Issues”.
Dal 2010 Raoul è membro del PSG (Permanent Stakeholders Group) di ENISA, European Network & Information Security Agency, con mandato sino al 2015.

Stefano Cremonesi si è laureato nel 1994 in Ingegneria Elettronica, con specializzazione Informatica, presso il Politecnico di Milano. Da subito ha iniziato ad occuparsi di progettazione e sviluppo dei sistemi informativi in ambienti ospedalieri presso il Consorzio di Bioingegneria ed Informatica Medica. La dimensione delle aziende coinvolte (ospedale San Matteo di Pavia, ospedale di Circolo di Varese, Bambin Gesù di Roma, ospedali Riuniti di Bergamo) e la necessità di affrontare a 360 gradi tutte le fasi di un progetto di informatizzazione sono state la base fondamentale per l'identificazione delle problematiche che lo hanno a vario titolo coinvolto nella sicurezza informatica. Come Project Manager si è successivamente occupato di progettare sistemi informatici in ambito retail, acquisendo competenze nella gestione e sviluppo di progetti di business continuity. Come consulente si è occupato dello progettazione e realizzazione della server consolidation della server farm dell'ospedale di Legnano. Attualmente è Project Manager dell'area Tecnologica del gruppo ospedaliero Multimedica occupandosi della progettazione, realizzazione e gestione di tutta l'infrastruttura tecnologica del gruppo.

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.

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 e membro del Direttivo del Clusis (l'Associazione Svizzera per la Sicurezza delle Informazioni).

Fabio Guasconi, Laureatosi in Informatica a Torino, è attivo da oltre 10 anni nella consulenza sulla sicurezza delle informazioni, con particolare attenzione per le tematiche di analisi del rischio, di organizzazione della sicurezza e verso le norme internazionali, alla cui stesura contribuisce attivamente. Ha ottenuto le qualifiche di CISA, CISM, ITILv3 ISFS, ed è lead auditor sullo schema ISO/IEC 27001, di cui ha curato la traduzione in italiano. Ha maturato un'esperienza significativa sulla sicurezza dei dati delle carte di pagamento come QSA in ambito PCI-DSS, tema sul quale è coautore di un quaderno Clusit. Partecipa regolarmente ad eventi e pubblicazioni nazionali ed estere sulla sicurezza. Attualmente presiede il comitato italiano ISO/IEC JTC1 SC27 per la sicurezza delle informazioni di UNINFO, ne è membro del consiglio direttivo, così come per Clusit, e partecipa attivamente ad AIIC e ISACA Roma.

Antonio Ieranò Security Consultant, Speaker, Trainer e Blogger per passione si occupa di sicurezza informatica da oltre un decennio. Ha coperto ruoli diversi in diverse società internazionali tra cui European Security Evangelist e PM presso Cisco Systems con l'incarico di analizzare il panorama europeo della sicurezza e delle minacce informatiche. Antonio possiede una profonda conoscenza di tecnologie IT e di prodotti e questioni legate alla sicurezza dal punto di vista tecnico e legale. Prima di lavorare in Cisco attraverso l'acquisizione IronPort nel gennaio del 2007 – ha ricoperto diversi incarichi a livello europeo in Brightmail prima e poi in Symantec.

Marco Misitano, si è occupato professionalmente di sicurezza dell'informazione da metà degli anni 90, esplorando gli elementi piu disparati, fra cui sicurezza delle reti Wireless, tecnologie di Admission Control, sicurezza delle soluzioni VoIP, IPv6. Ha all'attivo diverse pubblicazioni. Si è occupato anche di Videosorveglianza, Controllo Accessi e della Convergenza fra Sicurezza Fisica e Logica con particolare attenzione al ruolo dell'infrastrutura di rete. Fra i primi certificati CISSP Italiani, dal 2001 lavora per Cisco dove ha la responsabilità della accelerazione di nuove tecnologie sul mercato in Europa, Medio Oriente, Africa e Russia. Socio Clusit di lunga data, è al suo terzo mandato come consigliere del Comitato Direttivo. È Presidente del Capitolo Italiano di (ISC)2 ed è stato fra i soci fondatori del capitolo italiano di ISSA.

Paolo Passeri si occupa di sicurezza informatica da oltre 15 anni. L'interesse per la materia è nato dopo la Laurea in Fisica presso l'Università degli Studi di Milano, ed è stato messo a frutto grazie a numerose esperienze di consulenza e project management per diversi system integrator.
Attualmente occupa il ruolo di Senior System Engineer presso Lastline, Inc. azienda USA leader nel contrasto delle forme di malware avanzato.
Nel corso della sua carriera ha prestato attività di consulenza e realizzato progetti di sicurezza per Operatori TLC,

Pubbliche Amministrazioni e Importanti Gruppi Bancari, venendo a contatto con ambienti e problematiche eterogenee, e accumulando un'ampia esperienza di consulenza, disegno e realizzazione di soluzioni di sicurezza in diversi contesti.
La sua sfera di competenza copre il mondo della sicurezza informatica a 360 gradi, con particolare attenzione all'analisi del malware, al contrasto del Cyber Crime, e alle problematiche di sicurezza generate dalle nuove tecnologie quali mobile security e social network.

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.

Mario Salvatori, giornalista, è stato per 18 anni il direttore dei mensili Assicura e AziendaBanca e il responsabile di tutte le attività collaterali convegni, corsi di formazione, ricerche, libri e delle attività on line. Ora segue esclusivamente lo sviluppo della informazione professionale nel settore assicurativo con Assicura On Line, iniziativa innovativa che comprende sito web, newsletter via email, social network. Giornalista dal 1980, è appassionato di innovazione distributiva, organizzativa e tecnologica nel settore finanziario e curioso dei nuovi media.

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. È 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".

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 e Direttore Generale di Security Brokers, essendo tra i soci fondatori di entrambe le aziende. È membro del gruppo di lavoro "CyberWorld" nell'ambito dell'Osservatorio per la Sicurezza Nazionale del Centro Militare di Studi Strategici. È 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 Rapporti Clusit 2012 e 2013 sulla sicurezza ICT in Italia, oltre ad essere l'autore del focus on "Social Media Security", 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, le organizzazioni e le persone che hanno contribuito alla realizzazione del Rapporto Clusit 2013.
In particolare: 3BitCom, ADS, Aglea, AISIS, Alba ST, Alfa Group, ASIS International, Assintel, AT4M, Attachmate, Biteam, Azienda Napoletana Mobilità, BSC Consulting, Cisco Systems, CLUSIF, CNAIPIC, CRAG Partners, Credit Suisse, CSQA Certificazioni, Deloitte ERS, Electrolux, eMaze Networks, ENISA, Eris Consulting, Future Time, Hypergrid, IBM, iDialoghi, IFOA, Infocert, Insiel, Innovery, Iside, Italia Lavoro, Joram, Kaspersky Lab, KPMG, KPMG Advisory, Logical Security, McAfee, Mediaservice, MELANI, Michael Slim International, Neonevis, Net1 di Fornaro Natale, NexSoft, Networking & Security Consulting, NTT DATA, Obiectivo Technology, Oracle, Oracle Community For Security, Palo Alto Networks, P.D.C.A., Present, Prolan, Protiviti, Reality Net, SafeNet, Security Brokers, Selex ES, Servizi Informatici Bancari Trentini, Shorr-Kan, SISAL, SonicWALL, Spike Reply, Systemeng, Tech Gap, Trend Micro, Xech.
E ancora: Gianluigi Angotti, Davide Aprea, Andrea Ardizzone, Orlando Arena, Gabriele Baduini, Pasqualino Baldassarre, Giuseppe Bartone, Luca Bechelli, Simona Bechelli, Bruno Bernardi, Giovanni Besozzi, Gianluca Bocci, Luca Boselli, Jonathan Brera, Giorgio Brunelli, Danilo Bruschi, Simone Bruschi, Fabio Bucciarelli, Francesco Buzzoni, Claudio Caccia, Cristiano Cafferata, Gianpietro Calai, Paolo Capozucca, Davide Casale, Matteo Cavallini, Daniela Cembi, Angela Cera, Raoul Chiesa, Mauro Cicognini, Fabrizio Cirilli, Ombretta Comi, Garibaldi Conte, Stefano Corazza, Corradino Corradi, Paolo Cremascoli, Stefano Cremonesi, Luigi Cristiani, Giulia Cucuzza, Domenico Cuoccio, Alessandro Da Re, Maurizio Dell'Oca, Davide Del Vecchio, Gianna Detoni, Francesco Di Maio, Fabrizio Di Narda, Francesco Fortunato Donato, Mattia Epifani, Alfredo Esposito, Gabriele Faggioli, Mariangela Fagnani, Valentina Falcioni, Alessandro Feltrin, Evelyn Ferraro, Enrico Ferretti, Alessandro Fiorenzi, Ivano Gabrielli, Cesare Gallotti, Domenico Garbarino, Loredana Gazzaniga, Massimo Giaimo, Paolo Giardini, Fabio Guasconi, Antonio Ieranò, Davide Lattuada, Alessandro Lega, Salvatore Lombardi, Simone Maga, Michele Magri, Massimo Manara, Alberto Manfredi, Riccardo Mangiaracina, Luca Marzegalli, Raffaele Mazzitelli, Marco Mella, Paolo Mereghetti, Andrea Merolla, Paola Meroni, Diego Mezzina, Lorenzo Migliorino, Marco Misitano, Flaviano Molinari, Gabriella Molinelli, Giovanni Montoncello, Giorgio Mosca, Cristian Nardella, Roberto Obialero, Pamela Pace, Roberto Pachì, Marco Palazzesi, Francesco Palmisano, Paolo Passeri, Alessio Pennasilico, Alessandro Peta, Luca Pierro, Sebastiano Placidini, Daniele Poma, Franco Prosperi, Cesare Radaelli, Silvano Ronchi, Mario Salvatori, Luca Sambucci, Fabio Saulli, Roberto Sarra, Giampaolo Scafuro, Sofia Scozzari, Francesco Spadi, Valentino Squilloni, Claudio Squinzi, Tommaso Stranieri, Francesco Suglia, Stefano Tagliabue, Gigi Tagliapietra, Paola Tamburini, Carla Targa, Claudio Telmon, Enzo Maria Tieghi, Francesca Tolimieri, Alessandro Vallega, Davide Varesano, Giovanni Battista Vassallo, Francesco Vecchione, Alessandra Venneri, Salvatore Ventura, Gaia Vinciguerra Frezza, Francesco Maria Vizzani, Davide Yachaya, Giulia Zanutto, Andrea Zapparoli Manzoni, Francesco Zenti.
Un ringraziamento particolare va alla Polizia Postale e delle Comunicazioni ed al suo Direttore, Antonio Apruzzese.

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 – 9a 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, Ministero dell'Interno, Ministero della Giustizia, Ministero della Difesa, Ministero dell'Economia e delle Finanze, Ministero dello Sviluppo Economico, 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: CERT, 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, ISCÇ, 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 Cardi Eventi, la divisione "Conference" di Cardi Editore, organizzatore di eventi nel mondo finanziario e dell'Ict.

I docenti e relatori.
Nelle precedenti edizioni del Security Summit sono intervenuti oltre 300 docenti e relatori, rappresentanti delle istituzioni, docenti universitari, uomini d'azienda e professionisti del settore.

I partecipanti
Nel corso delle prime 4 edizioni, il Security Summit è stato frequentato da oltre 6.000 persone e sono stati rilasciati circa 4.000 attestati validi per l'attribuzione di crediti formativi (CPE) e 750 diplomi.

L'edizione 2013
La quinta edizione del Security Summit si terrà a Milano dal 12 al 13 marzo, a Bari il 16 aprile, a Roma il 5 e 6 giugno e a Verona il 3 ottobre.

Informazioni
Agenda e contenuti: info@clusit.it, +39 349 7768 882.
Altre informazioni: ceventi@cardieditore.com, +39 335 6528 130.
Video riprese e interviste precedenti edizioni:
http://www.youtube.com/user/SecuritySummit
Foto reportage:
http://www.facebook.com/group.php?gid=64807913680&v=photos
Sito web: http://www.securitysummit.it/
Security Summit Milano 2012: http://milano2012.securitysummit.it/
Security Summit Roma 2012: http://roma2012.securitysummit.it/
Security Summit Verona 2012: http://verona2012.securitysummit.it/

Finito di stampare per conto di Cardi Editore nel mese di marzo 2013

con il contributo di

www.securitysummit.it