Rapporto

2015

sulla sicurezza ICT
in Italia

Indice

Prefazione di Gabriele Faggioli **3**

Introduzione al rapporto **5**

Panoramica degli attacchi informatici più significativi del 2014 e tendenze per il 2015 7

- Analisi dei principali attacchi a livello internazionale 16
- Analisi degli attacchi italiani 30
- BIBLIOGRAFIA 34
- Analisi FASTWEB della situazione italiana in materia di cyber-crime e incidenti informatici 36
- Alcuni elementi sul cyber-crime in Europa e nel Medio Oriente (a cura di IBM) 54
- Rapporto 2014 sullo stato di Internet e analisi globale degli attacchi DDoS (a cura di Akamai) 62
- La Polizia Postale e delle Comunicazioni e il contrasto al cyber crime 81
- Il Nucleo Speciale Frodi Informatiche della Guardia di Finanza e il contrasto alle attività illecite su Internet 91

FOCUS ON 2015 99

- Internet of (Hacked) Things 100
- M-Commerce 107
- Bitcoin, aspetti tecnici e legali della criptovaluta 113
- Doppia autenticazione per l'accesso ai servizi di posta elettronica 122
- Lo stato della sicurezza dei siti web della pubblica amministrazione 130
- Il Regolamento generale sulla protezione dei dati: novità per i cittadini, le imprese e le istituzioni 140
- Cloud e sicurezza: profili legali 148
- Return on Security Investment 155
- L'impatto della Direttiva 263/agg.15 di Banca d'Italia sugli operatori del settore bancario 162

Gli autori del Rapporto Clusit 2015 ..... **169**

Ringraziamenti **182**

Descrizione CLUSIT e Security Summit **183**

Copyright © 2015 CLUSIT
Tutti i diritti dell'Opera sono riservati agli Autori e al Clusit.
È vietata la riproduzione anche parziale di quanto pubblicato
senza la preventiva autorizzazione scritta del CLUSIT.

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

Prefazione

Il rapporto CLUSIT che vi accingete a leggere è il risultato di un team di lavoro che ha analizzato una serie di documenti e di casistiche dalle quali emerge in tutta evidenza uno scenario preoccupante e in gran parte fuori controllo.

Purtroppo siamo ancora ben lontani dalla consapevolezza che l'adozione di comportamenti e contromisure adeguati alla mitigazione delle crescenti minacce "cyber" è elemento imprescindibile se si vuole tutelare la nostra pubblica amministrazione, le nostre imprese, i professionisti, i cittadini e, quindi, la nostra società e il nostro ordinamento.

A fronte comunque di importanti sforzi da parte delle Forze dell'Ordine di tutto il mondo, si sono ottenuti risultati poco significativi nel contrasto al cyber crime ed al cyber espionage, è mancata una strategia ampia di contrasto al fenomeno e ciò nonostante l'aumento dei rischi e delle minacce.

Se da un lato aumentano in percentuale rilevante gli investimenti in sicurezza informatica (saliti dell'8% nel 2014 a livello globale, nonostante il perdurare della crisi economica), il numero e la gravità degli attacchi (percepiti, visto che 2/3 degli attacchi si stima che non vengano neanche rilevati) continuano ad aumentare.

Considerando che in Italia i danni derivanti da attacchi informatici si stima ammontino a 9 miliardi di euro, si può capire l'importanza del rapporto CLUSIT: strumento essenziale per tutti gli operatori del settore che vogliono comprendere, ho hanno capito e vogliono approfondire, la rilevanza del tema della sicurezza informatica per la nostra vita e la vita del nostro paese.

In questo contesto, non è rilevante capire se si subirà un attacco quanto invece quando ciò accadrà e quali saranno, probabilmente, le modalità attraverso le quali si resterà vittime.

Il rapporto CLUSIT mira alla sensibilizzazione e alla formazione sul problema. Anche per questo abbiamo chiesto ad alcuni dei maggiori esperti italiani di approfondire dei temi particolarmente rilevanti e quindi nel rapporto sono presenti i "focus on", brevi saggi su argomenti oggi di attualità, come: internet oh things, bitcoin, ritorno dell'investimento in sicurezza, cloud.

2.500 copie cartacee, oltre 50.000 copie in elettronico e quasi 200 articoli pubblicati nel 2014, sono l'evidenza della rilevanza del rapporto CLUSIT ed è quindi importante diffonderlo, leggerlo, farlo conoscere, perché solo dalla consapevolezza può derivare la conoscenza del problema, la capacità di adottare scelte idonee e quindi la sicurezza nostra e di tutti.

Buona lettura

Gabriele Faggioli
Presidente CLUSIT

Introduzione al rapporto

Il rapporto che vi consegniamo, il quarto della serie, rappresenta come al solito la situazione italiana per quanto riguarda lo stato della sicurezza e dei relativi incidenti nell'anno appena trascorso. Quello di quest'anno è però il più ampio e corposo sinora realizzato, con 184 pagine.
Come sempre è stato messo a punto grazie alla preziosa collaborazione di un gran numero di soggetti pubblici e privati, commerciali e istituzionali, i quali hanno gentilmente condiviso col Clusit le informazioni e i dati di prima mano di cui disponevano, o condiviso le proprie specifiche esperienze sul campo: ma mai come quest'anno il rapporto ha potuto contare su un numero così elevato di contributi e contributori.

Il risultato di questo sforzo si può ben definire, senza falsa modestia, un quadro allo stato dell'arte del panorama italiano della cybersecurity: esso infatti attinge da fonti di prima mano che rappresentano tutto ciò che sappiamo sui fenomeni legati alla sicurezza ed alle sue violazioni accaduti durante il 2014 nel nostro Paese. Ciò non significa, attenzione, che esso rappresenti lo stato effettivo della sicurezza italiana: i dati e i fatti utilizzati per stilare il rapporto, infatti, non sono certamente tutti quelli effettivamente verificatisi durante l'anno, ma solo quelli rilevati direttamente o indirettamente dai diversi osservatori. Moltissimi incidenti, ed è purtroppo difficile stimarne il numero, non sono compresi nelle nostre analisi in quanto non noti alla comunità dei ricercatori, semplicemente perché non sono stati rivelati da coloro che li hanno subiti.

Purtroppo non esiste, almeno allo stato attuale delle cose, un organismo o autorità, nazionale o sovranazionale, avente il compito di raccogliere sistematicamente le segnalazioni degli incidenti occorsi ad imprese ed organizzazioni; né tantomeno vige l'obbligo generalizzato, per chi subisce un incidente, di segnalarlo. Il legislatore europeo ha attualmente imposto tale tipo di segnalazione (tecnicamente detta "data breach notification") solo per alcuni incidenti specifici legati al mondo dei fornitori di servizi di telecomunicazione, anche se si vorrebbe estendere un obbligo analogo anche ad altri settori. Nel frattempo dunque, in mancanza di una fonte ufficiale di dati sugli incidenti che sarebbe per definizione la più completa ed esaustiva, questo rapporto presenta la visione più accurata possibile del quadro complessivo della sicurezza nel nostro Paese.

Naturalmente il rapporto Clusit non è, e non sarebbe neanche giusto che fosse, l'unico momento di osservazione sullo stato della sicurezza nazionale. Ed in effetti negli ultimi anni è cresciuto il numero delle organizzazioni di mercato o accademiche che, ciascuna dal proprio specifico punto di osservazione, hanno iniziato a pubblicare studi analoghi. Per quanto riguarda l'Europa, lo scorso dicembre ENISA ha presentato il suo massiccio "European Threat Landscape 2014" che descrive ed analizza con grande profondità il panorama delle minacce globali ed i loro trend, effettuando valutazioni non solo tecniche ma anche

politiche; mentre per quanto riguarda l'Italia, a gennaio il CIS della Sapienza Università di Roma ha presentato un ampio studio, svolto assieme al Dipartimento per le informazioni e la sicurezza della Presidenza del Consiglio e all'Agenzia per l'Italia digitale, sulla "Consapevolezza della minaccia e capacità difensiva della Pubblica Amministrazione", orientato più ad analizzare le capacità organizzative di "readiness and preparedness" della nostra PA. Questa proliferazione di autorevoli studi specifici è naturalmente un bene, in quanto più informazioni si hanno su un fenomeno e più se ne giova la comunità di ricercatori che lo osservano e l'intero mercato che ne partecipa. Occorre tuttavia fare attenzione a non paragonare direttamente i risultati di studi differenti, per non correre il rischio di confrontare mele con pere se, come solitamente accade, le basi di osservazione e le metodologie di analisi adottate dai diversi ricercatori non sono equivalenti. Nei casi in questione i vari approfondimenti sono essenzialmente complementari tra loro, e quindi una loro lettura combinata permette di farsi la migliore idea possibile dello stato delle cose.

Detto ciò vi lasciamo alla lettura del nostro rapporto 2015 sulla sicurezza ICT in Italia, che consta di due parti principali. La prima è il rapporto vero e proprio, costituito principalmente dalla classificazione ed analisi (con rinnovata metodologia) degli incidenti rilevati in Italia, ed arricchito dai punti di vista di tre importanti aziende (Fastweb, IBM e Akamai) e di due Forze dell'ordine in prima linea nel contrasto ai fenomeni di cybercrime (Polizia Postale e Guardia di Finanza). La seconda presenta invece ben nove saggi, redatti da esperti del settore, che approfondiscono determinati aspetti specifici di temi particolarmente rilevanti nel contesto.

Panoramica degli attacchi informatici più significativi del 2014 e tendenze per il 2015

2015, punto di svolta

Nella prima edizione del Rapporto Clusit, ovvero nell'ormai remoto febbraio 2012, in riferimento alla preoccupante impennata di attacchi rilevati nel corso del 2011, scrivevamo:
Questo scenario sostanzialmente fuori controllo è il risultato di una diffusa disattenzione per il tema della sicurezza informatica da parte di tutti gli stakeholders della nostra civiltà tecnologica (politica, istituzioni, imprese, cittadini), civiltà che si è "digitalizzata" in tempi rapidissimi ed in modo tumultuoso, disordinato, riponendo una fiducia sempre maggiore nei computer, in Internet, nei device mobili e negli innumerevoli servizi resi disponibili per loro tramite, senza comprenderne le criticità e senza farsi carico di gestire in modo adeguato gli inevitabili rischi.
Trascorsi tre lunghissimi anni dobbiamo constatare che, dal punto di vista dell'adozione di comportamenti e contromisure adeguati alla mitigazione delle crescenti minacce "cyber", si sono fatti passi avanti insufficienti e, all'atto pratico, nonostante gli sforzi egregi delle Forze dell'Ordine di tutto il mondo, si sono ottenuti risultati poco significativi nel contrasto al cyber crime ed al cyber espionage, mentre nello stesso periodo i rischi connessi allo scoppio di ostilità condotte (anche) tramite tecniche di information warfare si sono moltiplicati sensibilmente.
Detto diversamente, in questa fase storica la superficie di attacco complessivamente esposta dalla nostra civiltà digitale cresce più velocemente della nostra capacità di proteggerla.
Questo nonostante anche nel nostro Paese il tema della "sicurezza cibernetica" sia diventato mainstream, non solo a livello istituzionale (con la predisposizione nel 2013 di un Quadro Strategico Nazionale e di documenti programmatici apprezzati in tutto il mondo), ma anche presso il grande pubblico, tanto che notizie relative ai più eclatanti attacchi informatici sono ormai regolarmente pubblicate da ogni testata giornalistica (per lo più tra il gossip e la cronaca nera).
I difensori dunque non riescono ad essere abbastanza efficaci: come spiegare altrimenti il fatto che, a fronte di crescenti investimenti in sicurezza informatica[1] (saliti globalmente dell'8% nel 2014, nonostante il perdurare della crisi economica), il numero e la gravità degli attacchi continuino ad aumentare, in un contesto nel quale, per altro, si stima che 2/3 degli incidenti non vengano nemmeno rilevati dalle vittime[2] ?

---

1 http://www.gartner.com/newsroom/id/2828722

2 http://www.academia.edu/9423817/Bloechl_-_IWGS_2014_Paper_-_The_Known_Unknowns_of_the_Cyber_Threat_-_27_Oct_14_Final

Come interpretare il fatto che in Italia i danni complessivi derivanti da attacchi informatici (stimati in 9 miliardi di euro, inclusi i costi di ripristino[3]) siano ormai pari alla somma delle perdite dovute a crash dell'hardware, del software ed alla perdita di alimentazione elettrica[4]?
Questa settima edizione[5] del Rapporto CLUSIT vuole testimoniare una svolta, un passaggio epocale nella pur breve storia dell'ICT, ovvero il momento in cui, per tutte le diverse tipologie di soggetti interessati (cittadini, aziende, istituzioni, Governi), il rischio teorico di essere colpiti da un attacco informatico di qualche genere è diventato in pratica, nel breve-medio termine, una certezza.
In uno studio condotto nel corso del 2014[6] sono state monitorate su scala globale 1.600 aziende appartenenti a 20 diversi settori merceologici, osservando che nel periodo considerato, in media, la percentuale di organizzazioni compromesse è stata superiore al 90%, con alcuni particolari settori (Legal, Healthcare e Pharma, Retail) che hanno avuto un tasso di compromissione del 100%.
Questa "fotografia" scoraggiante dello stato della (in)sicurezza informatica globale è corroborata, oltre che dai nostri dati, da innumerevoli altri studi[7], e si riflette anche nelle analisi elaborate dai diversi soggetti che hanno contribuito a questo Rapporto: ovunque, pur utilizzando punti di vista e metriche differenti, emerge una situazione di grandissima fragilità, diffusa in ogni Paese (incluso il nostro, quindi), sia nel pubblico che nel privato, che riguarda ogni tipo di organizzazione, indipendentemente dall'ambito e dalla dimensione.
In questo primo scorcio di 2015 dunque la vera questione per i difensori (con riferimento ai dati, alle infrastrutture informatiche ed a tutti quei servizi, molti dei quali critici, oggi realizzati tramite l'ICT) non è più "se", ma "quando" si subirà un attacco informatico (dalle conseguenze più o meno dannose), e quali saranno gli impatti conseguenti.
Un cambiamento di scenario sostanziale, che mettendo in discussione tre decenni di progettazione e di gestione dell'ICT, inclusi i più recenti sviluppi in materia di Cloud, Mobile, Social Media e Internet of Things, non solo rende obsolete prassi consolidate, ma minaccia di far "saltare" i budget di spesa allocati e gli obiettivi di business prefissati, cogliendo in contropiede sia la società nel suo complesso che le istituzioni e, cosa più grave, trovando impreparati la maggior parte dei vendor di tecnologie e degli addetti ai lavori.
È proprio in conseguenza di questa impreparazione che nel panorama nazionale si rileva una scarsissima diffusione di strumenti (metodologici e tecnologici) utili a valutare quali potranno essere gli impatti di un'azione ostile, il che impedisce sia di fare prevenzione che di predisporre piani efficaci di gestione e di mitigazione delle crisi, e quindi mette seriamente in discussione la capacità delle organizzazioni colpite di riprendersi[8] dalle conseguenze di

[3] http://www.mcafee.com/us/resources/reports/rp-economic-impact-cybercrime2-summary.pdf

[4] http://www.emc.com/microsites/emc-global-data-protection-index/index.htm#

[5] Considerando gli aggiornamenti semestrali

[6] https://www2.fireeye.com/rs/fireye/images/rpt-maginot-revisited.pdf

[7] http://report2014.group-ib.com/

[8] http://www.pcworld.com/article/2365602/hacker-puts-full-redundancy-codehosting-firm-out-of-business.html

un attacco dal punto di vista operativo, economico e di immagine.
I livelli allarmanti di in-sicurezza informatica non rappresentano dunque solo "una tassa sull'innovazione"[9], ma sono già oggi diventati una minaccia esistenziale per ogni genere di organizzazione, a tutti i livelli: per il professionista che vede tutti i suoi dati criptati da un ransomware[10], per la PMI che scopre (magari con mesi o anni di ritardo) di essere stata derubata del proprio know-how[11], per la PA che si ritrova nell'impossibilità di offrire servizi essenziali ai cittadini[12], per la grande impresa che subisce un danno economico importante a seguito di un attacco DDoS[13] o al furto di milioni di dati personali dei propri clienti[14], eccetera.
Questa affermazione, apparentemente molto forte, va senz'altro contestualizzata e sostenuta con esempi e dati, di cui questa edizione del Rapporto è particolarmente ricca, anche grazie al contributo della Polizia Postale, della Guardia di Finanza e di Aziende particolarmente attive, a vario titolo, nel campo della sicurezza informatica, come si vedrà nei prossimi capitoli.

Prima di commentare i dati che abbiamo raccolto ed analizzato però, è opportuno svolgere una riflessione a più alto livello, e domandarsi perché siamo giunti a questa situazione, e come possiamo ragionevolmente pensare di correggerla nel più breve tempo possibile.

[9] Jim Lewis, Direttore del Center for Strategic and International Studies (CSIS)

[10] http://www.ilsoftware.it/articoli.asp?tag=Cryptolocker-e-CryptoWall-Italia-sotto-attacco_11627

[11] http://www.techweekeurope.it/security/clusit-allarme-proprieta-intellettuale-pmi-tiro-69295

[12] http://iltirreno.gelocal.it/prato/cronaca/2014/09/04/news/gli-hacker-attaccano-il-sito-del-comune-1.9871010

[13] http://www.tomshw.it/cont/news/attacco-ddos-da-record-in-italia/59565/1.html

[14] http://www.cnet.com/news/cost-of-anthems-data-breach-likely-to-exceed-100-million/

Tutti in prima linea

Dati alla mano, ed allarmati per il quadro che emergeva dalle nostre analisi dei dati relativi al 2013, dodici mesi fa avevamo intitolato un capitolo del Rapporto Clusit 2014 « L'insicurezza informatica è il "new normal" » (non senza attirare qualche critica).
Date le premesse, come era purtroppo lecito attendersi l'interminabile sequenza di attacchi informatici registrati nel 2014, caratterizzati da un costante aumento della gravità degli impatti sulle vittime, non solo ha confermato la nostra ipotesi ma, interpretando con attenzione le dinamiche che stanno alla base di questi fenomeni, ci induce a segnalare l'emergenza di un *nuovo paradigma*, ovvero che non è più possibile utilizzare strumenti informatici senza, per questo stesso fatto, essere *costantemente* sotto attacco[15].
Parafrasando la Prof. Shoshanna Zuboff[16] della Harward Business School, che negli anni '80 del secolo scorso affermava "tutto ciò che può essere informatizzato lo sarà", potremmo dire che siamo giunti al punto in cui "tutto ciò che può essere attaccato lo sarà".

Questo perché i malintenzionati (indipendentemente dalla loro natura e dai loro scopi), attirati da sostanziosi guadagni (economici e non) sono aumentati di numero, si sono organizzati, ed hanno a disposizione strumenti sempre più sofisticati, che possono adattare e sostituire al bisogno con stupefacente rapidità, acquistandoli a costi mediamente irrisori in un immenso mercato underground di prodotti e servizi cyber criminali[17] che ha tutte le caratteristiche di un'industria high-tech di prim'ordine[18], con l'aggravante che questa particolare industria gode del "vantaggio competitivo" di essere totalmente non regolamentata e di non essere soggetta ad alcun tipo di limitazione (salvo il contrasto delle Forze dell'Ordine).
Inoltre va sottolineato che i criminali si avvalgono (ormai da anni) di strumenti totalmente automatizzati[19], in grado di colpire milioni di sistemi in poche ore[20], il che consente loro di cambiare tattiche e strategie in tempo reale e di operare senza interruzione da qualsiasi punto del pianeta.
Questo approccio sistematico è molto facilitato dalla diffusione endemica di vulnerabilità non gestite e dalla situazione di sostanziale "monocultura" tecnologica[21] che si è determinata negli anni, la quale rende particolarmente efficace questo genere di automazione e genera pericolose "economie di scala" a favore degli attaccanti.

---

15 http://www.ted.com/talks/avi_rubin_all_your_devices_can_be_hacked

16 http://en.wikipedia.org/wiki/Shoshana_Zuboff

17 http://www.itpro.co.uk/security/23200/crime-as-a-service-lowers-entry-barriers-to-cybercrime-world

18 http://www.techradar.com/news/world-of-tech/predictions-for-cyber-crime-in-2015-and-how-the-security-industry-will-respond-1281179

19 http://www.eweek.com/c/a/Security/CyberCriminals-Use-Botnets-Automation-to-Launch-Multiple-Blended-Attacks-656032

20 http://blog.trendmicro.com/trendlabs-security-intelligence/bash-vulnerability-shellshock-exploit-emerges-in-the-wild-leads-to-flooder/

21 https://securityledger.com/2014/04/heartbleed-technology-monocultures-second-act/

Il problema infatti non è meramente tecnologico. La ragione principale per cui gli attaccanti hanno la meglio è economica, e risiede nella crescente asimmetria tra i differenti "modelli di business": per ogni dollaro investito dagli attaccanti nello sviluppo di nuovo malware, o nella ricombinazione di malware esistente per nuovi scopi, il costo sopportato dai difensori (ancora legati ad un modello reattivo, e dunque incapaci di anticipare le mosse degli avversari) è di milioni di dollari.
A titolo di esempio il malware BlackPOS, in vendita per 1.800$ nel mercato underground, che contiene ben otto componenti "riciclate" e già note da anni[22], nel 2014 (considerando due soli attacchi) ha causato danni accertati per 62 milioni di dollari a HomeDepot, e per 148 milioni a Target.
Va qui anche ricordato che nel corso del 2014 è (purtroppo) venuto a cadere il "mito" della superiorità dell'Open Source (ed in particolare di Linux) dal punto di vista della sua maggiore sicurezza intrinseca, a seguito della scoperta di vulnerabilità gravissime[23], presenti da anni nel codice di importanti componenti, sfuggite al vaglio della "Community" principalmente per mancanza di risorse[24].
Per quanto le principali distribuzioni siano state corrette in tempi brevissimi, considerando che moltissimi sistemi embedded costantemente connessi in Rete come router casalinghi, appliance di ogni genere, telecamere di sicurezza, stampanti, vending machines, smart tv, giochi per bambini (etc) contengono una qualche variante di Linux nel proprio firmware, e che tutti questi miliardi di sistemi difficilmente riceveranno patch per vulnerabilità come Heartbleed, ShellShock o Poodle[25], si comprende quanto grave sia davvero il problema.
Un simile scenario di "industrializzazione delle minacce", unito alla bassa sicurezza presente nei sistemi informatici in generale, modifica sostanzialmente tutti i ragionamenti fatti fin'ora in termini di gestione del rischio informatico e di valutazione degli economics (e quindi del ROI) dell'ICT, e richiede a tutti (utenti finali, vendor, istituzioni civili e militari, imprese) un ripensamento profondo delle strategie di implementazione di nuovi prodotti e servizi basati sull'informatica e sulla Rete.
Infine, non vanno sottovalutati i possibili *effetti sistemici* di quanto sopra. Da un lato sofisticate tecniche di attacco sviluppate da team governativi (anche queste poi "riciclate" dall'underground criminale, come nel caso del malware Gyges[26]) sono già usate su larga scala da un certo numero di nazioni con finalità di spionaggio e di infiltrazione dei sistemi altrui, allo scopo di fare "pressione" sui bersagli e/o di poterli danneggiare o disattivare, e dall'altro strumenti analoghi stanno entrando nella disponibilità di organizzazioni terroristiche, che si approvvigionano di tramite gruppi cyber criminali.

---

22 http://www.cyactive.com/wp-content/uploads/2014/12/Infamous-5-Report.pdf

23 https://blog.cloudflare.com/inside-shellshock/

24 http://www.propublica.org/article/the-worlds-email-encryption-software-relies-on-one-guy-who-is-going-broke

25 https://www.us-cert.gov/ncas/alerts/TA14-290A

26 http://www.darkreading.com/government-grade-stealth-malware-in-hands-of-criminals/d/d-id/1297362

Le possibili conseguenze di questa selvaggia corsa ai cyber-armamenti (ambito non normato a livello internazionale) sono francamente straordinarie[27], e non riguardano solo le c.d. "infrastrutture critiche" definite come tali in base alle normative, ma una quantità crescente di servizi erogati da aziende private e da pubbliche amministrazioni che, se resi indisponibili a seguito di un attacco, creerebbero enormi disagi alla popolazione e, in certi scenari, anche perdite di vite umane[28].

[27] http://www.weforum.org/reports/global-risks-report-2015

[28] http://www.defenseone.com/threats/2014/10/cyber-attack-will-cause-significant-loss-life-2025-experts-predict/97688/

Prepararsi all'impatto

La comprensione dei fenomeni sopra discussi dovrebbe spingere tutti i responsabili (non solo in ambito ICT) a rivedere con estrema urgenza le proprie attuali politiche di gestione del rischio informatico (quando esistenti) o convincerli ad adottarne, innalzando i livelli di investimento in formazione, processi e strumenti deputati alla sicurezza cibernetica, che allo stato attuale si dimostrano ancora palesemente inadeguati, sia perché troppo limitati, sia perché orientati nella maggioranza dei casi a forme di difesa reattiva "tradizionali", statiche, che ormai non tengono più il passo con l'evoluzione delle minacce.
Osserviamo con estrema preoccupazione che purtroppo ciò non sta ancora accadendo. Manca attenzione per i fenomeni in atto, si confondono ancora gli investimenti in compliance (certamente necessari) con quelli in sicurezza[29], non esistono forme di coordinamento nè di "mutuo soccorso" p.es. tra partner o tra clienti ed outsourcer, i contratti non tengono ancora debitamente conto dell'aumentata rischiosità dell'ICT, le possibilità di trasferimento dei rischi "cyber"tramite polizze assicurative sono ancora limitate e poco utilizzate[30], si sottovalutano gli effetti domino che inevitabilmente discendono dalla crescente interconnessione tra organizzazioni, non si applicano forme strutturate di information sharing[31], eccetera.
Considerata l'importanza assunta dall'ICT in ogni ambito della nostra esistenza, questo sorprendente scollamento tra realtà e percezione andrebbe approfondito sotto vari punti di vista non tecnici (culturali, antropologici, economici), analisi che però esula dal Rapporto Clusit, quantomeno nella sua forma attuale.
Ci limitiamo a sottolineare che nello scenario odierno occorre porre la sicurezza informatica *al centro* e *a monte* di qualsiasi progetto che includa l'utilizzo di sistemi ICT, e non considerarla più un aspetto secondario (o peggio una "tassa"), ma l'elemento abilitante più essenziale ed irrinunciabile per evitare che scelte avventate (o semplicemente non informate) producano effetti contrari a quelli desiderati, se non deleteri.
Tali effetti nell'immediato possono sostanziarsi in gravi danni economici, violazioni della privacy su larga scala e furti di proprietà intellettuale ma in prospettiva, su un più ampio piano socio-culturale, con l'aumentare degli incidenti, possono indurre un rigetto della tecnologia da parte degli utenti, e/o facilitare l'instaurazione di regimi "orwelliani" di monitoraggio di massa e di compressione delle libertà personali, introdotti con la motivazione di "combattere le minacce cyber". Sono tutti rischi molto concreti che non possiamo permetterci di correre.
In un contesto di questo genere, le principali contromisure da applicare sono legate a processi e tecnologie in alcuni casi noti da anni, ma raramente utilizzati al massimo delle loro possibilità, ed in altri casi a nuove soluzioni: strumenti per monitorare le infrastrutture in modo puntuale ed in tempo reale correlando in modo significativo gli eventi, servizi di Cy-

[29] http://www.nuix.com/2014/08/22/compliance-does-not-equal-security

[30] http://www.cyberrisknetwork.com/2014/11/06/spending-cyber-risk-mitigation-insurance-increases/

[31] http://www.cyberrisknetwork.com/2015/02/12/bill-introduced-u-s-senate-share-cyber-data/

ber Intelligence e di Early Warning utili a prevenire le minacce o quantomeno ad innalzare il livello di allerta nell'imminenza di un attacco, processi di Incident Handling sistematici, efficaci e consistenti, sistemi di Business Continuity adeguati ed opportunamente testati, procedure operative concrete per la gestione delle crisi, eccetera.
Soprattutto sono necessarie cospicue risorse economiche, forti competenze (al momento difficilmente reperibili sul mercato) ed è essenziale un forte impegno da parte degli stakeholders, a tutti i livelli.
La parola d'ordine del 2015 è "prepararsi all'impatto", adottando logiche di Cyber Resilience[32], ciascun soggetto in base alle proprie esigenze e capacità ma nell'ambito di una regia istituzionale forte, innanzi tutto applicando l'antica massima "conosci te stesso" (e quindi le proprie vulnerabilità e criticità), e poi predisponendo un modello di rischio accurato, costantemente aggiornato, stimando le perdite potenziali tramite lo studio di un certo numero di scenari realistici per determinare correttamente gli investimenti necessari.
Il tema della Cyber Resilience, che fa convergere compliance e cyber security, governance e risk management, cyber intelligence e crisis management, attività di prevenzione e di reazione rapida, cooperazione tra pubblico e privato[33] ed information sharing tra tutte le parti coinvolte[34], pur richiedendo per essere consolidato ed applicato con successo apporti multidisciplinari di alto profilo e metodologie ancora poco diffuse, in sé non è affatto nuovo: è semplicemente diventato di estrema attualità in conseguenza dell'evoluzione rapidissima delle minacce, e della loro crescente gravità.
L'Unione Europea lo sta elaborando fin dal 2009, con il progetto dell'ENISA "European Public-Private Partnership for Resilience (EP3R)"[35], gli Stati Uniti ne hanno fatto ufficialmente uno dei pilastri della loro strategia di Cyber Security nel 2013[36], e l'Italia stessa, oltre ad includerlo nell'ambito del suo Quadro Strategico Nazionale[37], ha organizzato in merito un importante convegno a Roma dal titolo "The Role of Cyber Defence to Protect and Sustain EU Economy"[38] durante il recente semestre italiano di Presidenza Europea.
L'importante è che il concetto di Cyber Resilience non diventi l'ennesimo "mantra" commerciale, l'ennesimo escamotage per rimarchiare prodotti e soluzioni superati, ormai inefficaci, e che si pongano invece le basi per includere tutti i soggetti (e non solo le grandissime aziende, che possono investire autonomamente cifre importanti) all'interno del suo perimetro, onde evitare che si creino cittadini ed organizzazioni (pubbliche e private) di serie A, relativamente sicuri, e cittadini ed organizzazioni di serie B, lasciati in balia di ogni genere di

[32] http://www.weforum.org/projects/partnership-cyber-resilience

[33] http://www.sicurezzanazionale.gov.it/sisr.nsf/approfondimenti/la-cooperazione-pubblico-privato-nella-cyber-security.html

[34] http://csrc.nist.gov/publications/drafts/800-150/sp800_150_draft.pdf

[35] http://www.enisa.europa.eu/activities/Resilience-and-CIIP/public-private-partnership/european-public-private-partnership-for-resilience-ep3r/ep3r

[36] http://www.whitehouse.gov/the-press-office/2013/02/12/presidential-policy-directive-critical-infrastructure-security-and-resil

[37] http://www.agid.gov.it/sites/default/files/leggi_decreti_direttive/quadro-strategico-nazionale-cyber_0.pdf

[38] http://www.difesa.it/EN/Primo_Piano/Pagine/ItalianPresidencyoftheCouncilofEuropeanUnionTheRoleofCyberDefence.aspx

malintenzionato: un livello soddisfacente di sicurezza informatica infatti può realizzarsi solo nel momento in cui tutti coloro che sono in qualche modo connessi in Rete e coesistono nel cyberspazio sono ragionevolmente sicuri.
Come egregiamente illustrato dal World Economic Forum nel fondamentale documento "Risk and Responsibility in a Hyperconnected Word" del gennaio 2014, nei prossimi cinque anni abbiamo di fronte tre possibili scenari, e solo uno è auspicabile:

FIGURE 12: ALTERNATIVE FUTURE SCENARIOS FOR 2020

Minimal increase ■ Moderate increase ■ Step change

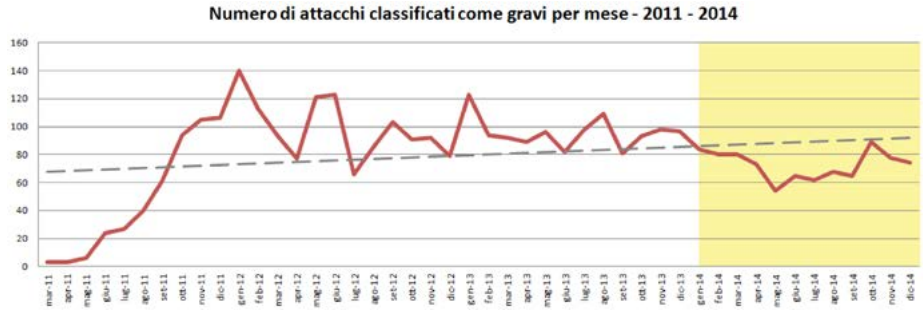
	Description	Pace of increase in intensity of threat	Pace of increase in quality of response: Private institutions	Pace of increase in quality of response: Public sector
1 **Muddling into the future**	Attackers retain an advantage over defenders who continue to respond to threats reactively, albeit successfully	■	■	■
2 **Backlash decelerates digitization**	Attack tools proliferate leading to widespread and highly public attacks, governments react by enforcing tighter controls	■	■	■
3 **Cyber resilience accelerates digitization**	Defensive capabilities dramatically improve significantly reducing fears of major cybersecurity events	■	■	■

World Economic Forum - Risk and Responsibility in a Hyperconnected Word – pag. 26

Pur considerando la situazione niente affatto rosea, vogliamo concludere questa prima sezione del Rapporto 2015 con una nota di cauto ottimismo: uscire dalla "trappola" dell'insicurezza informatica applicando estesamente logiche di Cyber Resilience è non solo necessario ma anche certamente possibile: quello che ci aspetta nel breve termine è un importante lavoro di presa di coscienza, ri-allocazione di risorse (economiche ed umane), valutazione puntuale dei rischi ed ottimizzazione della spesa in sicurezza, che deve crescere non solo in quantità ma anche e soprattutto in qualità ed efficacia, per il bene di tutti.

Analisi dei principali attacchi gravi a livello internazionale del 2014

Anche in questa edizione il Rapporto CLUSIT propone una dettagliata analisi degli incidenti di sicurezza più significativi avvenuti a livello globale negli ultimi dodici mesi, confrontandoli con i 36 mesi precedenti. Lo studio si basa su un campione di quasi 3.700 incidenti noti avvenuti nel mondo ed in Italia negli ultimi 48 mesi (dal primo gennaio 2011 al 31 dicembre 2014), di cui circa 900 sono relativi al 2014, selezionati tra quelli che hanno avuto un impatto particolarmente significativo per le vittime in termini di perdite economiche, di reputazione, o di diffusione di dati sensibili (personali e non).
Al termine di questa analisi, nei capitoli successivi, seguono una serie di contributi di grande interesse: oltre a presentare anche quest'anno i dati relativi agli incidenti (di qualsiasi dimensione ed impatto) rilevati in Italia dal Security Operations Center di FASTWEB, aggregati in forma anonima ed opportunamente classificati, presentiamo un'analisi della situazione a livello europeo svolta da IBM, un approfondimento specifico del tema DDoS realizzato da parte di Akamai, ed i preziosi contributi di Polizia Postale e Guardia di Finanza.
Una nota metodologica: dal momento che nell'arco di questi 48 mesi si è verificata una sensibile evoluzione degli scenari, e che alcune categorie di attacchi, che potevano essere considerati "gravi" nel 2011, sono oggi diventati ordinaria amministrazione, abbiamo ritenuto di dover aggiornare di conseguenza i nostri criteri di classificazione, rendendoli più restrittivi. Pertanto, dal punto di vista numerico, applicando criteri più stringenti quest'anno abbiamo classificato come gravi un numero di attacchi che è leggermente inferiore rispetto all'anno precedente, scartando una grandissima quantità di incidenti "minori" per evitare di confrontare, nell'ambito dello stesso campione, situazioni che hanno causato la perdita di milioni di euro o il furto di milioni di account con, per esempio, il mero defacement[39] di un sito istituzionale: incidente che, per quanto la notizia possa fare sensazione, non è paragonabile in termini di impatti. L'effetto di questo aggiornamento è visibile nel grafico sottostante:



© Clusit - Rapporto 2015 sulla Sicurezza ICT in Italia

[39] http://en.wikipedia.org/wiki/Website_defacement

Dieci incidenti rappresentativi del 2014

Prima di analizzare quanto avvenuto nel 2014 a livello globale ed italiano, quest'anno vogliamo partire da dieci incidenti a nostro avviso particolarmente significativi, selezionati non tanto per la loro gravità in termini assoluti (per quanto alcuni siano stati particolarmente gravi), quanto piuttosto per rappresentare la varietà di situazioni che si sono verificate nel corso dell'anno.

Vittima	Attaccante	Tecniche usate
JP Morgan Chase[40]	Cyber Espionage, State sponsored?	Known vulnerabilities, APT

La nota banca americana è stata oggetto di un attacco particolarmente sofisticato, che ha causato la sottrazione di circa 79 milioni di record relativi ai propri clienti. Il punto di attacco iniziale, come spesso accade, è stato un server poco usato e quindi trascurato, utilizzato come "trampolino di lancio" per portare attacchi a sistemi interni sensibili.

Vittima	Attaccante	Tecniche usate
Home Depot[41]	Cyber Crime	APT, custom malware

Nonostante avesse subito attacchi minori in precedenza, la grande catena di negozi di bricolage non ha posto in essere contromisure adeguate, e addirittura ha disattivato un sistema di sicurezza che avrebbe potuto impedire l'attacco, secondo alcuni ex-dipendenti. Come conseguenza, l'azienda ha subito il furto di 56 milioni di carte di credito / debito, sopportando centinaia di milioni di dollari di danni.

Vittima	Attaccante	Tecniche usate
Target[42]	Cyber Crime	Vulnerabilities, malware

La catena di supermercati, pur avendo installato dei sistemi avanzati di protezione, non ha reagito tempestivamente alla segnalazione di un attacco in corso inviata dal proprio SOC di Bangalore. Di conseguenza è stato perso tempo prezioso, che ha consentito agli attaccanti di sottrarre circa 40 milioni di carte di credito dai POS dei punti vendita. Oltre ad aver causato il licenziamento di 8 membri su 10 del Board, l'attacco ha causato all'azienda perdite complessivamente stimate in un miliardo di dollari.

[40] http://www.theregister.co.uk/2014/12/23/jpmorgan_breach_probe_latest/

[41] http://www.bloomberg.com/bw/articles/2014-09-18/home-depot-hacked-wide-open

[42] http://www.bloomberg.com/bw/articles/2014-03-13/target-missed-alarms-in-epic-hack-of-credit-card-data

Vittima	Attaccante	Tecniche usate
Ebay[43]	Cyber Crime	Multiple

La nota piattaforma di e-commerce è stata violata, e gli attaccanti hanno compromesso un database, sottraendo 145 milioni di record, contenenti dati personali e password criptate. Prudenzialmente l'azienda ha immediatamente invitato tutti i propri utenti a cambiare password.

Vittime multiple	Attaccante	Tecniche usate
Operazione "Newscaster"[44]	Cyber Espionage (Iran?)	Social Engineering

Questa campagna di spionaggio, realizzata tramite la creazione e l'utilizzo di numerosi falsi profili su diversi social network e la creazione di una falsa agenzia giornalistica (chiamata "NewsOnAir") è durata dal 2011 al 2014 ed ha colpito oltre 2.000 individui, principalmente personale militare, diplomatici, giornalisti e contractor della difesa americani, inglesi, sauditi, irakeni ed israeliani.

Vittima	Attaccante	Tecniche usate
Gruppo Benetton[45]	Cyber Espionage (Siria?)	custom malware ?

La multinazionale trevigiana ha dichiarato di aver subito un attacco informatico "sofisticato", che ha consentito agli attaccanti di sottrarre i bozzetti della collezione di abbigliamento "0-12" e di replicare gli abiti, finiti in vendita in alcuni negozi siriani. Il riserbo sulle modalità dell'attacco è stato totale, anche se l'azienda ha dichiarato che "i danni sono stati limitati, sia quelli effettivi, sia quelli potenziali".

Vittime multiple	Attaccante	Tecniche usate
Operazione "Putter Panda"[46]	Cyber Espionage (Cina?)	Multiple

Il gruppo di hacker governativi denominato "Putter Panda", appartenente alla famigerata "Unit 61486" (in attività almeno dal 2007), è stato accusato dagli Stati Uniti di gravi attività di cyber-espionage verso ambienti militari, governativi e contractor della difesa. In conseguenza di un'indagine condotta nel 2014, il governo USA ha formalmente accusato 5 alti ufficiali cinesi di spionaggio industriale, richiedendone (invano) l'arresto e sollevando le sdegnate proteste cinesi.

[43] http://bgr.com/2014/05/27/ebay-hack-145-million-accounts-compromised/

[44] http://www.securityweek.com/iranian-hackers-targeted-us-officials-elaborate-social-media-attack-operation

[45] http://mattinopadova.gelocal.it/regione/2014/04/18/news/gli-hacker-rubano-e-clonano-la-collezione-benetton-1.9070153

[46] http://www.darkreading.com/attacks-breaches/-putter-panda-tip-of-the-iceberg-/a/d-id/1269549

Vittima	Attaccante	Tecniche usate
Sony[47]	Cyber Crime, State Sponsored ?	Multiple

La vicenda dell'ultimo attacco a Sony è particolarmente confusa e complessa, sia per quanto riguarda la diatriba sull'attribuzione della responsabilità, sia per le modalità dell'incidente. L'azienda è stata pesantemente compromessa, il che ha portato (fatto inaudito) a disattivare l'intero sistema informatico aziendale per quasi 3 giorni. Ciò nonostante, oltre al blocco dei sistemi sono stati trafugati 38 milioni di file, tra cui 10 anni di email, stipendi, numeri di social security, film ancora non usciti, ed una serie di documenti riservati a vario titolo imbarazzanti o sensibili, oppure addirittura relativi ad altre aziende.

Vittima	Attaccante	Tecniche usate
Anthem[48]	Cyber Crime	APT, Custom Malware

L'attacco a questa primaria compagnia di assicurazione sanitaria, iniziato ad aprile 2014 ma scoperto solo a gennaio 2015, ha provocando il furto di circa 80 milioni di record contenenti i dati personali dei clienti e degli impiegati (CEO compreso) compresi nomi, date di nascita, indirizzi email, dati sul reddito e altro ancora. La stima dei danni è ancora in corso, ma si preannuncia molto pesante sia intermini di immagine che di risarcimenti agli utenti.

Vittima	Attaccante	Tecniche usate
Korea Hydro & Nuclear Power[49]	Hacktivist ?	Sconosciute

Un hacker solitario ha potuto penetrare la parte business della rete dell'operatore nazionale per l'energia della Corea del Sud, sottraendo e diffondendo una grande quantità di dati tecnici sugli impianti, in particolare su tre reattori nucleari, dei quali l'attaccante ha richiesto la chiusura. L'azienda energetica ha ribadito che i sistemi di controllo dei reattori non sono stati compromessi.

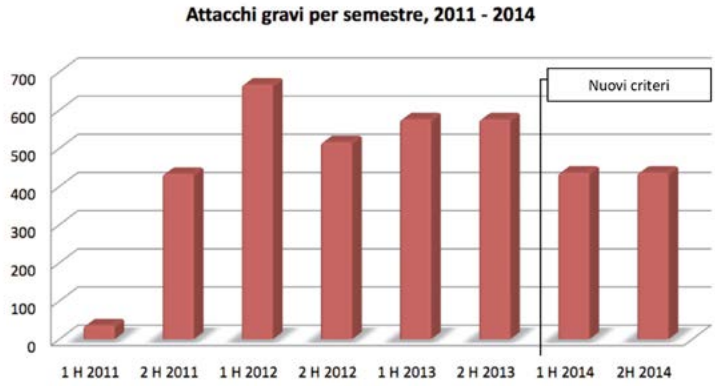
[47] http://www.wired.it/attualita/tech/2014/12/22/tutto-sony-hack/

[48] http://www.theguardian.com/us-news/2015/feb/05/millions-of-customers-health-insurance-details-stolen-in-anthem-hack-attack

[49] http://rt.com/news/216599-korea-nuclear-plant-hacked/

Analisi dei principali attacchi noti a livello globale

Dei 3.677 attacchi di pubblico dominio che costituiscono il nostro database di incidenti degli ultimi 4 anni, nel 2014 ne abbiamo classificati come gravi 873. Questa la distribuzione degli attacchi registrati nel periodo, suddivisi per semestre:



© Clusit - Rapporto 2015 sulla Sicurezza ICT in Italia

Va tenuto presente che i dati di seguito sintetizzati rappresentano solo una frazione, per quanto significativa, del totale degli attacchi gravi presumibilmente compiuti in Italia e nel mondo nel corso dell'anno passato.
Questo campione infatti presenta ragionevolmente delle lacune, dovute al fatto che alcuni ambienti sono particolarmente efficaci nel minimizzare la diffusione pubblica di informazioni relative agli attacchi che subiscono, e risultano pertanto qui sotto-rappresentati.
Inoltre mentre ad oggi negli Stati Uniti è in vigore una normativa che obbliga le vittime a fare disclosure a seguito di un data breach, così non è nella maggior parte delle altre nazioni, Europa inclusa, di conseguenza gli attacchi noti contro bersagli americani risultano essere la maggioranza.
Infine alcuni tipi di attacchi (i più subdoli e silenziosi, per esempio quelli legati allo spionaggio industriale, o ad attività di Information Warfare) sono compiuti nell'arco di periodi piuttosto lunghi e dunque, sempre che diventino di dominio pubblico, emergono solo ad anni di distanza[50].

Le tre tabelle seguenti rappresentano una sintesi dei dati che abbiamo raccolto.
Come in passato abbiamo segnalato in arancio gli incrementi percentuali che risultano es-

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

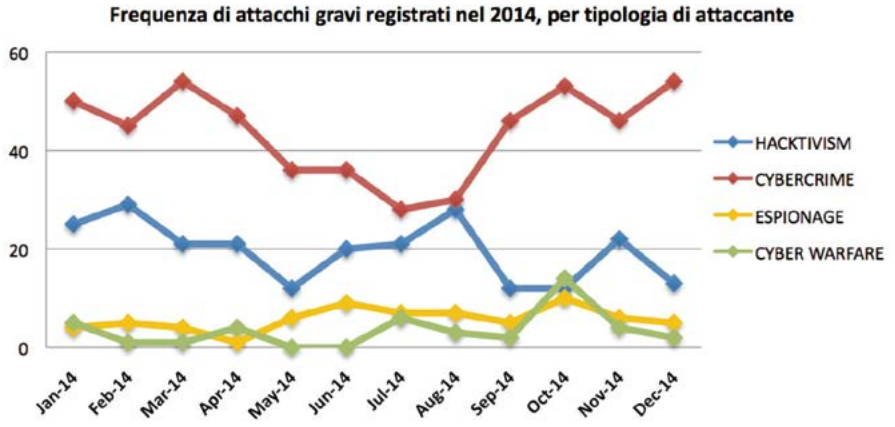
sere superiori alla media[51], mentre abbiamo evidenziato in una nuova colonna le principali tendenze in atto.

Distribuzione degli attaccanti per tipologia

ATTACCANTI PER TIPOLOGIA	2011	2012	2013	2014	Variazioni 2012 su 2011	Variazioni 2013 su 2012	Variazioni 2014 su 2013	Variazioni 2014 su 2011	Trend 2015
Cybercrime	170	633	609	525	272,35%	-3,79%	-13,79%	208,82%	↑
Hacktivism	114	368	451	236	222,81%	22,55%	-47,67%	107,02%	↓
Espionage	23	29	67	69	26,09%	131,03%	2,99%	200,00%	→
Information Warfare	14	43	25	42	207,14%	-41,86%	68,00%	200,00%	↑

© Clusit - Rapporto 2015 sulla Sicurezza ICT in Italia

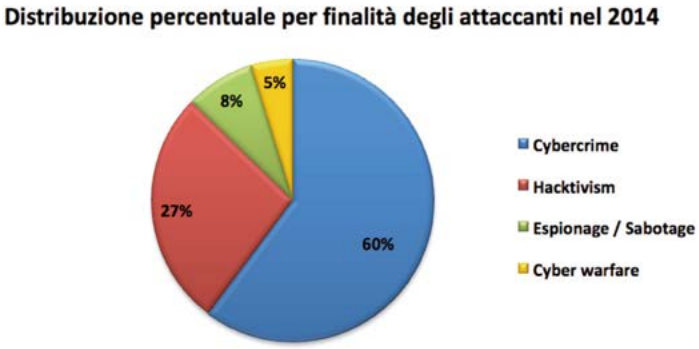
Dal campione emerge chiaramente che, con l'esclusione delle attività riferibili ad attaccanti della categoria "Hacktivism", gli attacchi compiuti per altre finalità sono in aumento, in particolare per quanto riguarda le categorie "Cybercrime" ed "Information Warfare". Queste ultime presentano il tasso di crescita più marcato.



© Clusit - Rapporto 2015 sulla Sicurezza ICT in Italia

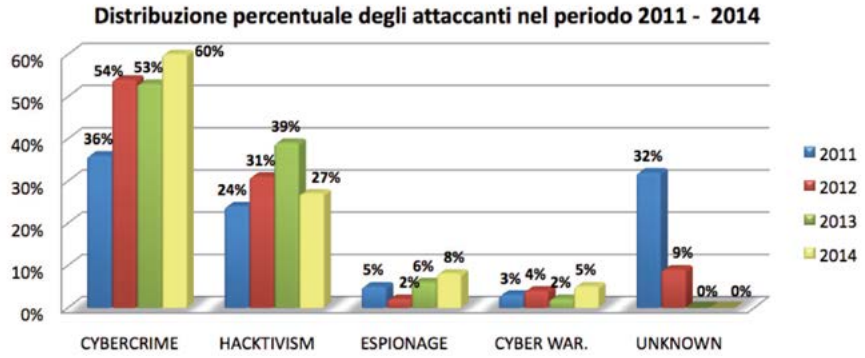
[51] Tenendo in considerazione l'aggiornamento dei criteri di classificazione applicati ai dati 2014.

Anche da questa rappresentazione per mese del numero di attacchi rilevati si evince la dinamica in atto: nel corso dell'anno tendono a diminuire gli attacchi gravi con finalità dimostrative tipici dell'Hacktivism, crescono gli attacchi con finalità criminali, rimangono sostanzialmente stabili gli attacchi (quantomeno quelli noti) legati ad attività di spionaggio, ed aumentano quelli realizzati in supporto ad attività militari e paramilitari.



© Clusit - Rapporto 2015 sulla Sicurezza ICT in Italia

Nel 2014 il Cybercrime si conferma la prima causa di attacchi gravi a livello globale, attestandosi al 60% dei casi (era il 36% nel 2011, e cresce del 7% rispetto al 2013).
Tenendo presente che quest'anno abbiamo reso più restrittivi i criteri utilizzati per definire un attacco come "grave", va sottolineato che con i criteri precedenti questa crescita sarebbe risultata maggiore.



© Clusit - Rapporto 2015 sulla Sicurezza ICT in Italia

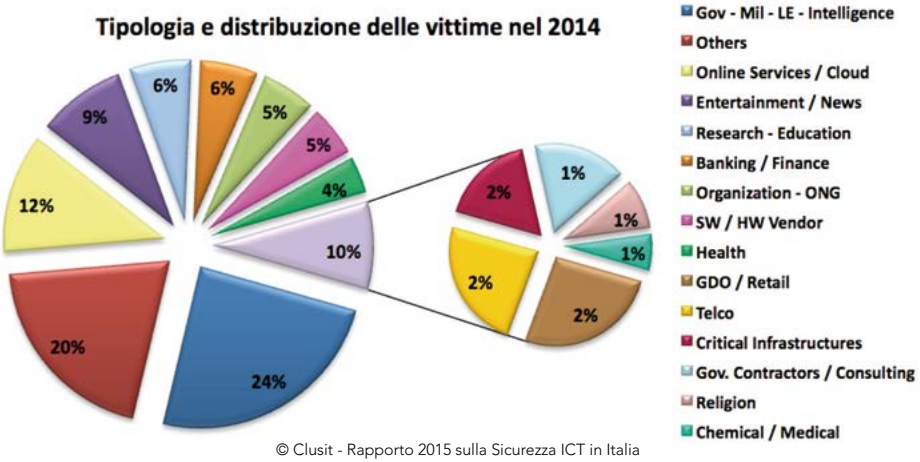
L'Hacktivism diminuisce di oltre 10 punti percentuali, passando da oltre un terzo a meno di un quarto dei casi analizzati, mentre rispetto al 2013 l'Espionage sale del 2%, e l'Information Warfare del 3%.

Distribuzione delle vittime per tipologia

VITTIME PER TIPOLOGIA	2011	2012	2013	2014	Variazioni 2012 su 2011	Variazioni 2013 su 2012	Variazioni 2014 su 2013	Variazioni 2014 su 2011	Trend 2015
Gov - Mil - LEAs - Intelligence	153	374	402	211	144,44%	7,49%	-47,51%	37,91%	↑
Others	97	194	146	173	100,00%	-24,74%	18,49%	78,35%	↓
Entertainment / News	76	175	147	77	130,26%	-16,00%	-47,62%	1,32%	↑
Online Services / Cloud	15	136	114	103	806,67%	-16,18%	-9,65%	586,67%	↓
Research - Education	26	104	70	54	300,00%	-32,69%	-22,86%	107,69%	↓
Banking / Finance	17	59	108	50	247,06%	83,05%	-53,70%	194,12%	↓
Software / Hardware Vendor	27	59	46	44	118,52%	-22,03%	-4,35%	62,96%	↑
Telco	11	19	19	18	72,73%	0,00%	-5,26%	63,64%	↑
Gov. Contractors / Consulting	18	15	2	13	-16,67%	-86,67%	550,00%	-27,78%	→
Security Industry	17	14	6	2	-17,65%	-57,14%	-66,67%	-88,24%	→
Religion	0	14	7	7	-	-50,00%	0,00%	-	↑
Health	10	11	11	32	10,00%	0,00%	190,91%	220,00%	↓
Chemical / Medical	2	9	1	5	350,00%	-88,89%	400,00%	150,00%	↓
Critical Infrastructures	-	-	37	13	-	-	-64,86%	-	↑
Automotive	-	-	17	3	-	-	-82,35%	-	↑
Organizations / ONG	-	-	19	47	-	-	147,37%	-	↓
GDO / Retail	-	-	-	20	-	-	-	-	↓

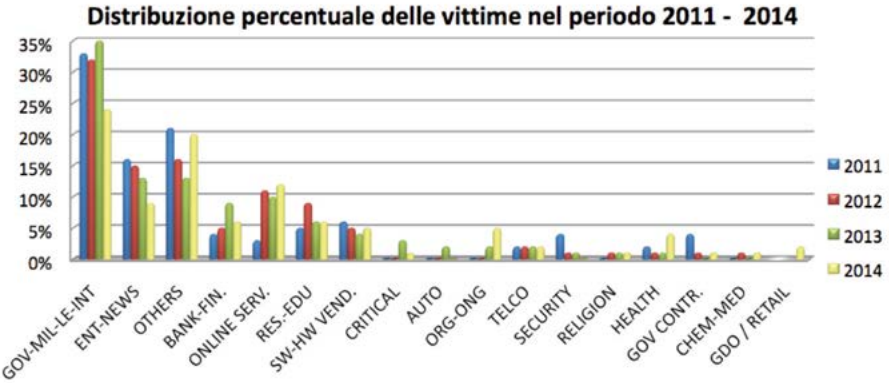
© Clusit - Rapporto 2015 sulla Sicurezza ICT in Italia

Nel 2014 cresce la gravità degli attacchi verso le categorie "Online Services / Cloud", "Banking / Finance", "Health e Pharma" e l'ampia categoria delle Associazioni. La categoria "Retail" (che include la grande distribuzione organizzata, le catene di punti vendita in franchising ed i siti di e-commerce) entra prepotentemente nel mirino dei cyber criminali, registrando globalmente perdite ingentissime rispetto al numero di attacchi registrati (20).



© Clusit - Rapporto 2015 sulla Sicurezza ICT in Italia

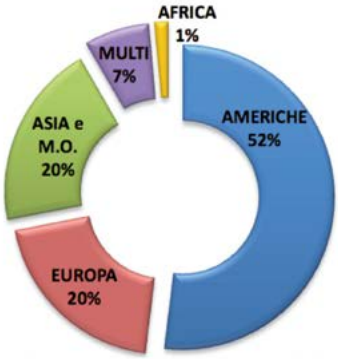
Al primo posto assoluto, per quanto in netta diminuzione, ancora il settore governativo in senso esteso, con quasi un quarto degli attacchi. Al secondo posto, con un quinto degli attacchi, il gruppo "Others", a dimostrare quanto ormai gli attacchi gravi siano diffusi contro organizzazioni appartenenti ad ogni settore merceologico. La crescita percentuale maggiore rispetto al 2013 è comunque registrata dal settore "Health".



© Clusit - Rapporto 2015 sulla Sicurezza ICT in Italia

Introduciamo quest'anno anche una classificazione delle vittime per nazione di appartenenza, che sintetizziamo qui per area geografica, su base continentale.
Da notare che ben il 7% delle vittime, per la natura transnazionale (e transcontinentale) delle loro operazioni, rientrano nella categoria "Multi".

Appartenenza geografica delle vittime per continente nel 2014



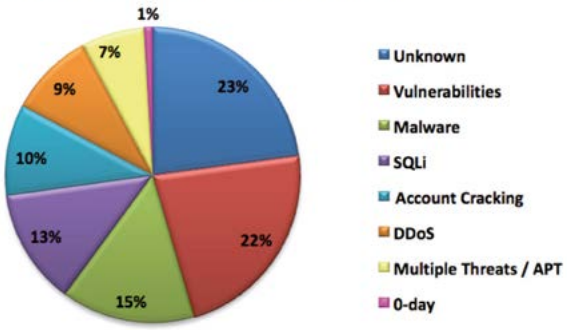
© Clusit - Rapporto 2015 sulla Sicurezza ICT in Italia

Distribuzione delle tecniche di attacco

TECNICHE DI ATTACCO	2011	2012	2013	2014	Variazioni 2012 su 2011	Variazioni 2013 su 2012	Variazioni 2014 su 2013	Variazioni 2014 su 2011	Trend 2015
SQL Injection	197	435	217	110	120,81%	-50,11%	-49,31%	-44,16%	↓
Unknown	73	294	239	198	302,74%	-18,71%	-17,15%	171,23%	↑
DDoS	27	165	191	81	511,11%	15,76%	-57,59%	200,00%	→
Vulnerabilità note	107	142	256	195	32,71%	80,28%	-23,83%	82,24%	→
Malware	34	61	57	127	79,41%	-6,56%	122,81%	273,53%	↑
Account Hijacking / Theft	10	41	115	86	310,00%	180,49%	-25,22%	760,00%	↑
Phishing / Social Engineering	10	21	3	4	110,00%	-85,71%	33,33%	-60,00%	→
Multiple Techniques / APT	6	13	71	60	116,67%	446,15%	-15,49%	900,00%	↑
0-day	5	8	3	8	60,00%	-62,50%	166,67%	60,00%	→
Phone Hacking	0	3	0	3	-	-	-	-	↓

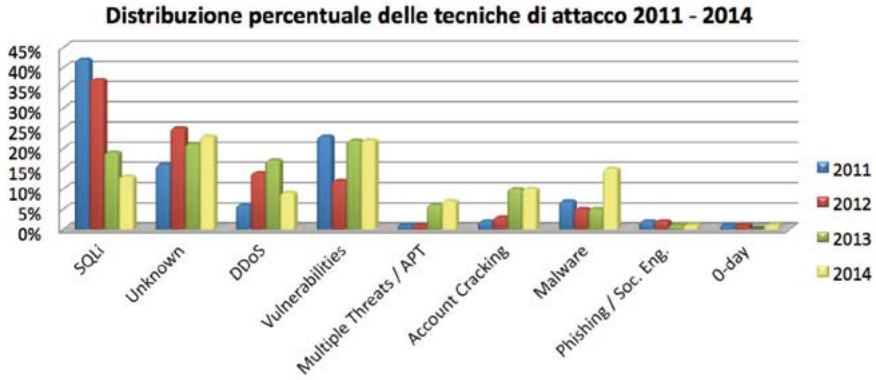
Rispetto al 2013 diminuiscono sensibilmente le SQL Injection e in misura minore le Vulnerabilità note. Diminuiscono anche gli attacchi DDoS (principalmente utilizzati per azioni meramente dimostrative, che quest'anno abbiamo tendenzialmente escluso dal nostro campione, salvo casi particolari) mentre cresce sensibilmente l'utilizzo di Malware (+122%).

Tipologia e distribuzione delle tecniche d'attacco nel 2014



© Clusit - Rapporto 2015 sulla Sicurezza ICT in Italia

Ritorna al primo posto la categoria "Unknown", che comprende tutti quegli incidenti nei quali non è stato possibile raccogliere informazioni sufficienti sulle tecniche di attacco utilizzate, il che spiega anche la lieve flessione della categoria "APT".



© Clusit - Rapporto 2015 sulla Sicurezza ICT in Italia

Anche nel 2014 le vulnerabilità note e le tecniche di attacco più banali, ovvero più facili da contrastare, sono quelle che hanno causato più incidenti. Se si escludono le categorie "APT", "0-day" ed "Unknown", la somma in percentuale delle altre categorie è ancora altissima, prossima al 70%.
Considerato che stiamo analizzando gli attacchi più gravi del periodo, compiuti contro primarie organizzazioni pubbliche e private, spesso di livello mondiale, questa percentuale dimostra chiaramente che esistono ancora importanti margini di miglioramento.

Trend globali per il 2015

Dopo aver analizzato i dati del 2014, siamo in grado di esprimere quelle che a nostro avviso saranno le principali tendenze per il 2015.

Social Networks al centro del mirino

Le piattaforme di Social Networking saranno utilizzate non solo, come già avviene, come uno dei principali vettori di attacco per la diffusione di malware e per effettuare frodi basate su social engineering, ma anche come campo di battaglia nella lotta tra governi ed organizzazioni terroristiche (tra le quali l'IS). In quest'ottica, gli utenti saranno oggetto di crescenti attività di psychological warfare[52] e di perception management[53] su larga scala. Nell'ambito di queste attività di Information Warfare le stesse piattaforme di Social Networking potrebbero essere direttamente attaccate.

POS, il tallone d'Achille del Retail

Data la fragilità intrinseca dei sistemi POS rispetto all'evoluzione delle minacce occorsa nel 2014, la difficoltà oggettiva nel sostituirli rapidamente e la facilità con la quale i criminali possono monetizzare questo genere di attacchi, questi apparecchi saranno sempre più bersagliati. Non saranno colpite soltanto le grandi organizzazioni ma, con la diffusione di malware sviluppato ad-hoc acquistabile per pochi dollari da criminali comuni, subiranno attacchi anche singoli ristoranti, bar, benzinai, negozi etc. Le banche dovranno fare fronte ad una quantità maggiore di frodi e al crescente scontento degli utenti finali.

Mobile, strategie da rivedere velocemente

La grande rapidità mostrata dagli attaccanti nel cambiare "modello di business" unita alla definitiva affermazione dei device mobili (smartphone e tablets) sui PC tradizionali implica un aumento sostanziale di attacchi verso questo genere di strumenti, peraltro già in atto. Tutte le piattaforme saranno sotto assedio, ed in particolare quelle più difficili da compromettere (iOS e Windows Phone) saranno oggetto di crescenti attenzioni da parte di agenzie governative, spie mercenarie e criminali. In conseguenza di ciò, produttori di device mobili, sviluppatori di applicazioni ed utenti (corporate e finali) saranno costretti a rivedere le proprie strategie ed i propri investimenti in materia di mobile, ponendo l'accento sulla sicurezza e non più solo sugli aspetti marketing o di business.

[52] http://en.wikipedia.org/wiki/Psychological_warfare

[53] http://en.wikipedia.org/wiki/Perception_management

Ricatti ed estorsioni nei confronti di aziende, PA ed Infrastrutture Critiche

Le logiche estorsive che hanno dato origine a ransomware di grande successo quali Cryptolocker[54] continueranno ad estendersi, colpendo non solo gli utenti finali e le aziende, ma anche la PA ed i sistemi industriali, incluse le Infrastrutture Critiche. Questi attacchi saranno compiuti sia per ragioni politiche che economiche, consolidando un trend di crescente collaborazione tra gruppi cyber criminali e gruppi terroristici o paramilitari. Sarà di estrema importanza prevenire nei modi più opportuni queste minacce, e gestirle al meglio qualora si dovessero concretizzare.

Diffusione di strumenti assicurativi contro rischi "cyber"

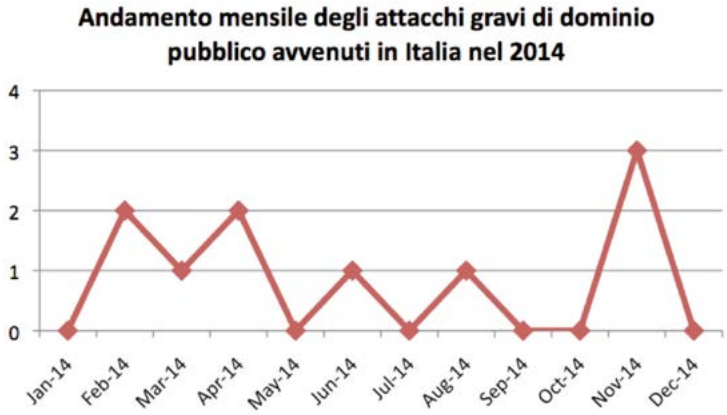
A fronte dell'aumentata rischiosità per le imprese di fare business tramite la Rete e gli strumenti informatici, e della difficoltà di implementare rapidamente misure correttive adeguate a mitigarli, si diffonderà una domanda di strumenti assicurativi per trasferire i rischi "cyber".

Questa domanda sarà parzialmente frustrata dalla scarsità di offerta, e soprattutto dall'impossibilità di assicurare organizzazioni spesso prive delle più elementari misure di sicurezza (in particolare PMI e studi professionali) per mancanza di requisiti. Si diffonderanno comunque per prime quelle polizze che offrono qualche forma di tutela legale per le vittime, e con maggiore lentezza quelle che prevedono un risarcimento dei danni subiti.

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

Analisi degli attacchi italiani gravi di dominio pubblico del 2014

All'interno del database CLUSIT solo 10 attacchi del 2014 si riferiscono a bersagli italiani (poco più dell'1% del totale mondiale), numero certamente poco plausibile, dato che l'Italia si posiziona ai primi posti nel mondo per diffusione di malware[55], e che il 39% delle aziende italiane intervistate nel 2014 dal Ponemon Institute ha dichiarato di aver subito almeno un attacco informatico andato a buon fine nei 12 mesi precedenti[56].
Ancora, il Microsoft Security Intelligence Report[57] nel 1H 2014 riporta per l'Italia un tasso di esposizione a malware del 20%, contro una media mondiale del 19% (ed una percentuale addirittura doppia di infezioni da Password Stealers e Monitoring Tools rispetto ai principali Paesi), mentre negli Stati Uniti, in Inghilterra e in Francia questo valore è compreso tra il 12 e il 13%.
Infine, dall'analisi FASTWEB delle prossime pagine emerge chiaramente quale sia la situazione reale sul campo. La bassa percentuale di attacchi gravi di dominio pubblico contro bersagli italiani conferma quindi solo la cronica mancanza di informazioni che affligge il nostro Paese su questo tema, il che rappresenta un ulteriore vantaggio per criminali e malintenzionati.
Ciò premesso, analizziamo e commentiamo i 10 incidenti italiani del nostro campione, cominciando dalla distribuzione temporale degli attacchi.



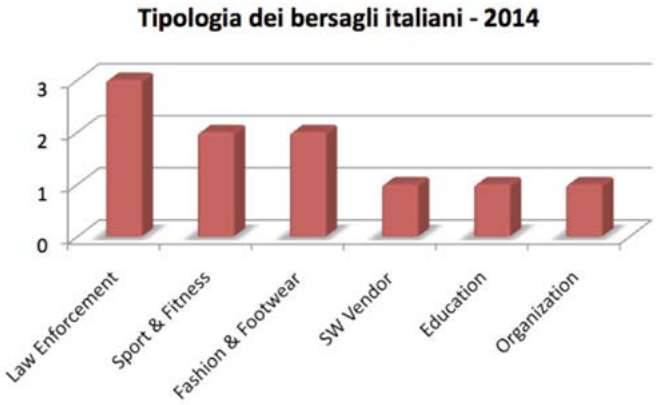
© Clusit - Rapporto 2015 sulla Sicurezza ICT in Italia

[55] http://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/

[56] http://www-935.ibm.com/services/us/en/it-services/security-services/cost-of-data-breach/

[57] http://www.microsoft.com/en-us/download/details.aspx?id=44937

La classificazione dei bersagli colpiti è la seguente:

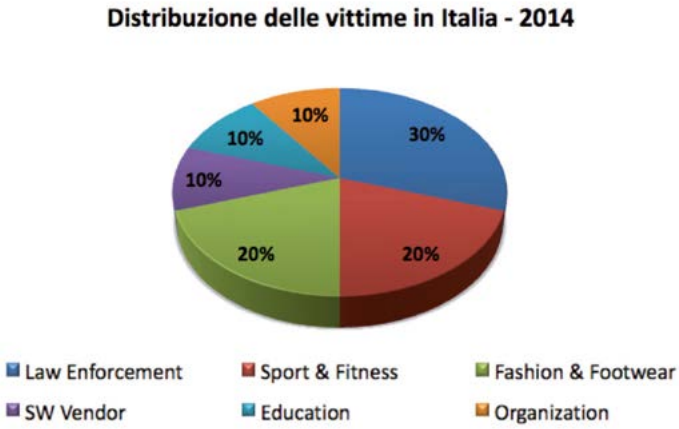


© Clusit - Rapporto 2015 sulla Sicurezza ICT in Italia

Mentre i bersagli appartenenti alla categoria Law Enforcement sono stati colpiti da attaccanti appartenenti all'Hacktivism (40%), tutti gli altri sono stati oggetto di attività cyber criminali (60%):

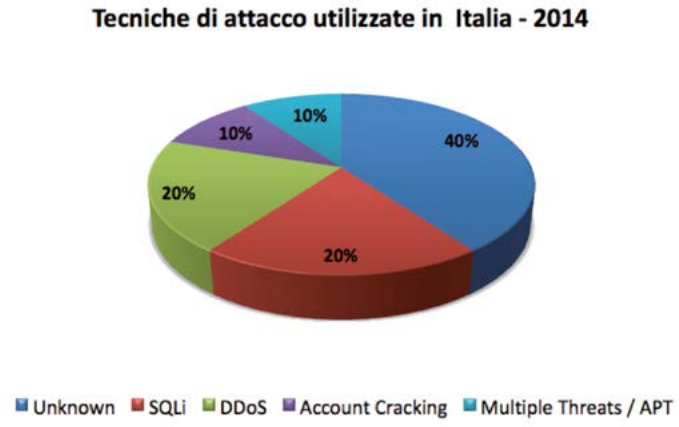
© Clusit - Rapporto 2015 sulla Sicurezza ICT in Italia

Questa la distribuzione percentuale delle vittime nel 2014, decisamente differente da quella rilevata l'anno scorso, quando la categoria dei bersagli governativi era prevalente (68%), mentre quest'anno rappresenta solo il 30% degli incidenti noti:



© Clusit - Rapporto 2015 sulla Sicurezza ICT in Italia

Per quanto riguarda la classificazione delle tecniche di attacco utilizzate, dal grafico seguente si possono ricavare una serie di interessanti considerazioni:



© Clusit - Rapporto 2015 sulla Sicurezza ICT in Italia

In un campione dominato dalla presenza di attaccanti di tipo criminale, prevalgono gli incidenti causati da tecniche sconosciute (che passano al 40% dal 14% del 2013), SQLi (in crescita al 20% dal 11% del 2013) e DDoS (in calo, essendo lo strumento più usato dagli Hacktivist), seguiti da quelli basati sul furto di account (in crescita dal 3% del 2013) e dalle APT, che passano dal 3% al 10%.
In particolare quest'ultimo dato, unito alla prevalenza relativa di vulnerabilità Unknown, dà una misura dell'incremento dei livelli di rischio avvenuto nell'ultimo anno.

BIBLIOGRAFIA

Oltre alle fonti già citate in questa «Panoramica degli eventi di cyber-crime e incidenti informatici più significativi del 2014 e tendenze per il 2015», segnaliamo altre fonti e Report che abbiamo preso in considerazione.

[1] Akamai Security Reports
http://www.stateoftheinternet.com/resources-state-of-the-internet-security-and-prolexic-global-ddos-attack-reports.html

[2] Report semestrale sulla sicurezza Cisco 2014
http://www.cisco.com/web/IT/offers/lp/midyear-security-report/index.html

[3] "Sicurezza Informatica in Azienda" Ricerca Europea Cisco 2014
http://www.cisco.com/web/IT/press/cs14/20141027.html

[4] Cisco Annual Security Report 2015
www.cisco.com/web/offers/lp/2015-annual-security-report/index.html?keycode=000656511

[5] Panorama de la Cyber-Criminalité – Année 2014 - CLUSIF
https://www.clusif.asso.fr/fr/production/ouvrages/pdf/CLUSIF_Pano-2014_20150114_VF.pdf

[6] Threat Landscape and Good Practice Guide for Internet Infrastructure - ENISA
http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-thematic-landscapes/threat-landscape-of-the-internet-infrastructure/iitl/at_download/fullReport

[7] ENISA Threat Landscape 2014 - Overview of current and emerging cyber-threats - ENISA
http://www.enisa.europa.eu/activities/risk-management/evolving-threat-environment/enisa-threat-landscape/enisa-threat-landscape-2014/at_download/fullReport

[8] IBM X-Force Threat Intelligence 2014
http://www.ibm.com/security/xforce/

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

[10] FEEL FREE – a new approach to Cyber Security - KPMG
http://www.kpmg.com/IT/it/IssuesAndInsights/ArticlesPublications/Pagine/Free-Feel.aspx

[11] FTSE 350 Cyber Governance Health Check Tracker Report - KPMG
http://www.kpmg.com/uk/en/topics/cyber-security/Pages/ftse350-cyber-governance-health-check.aspx

[12] Razor Sharp Insights - KPMG
https://www.kpmg.com/UK/en/topics/cyber-security/Pages/razor-sharp-insights.aspx

[13] Rapporti semestrali – MELANI
http://www.melani.admin.ch/dokumentation/00123/00124/01590/index.html?lang=it

[14] 2014 Italian Cyber Security Report – Consapevolezza della minaccia e capacità difensiva della Pubblica Amministrazione Italiana - Research Center of Cyber Intelligence and Information Security "SAPIENZA" - Università di Roma
http://www.cis.uniroma1.it/media/CIS%20Resources/2014CIS-Report_web.pdf

[15] Harvard Business Report di TrendMicro
http://www.trendmicro.it/campaigns/harvard-business-review/report/index.php

[16] Previsioni Trend Micro per il 2015
http://www.trendmicro.it/trendlabs/security-roundup/2014/previsioni-sulla-sicurezza-2015/index.html

[17] Report delle minacce del primo trimestre 2014
http://www.trendmicro.it/newsroom/pr/litalia-conferma-il--posto-nella-classifica-delle-nazioni-che-spammano-di-pi/index.html

[18] Report delle minacce del secondo trimestre 2014
http://www.trendmicro.it/newsroom/pr/italia-terza-al-mondo-per-visite-a-siti-maligni/index.html

[19] Report delle minacce del terzo trimestre 2014
http://www.trendmicro.co.uk/media/misc/rpt-vulnerabilities-under-attack.pdf

[20] Websense 2015 Security Predictions Report – WEBSENSE
http://it.websense.com/content/2015-predictions-report.aspx

© Clusit 2015

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

Introduzione e visione d'insieme

Il 2014 ha visto sicuramente un incremento della sensibilità riguardo i rischi legati alla sicurezza informatica in tutti gli attori coinvolti.

La maggior parte delle aziende italiane non ha una persona dedicata ad occuparsi dei rischi informatici; solitamente nelle piccole e medie aziende questa responsabilità ricade sul responsabile dei sistemi informativi. Dalla mancanza di una figura, come l'IT Security Manager, in grado di far dialogare in maniera proficua il business con i problemi tecnici ed i rischi ad essi connessi, ne consegue una ridotta capacità nel pianificare un'adeguata strategia mirata ad affrontare il problema.

Occorre inoltre prendere atto che, la sensibilità su questi argomenti nasce più dalle informazioni apprese attraverso i mass media, che tramite i canali specializzati (paper scientifici, corsi, congressi, etc).
Ne scaturisce un'idea vaga di come e dove investire il budget dedicato ad affrontare questi problemi così che spesso si rischia di essere guidati più dalle sensazioni che dal livello effettivo di rischio.

Proprio per questo motivo, Fastweb ha deciso di raccogliere, aggregare, anonimizzare, catalogare ed analizzare tutte le minacce informatiche gestite dal Security Operation Center durante il 2014, per poter mettere a disposizione di tutti una base statistica che costituisca un buon punto di partenza per affrontare questi temi in un'ottica di collaborazione tra le entità coinvolte dal fenomeno.

Una prima risposta è arrivata dal settore del banking/finance. Gli istituti finanziari hanno infatti quasi tutti sottoscritto servizi per la protezione da attacchi DDoS, e qualora non lo avessero già fatto, ne hanno quantomeno esplorato costi e modalità di funzionamento.
Gli attacchi di questo tipo sono infatti un fenomeno talmente frequente che, se si effettua business online o internet è parte integrante del core business dell'azienda, non si può più pensare di ignorarlo.

Dati analizzati

Per riuscire a comprendere al meglio i contenuti dell'analisi è necessario un piccolo approfondimento legato ai dati utilizzati per scrivere questo rapporto.
In particolare, quest'anno abbiamo analizzato oltre 5 milioni di eventi di sicurezza contro i 172 mila circa dell'anno scorso. Abbiamo quindi ampliato la base di dati utilizzata perfezionando ulteriormente l'analisi.

Il dominio di analisi è costituito dai dati relativi a circa 6 milioni di indirizzi IPv4 appartenenti all'AS Fastweb SpA (quindi sia quelli dei Clienti che di Fastweb stessa) raccolti ed analizzati dal Security Operations Center.
In particolare, i dati relativi a malware e botnet sono stati ricavati da un mix di strumenti interni e servizi esterni come quelli offerti, ad esempio, dall'organizzazione Shadowserver Foundation.
I dati relativi a casi di *defacement*, sono stati ricavati sia da segnalazioni ricevute internamente che da fonti pubblicamente accessibili su Internet.
I dati sugli attacchi di Distributed Denial of Service sono stati ricavati da tutte le anomalie DDoS rilevate dalle tecnologie di Fastweb per il contrasto a questo tipo di attacchi.

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

Le minacce

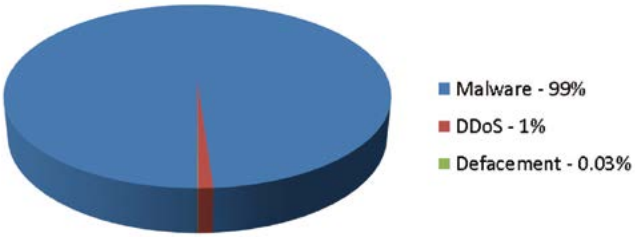
Le principali minacce

Ancora oggi ed in quantità sempre maggiore, la principale fonte di minacce continua ad essere la diffusione di software malevolo, utilizzato principalmente con finalità illecite, come le piccole frodi oppure la costruzione di reti di computer zombie (botnet) costruite con lo scopo di effettuare altre attività illecite come attacchi di tipo DDoS, invio di spam, etc.
Ricordiamo che alla base di questa enorme diffusione di questo vettore di attacco, vi sono alcuni fattori tra i quali:

- la facilità nel reperire gli strumenti necessari alla generazione di nuovo software malevolo: si vendono o trovano in rete dei "kit" per costruire un malware ad hoc a cui si possono comprare ed agganciare nuove funzionalità personalizzate;
- la remuneratività dell'utilizzo di questo come vettore d'attacco: il guadagno è inversamente proporzionale alla possibilità di essere rintracciati;
- la diffusione sempre maggiore di nuove piattaforme interconnesse tra loro, o direttamente connesse alla Big Internet ha ampliato il dominio delle vittime potenziali.

È comunque importante sottolineare come anche le tecniche di rilevazione siano decisamente evolute negli ultimi mesi, permettendo di scoprire alcune tipologie di malware che prima restavano sconosciute.
Le numeriche legate al fenomeno appena descritto, fanno quasi passare in secondo piano un secondo vettore d'attacco, che rimane comunque molto efficiente, gli attacchi DDoS. Il numero di eventi di questa categoria è cresciuto di sedici volte nell'ultimo anno. È opportuno sottolineare che vi è una correlazione alla base della crescita numerica di entrambe i fenomeni; infatti la diffusione di malware ha anche come obiettivo quello di costruire la

base operativa, chiamata in gerco tecnico botnet, utilizzata successivamente per lanciare attacchi di tipo DDoS.
Raddoppia quasi il numero di eventi in cui una pagina web è stata modificata illecitamente (*defacement*), azione che conserva la sua natura puramente dimostrativa.



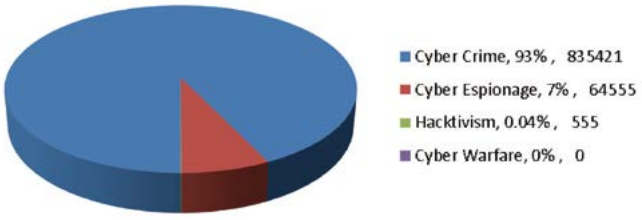
Dati FASTWEB relativi all'anno 2014

Figura 1: tipologie di attacchi informatici rilevati

Ovviamente, a causa della loro natura, non è dato sapere quale sia il valore di altre categorie, sicuramente meno appariscenti in termini di quantità ma non meno in termini di minaccia come gli APT (Advanced Persistent Threat) o più in generale attacchi 0day.

Motivazione degli attacchi

In analogia con quanto riportato nel precedente rapporto, la motivazione principale per cui vengono perpetrati attacchi informatici rimane quella criminale. In particolare il 93% degli attacchi è legato al Cyber Crime, mentre il 7% ha come obiettivo il furto di dati, come credenziali di accesso o altre informazioni sensibili.

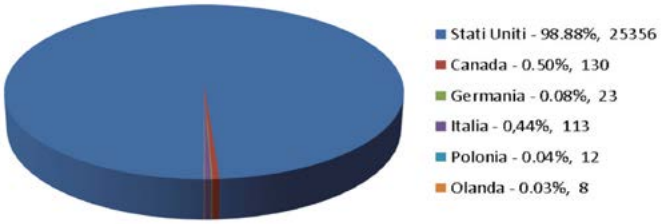


Dati FASTWEB relativi all'anno 2014

Figura 2: Motivazione degli attacchi

Distribuzione geografica dei centri di comando e controllo dei malware

I centri di comando e controllo (C&C) sono quegli host utilizzati per l'invio dei comandi alle macchine infette (bot) dal malware utilizzato per la costruzione della botnet. Tali host fungono da ponte nelle comunicazioni tra gli host infetti e chi gestisce la botnet, al fine di rendere più difficile la localizzazione di questi ultimi. Dai dati analizzati quest'anno, su un totale di oltre 25 mila C&C individuati, risulta un quadro diverso da quello presentato l'anno precedente, dove si denota una netta crescita, per non dire totale predominanza, della regione nord americana, in particolare gli Stati Uniti, che risultano essere lo stato dove sono dislocati quasi tutti i C&C che controllano gli host infetti appartenenti all'Autonomous System di Fastweb. Una sparuta rappresentanza di stati europei completa il quadro.
Inoltre un altro fattore molto interessante da analizzare è la netta diminuzione dei centri di controllo rilevati nella zona asiatica.



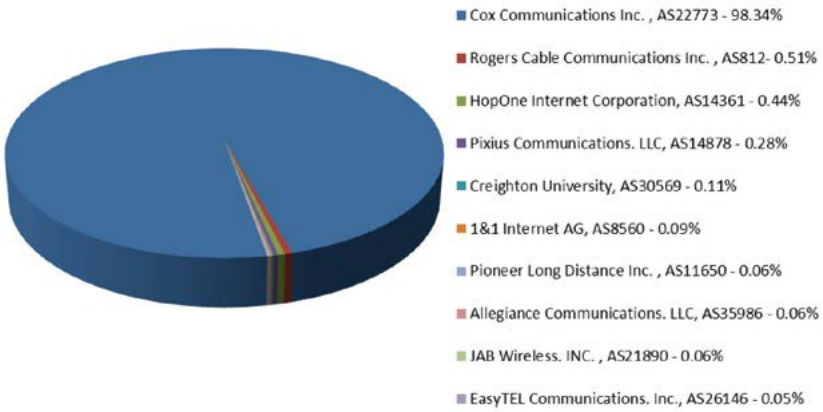
Dati FASTWEB relativi all'anno 2014

Figura 3: Distribuzione per nazione dei centri di controllo

Figura 4: Mappa geografica dei centri di controllo. Ad una maggiore intensità di colore, corrisponde una maggiore presenza di C&C.

Chi ospita più centri di comando e controllo ?

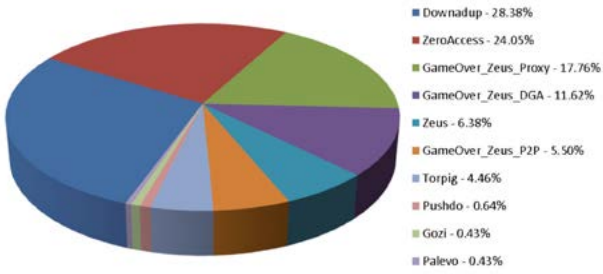
Un ulteriore aspetto interessante che abbiamo potuto cogliere quest'anno durante la fase di analisi è stata la possibilità di identificare quali società ospitano più Centri di Comando e Controllo di botnet. Tuttavia essendo quest'analisi basata sugli Autonomous System, occorre precisare che le società elencate in figura 5 sono da distinguere tra chi svolge il ruolo di ISP, come nel caso di Cox Communications , Rogers Cable o Pixius offrendo esclusivamente la connettività ai C&C e chi come HopOne e 1&1 Internet AG, offre un servizio hosting di server che consciamente o inconsciamente agiscono da C&C.



Dati FASTWEB relativi all'anno 2014

Figura 5: Distribuzione dei centri di controllo

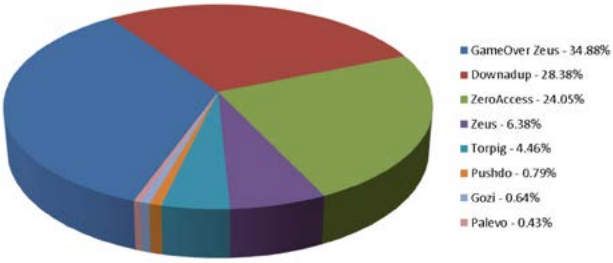
Come precedentemente esposto, i malware rappresentano la grande maggioranza delle minacce rilevate. Anche quest'anno sono state individuate tipologie di malware riconducibili alle famiglie di botnet presentate nella passata edizione del rapporto Clusit.



Dati FASTWEB relativi all'anno 2014

Figura 6: Tipologie Malware rilevate

Quest'anno troviamo in prima posizione tra la botnet GameOver Zeus la cui diffusione è garantita mediante ampie campagne di spam con mail contenenti allegati malevoli, ad esempio il famigerato Cryptolocker, o link che puntano a risorse malevole. In seconda posizione resiste ancora Downadup, alias Conficker, che nonostante passino gli anni rimane ampiamente diffusa, sfruttando una vulnerabilità presente in alcuni sistemi operativi Windows. Seppur abbia registrato un calo, sono ancora molti i sistemi infetti da ZeroAccess, un altro trojan horse che colpisce i sistemi operativi Microsoft Windows, tramite siti web che contengono script o plugin mirati a sfruttare eventuali vulnerabilità presenti nel browser del visitatore.



Dati FASTWEB relativi all'anno 2014

Figura 7: Le Botnet più diffuse

Nel campo dei Banking Trojan, oltre alla sempre presente botnet Zeus, troviamo casi di diffusione di Torpig, che tipicamente infetta il browser ed usa la tecnica del Man-in-the-Browser, ossia l'emulazione del comportamento dell'utente al fine da indurre il sito bancario a credere che le istruzioni alterate ricevute, siano quelle effettivamente inserite dall'utente. Si registrano infine casi di diffusione dei trojan Gozi, e di Pushdo.

Analisi temporale diffusione malware

I dati Fastweb, relativi alla diffusione malware, e riportati nei grafici sottostanti, mostrano un andamento piuttosto regolare durante il corso dell'intero anno.

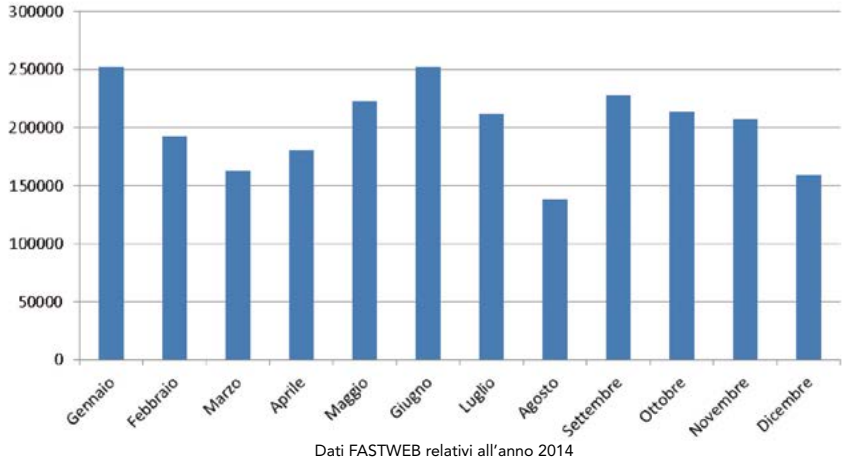


Figura 8: Distribuzione mensile malware

Il calo presente durante il mese di Agosto rispecchia il fermo delle attività lavorative per la pausa estiva, e il ridotto numero di host infetti o infettanti attivi sulla rete.
Rispetto al report dell'anno precedente, il metodo di analisi utilizzato ha, sia permesso l'aggregazione dei dati per una loro rappresentazione generale, sia l'analisi di singoli casi, come l'evoluzione nel tempo delle singole famiglie di malware.

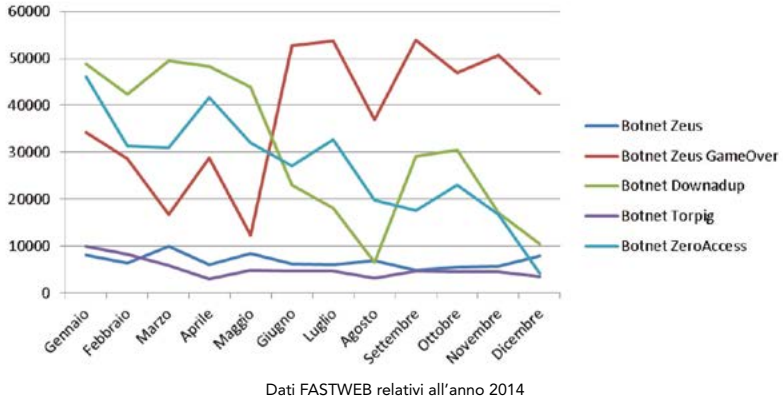


Fig 9: Diffusione delle 5 principali famiglie di malware

Lo stesso metodo di analisi ha permesso di approfondire l'andamento nel corso del 2014, della botnet Zeus GameOver, mostrato in dettaglio nella figura 10. Questo andamento rispecchia la risposta all'operazione Tovar, condotta durante l'estate scorsa dall'autorità giudiziaria americana con l'obiettivo di smantellare la rete P2P nata per decentralizzare le comunicazioni con i centri di comando e controllo. Nonostante tale tentativo, a partire dall'inizio di Luglio, si è vista la diffusione dell'altra variante del malware, DGA, che prende nome dell'algoritmo usato per generare randomicamente i domini e non fa più uso delle comunicazioni P2P ma si basa sulla tecnica Fast-Flux, che permette di nascondere i DNS usati per la risoluzione dei domini malevoli dietro ad una rete di macchine compromesse in continua mutazione e perciò difficili da mappare e spegnere.
Tale cambio di strategia ha permesso agli autori della botnet di riprenderne il controllo, e rafforzare la diffusione del malware dopo il temporaneo calo registrato a Giugno, come mostrato nel dettaglio nel grafico in fig. 10

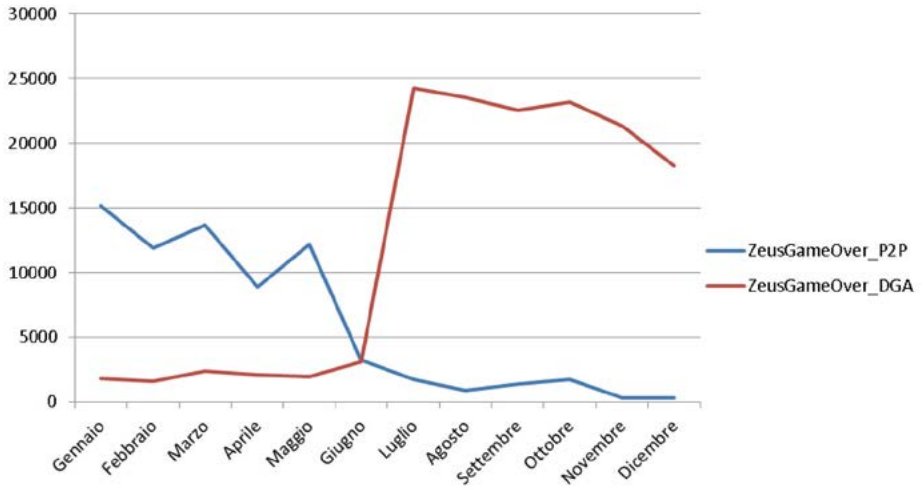


Figura 10: Distribuzione Temporale Zeus GameOver_P2P - ZeusGameOver_DGA

Defacement

Quanti sono i defacement?

Un altro diffuso scopo degli attacchi sono i defacement, cioè la variazione di una pagina web (tipicamente la home page) a scopi dimostrativi. Come possiamo facilmente notare dai grafici, questo tipo di attività non ha una enorme diffusione. Durante il 2014 abbiamo registrato oltre 550 casi di atti di defacement portati a buon fine, con un incremento degli eventi nel periodo estivo.

In questo caso la base di dati analizzata sono stati tutti i domini web di Clienti che hanno un IP appartenente all'Autonomous System di Fastweb. Nello specifico è stato fatto un conteggio per domini poichè è stato notato che quando un attaccante riesce ad entrare nel server dove il dominio è ospitato, generalmente modifica il numero più alto possibile di URL attestate sul medesimo dominio.

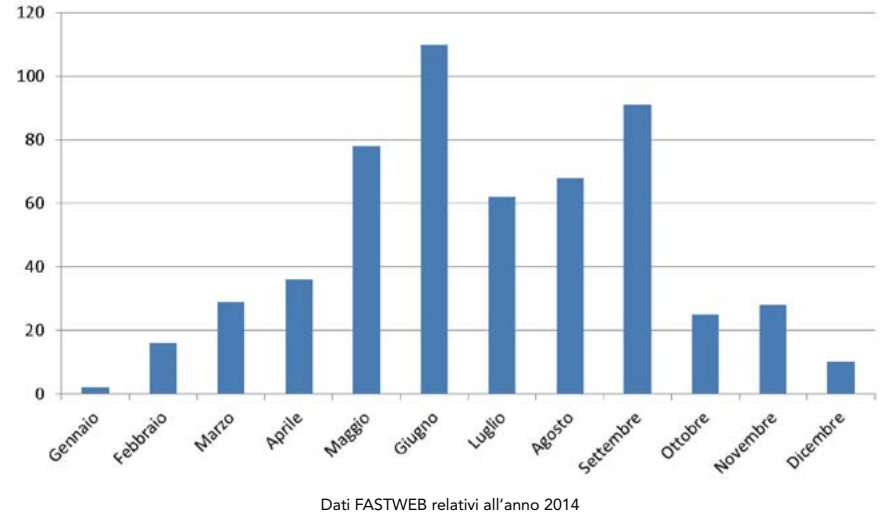
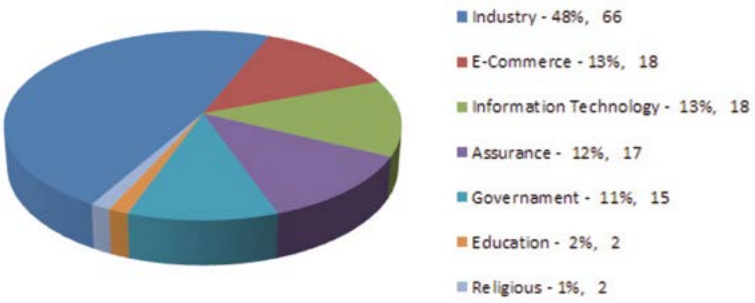


Figura 11: Numero defacement durante l'anno

Chi è obiettivo di un defacement?

I dati in merito ai defacement mostrano percentuali simili a quelle rilevate l'anno scorso. La maggior parte dei siti web che hanno subito un defacement appartengono al settore privato, ed in particolare siti web di piccole e medie imprese, seguiti dalla categoria dei siti E-Commerce, la cui percentuale è salita rispetto all'anno passato dell'11%, cosi come le categorie di siti Governativi e quelli legati all'ambiente Assicurativo. Questo non vuol dire necessariamente che le piccole e medie imprese siano prese di mira più facilmente, ma potrebbe voler dire che i siti di questo genere di imprese sono mediamente più vulnerabili.



Dati FASTWEB relativi all'anno 2014

Figura 12: Categorizzazione dei siti che hanno subito un defacement

Attacchi Distributed Denial of Service

Un capitolo a parte viene costituito dagli attacchi di tipo Distributed Denial of Service (DDoS), attacchi volti a rendere inaccessibili alcuni tipi di servizi. Questo genere di attacchi possono essere divisi in due tipologie differenti: volumetrici ed applicativi.
Gli attacchi di tipo volumetrico mirano a generare un volume di traffico maggiore o uguale alla banda disponibile in modo da saturarne le risorse.
Gli attacchi di tipo applicativo mirano a generare un numero di richieste maggiore o uguale al numero di richieste massimo a cui un server può rispondere (es. numero di richieste web HTTP/HTTPS concorrenti).

Come più volte sottolineato, compiere questo genere di attacchi è divenuto sempre più semplice, soprattutto grazie a servizi facilmente acquistabili tramite carte di credito prepagate e bitcoin che permettono di effettuare questi attacchi senza possedere alcuna capacità tecnica particolare.

Quanti sono i DDoS?

Durante il 2014 abbiamo rilevato più di 16000 anomalie riconducibili ad attacchi DDoS, dirette verso i Clienti Fastweb. L'andamento del primo semestre si è diversificato rispetto al secondo semestre, con un deciso incremento negli ultimi mesi dell'anno.
L'aumento generale delle anomalie rilevate, porta ad inserire questo vettore d'attacco come una tecnica diventata di uso comune, favorita anche dalla proliferazione di malware, che vengono creati appositamente per perpetrare attacchi simili.

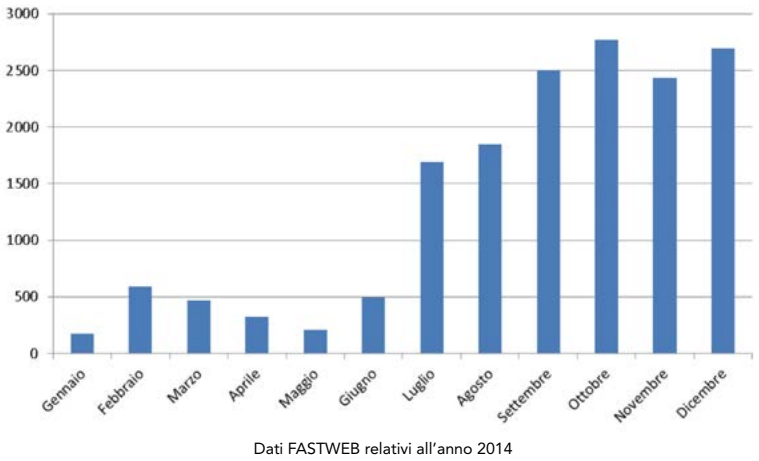
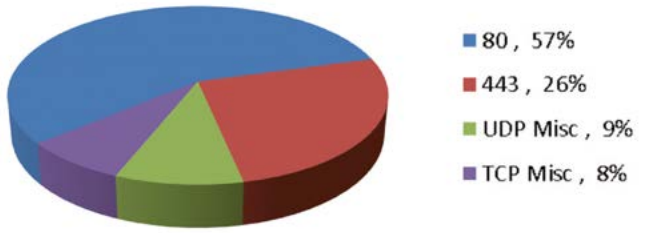


Figura 13: Distribuzione Mensile attacchi DDoS

Quali sono i servizi attaccati da un DDoS

Com' è possibile verificare dal grafico sotto riportato, gli attacchi DDoS vanno maggiormente ad impattare i servizi web, attaccando i protocolli http e https, mirando a rendere tali servizi irraggiungibili dagli utenti.
Tuttavia non è l'unico caso registrato, sono stati verificati anche casi in cui gli attacchi DDoS sono stati mirati a negare altre tipologie di servizi come, ad esempio, il servizio di risoluzione dei nomi, o DNS.

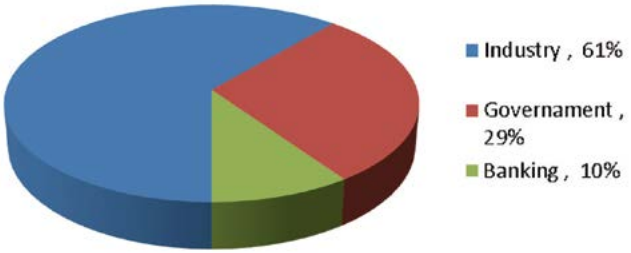


Dati FASTWEB relativi all'anno 2014

Figura 14: DDoS Top Target Ports

Chi è vittima di un attacco ddos?

La rilevazione effettuata durante l'anno indica che i tre principali obiettivi degli attacchi DDoS sono le istituzioni governative (Ministeri, Pubbliche Amministrazioni locali e centrali, etc), le banche ed il settore industriale.



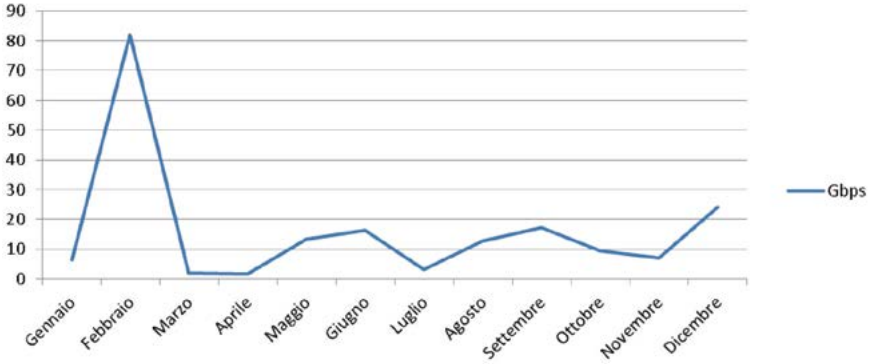
Dati FASTWEB relativi all'anno 2014

Figura 15: DDoS Target Categories

Il volume degli attacchi DDOS

L'anno precedente si era chiuso con un incremento del volume di traffico generato dagli attacchi DDoS e questo si è poi concretizzato nel corso del 2014, nel quale si sono registrati picchi di traffico che dimostrano come la potenza di attacco sia effettivamente aumentata, merito anche della sempre maggiore diffusione di connettività a banda larga che aumenta il fattore di amplificazione, incrementando perciò i volumi di traffico.

Questa considerazione nasce dall'osservazione che la tecnica di attacco DDoS più diffusa sia quella detta "reflected", i cui dettagli sono illustrati nel paragrafo successivo.



Dati FASTWEB relativi all'anno 2014

Figura 16: Volume traffico DDoS

I valori raggiunti portano a considerare ormai come prioritaria per le aziende, l'"implementazione di una strategia a protezione, o l'adozione di questa lato ISP.

Tecniche di attacco utilizzate

Le tecniche di attacco utilizzate durante l'esecuzione dei DDoS rilevati, non presentano particolari novità tecniche.
Parte degli attacchi rilevati è rappresentata da "TCP Synflood" (o half open) tramite il quale l'attaccante, forgiando pacchetti SYN in cui è falsificato l'IP mittente (spesso inesistente), impedisce la corretta chiusura del three-way handshake, in quanto, nel momento in cui il server web vittima invia il SYN/ACK, non ricevendo alcun ACK di chiusura, poichè l'IP destinatario è inesistente, lascerà la connessione "semi-aperta". Nel caso di un invio massivo di pacchetti SYN in concomitanza ad un alto tempo di timeout delle connessioni, il buffer del server verrebbe presto saturato, rendendo il server impossibilitato ad accettare ulteriori connessioni TCP, anche se legittime.

Vi è poi la variante "SYN-BY FIN", opposta alla precedente tipologia di attacco, durante la quale l'attaccante instaura delle brevi e legittime connessioni con il server target, connessioni che subito dopo cerca di terminare con l'invio di pacchetti FIN. L'host vittima, dopo aver inviato un pacchetto FIN/ACK all'attaccante, rimarrà (come nel caso delle connessioni semi-aperte) invano in attesa dell'ACK finale per chiudere la connessione. Anche in questo caso, l'nvio di un elevato numero di pacchetti FIN può portare alla saturazione del buffer causando un disservizio.
Successivamente abbiamo attacchi di tipo "UDP Flood", più semplici da realizzare in quan-

to, a differenza del protocollo TCP, il protocollo UDP non prevede l'instaurazione di una connessione vera e propria e possiede tempi di trasmissione/risposta estremamente ridotti. Tali condizioni offrono maggiori probabilità di esaurire il buffer tramite il semplice invio massivo di pacchetti UDP verso l'host target dell'attacco.
La tecnica più diffusa è il DRDoS – Distributed Reflection Denial of Service, la cui particolarità è quella di sfruttare host esposti sulla Big Internet come riflettori del traffico a loro indirizzato. Questa tipologia di attacco DDoS ha portato alla luce la presenza di vulnerabilità intrinsiche ad alcuni protocolli utilizzati giornalmente per attività lecite, come i protocolli NTP o DNS; il primo vulnerabile mediante il comando monlist, il secondo mediante un'errata configurazione del servizio di risoluzione dei nomi. Sfruttando lo spoofing dell'indirizzo IP di una vittima, un utente malintenzionato può inviare piccole richieste ad un host vulnerabile inducendolo ad indirizzare le risposte alla vittima dell'attacco. Questa tipologia di DDoS permette al malintenzionato di amplificare la potenza del suo attacco anche di 600 volte, come dimostrato nel caso del protocollo NTP.

Distribuzione mensile mitigation attivate

Di seguito viene riportata la distribuzione mensile delle mitigation attivate dal Security Service Operations Center di Fastweb. Con *mitigation* viene inteso l'insieme di contromisure messe in campo al fine di neutralizzare l'attacco DDoS in corso. Tali contromisure vengono applicate solo nel caso in cui, a seguito di analisi specialistica, l'anomalia di traffico rilevata e registrata dagli strumenti sia classificata come attacco conclamato e il Cliente abbia richiesto l'attivazione della protezione.

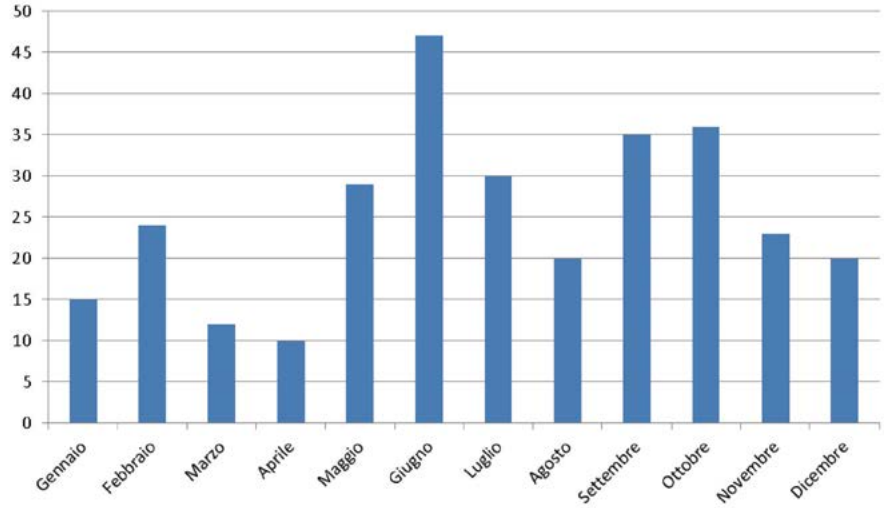
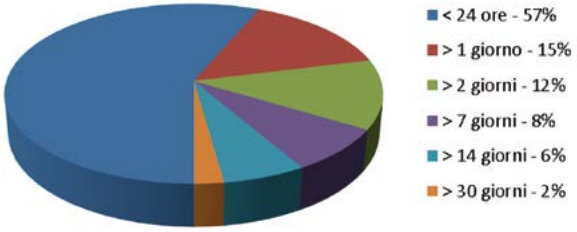


Figura 17: Mitigation Attivate

Quanto dura un attacco ddos?

I dati relativi alla durata degli attacchi DDoS dipingono uno scenario nel quale più della metà di questi dura meno di un giorno, mentre quasi il 90% del totale termina entro la settimana. Rispetto all'anno scorso il dato è decisamente cambiato, con un incremento di un fattore pari a dieci.

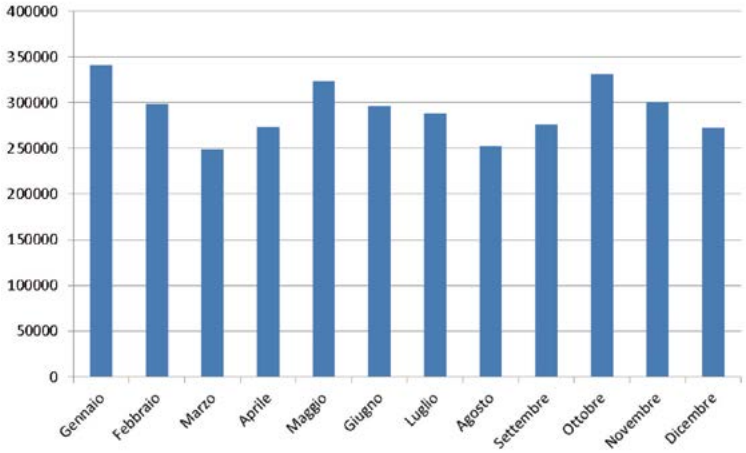


Dati FASTWEB relativi all'anno 2014

Figura 18: Durata Attacco DDoS

DNS Open Resolver

In questa sezione, si affronta il tema dei DNS Open Resolver, sistemi vulnerabili, che vengono utilizzati come stumento per perpetrare attacchi informatici. I dati sono stati raccolti, mediante l'analisi delle risposte ricevute a seguito dell'invio di una richiesta DNS a tutti gli host Fastweb con indirizzi IPv4 ,non protetti da firewall e servizio DNS attivo su porta 53/UDP. Di seguito si è proceduto a redigere una classifica delle regioni e province italiane dove sono presenti tali sistemi.



Dati FASTWEB relativi all'anno 2014

Figura 19: DNS - Distribuzione Mensile

I dati rilevati nel corso dell'anno mostrano un numero abbastanza omogeneo di DNS Open Resolver rilevati mensilmente, la cui media, fatta eccezione per alcuni casi, è intorno ai 250000 indirizzi IP. Inoltre si evince che la regione dove risultano essere presenti più server utili ad essere sfruttati, inconsapevolmente, per fini malevoli, è la regione Lombardia (l'anno scorso erano le Marche). La differenza con le altre regioni, in termini di quantità, risulta essere notevole.

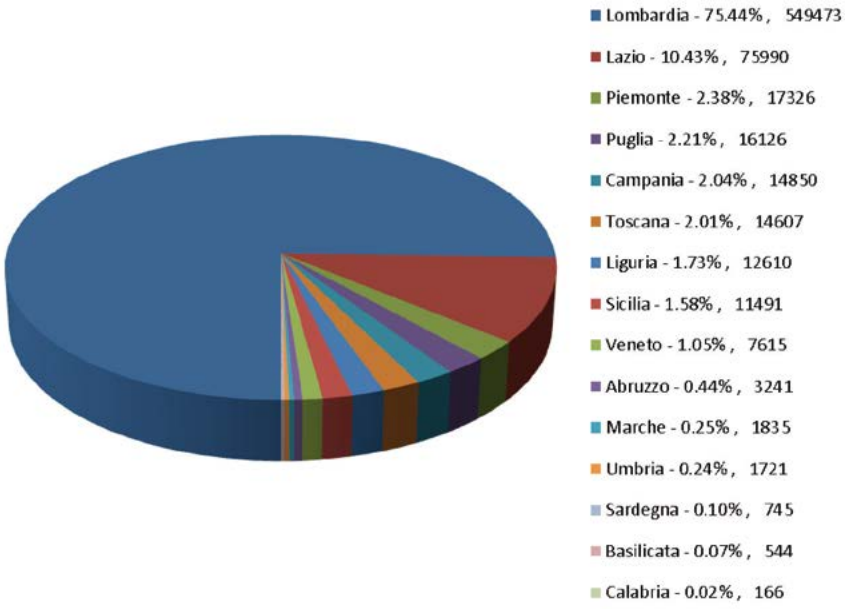


Figura 20: Diffusione sul territorio nazionale dei DNS Open Resolver - Regioni

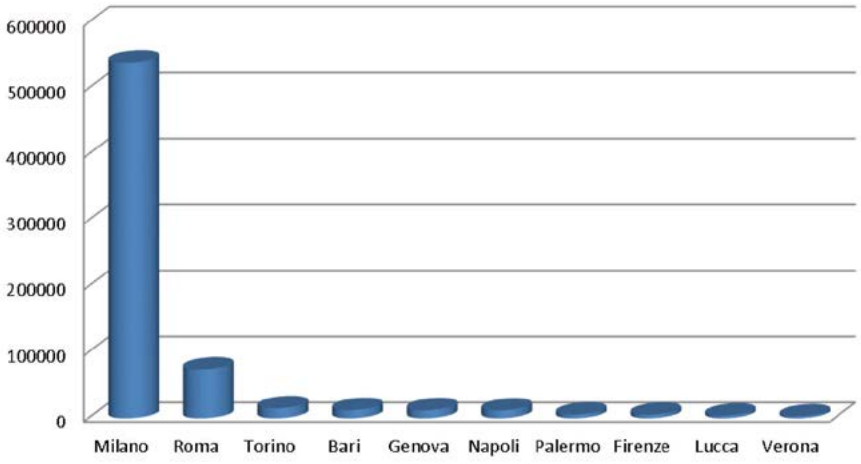


Figura 21: Diffusione sul territorio nazionale dei DNS Open Resolver - Province

Si ricorda che i dati, unicamente relativi all'AS di Fastweb, sono rilevati nell'ordine di migliaia di indirizzi IP, aggregati e riportati in un grafico esplicativo.

Considerazioni Finali

Il campo di gioco della sicurezza informatica è diventato sempre più vasto. La mole di informazioni necessaria a gestire i rischi informatici in termini di tecnologie, vulnerabilità, probabilità di sfruttamento e conoscenze è diventata talmente enorme che le forze in gioco per riuscire a contrastare queste minacce non sono più alla portata del singolo ma devono essere messe in campo delle complesse strategie che comprendano tecnologie, conoscenze ed investimenti, in uno spirito di coordinata collaborazione.

Per riuscire infatti a contrastare il cybercrime è ormai necessario uno sforzo congiunto tra tutti gli attori coinvolti: forze dell'ordine, ISP, hosting/housing provider, etc, poichè il fenomeno ha assunto una dimensione sempre più grande, su scala nazionale ed internazionale, colpendo ogni ambito lavorativo, con particolari conseguenze per le piccole/medie aziende ed i privati cittadini che sono maggiormente inconsapevoli dei rischi derivanti dal trascurare tale minaccia.

BIBLIOGRAFIA

www.f-secure.com/weblog/archives/Threat_Report_H1_2014.pdf

http://blog.shadowserver.org/2014/06/08/gameover-zeus-cryptolocker/

http://krebsonsecurity.com/2014/07/crooks-seek-rivival-of-gameover-zeus-botnet/

http://blog.malcovery.com/blog/breaking-gameover-zeus-returns?utm_campaign=Gameover+Zeus+Return&utm_source=hs_email&utm_medium=email&utm_content=13437848&_hsenc=p2ANqtz---FRHE6hHt0E6_5ZcoZgVJJWpxELsDzjKRsH4mPBla2W22gp7r3j3kV0OzKyefY88zdIjynDpBWBKF0jOLm68WSE7BKg&_hsmi=13437848

http://www.honeynet.org/node/131

https://www.fireeye.com/blog/threat-research/2014/07/operation-tovar-the-latest-attempt-to-eliminate-key-botnets.html

http://www.fbi.gov/news/stories/2014/june/gameover-zeus-botnet-disrupted

Alcuni elementi sul cyber-crime in Europa e nel Medio Oriente

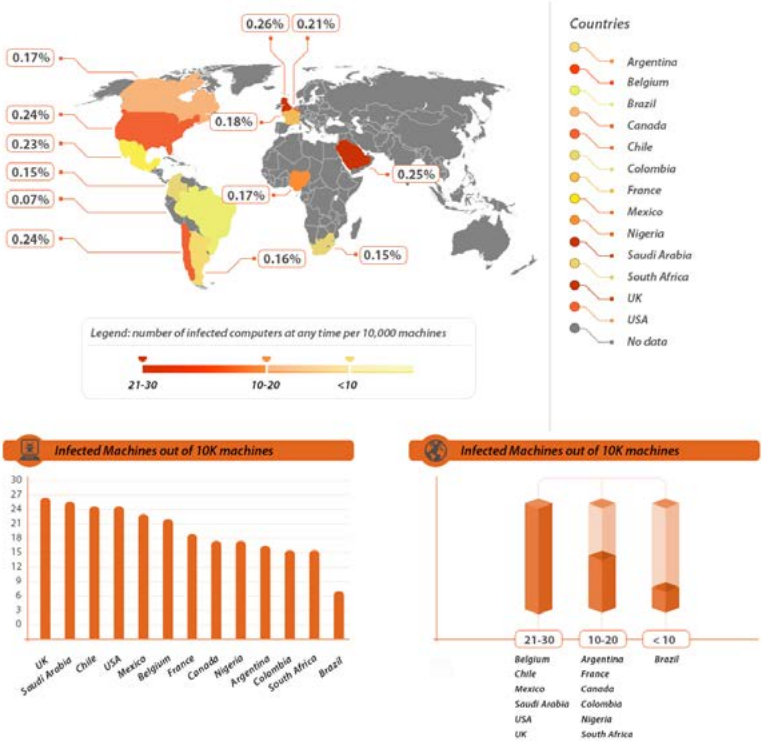
Advanced Persistent Threats

L'anno 2014 è stato caratterizzato da numerosi attacchi del tipo Advanced Persistent Threat (APT), basati su malware già noti in passato ma riutilizzati secondo una nuova connotazione. Gli APT sono schemi di attacco articolati, mirati a specifiche entità o organizzazioni, e che si contraddistinguono per un accurato studio del bersaglio, preventivo e che spesso continua anche durante l'attacco, l'impiego di tool e malware sofisticati, e la lunga durata o persistenza nel tempo cercando di rimanere inosservati per continuare a perpetrare quanto più possibile il proprio effetto.

Citadel, uno dei numerosi malware originariamente creati per attacchi e frodi a banche e istituzioni finanziarie, è stato utilizzato in maniera consistente durante l'anno anche per attacchi APT verso istituzioni non finanziarie, come ad esempio alcune aziende petrolchimiche del Medio Oriente. [PLR-101]
Citadel è una evoluzione del malware Zeus realizzato dopo la diffusione su Internet del codice sorgente di Zeus all'inizio del 2011. La prima versione di Citadel estendeva e migliorava le funzionalità già offerte da Zeus rendendolo di fatto obsoleto, includendo il supporto per Chrome e VNC, implementando tecniche di anti-tracking e codice eseguibile compresso e decompresso dinamicamente in memoria. Le comunicazioni con i server di Command-and-Control (C&C) erano state infine criptate con algoritmi derivati dall'AES, più volte aggiornati nelle successive versioni.
Citadel è un malware del tipo man-in-the-browser (MiTB) progettato e venduto nell'underground originariamente per rubare le credenziali di accesso a siti bancari e realizzare così schemi di attacco mirati alla frode finanziaria attraverso l'accesso fraudolento e il trasferimento all'esterno di quanto depositato sui conti. Il suo comportamento è tuttavia altamente configurabile attraverso un file di configurazione e comandi impartiti a runtime dai server di Command-and-Control ai quali ogni sistema infetto da Citadel si collega, realizzando così delle botnet. Queste caratteristiche rendono Citadel particolarmente flessibile nel costruire schemi di attacco verso bersagli di natura estremamente diversa e dinamicamente riconfigurabili durante l'attacco.
Gli attacchi analizzati [PLR-101] erano concentrati verso i sistemi webmail utilizzati per accedere alla email aziendale dall'esterno, rubando le credenziali di dipendenti e consulenti per poi riutilizzarle successivamente per autenticarsi ai sistemi aziendali e continuare l'accesso fraudolento.
L'analisi di IBM Security Trusteer [PLR-101] svela i dettagli dell'attacco. Il malware Citadel è stato configurato per monitorare l'accesso alle URL dei portali webmail delle aziende sotto attacco. Quando il browser accede alla URL il malware cattura tutte le informazioni dell'HTTP POST, incluse le credenziali per l'autenticazione, prima che queste vengano criptate dal browser per essere inviate all'interno del canale sicuro HTTPS.
Questa tecnica è nota come HTTP from grabbing, e rende spesso inefficacie la protezione

offerta dal meccanismo di cifratura HTTPS operata dal browser.
Le credenziali catturate vengono inviate alle organizzazioni di cyber criminali attraverso canali criptati, per poi essere riutilizzare in seguito.
Non è la prima volta che codice creato per frodi bancarie viene impiegato per altri scopi. Già del 2010 erano stati riportati casi di utilizzo del malware Zeus per attacchi verso aziende Corporate. [PLR-100]

SecurityIntelligence.com e IBM Security Trusteer mostrano [PLR-101] come il Regno Unito abbia il primato negativo della percentuale più alta al mondo di computer infetti da malware per attacchi APT con 26 computer infetti ogni 10000, seguiti in Europa dal Belgio con 21 computer ogni 10000 e dalla Francia con 18 computer ogni 10000. Questo è congruente con analisi di altri team di ricerca [PLR-102] che riportano come le organizzazioni vittime di Citadel, solo uno dei malware su cui sono costruiti gli schemi di attacco APT, siano localizzate prevalentemente in Europa.



Percentuale di computer infetti da malware per attacchi APT - Fonte: IBM Security - © 2014 IBM Corporation

Principali nazioni Europee sorgenti di malware

I ricercatori del team X-Force analizzano continuamente Internet con crawler automatici alla ricerca di siti contenti malware e mantengono aggiornato l'IP reputation database, una enorme mole di dati costituita dai risultati dell'analisi di oltre 23 miliardi di URL, applicazioni web, indirizzi IP, vulnerabilità e malware eventualmente individuato che costituisce una importante base dati per proteggere le nostre reti.

Nuovi siti o sistemi vengono continuamente creati per ospitare e distribuire malware, altri invece sono stati compromessi nel corso del tempo all'insaputa del gestore, ad esempio caricandovi codice malware all'interno di spazi pubblici di scambio file oppure ancora come allegati o link in forum pubblici.
Utenti ignari vengono poi indotti a installare malware da uno di questi siti attraverso spear phishing (phishing mirato ad uno specifico soggetto) oppure attraverso tecniche di watering-hole. Secondo quest'ultima tecnica i siti web o altre risorse condivise e utilizzate da un gruppo di utenti vengono compromesse con malware appositamente configurato per attacchi allo specifico gruppo di utilizzatori.
La Germania è la principale nazione europea per percentuale di sistemi sorgente di malware, intesi come sistemi dai quali il codice malware viene inavvertitamente installato, seguendo link o eseguendo le indicazioni di email fraudolente. In questa graduatoria la Germania da sola ospita l'8.3% di tutti i link contenenti malware [PLR-103], seguita con percentuali decrescenti da Federazione Russa, Olanda, Regno Unito (3.6%) e Francia (3.3%).
In questa graduatoria i due paesi maggiori sorgenti di malware a livello mondiale sono gli Stati Uniti, che da solo ospita il 43% dei sistemi sorgenti di malware, e la Cina con circa l'11%.
La graduatoria così presentata non tiene però conto della effettiva numerosità di sistemi e di indirizzi IP in uso in ciascuna nazione, e i risultati sono quindi sfavorevoli nei confronti delle nazioni con una più alta penetrazione di Internet. Normalizzando i dati in base allo spazio IP indirizzabile in ciascuna nazione ne esce una situazione decisamente diversa. La Lituania è il secondo paese al mondo con 9 sistemi sorgenti di malware per milione [PLR-103], preceduto solo da Hong Kong e seguito in Europa in ordine da Bulgaria, Slovacchia, Repubblica Ceca e Federazione Russa. I paesi dell'Europa dell'Est si confermano come principali sorgenti di malware, seguiti da un cospicuo gruppo nell'Europa Continentale e il Sud Europa (in ordine Irlanda, Olanda, Turchia, Germania) mentre il cyber-crime è pressoché assente nel Nord Europa, se non per la sola eccezione costituita dalla Danimarca, malgrado uno dei più alti tassi di penetrazione Internet a livello mondiale [PLR-104].
L'Europa dell'Est e in particolare la Russia continua ad essere considerata la patria di cyber-criminali altamente specializzati, in particolare sviluppatori di malware o di altri prodotti e servizi scambiati o venduti nell'underground.

Principali malware osservati nel corso dell'anno

I Ricercatori di IBM Security Trusteer hanno osservato una costante crescita del malware **Neverquest**, anche grazie ad una nuova variante [PLR-106] che ha contribuito a un picco di attività nella parte finale del 2014.
Secondo, in termini di attività, il malware Zeus 2 con un andamento piuttosto costante. Andamento invece irregolare dei malware Ramnit e Dyre, quest'ultimo individuato per la prima volta nel mese di Giugno 2014.
Nella parte conclusiva dell'anno è stato osservato anche un incremento di attività da parte di Bugat.

Neverquest è un malware scritto e usato prevalentemente per frodi bancarie, individuato per la prima volta nel 2013, ma che sembra in realtà l'evoluzione di una precedente famiglia di malware di cui in parte condivide l'infrastruttura dei server di Command-and-Control. Neverquest modifica la visualizzazione di alcuni siti bancari all'interno di browser compromessi, inserendo form e contenuti con l'obiettivo di catturare le credenziali di accesso inviandole verso l'esterno in forma criptata.
Tra gli obiettivi principali della nuova variante di Neverquest [PLR-106] ci sono alcune istituzioni finanziarie di Europa e Nord America. La variante analizzata comprendeva una lista di circa 300 obiettivi, prevalentemente istituzioni finanziarie oltre che siti di online gaming e i principali social networks.
Il malware è veicolato attraverso diversi canali, inclusi downloader e drive-by exploit kit. Uno dei downloader sfrutta la rete di anonimizzazione Tor per scaricare il nucleo principale del codice. Il fenomeno dei drive-by exploit kit è particolarmente insidioso e si realizza inducendo l'utente a navigare su pagine web che nascondono attacchi, appunto gli exploit-kit, per versioni vulnerabili di Java o dei plug-in del browser. Questi attacchi sono in grado di sfruttare macchine utente vulnerabili, impiantandovi malware, con la semplice navigazione su pagine infette [PLR-107] anche in assenza di una vera interazione dell'utente con la pagina.
Nel corso del 2013 e del 2014 gli exploit kit (o web browser exploit kit) hanno sfruttato la rara combinazione di portabilità del codice Java sia in termini di piattaforma che di browser, l'estrema diffusione di Java Runtime Environment su dispositivi di ogni tipo (inclusi i nuovi elementi costitutivi della Internet-of-Things), l'abbondante competenza specialistica nello scrivere codice Java, e il fiorente mercato underground per la vendita o il noleggio di exploit kit.
La nuova variante di Neverquest implementa tecniche mirate [PLR-106] a garantire un'alta resistenza ai prodotti antimalware, in particolare tiene costantemente sotto controllo l'integrità di tutte le sue componenti, ricreando dinamicamente quelle rimosse e riscrivendo le chiavi di registro eventualmente cancellate.

Il malware **Dyre** è stato identificato per la prima volta nel Giugno 2014 con attacchi mirati verso istituzioni finanziarie a livello mondiale e obiettivi importanti anche in Europa [PLR-109] [PLR-110].

Il principale vettore di infezione in questo caso sono attachment PDF allegati alle email. All'interno del PDF sono presenti del codice JavaScript e un'immagine BMP appositamente malformata che sfrutta una memory corruption risalente al 2013, per la quale erano state rilasciate da tempo advisories e relativi aggiornamenti correttivi del codice. Il downloader presente all'interno del PDF si occupa di scaricare la restante parte di codice dai server di Command-and-Control dai quali scarica anche i file di configurazione con una lista, nelle versioni analizzate, di oltre 100 siti di web banking [PLR-109].

Si sono quindi rivelati vulnerabili a Dyre i sistemi con Acrobar Reader non aggiornato da molto tempo, almeno un anno visto che Adobe aveva rilasciato gli aggiornamenti correttivi già nel Maggio 2013.
L'attività di Dyre in Europa ha seguito l'andamento mondiale, pressoché inesistente fino alla fine di Settembre 2014 e picchi importanti di attività nella seconda parte di Ottobre, in corrispondenza di specifiche campagne di phishing [PLR-108] mirate a veicolare i PDF malevoli come attachment.
Quando un computer infetto da Dyre naviga su uno dei siti oggetto dell'attacco, ad esempio un sito di web banking, il traffico viene ridirezionato verso un proxy server che a sua volta lo ridireziona verso i siti degli attaccanti che così vengono in possesso delle credenziali di accesso al sito di web banking.
L'esempio di Dyre ci suggerisce immediatamente come con il semplice aggiornamento periodico del Reader, ma più in generale di tutto il software installato, si sarebbero potuti contenere gli effetti di questo e di altri malware.

Se il contesto descritto è inquietante, poche semplici regole possono limitare la probabilità di compromissione del proprio computer e delle proprie credenziali e limitare l'impatto di azioni fraudolente:

- Diffidare da email non richieste o provenienti da mittenti sconosciuti o non credibili, specie se invitano ad accedere a contenuti esterni alla mail, come ad esempio a cliccare su link o aprire attachment
- Assicurarsi di avere abilitato sul proprio antivirus la funzione di scansione link e le analoghe funzioni sui browser (ad esempio il filtro SmartScreen di Internet Explorer o la protezione da phishing e malware presente in Firefox)
- Usare la massima cautela nell'aprire attachment, attendere sempre che l'antivirus ne completi la scansione
- Mantenere aggiornato il Sistema Operativo e tutto il software applicativo, abilitando i meccanismi di aggiornamento automatico e verificandone periodicamente il corretto funzionamento
- Ridurre la superficie di attacco verificando periodicamente i plug-in installati all'interno di tutti i browser, rimuovendo quelli non necessari o non utilizzati recentemente, aggiornando quelli necessari e disabilitando i plug-in vulnerabili per i quali non esistono aggiornamenti (i browser più comuni hanno strumenti automatici di verifica)

- Configurare il livello di sicurezza di Java su "Alto" o "Molto alto"
- Limitare l'esecuzione di applicazioni Java non firmate digitalmente o per le quali il certificato digitale non soddisfi i controlli operati dal browser
- Preferire eseguibili firmati digitalmente, per i quali il controllo del certificato operato dal sistema operativo consenta di verificare con certezza l'origine del software e che il codice non è stato alterato dopo la pubblicazione (integrità)
- Aggiornare costantemente il Java Runtime Environment, configurando possibilmente l'aggiornamento automatico
- Verificare il corretto funzionamento dell'antivirus, in particolare relativamente agli aggiornamenti delle signature che devono essere quotidiani e andare sempre a buon fine in quanto alcuni malware cercano di sovvertire proprio il meccanismo di aggiornamento dell'antivirus
- Iniziare quanto prima ad utilizzare soluzioni specifiche anti-malware che impediscano attacchi man-in-the-browser (MiTB) e proteggano la confidenzialità e l'integrità delle sessioni di navigazione ai siti di online banking
- Accertarsi sempre della fonte e dell'autorevolezza del software installato, specie quando si tratta di software gratuito cercato su Internet
- Fare backup periodici dei propri dati (con frequenza quotidiana o almeno settimanale) su supporti esterni, multipli (almeno 2 diversi), alternati periodicamente e mantenuti in località diverse (ad esempio uno a casa e uno in ufficio).

Le grandi organizzazioni dovrebbero inoltre implementare strategie più articolate per evitare o limitare attacchi Corporate, come ad esempio:

- Sensibilizzare i collaboratori sull'esistenza di attacchi mirati a specifiche organizzazioni, particolarmente convincenti e perpetrati attraverso schemi di spear-phishing o watering-hole;
- Utilizzare servizi di IP address reputation che consentano il blocco selettivo di IP, siti e URL ritenuti pericolosi;
- Implementare soluzioni per la protezione dell'end-point, con verifica dell'integrità del browser e dell'intero sistema, protezione dell'integrità e confidenzialità del contenuto delle transazioni, prevenzione del riuso delle stesse password aziendali su siti esterni;
- Implementare soluzioni per la verifica automatica della security posture di tutti i dispositivi aziendali indipendentemente dalla piattaforma e sistema operativo, bloccando l'attività di quelli che hanno settaggi insicuri o correggendo in automatico le configurazioni
- Introdurre soluzioni per il calcolo in tempo reale del fattore di rischio di ciascuna transazione, prendendo come base l'insieme di fattori di rischio costituiti dalle specifiche configurazioni del dispositivo, dell'applicazione, dei siti coinvolti e della sensitività della transazione
- Introdurre soluzioni per la cattura automatica di eventuale malware e trasmissione sicura verso i laboratori di analisi.

Le istituzioni finanziare dovrebbero applicare livelli di protezione ancora più avanzata ri-

spetto a quando appena elencato, come ad esempio:
- Utilizzare soluzioni specifiche per la fraud-detection e l'account take-over
- Limitare l'accesso ai soli dispositivi che superino un livello considerato minimo di sicurezza
- Autenticazione a fattori multipli, autenticazione out-of-band (ad esempio SMS), utilizzo della geolocalizzazione del dispositivo mobile come ulteriore fattore di autenticazione.

Chi fornisce o sviluppa servizi sia sotto forma di web applications che di App per dispositivi mobili dovrebbe invece avvalersi degli specifici SDK, testati e aggiornati e che forniscono già servizi completidi anti-malware, protezione delle sessioni di navigazione, identificazione di dispositivi rooted o jailbroken, protezione delle connessioni wifi pubbliche e insicure, limitando invece al minimo tutte le soluzioni che non abbiano subito rigorosi test e non siano aggiornate per inseguire costantemente l'evoluzione del malware.

Bibliografia

[PLR-100] A. Klein Financial Malware Uses Configuration File to Target Enterprise - SecurityIntelligence.com, November 2010
http://securityintelligence.com/financial-malware-uses-configuration-file-target-enterprise/

[PLR-101] D. Tamir Massively Distributed Citadel Malware Targets Middle Eastern Petrochemical New Neverquest Variant Spotted in the Wild - SecurityIntelligence.com, September 2014
http://securityintelligence.com/massively-distributed-citadel-malware-targets-middle-eastern-petrochemical-organizations/

[PLR-102] R. Sherstobitoff White Paper: Inside the World of the Citadel Trojan – McAfee Labs, 2013
http://www.mcafee.com/us/resources/white-papers/wp-citadel-trojan.pdf

[PLR-103] IBM X-Force Threat Intelligence Quarterly, 4Q 2014 - IBM Security Systems, November 2014
http://www.ibm.com/security/xforce/

[PLR-104] Internet World Stats, Usage and Population Statistics
http://www.internetworldstats.com

[PLR-105] The Internet Organised Crime Threat Assessment (iOCTA) 2014 - EUROPOL EC3 European Cybercrime Centre
https://www.europol.europa.eu/iocta/2014/

[PLR-106] I. Kolmanovich New Neverquest Variant Spotted in the Wild - SecurityIntelligence.com, December 2014
http://securityintelligence.com/new-neverquest-variant-spotted-in-the-wild/

[PLR-107] IBM Security Systems IBM X-Force 2013 Mid-Year Trend and Risk Report, September 2013

[PLR-108] O. Bach Phishing Campaign Linked with "Dyre" Banking Malware – US-CERT, October 2014
https://www.us-cert.gov/ncas/alerts/TA14-300A

[PLR-109] Protecting Against the Dyre Trojan: Don't Bring a Knife to a Gunfight - SecurityIntelligence.com, December 2014
http://securityintelligence.com/protecting-against-the-dyre-trojan-dont-bring-a-knife-to-a-gunfight/

[PLR-110] D. Tamir Dyre Banking Trojan Used in APT-Style Attacks Against Enterprises - SecurityIntelligence.com, September 2014
http://securityintelligence.com/dyre-banking-trojan-used-in-apt-style-attacks-against-enterprises/

© Clusit 2015

Rapporto 2014 sullo stato di Internet ed analisi globale degli attacchi DDoS (dati aggiornati al 3° trimestre 2014)

Minacce emergenti – L' Internet of Things (IoT)

Nel 2014 si sono verificati numerosi eventi significativi riguardanti la sicurezza in Internet, che sono stati successivamente utilizzati per attacchi su vasta scala. Il primo è stato il bug Heartbleed (Open SSL).

Un altro attualmente molto utilizzato è il bug Shellshock (bug Bash), inizialmente identificato come CVE-2014-6271, a cui si aggiunge ora il bug Poodle (SSL 3.0) recentemente scoperto. Per effetto del massiccio utilizzo di questi bug e di altre vulnerabilità, cresce il numero di risorse a disposizione dell'ecosistema DDoS. Molte piattaforme sono oggi aperte all'utilizzo da parte di autori di attacchi DDoS e sono in aumento i malware multi-piattaforma come il toolkit DDoS Spike.

La diffusione dei dispositivi con funzionalità Internet e l'espansione dell'Internet of Things (IoT) comporteranno anche l'ampliamento della superficie di attacco a disposizione dei pirati informatici, i quali stanno iniziando ad abbandonare le classiche botnet di PC e server e a orientarsi verso payload di malware specificamente sviluppati per i dispositivi embedded con funzionalità Internet.

Le botnet di grandi dimensioni, maggiormente diversificate e complesse e costituite da più architetture di sistemi sono ormai una realtà.

Di conseguenza, è probabile che nel prossimo futuro si verifichino con maggiore frequenza campagne di attacchi DDoS particolarmente pericolose, con larghezza di banda o volume elevati. L'ecosistema dei crimini DDoS motivato da scopi di lucro probabilmente si espanderà per sfruttare l'opportunità, aggiungendo nuove risorse DDoS-for-hire e nuovi toolkit DDoS, con conseguente aumento delle campagne di attacchi multi-vettore che necessitano di protezione specifica con sistemi di difesa e tecnologie di mitigazione ad alta specializzazione.

Le nuove risorse dell'ecosistema DDoS influiranno sulle campagne indotte dal malcontento sociale e da rivalità geopolitiche e sulle campagne sponsorizzate da stati. Queste nuove condizioni creeranno una difficile situazione per le aziende, le organizzazioni e i governi con una presenza in Internet.

È necessario che i produttori supportino l›architettura del sistema operativo e i processi di gestione del software dei dispositivi con funzionalità Internet in un modo che ne consenta adeguatamente la gestione, l›applicazione di patch e l›aggiornamento quando vengono scoperte nuove vulnerabilità.

Citando la presentazione di Dan Geer alla conferenza Black Hat USA 2014: "*I sistemi embedded devono avere un'interfaccia di gestione remota o devono avere una durata limitata: non possono essere immortali e impossibili da riparare*". La mancata predisposizione di adeguate funzionalità di gestione in questi dispositivi prima della loro implementazione sarà causa di futuri incidenti a carico della cybersicurezza con costose conseguenze.

"I sistemi embedded devono avere un'interfaccia di gestione remota o devono avere una durata limitata: non possono essere immortali e impossibili da riparare."

Analisi e trends

Le campagne di attacchi DDoS da record verificatesi nel 2014 hanno registrato un notevole aumento percentuale della media dei picchi di banda rispetto all'anno precedente. Un fattore che ha contribuito a tale aumento è stato un attacco di 321 Gbps (gigabit al secondo), mentre un altro è rappresentato dall'utilizzo di nuovi vettori di attacco da parte dei pirati informatici e dal potenziamento dei vettori di attacco già noti per utilizzare una maggiore larghezza di banda. Inoltre, viene utilizzata una base più ampia di dispositivi per espandere le botnet DDoS. Oltre all'aumento della larghezza di banda degli attacchi, il 2014 ha visto aumentare anche la media dei picchi di pacchetti al secondo.
Rispetto all'anno precedente, i volumi degli attacchi sono aumentati del 366%. I payload degli attacchi con dimensioni dei pacchetti più grandi producono in genere una maggiore larghezza di banda e una velocità dei pacchetti più bassa, per cui i malintenzionati utilizzano spesso una combinazione di vettori per controbilanciare questa situazione. Anche gli attacchi basati su tecniche di riflessione e amplificazione hanno svolto un ruolo importante nell'aumento del volume degli attacchi.
Questa tendenza in salita della media dei volumi di picco è destinata a continuare.
L'attività DDoS è andata progressivamente aumentando durante tutto il 2014. La più vasta campagna DDoS, con una larghezza di banda totale degli attacchi di 321 Gbps, è stata osservata nel 3° trimestre.
I pirati informatici hanno continuato a preferire con un largo margine gli attacchi basati sull'infrastruttura e hanno creato toolkit DDoS con Linux e vettori di attacco di livello 3.
Le campagne di attacchi DDoS sono state caratterizzate nel 2014 da alti volumi di traffico e maggiore durata degli attacchi, raggiungendo una media di 22 ore nel 3° trimestre, rispetto alle 17 ore del 2° trimestre e alle 21 ore dell'anno precedente (3° trimestre 2013).
Gli attacchi multi-vettore, più sofisticati, sono diventati la norma nel 2014 e più della metà (53%) di tutti gli attacchi ha utilizzato più vettori, come illustrato nella **Figura 1**. Gli attacchi multi-vettore sono stati alimentati dalla maggiore disponibilità di toolkit di attacco con interfacce di facile utilizzo, nonché dal settore criminale in ascesa dei DDoS-for-hire. Nel panorama delle minacce DDoS, una tendenza attuale è rappresentata dall'aumento delle metriche degli attacchi volumetrici.
L'elemento principale che ha guidato lo sviluppo delle botnet nel 2014 è stato l'utilizzo su vasta scala delle vulnerabilità del Web pubblico, che in passato è stato alla base di alcune delle più sofisticate campagne di attacchi DDoS. L'approccio utilizzato dai pirati informatici nel 2014 è stato caratterizzato dalla forza e non dalla tecnica: un approccio in cui gli strumenti di attacco includono binari DDoS in grado di generare payload con elevata larghezza di banda che spesso coinvolgono i sistemi Linux, una particolare attenzione ai payload SYN e UDP e campagne di attacchi di lunga durata.
Questo approccio ha soppiantato i precedenti trend che vedevano i responsabili degli at-

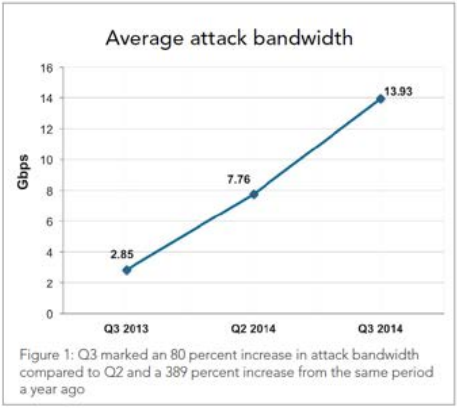


Figure 1: Q3 marked an 80 percent increase in attack bandwidth compared to Q2 and a 389 percent increase from the same period a year ago

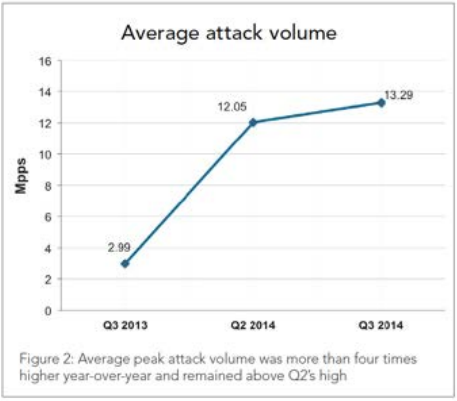


Figure 2: Average peak attack volume was more than four times higher year-over-year and remained above Q2's high

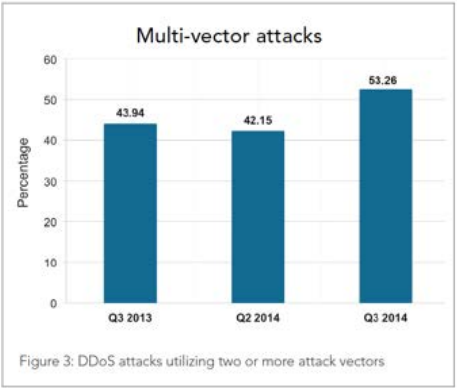


Figure 3: DDoS attacks utilizing two or more attack vectors

Fig.1: Vettori di attacco multipli

tacchi privilegiare tecniche di riflessione basate su protocolli come NTP (Network Time Protocol), SNMP (Simple Network Management Protocol), CHARGEN (Character Generation) e DNS (Domain Name System).

I malintenzionati hanno incentrato la propria attenzione sulla raccolta di risorse e sulla creazione e l'ampliamento delle botnet, anziché affinare i payload con l'intento di bypassare le tecnologie di mitigazione. Un altro segnale che conferma questa tendenza è l'individuazione e la comparsa di payload sviluppati per sistemi di elaborazione che vanno al di là dei classici sistemi operativi di PC e server.

Questi includono binari DDoS basati su ARM che tentano di colpire i dispositivi CPE (Customer-Premises Equipment), i modem via cavo domestici, i dispositivi mobili e una grande varietà di dispositivi con funzionalità Internet come server rack, ripetitori a radiofrequenza industriale, storage di rete industriale e persino dispositivi domestici e indossabili facenti parte della categoria delle tecnologie IoT.

Sono inoltre apparsi nuovi attacchi a riflessione e amplificazione basati sul protocollo SSDP (Simple Service Discovery Protocol) e sul framework UPnP (Universal Plug and Play), che sfruttano le richieste di protocollo utilizzate per individuare e gestire i dispositivi UPnP.

La ricerca di Akamai ha rivelato che il 38% dei dispositivi in uso di questo tipo può essere soggetto a sfruttamento. Il panorama delle minacce DDoS probabilmente muterà man mano che milioni di nuovi dispositivi IoT verranno aggiunti al pool di risorse che i malintenzionati potrebbero sfruttare per sferrare attacchi DDoS.

Le botnet di domani potrebbero essere diverse da quelle attuali e sono destinate a diventare più grandi e multi-livello con vari tipi di dispositivi e a generare volumi di larghezza di banda e velocità di connessione considerevoli. Quest'anno la percentuale di attacchi basati sulle applicazioni non ha ancora superato il 10% di tutti gli attacchi. Questa tendenza potrebbe cambiare man mano che i malintenzionati espandono le proprie risorse DDoS e modificano i vettori e i payload degli attacchi. (**Figura 1**)

La campagna di attacchi più aggressiva del 3° trimestre, a 321 Gbps, è un esempio della perseveranza di un pirata informatico motivato. Questo approccio basato più sulla quantità che sulla "qualità" ha caratterizzato le campagne più significative durante il 2014. Tutti gli attacchi più estesi sono stati realizzati con più vettori di attacco e tutti hanno incluso un SYN flood, un tipo di attacco che utilizza una notevole quantità di larghezza di banda e genera elevate velocità di pacchetti al secondo. Il secondo vettore di attacco più diffuso utilizzato in questi attacchi di oltre 100 Gbps è stato un UDP flood e ha prodotto anche l'attacco più imponente a 321 Gbps. Il payload è simile a quello del SYN flood. Le vulnerabilità come gli exploit Heartbleed e Shellshock (Bash) potrebbero favorire un aumento degli attacchi DDoS. D'altra parte, poiché i malintenzionati sono opportunisti, la disponibilità di nuovi attacchi basati su tecniche di riflessione come l'SSDP potrebbe convincerli a cambiare tattica, facendoli optare per attacchi DDoS a elevata larghezza di banda che si affidano principalmente alla riflessione.

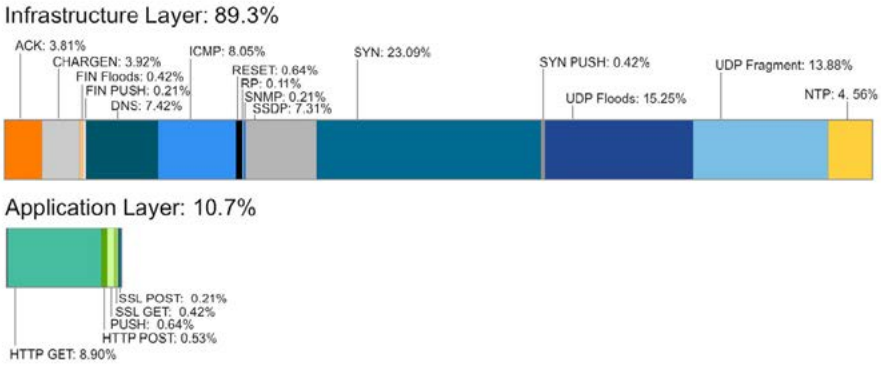


Fig. 2: Vettori multipli di attacco (Q3 2014)

Vettori di attacco

A livello di infrastruttura e quelli basati sulle applicazioni, del tutto simile agli ultimi trimestri.

Gli attacchi a livello di infrastruttura si sono attestati sull'89% rispetto all'11% degli attacchi a livello di applicazione, come illustrato nelle **Figure 2 e 3**.

La campagna di attacchi DDoS più imponente mai registrata sulle reti Akamai si è verifi-

cata nel 3° trimestre ed è stata basata principalmente su SYN flood e UDP flood di livello 3 (infrastruttura),
raggiungendo un picco di 321 Gbps e 72 milioni di pacchetti al secondo.
Le campagne realizzate con vettori di attacco volumetrici sono state frequenti durante tutto il 2014.
Il team PLXsert ha rilevato la creazione di botnet con cui i malintenzionati hanno attaccato server Web vulnerabili e hanno sviluppato payload DDoS a livello di infrastruttura.
Essi hanno inoltre attaccato i dispositivi embedded mediante payload multi-piattaforma di malware DDoS, il che rientra perfettamente nel trend che vede i pirati informatici sfruttare un'ampia serie di dispositivi per attività malevole.
I bersagli recentemente osservati includono dispositivi CPE, modem via cavo, dispositivi mobili, dispositivi di storage e dispositivi IoT. Sebbene utilizzino in genere poca potenza e una ridotta larghezza di banda, se utilizzati in grandi quantità questi dispositivi apportano potenza e risorse alle botnet DDoS.
La minaccia rappresentata dai vettori DDoS basati sulla riflessione è notevole. Restano ancora a disposizione dei malintenzionati milioni di host da sfruttare negli attacchi e relativamente facili da utilizzare. Gli attacchi basati su botnet hanno maggiori probabilità di accedere a server ben connessi con ottimi collegamenti upstream. Tuttavia, la minaccia più grande degli attacchi basati sulla riflessione, ad esempio del tipo SSDP, è legata alla loro facilità di esecuzione. Con gli attacchi basati sulla riflessione non c'è alcun bisogno di infettare migliaia di host: gli host sono semplicemente lì in attesa della richiesta successiva.
Nei primi tre trimestri del 2014 è stato osservato un rapporto costante tra attacchi basati su applicazioni e attacchi a livello di infrastruttura: gli attacchi a livello di applicazione sono stati utilizzati una sola volta ogni nove attacchi a livello di infrastruttura. Nel 2014 l'utilizzo degli attacchi a livello di applicazione è stato notevolmente inferiore rispetto agli anni precedenti. L'attacco a livello di applicazione più utilizzato è stato il GET flood.Il team PLXsert ha rilevato che il GET flood è stato il principale vettore di livello 7.
I GET flood sono inclusi in molti toolkit DDoS multi-livello recentemente sviluppati, come Spike.
Gli attacchi a livello di applicazione hanno rappresentato l'11% degli attacchi e i più comuni sono stati di tipo HTTP GET flood con una percentuale del 9% (**Figura 3**).

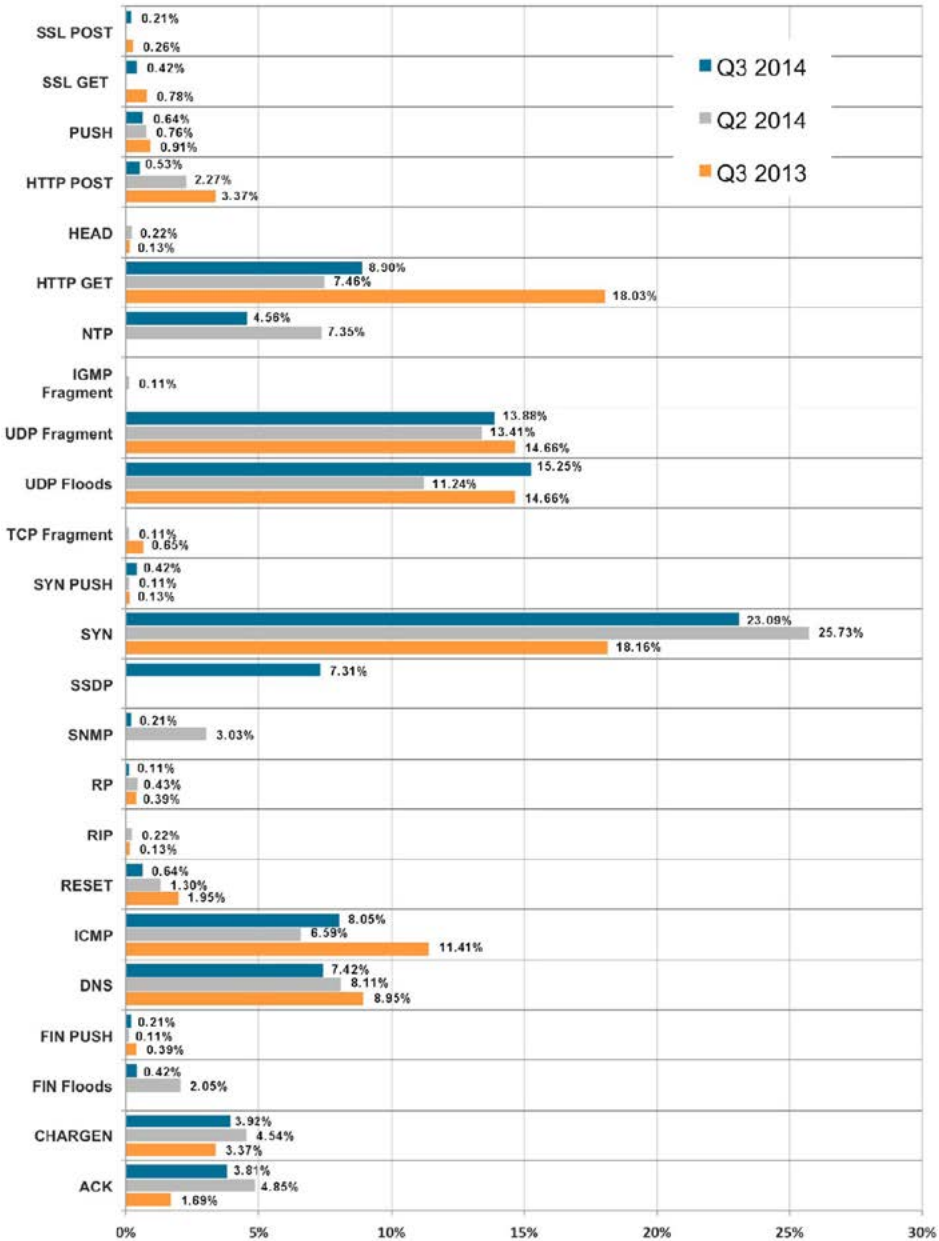


Fig. 3: Trend dei vettori di attacco

© Clusit 2015

Settori soggetti ad attacco

I dati riportati nella **Figura 4** illustrano i settori soggetti con maggiore frequenza ad attacchi DDoS nel 3° trimestre. I cinque più attaccati sono stati i settori gaming, media e intrattenimento, software e tecnologia, servizi finanziari e Internet e telecomunicazioni.
Il settore dell'intrattenimento online ha sostenuto il maggior carico essendo stato oggetto del 34% degli attacchi DDoS, con una leggera riduzione rispetto all'ultimo trimestre. Il settore dei media si colloca al secondo posto, colpito dal 24% degli attacchi. Il settore software e tecnologia è stato colpito dal 20% degli attacchi, quello dei servizi finanziari dal 9%, così come quello di Internet e telecomunicazioni.

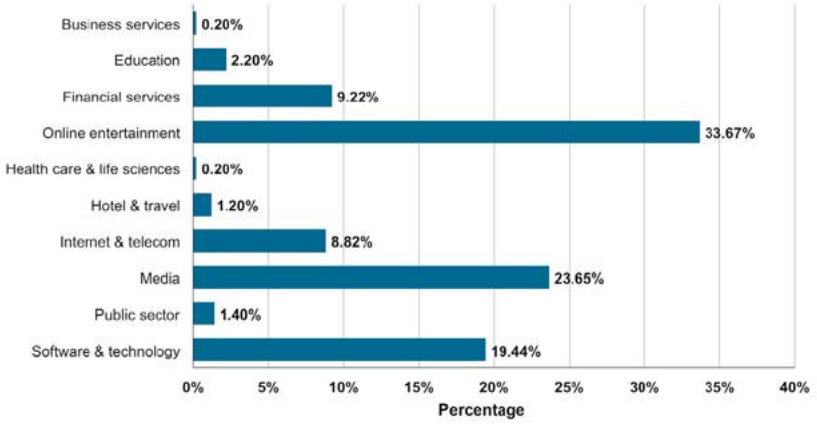


Fig. 4: Settori soggetti con maggiore frequenza ad attacchi DDoS nel 3° trimestre

Intrattenimento online

Nel settore dell'intrattenimento online sono comprese le aziende che si occupano di gaming online o dei contenuti correlati al gaming. Come nel 2° trimestre 2014, ha rappresentato il settore più colpito registrando il 33% di tutti gli attacchi. Gli attacchi indirizzati a tale settore sono in genere provocati da giocatori che cercano di ottenere un vantaggio competitivo sugli altri e da malintenzionati che tentano di sottrarre i dati personali dei giocatori. In alcuni casi, i malintenzionati incrementano gli attacchi al settore del gaming per ottenere l'attenzione dei media o notorietà presso gruppi di loro pari.
Nella maggior parte dei casi, si è trattato di attacchi a livello di infrastruttura. Il settore del gaming ha ricevuto il 65% di tutti i SYN flood, il 42% di tutti gli UDP flood e il 21% dei flood a riflessione SSDP.

Software e tecnologia

Nel settore software e tecnologia sono comprese le aziende che forniscono soluzioni come il

SaaS (Software-as-a-Service) e tecnologie basate sul cloud. Questo settore ha visto aumentare gli attacchi mirati alle infrastrutture, registrando il 20% di tutti gli ACK flood e il 15% di tutti i flood a riflessione SSDP. È inoltre stato oggetto del 12% di tutti gli attacchi NTP e del 16% di tutti i GET flood.
In quanto terzo settore più attaccato nel 3° trimestre, ha perso una posizione rispetto al precedente trimestre dove occupava il secondo posto.

Media

Il settore dei media è stato il secondo settore maggiormente colpito in questo trimestre.
Gli interessi dei malintenzionati variano di pari passo con il mutare della situazione politica e sociale.
I numeri di questo trimestre sembrano coincidere con le problematiche globali che spingerebbero gli autori degli attacchi a concentrarsi su questo settore per elevare al massimo la propria esposizione e portata. Il settore dei media è stato colpito principalmente da attacchi mirati alle infrastrutture, ricevendo soprattutto SYN flood nell'86% dei casi. È stato colpito dalla percentuale più elevata (26%) di tutti i GET flood a livello di applicazione.

Settore finanziario

Nel settore finanziario sono comprese le principali istituzioni finanziarie come banche e piattaforme di trading. Questo settore è stato il bersaglio del 9% di tutti gli attacchi DDoS osservati.
Nel caso degli attacchi mirati al settore finanziario, si tratta spesso di campagne sponsorizzate da stati o indotte da motivazioni politiche, che ottengono una notevole attenzione da parte dei media a causa delle conseguenze che un attacco di successo comporta. L'attacco più frequentemente utilizzato contro il settore finanziario nel 3° trimestre è stato l'NTP, che rappresenta il 16% di tutti gli attacchi NTP osservati.

Internet e telecomunicazioni

Nel settore Internet e telecomunicazioni sono comprese le aziende che offrono servizi correlati a Internet, come ISP e CDN. Al quinto posto tra i settori maggiormente colpiti in questo trimestre, è stato bersaglio del 9% di tutti gli attacchi, con un sostanziale aumento del 120% rispetto al trimestre precedente. Questo settore ha ricevuto il 14% di tutti i DNS flood, il 14% di tutti i SYN flood e il 13% di tutti gli UDP flood.

I 10 principali paesi di origine

Nel 3° trimestre gli Stati Uniti sono stati il paese di origine principale degli attacchi DDoS, rappresentando la fonte del 24% di tutti gli attacchi, come illustrato nella **Figura 5**. Dopo gli Stati Uniti, nella top ten dei paesi di origine degli attacchi figurano la Cina con il 20%, il Brasile con il 18% e il Messico con il 14%. La Corea si è classificata al quinto posto con il 6%, seguita dalla Germania con il 6% e dal Giappone con il 4%. Insieme, il Brasile, la Russia, l'India e la Cina hanno dato origine al 43% del traffico DDoS. Più di un terzo del

traffico globale legato agli attacchi DDoS (36%) ha avuto origine in paesi asiatici, situazione che può essere attribuita a un aumento del malware correlato a DDoS come IptabLes e IptabLex.

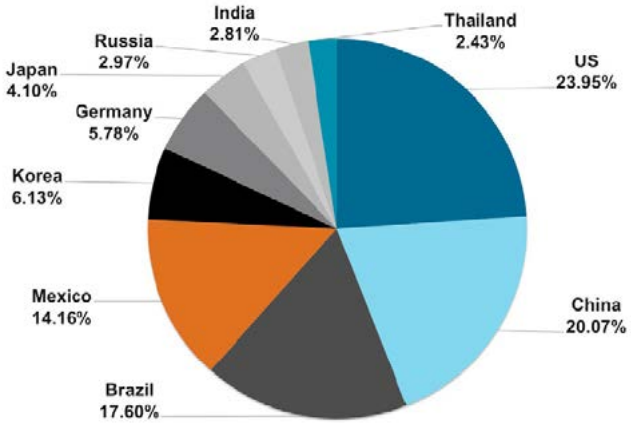


Fig. 5: Le 10 principali origini geografiche degli IP legati agli attacchi nel 3° trimestre 2014

Un attacco in evidenza

Un attacco DDoS da 321Gb

Sono due i fattori che in genere consentono a un attacco DDoS di differenziarsi dagli altri: un flusso di traffico record diretto a una rete bersaglio o un approccio innovativo per la generazione di un flusso.

L'attacco in questione è stato solo uno di una serie di campagne di attacchi dirette a un cliente di Akamai del settore dell'intrattenimento nell'arco di una settimana.

Questo attacco ha raggiunto picchi di 321 Gbps e 72 Mpps sulla rete Akamai. Velocità dati così elevate avrebbero potuto probabilmente spostare gli indici della larghezza di banda lungo il percorso dall'origine al bersaglio. L'attacco lanciato durante le campagne è stato costituito da SYN flood e UDP flood. Anche l'infrastruttura FastDns di Akamai è stata attaccata dagli hacker. La maggior parte degli attacchi osservati durante queste campagne conteneva traffico SYN flood. Una tipica connessione TCP a un sito Web richiede un handshake TCP a tre vie:

l'host invia un SYN iniziale, il server risponde con un SYN-ACK, l'host invia un altro ACK e quindi la comunicazione ha inizio. Gli autori di attacchi DDoS spesso creano pacchetti non validi al lancio dei SYN flood. Questi pacchetti violano deliberatamente il flusso di lavoro regolare di una connessione TCP/IP nel tentativo di sovraccaricare di richieste anomale il

sistema bersaglio con un elevatissimo volume di traffico o con molti tentativi di connessione simultanei. Le richieste SYN malevole vengono inviate in rapida frequenza verso l'host o la rete bersaglio; le bot di attacco non attendono che il server risponda (ACK) alle richieste SYN prima di inviare altre richieste.
L'obiettivo è sovraccaricare l'infrastruttura oggetto dell'attacco e renderla non disponibile agli utenti legittimi. Anche SYN flood di ridotte dimensioni possono impedire a un server non protetto di rispondere alle richieste legittime. Un altro vettore di attacco utilizzato in questa campagna è stato un attacco UDP flood. Il protocollo UDP non richiede un handshake affinché la comunicazione abbia luogo ed è quindi più efficiente e di conseguenza ideale per le applicazioni a bassa latenza, come quelle VOIP (Voice Over IP) e i videogiochi online. Gli autori degli attacchi sfruttano tale funzionalità creando pacchetti UDP di grandi dimensioni e inviandoli all'indirizzo IP bersaglio. Senza il requisito dell'handshake, gli autori degli attacchi possono inviare pacchetti UDP malevoli che effettuano lo spoofing dell'indirizzo IP di origine, rendendo così difficile la mitigazione di questi attacchi da parte dei sistemi di difesa.
Spesso, gli autori degli attacchi utilizzano indirizzi di origine non conformi a RFC per il traffico Internet (IP LAN private) o indirizzi IP di provider di servizi legittimi che presentano una minore probabilità di essere bloccati dal bersaglio dell'attacco. Alcuni toolkit per attacchi DDoS supportano la randomizzazione degli IP di origine e porte di destinazione personalizzabili. In totale, gli hacker hanno lanciato 10 campagne di attacchi distinte contro Akamai e il suo cliente. Nella **Figura 6** sono riportate le statistiche relative a ciascuna di queste 10 campagne.
I primi tre attacchi erano diretti al server Web del cliente e, ad eccezione del secondo attacco, ciascuno di essi ha superato i 100 Gbps. Dopo la terza campagna, gli autori degli attacchi si sono resi conto che il bersaglio era protetto dalla tecnologia Akamai. A quel punto sono passati ad attaccare blocchi di rete di proprietà di Akamai e specificamente una subnet /24. Un attacco diretto a tale blocco ha raggiunto un picco record di 321 Gbps.

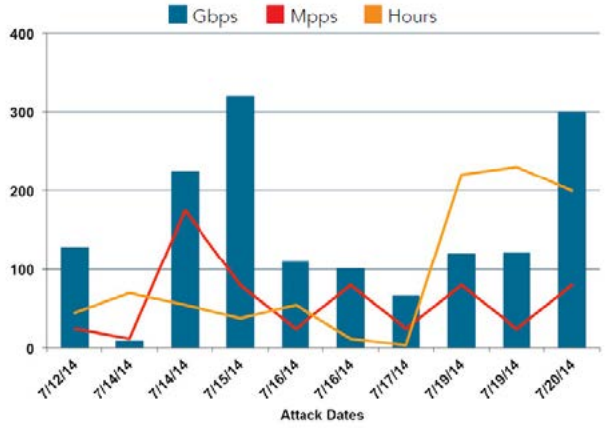


Fig. 6: Larghezza di banda, volume e durata degli attacchi

© Clusit 2015

Di fatto, gli hacker hanno spostato l'attacco di alcune ore per colpire il sito Web del cliente. Durante le campagne erano in azione meccanismi di mitigazione DDoS. Il 17 e il 19 luglio gli attacchi sono stati diretti nuovamente al sito Web del cliente sulla porta 80. Uno di essi conteneva una combinazione di SYN flood, GET flood, ICMP flood e RESET flood. Un GET flood è un attacco basato su TCP che richiede un handshake a tre vie. L'efficacia di questo tipo di attacco è dovuta alla possibilità di inviare una grande quantità di richieste di connessione simultanee a un server Web, consumandone le risorse e quindi arrestando il sito Web.
Nella **Figura 7** è riportata la larghezza di banda ricevuta presso ogni scrubbing center per la mitigazione DDoS di Akamai. Una tipica azienda con un server Web standard avrebbe normalmente meno di 1 Gbps di larghezza di banda disponibile presso un singolo data center e questo livello di volume di attacchi renderebbe indisponibili tutti i servizi ospitati presso la sede presa di mira.
Attaccando Akamai direttamente, gli hacker intendevano probabilmente bypassare la tecnologia di mitigazione DDoS o causarne l'interruzione e quindi attaccare nuovamente il sito Web del cliente.

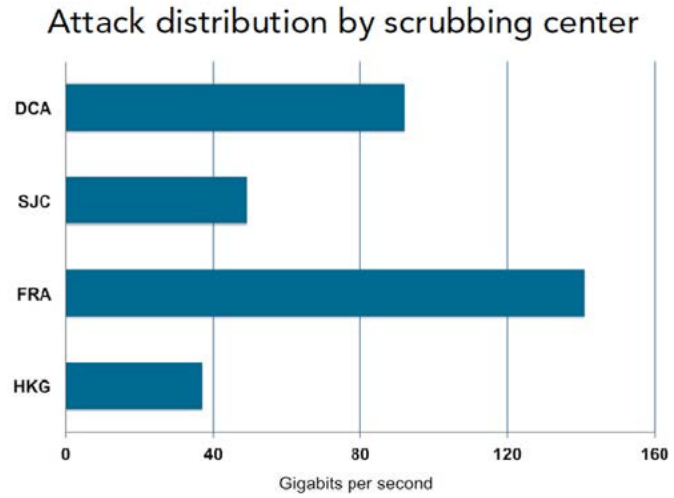


Fig.7: Distribuzione degli attacchi per scrubbing center Akamai

A differenza degli attacchi TCP SYN flood o basati su UDP con spoofing, un attacco GET flood consente in genere di rilevare gli effettivi IP di origine dell'attacco, come illustrato nel grafico a torta dei paesi di origine riportato nella **Figura 8**. In questi attacchi DDoS, gli Stati Uniti, la Germania e la Cina sono stati i principali paesi di origine del traffico malevolo.

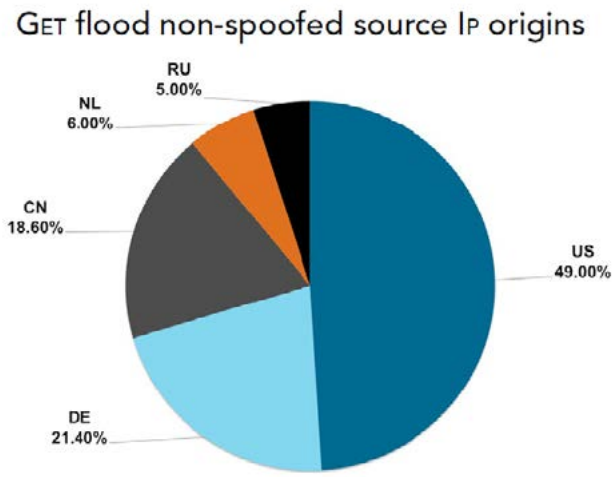


Fig.8: Attacchi per Paese di origine

Conclusioni

Con statistiche record in fatto di attacchi e una combinazione di vettori di attacco di livello 7 e livello 3, questa botnet ha sferrato imponenti campagne di attacchi contro il settore dell'intrattenimento in Asia.
Gli hacker hanno diretto gli attacchi contro blocchi IP specifici dell'infrastruttura Akamai per colpire le vittime designate poste sotto la protezione DDoS. Secondo fonti di intelligence dietro queste campagne DDoS potrebbe esserci il crimine organizzato. Gli autori degli attacchi stanno creando questa botnet puntando ai server Web (principalmente basati su Linux) e utilizzando metodi di infezione basati su client, ma durante l'analisi forense delle campagne sono stati identificati anche alcuni dispositivi CPE.
Gli attacchi sono stati mitigati con successo e gli indirizzi IP di origine senza spoofing sono attualmente sotto monitoraggio all'interno della piattaforma di mitigazione DDoS di Akamai.
È probabile che questa botnet venga utilizzata contro altri settori in quanto i malintenzionati ne traggono profitto attraverso servizi DDoS-for-hire.

© Clusit 2015

Case Study

Botnet DDoS realizzate con dispositivi diversi da PC e server.

L'Internet of Things (IOT)

I malintenzionati sono costantemente alla ricerca di nuovi modi per espandere le proprie risorse e creare nuovi vettori di attacco DDoS, in quanto hanno bisogno di capacità per produrre attacchi a elevata larghezza di banda, creare più connessioni simultanee e utilizzare risorse geograficamente distribuite. L'impiego di queste capacità determina una maggiore difficoltà di mitigazione degli attacchi DDoS da parte dei sistemi di difesa e la possibilità che tali sistemi blocchino anche il traffico legittimo causando ulteriori danni collaterali a seguito di attacchi di grande entità. Di conseguenza, i malintenzionati stanno coinvolgendo nuovi tipi di dispositivi e piattaforme nelle proprie botnet DDoS.

Gli sforzi della community per rafforzare e proteggere PC e server dall'infezione da malware bot hanno portato a un aumento del tempo e del livello di competenze necessari ai malintenzionati per bypassare le protezioni e realizzare exploit efficaci. A seguito di ciò, il team PLXsert ha osservato in molte campagne firme che non corrispondono a PC e server comunemente utilizzati, una tendenza che è andata aumentando negli ultimi due anni. Le nuove firme suggeriscono l'ampliamento della superficie di attacco, mirando a dispositivi che non erano stati utilizzati molto spesso nelle botnet del passato.

Queste nuove firme provengono da dispositivi quali router commerciali, dispositivi CPE, dispositivi mobili, dispositivi per videoconferenza e dispositivi IoT.

Alcuni di questi dispositivi sono pensati come dispositivi a basso consumo e bassa larghezza di banda, ma l'utilizzo di migliaia di dispositivi del genere in una botnet DDoS apporta una notevole potenza.

La ricerca condotta sui dispositivi CPE e SOHO (Small Office, Home Office) da Team Cymru indica che questi dispositivi possono essere sfruttati e utilizzati per finalità malevole, tra cui gli attacchi DDoS.

Alcuni dei fattori principali nella scelta dei dispositivi da utilizzare nelle botnet DDoS sono:

- Dispositivi che eseguono configurazioni non protette per impostazione predefinita
- Dispositivi che eseguono firmware non aggiornato e vulnerabile
- Mancanza di gestione e interfacce utente assenti o insufficienti per risolvere problemi di sicurezza ed effettuare aggiornamenti

I dispositivi embedded con queste caratteristiche stanno diventando sempre più diffusi.

Lontano dagli occhi, lontano dalla mente

La maggior parte dei dispositivi embedded ha un elemento in comune: essi appaiono trasparenti all'utente finale o necessitano di competenze al di sopra della media per accedervi e gestirli.

Di conseguenza, spesso non vengono gestiti e monitorati per lunghi periodi di tempo.

Questa mancanza di attenzione determina in genere un accesso aperto con credenziali predefinite o credenziali esposte a Internet. Un valido esempio è la scoperta di vulnerabilità

in due marche di modem via cavo che hanno permesso ai malintenzionati di accedere da remoto ai dispositivi e di recuperare informazioni sensibili, portando eventualmente alla compromissione del dispositivo.
Secondo Shodan, un popolare motore di ricerca di vulnerabilità, oltre 50.000 dispositivi di questo tipo espongono il protocollo SNMP a Internet, come ha scritto Tod Beardsley di Rapid& in un post su Metasploit. Nel maggio 2014 il team PLXsert ha rilasciato una notifica di minaccia riguardante il problema dei server SNMP aperti in Internet e gli attacchi a riflessione basati su SNMP. Esistono molti esempi di dispositivi embedded che tendono a essere sottovalutati e gestiti male.

Gli stessi problemi possono sorgere con dispositivi aziendali come router commerciali e dispositivi per videoconferenza che devono essere protetti, aggiornati o monitorati, poiché si trovano in case e piccoli uffici dove è poco probabile che ci sia personale dotato delle conoscenze e delle competenze nel campo della sicurezza IT necessarie per gestirli. Nel 2013, in tutto il mondo erano presenti 161 milioni di punti di accesso wireless. I principali fornitori di questo tipo di dispositivi sono TP-Link con una quota di mercato del 39% e D-Link e Netgear, ciascuno con l'11%. Poiché questi dispositivi costituiscono i gateway per l'accesso a Internet di uffici domestici e piccole aziende, quando vengono scoperte vulnerabilità al loro interno, le implicazioni sono considerevoli. I malintenzionati possono attaccare questi gateway e utilizzarli come zombie in una botnet DDoS. Simili tecniche di attacco e vulnerabilità possono essere applicate anche ad altri dispositivi con funzionalità Internet, come telecamere, media center, dispositivi di storage, sistemi di allarme, controller di dispositivi, stazioni wireless a banda larga e così via. I malintenzionati non devono più attaccare i computer collegati a questi dispositivi, i quali hanno una maggiore probabilità di essere protetti da software antivirus e firewall. La maggior parte degli attacchi malware diretti a questi tipi di dispositivi ai fini dell'utilizzo in una botnet DDoS passerà inosservata, dato che gli utenti non dispongono di meccanismi di protezione.
Le campagne di creazione delle botnet DDoS potrebbero, pertanto, passare inosservate per lunghi periodi di tempo a causa della mancanza di comunicazione tra l'Internet provider, il fornitore dell'hardware e la community impegnata nella sicurezza. Una semplice ricerca delle vulnerabilità pubbliche in dispositivi venduti dai tre principali fornitori di dispositivi con funzionalità wireless rivela numerosi vettori di attacco che possono essere utilizzati contro questi dispositivi. Alcune vulnerabilità sono state scoperte abbastanza di recente.
La maggior parte delle vulnerabilità può essere sintetizzata come segue:

- Funzioni di amministrazione facilmente intuibili e di semplice accesso da remoto o attaccando gli utenti interni tramite phishing o campagne di malware indotto
- Sovraccarichi del buffer causati da codice generato che arresta servizi o protocolli con conseguente negazione di servizi o esecuzione di codice
- Caricamenti senza limitazioni che consentono a un malintenzionato di eseguire il push di informazioni di configurazione malevole, nuove o modificate, nei dispositivi
- Iniezione di codice tramite un'interfaccia Web che consente a un malintenzionato di

iniettare comandi che conducono alla compromissione o allo sfruttamento di funzioni del dispositivo.
- Password hard-coded nell'interfaccia del dispositivo che possono essere recuperate da remoto o vulnerabilità Arbitrary File Read tramite richieste Web remote I router domestici e delle piccole aziende e alcuni tipi di dispositivi con funzionalità Internet utilizzano spesso processori con architettura MIPS Technologies (una popolare famiglia di processori per dispositivi embedded).
- Tuttavia, questi dispositivi utilizzano sempre più spesso CPU basate su ARM prodotte da ARM Holdings, un altro fornitore di processori RISC (Reduced-Instruction Set Computing).

Il team PLXsert ha osservato payload diretti a dispositivi basati su ARM, che vanno da dispositivi con funzionalità Internet per uso domestico a dispositivi di storage NAT di alto livello, stazioni a banda larga wireless, controller di storage industriali e sistemi di domotica di fascia alta. Molti di questi dispositivi sono soggetti a vulnerabilità simili a quelle descritte per i dispositivi CPE.

Utilizzo dei dispositivi CPE

Un altro segnale della volontà dei malintenzionati di ampliare la loro gamma di risorse è la comparsa di strumenti per lo sviluppo di botnet pensati per cercare e trovare firme e banner specifici di nuovi tipi di dispositivi. Il protocollo SSDP è la base del protocollo di individuazione dei dispositivi UPnP (Universal Plug and Play) ed è destinato all'utilizzo in ambienti domestici e piccoli uffici.
Tale protocollo è basato sul protocollo UDP, che consente ai malintenzionati di eseguire lo spoofing delle origini durante l'esecuzione degli attacchi. Questi dispositivi sono molto numerosi in Internet.
La Shadowserver Foundation ha condotto una ricerca a livello di Internet dei dispositivi con funzionalità SSDP e ha trovato ben 17 milioni di dispositivi che hanno risposto ai probe SSDP.
Il framework Metasploit offre uno strumento per ricercare dispositivi con funzionalità UPnP.
Una volta identificati, questi dispositivi vengono attaccati per l'utilizzo da remoto o lo sfruttamento con tecniche di riflessione. Il team US-CERT ha rilasciato una notifica per gli attacchi ad amplificazione basati su UDP. Questi attacchi utilizzano dispositivi con porte e protocolli aperti per amplificare le risposte contro bersagli designati, consentendo ai malintenzionati di genere un volume di attacchi più elevato con una quantità di risorse minore.
Esistono inoltre exploit pubblici che sono diretti a modelli specifici o a firmware di questi dispositivi e si tratta per lo più di exploit recenti.
I malintenzionati più esperti potrebbero essere in grado di modificare e aggiornare alcuni di questi exploit, creando le condizioni per un utilizzo su vasca scala. Il team PLXsert è riusci-

to a individuare oltre 10.957.000 dispositivi per interazioni pubbliche che sono vulnerabili allo sfruttamento con tecniche di amplificazione. Utilizzando i nostri dati sugli attacchi, abbiamo verificato che alcuni di questi dispositivi vengono utilizzati attivamente in campagne dirette contro clienti Akamai. I malintenzionati possono attaccare questi dispositivi anche per un utilizzo singolo. Possono inoltre scaricare ed eseguire payload malevoli. L'attenzione dei malintenzionati verso dispositivi con funzionalità Internet suggerisce il passaggio a uno scenario in cui una botnet DDoS potrebbe non essere costituita principalmente da PC/server. Ciò pone ovviamente delle difficoltà in quanto la maggior parte di questi dispositivi presenta un basso utilizzo di potenza e di larghezza di banda. Tuttavia, i dispositivi per uso industriale si trovano probabilmente in luoghi in cui l'infrastruttura sottostante supporta capacità di larghezza di banda maggiori e potrebbe essere altrettanto compromessa come illustrato in questo case study.

Campagna in evidenza

Nel 3° trimestre 2014 è stata osservata la seguente campagna di attacchi DDoS con payload basati su ARM. L'aggiunta di questa nuova classe di dispositivi determina un aumento delle risorse di larghezza di banda, della potenza di elaborazione e della distribuzione geografica delle origini degli attacchi, creando quindi una maggiore complessità nella mitigazione delle campagne DDoS. Nella **Figura 9** è illustrata la distribuzione dell'attacco negli scrubbing center DDoS di Akamai. L'attacco ha raggiunto un picco di 215 Gbps e 150 Mpps. La **Figura 10** e la **Figura 11** mostrano la distribuzione geografica delle bot di attacco.
Quasi il 10% degli indirizzi IP di attacco ha coinvolto dispositivi CPE con payload corrispondenti al toolkit Spike, aspetto che è trattato nella notifica di minaccia relativa al toolkit DDoS Spike rilasciata dal team PLXsert.

	Peak bits per second	Peak packets per second
London	40 Gbps	35 Mpps
Hong Kong	30 Gbps	28 Mpps
Washington DC	70 Gbps	28 Mpps
San Jose	25 Gbps	14 Mpps
Frankfurt	50 Gbps	45 Mpps

Fig. 9: Distribuzione dell'attacco per scrubbing center

Mitigazione DDoS

La mitigazione è necessaria sia a livello di dispositivo che a livello di amministratore.
I produttori OEM e gli sviluppatori di piattaforme e applicazioni devono prestare maggiore attenzione quando sviluppano software e firmware per questi dispositivi. La sicurezza deve costituire una parte fondamentale dello sviluppo di firmware e applicazioni. I meccanismi devono prevedere la disponibilità di sistemi di aggiornamento e di patch che potrebbero diventare vulnerabili durante il ciclo di vita.
Per i dispositivi esistenti, le misure di sicurezza correttive per gli amministratori includono le seguenti:

- Best practice ARM per la sicurezza dei dispositivi ARM10
- Linee guida della National Security Agency per la protezione di vari sistemi operativi 11
- Consigli di Tripwire per la sicurezza dei router SOHO12
- Guida NIST per la sicurezza dei dispositivi mobili nelle aziende13
- Guida della University of Michigan per la protezione e la gestione di telefoni/tablet Android14
- Elenco OWASP dei 10 rischi per la sicurezza più critici associati all'Internet of Things (IoT)

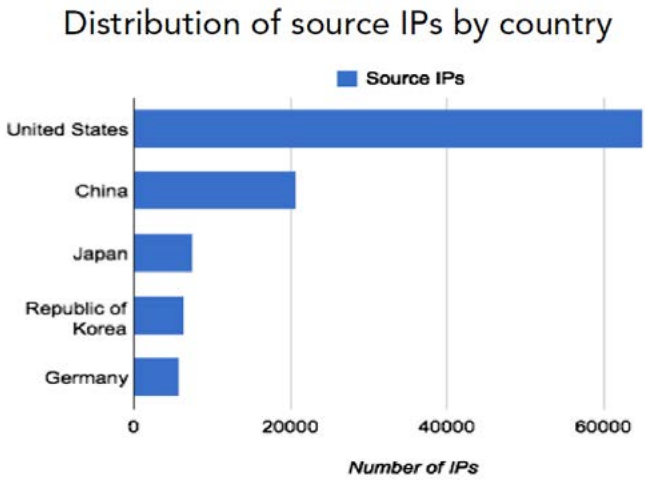


Fig. 10: Distribuzione degli IPs per Nazione

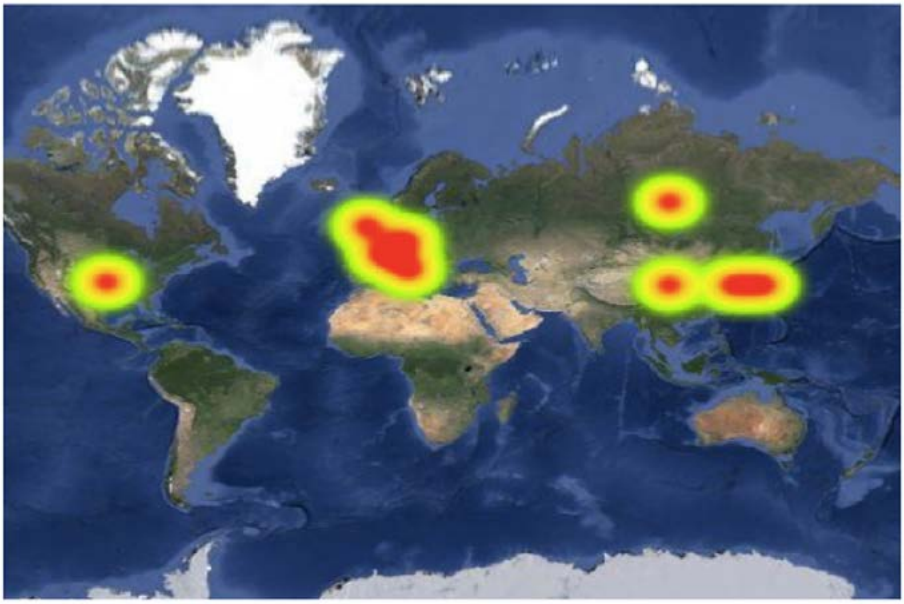


Fig. 11: Mappa termica degli indirizzi IP di origine dell'attacco

Conclusioni

I pirati informatici stanno spostando l'attenzione verso i dispositivi embedded, i dispositivi basati su ARM e i dispositivi con funzionalità Internet al di là dei PC e dei server comunemente attaccati.
I sistemi con potenza di elaborazione di alto livello e la capacità di larghezza di banda elevata resa disponibile attraverso la compromissione di questi dispositivi, nonché le applicazioni basate sul cloud che interagiscono con essi, presentano uno scenario complesso.
Dalla fine del 2013 fino a tutto il 2014, il team PLXsert ha osservato attacchi DDoS che hanno implicato dispositivi mobili, dispositivi CPE e ora payload specifici diretti a dispositivi basati su ARM.
Il passaggio all'impiego di bot DDoS da questa classe di dispositivi determinerà attacchi più complessi e un rapporto più elevato tra volume della larghezza di banda e connessioni nelle campagne DDoS.
Genererà inoltre nuovi tipi di attacchi. Il team PLXsert ha osservato un nuovo tipo di attacco a riflessione basato su UPnP: il protocollo SSDP. Tale protocollo consente ai malintenzionati di creare richieste malevole che causano un traffico riflesso e amplificato diretto contro i bersagli designati.

© Clusit 2015

È necessario coordinare gli sforzi della community impegnata nella sicurezza per scoprire, gestire e mitigare le vulnerabilità presenti in questi dispositivi e per evitare l›ulteriore espansione di queste campagne malevole. La maggior parte di questi dispositivi non è gestita ed è priva di patch, software e firmware aggiornati e rappresenta pertanto un terreno fertile per lo sfruttamento.
Il team PLXsert ha individuato quasi 11 milioni di dispositivi con funzionalità SSDP e circa il 40% di essi è potenzialmente soggetto a sfruttamento. I malintenzionati disporranno di ampie risorse per produrre campagne DDoS. La collaborazione tra tutti i settori è indispensabile per affrontare questa minaccia crescente. Sono necessari fornitori di hardware e sviluppatori di software per la pulitura, la mitigazione e la gestione delle vulnerabilità esistenti e di quelle potenziali durante il ciclo di vita di questi dispositivi.

La Polizia Postale e delle Comunicazioni e il contrasto al cybercrime

La Polizia Postale e delle Comunicazioni

Il Servizio centrale della Polizia Postale e delle Comunicazioni coordina 20 compartimenti regionali e 80 sezioni territoriali con circa duemila risorse con approfondite conoscenze informatiche e di polizia giudiziaria. Il Servizio costituisce il punto di contatto dell'Italia con gli uffici di polizia dei Paesi aderenti al G8 e che si occupano di crimini informatici e collabora a livello internazionale con numerose realtà pubbliche e private per tutelare i propri cittadini da reati commessi in uno spazio, ormai globale, qual è internet.
Il Servizio, a livello operativo, è organizzato in otto aree di intervento in modo da presidiare tutte le tipologie di attività criminali che possano essere perpetrate sulla rete:

- **Pedopornografia:** la Polizia Postale e delle comunicazioni, attraverso il Centro Nazionale per il contrasto della pedopornografia su internet riceve tutta una serie di segnalazioni e coordina le indagini sulla diffusione di immagini di violenza sessuale sui minori che avvengono via Internet e altre reti di comunicazioni e redige le black list dei siti con contenuto pedopornografico.
- **Cyberterrorismo:** le nuove tecnologie vengono sfruttate sempre più da gruppi antagonisti ed eversivi nazionali e stranieri soprattutto per diffondere messaggi e fare campagne di reclutamento. Un team di investigatori specializzati ha il compito di monitorare internet alla ricerca di questi fenomeni per poi effettuare le indagini di merito.
- **Copyright:** anche i circuiti di condivisione di file (file sharing), che speso violano il copyright, sono sotto osservazione per tutelare i diritti d'autore e bloccare la diffusione illegale di file
- **Hacking:** gli investigatori della Polizia Postale svolgono il monitoraggio anche di tutte le attività illecite su internet dedite al danneggiamento, alla compromissione o allo sfruttamento stesso della rete per ridurne o modificarne le capacità stesse.
- **Protezione delle Infrastrutture Critiche del Paese:** attraverso l'attività del C.N.A.I.P.I.C. – Centro Nazionale Anticrimine Informatico per la protezione delle Infrastrutture Critiche vengono condotte attività di prevenzione e contrasto della criminalità informatica ordinaria, organizzata e di matrice terroristica nei confronti delle infrastrutture critiche informatizzate nazionali. Tali attività avvengono, così come stabilito dalla legge istitutiva del Centro (L.155 del 2005 c.d. normativa Pisanu antiterrorismo), attraverso forme di partenariato pubblico privato tra le infrastrutture critiche informatiche del Paese ed il centro stesso.
- **E-banking:** le nuove forme online di pagamento, di transazioni bancarie e gestione dei portafogli richiedono sempre più l'attenzione della Polizia per la prevenzione e il contrasto delle frodi per garantire la sicurezza dei cittadini e la fiducia in questi nuovi strumenti.
- **Analisi criminologica dei fenomeni emergenti:** le nuove frontiere del crimine informatico vengono analizzate da psicologi e investigatori qualificati, organizzati in equipe in

grado di porre il sapere clinico e criminologico delle scienze sociali per la prevenzione e la repressione dei reati informatici.
- **Giochi e scommesse on line:** attraverso il monitoraggio della Rete e un'attenta analisi dei siti dedicati si individuano le attività non autorizzate dal Ministero delle Finanze - Amministrazione autonoma monopoli di Stato

La Polizia Postale, da sempre vicina al cittadino, ha attivato anche i cosiddetti Commissariati Online. I commissariati online sono stati creati con l'intento di ridurre i tempi di risposta della Polizia e facilitare il contatto con il pubblico, dando la possibilità allo stesso di informare o parlare con la Polizia anche da casa propria. I commissariati online si presentano come un sito web (**www.commissariatodips.it**), e hanno tre macro aree di intervento, facilmente consultabili online:
- **Informati** – fornisce informazioni e consigli;
- **Domanda** – fornisce la possibilità di contattare gli esperti per richiedere informazioni e consigli;
- **Collabora** – permette di effettuare segnalazioni e sporgere denunce on-line su reati telematici.

All'interno del Servizio, è attiva anche un'Unità d'analisi del crimine informatico (U.A.C.I.) con l'obiettivo di studiare ed analizzare il fenomeno del computer crime, grazie ad una stretta collaborazione con il mondo accademico italiano.
Le principali attività del U.A.C.I. sono:
- ricerche e studi sul fenomeno della criminalità informatica in collaborazione con Università, Aziende ed Istituzioni;
- sperimentazione di nuove tecniche investigative in materia di computer crime;
- progettazione di percorsi di formazione sulla sicurezza informatica e computer crime in collaborazione con Università e aziende;
- divulgazione di informazioni e risultati di ricerche in contesti scientifici;
- assistenza psicologica degli investigatori che si occupano di computer crime (pedofilia).

Come accennato in precedenza, ci sono poi dei centri di eccellenza all'interno del Servizio della Polizia Postale e delle comunicazioni che sono stati creati con l'intento di specializzarsi in determinati settori quali pedopornografia e protezione delle infrastrutture critiche.

Centro Nazionale Contrasto Pedopornografia On-line

Il Centro Nazionale per il Contrasto della Pedopornografia On-line è stato istituito presso il Servizio Polizia postale e delle Comunicazioni del Dipartimento della Pubblica Sicurezza. L'obiettivo primario è la difesa dei minorenni attraverso il monitoraggio della rete per identificare gli spazi virtuali clandestini dove vengono condivise immagini e filmati di minori abusati.
Il Centro è il punto di raccordo per le segnalazioni provenienti sia da cittadini, sia da associazioni di volontariato, sia da provider, sia da Forze di Polizia straniere.

Come espresso in precedenza, il Centro stila una black list di siti pedopornografici che poi vengono forniti agli Internet Service Provider in modo che ne possano bloccare la navigazione attraverso un sistema di filtraggio. In questo campo, la Polizia collabora anche con i sistemi nazionali bancario e finanziario, tramite la mediazione della Banca d'Italia, per acquisire informazioni su transazioni e spese illecite sul mercato online con lo scopo di acquistare foto o filmati di abusi su minorenni.
In ambito internazionale, il Centro partecipa ad una coalizione mondiale sotto la guida dell'Interpol, con la partecipazione di Europol, per l'identificazione delle vittime della pedopornografia in tutto il mondo.

CNAIPIC - Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche.

Il C.N.A.I.P.I.C. è il centro preposto alla prevenzione e repressione dei crimini informatici che hanno come obiettivo le infrastrutture critiche informatizzate di rilevanza nazionale. Il Centro ha in dotazione una sala operativa h24 in grado di accogliere le segnalazioni sia da parte delle Infrastrutture Critiche nazionali sia da altri attori a livello internazionale impegnati nella protezione delle infrastrutture critiche.
La legge 31 luglio 2005 n. 155, recante: "Misure urgenti per il contrasto del terrorismo internazionale" (normativa Pisanu) ha attribuito al Servizio Polizia Postale e delle Comunicazioni, in qualità di "organo del Ministero dell'Interno per la sicurezza e la regolarità delle telecomunicazioni", la competenza esclusiva all'erogazione dei servizi di protezione delle infrastrutture critiche informatiche da realizzarsi attraverso "[…] collegamenti telematici definiti con apposite convenzioni con i responsabili delle strutture interessate".
Successivamente il Ministro dell'Interno, con proprio decreto del 9 gennaio 2008, ha istituito in seno al Servizio Polizia Postale e delle Comunicazioni, il Centro Nazionale Anticrimine Informatico per la Protezione delle Infrastrutture Critiche – C.N.A.I.P.I.C.
Il Legislatore Italiano tra i primi nel panorama internazionale intuendo il portato della problematica di sicurezza nazionale ha voluto la realizzazione di un "centro stella" che, attraverso un innovativo sistema di partenerariato pubblico - privato con le Infrastrutture Critiche Informatizzate, potesse svolgere la più efficace ed efficiente attività di prevenzione e contrasto a forme di criminalità informatica particolarmente evolute e pericolose.
Il Centro è strutturato in:

- una Sala Operativa attiva 24 ore su 24 – 7 giorni su 7 che eroga l' attività di prima risposta in caso di emergenze cyber, ed effettua costantemente un monitoraggio attivo della rete e l' analisi delle fonti e delle informazioni acquisite (reportistica di settore, informazioni provenienti dalle I.C.I. – Infrastrutture Critiche Informatizzate – o da organismi investigativi e di intelligence)
- una sezione investigativa composta da personale specializzato nel contrasto ai crimini informatici con la possibilità di effettuare attività sotto copertura ed intercettazioni preventive;

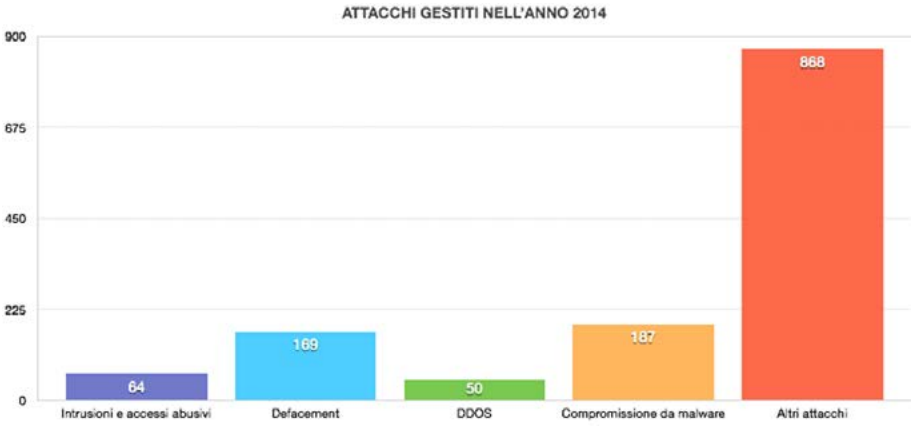
- una sezione tecnica a supporto delle attività operative, che cura altresì la formazione e l'aggiornamento professionale degli operatori.

Il CNAIPIC inoltre è

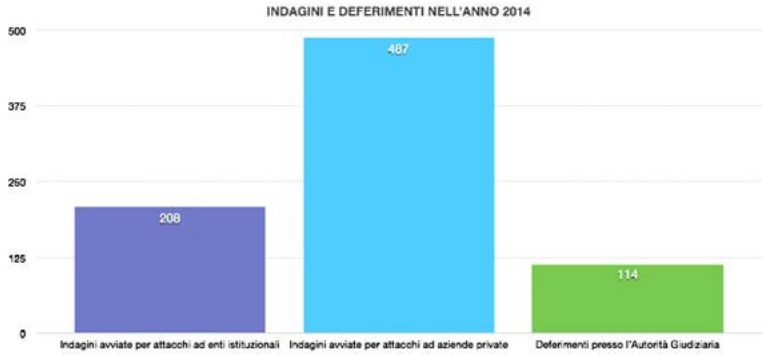
- punto di contatto nazionale della rete G7 HTC emergency operativo 24/7 prevista dalla Convenzione di Budapest, nonché della rete di esperti sul cybercrime di Interpol, per la gestione delle emergenze investigative (congelamento dati, attivazione dei canali di cooperazione internazionale),
- punto di contatto per l'emergenza cyber del Progetto Galileo, per la realizzazione del sistema GPS satellitare Europeo.

Il Servizio Polizia Postale e delle Comunicazioni – CNAIPIC è il rappresentante designato del Ministero dell'Interno in seno al Nucleo Sicurezza Cibernetica della Presidenza del Consiglio, recentemente istituito dal DPCM 24 gennaio 2013 che ridefinisce l'architettura istituzionale in tema di cyber sicurezza

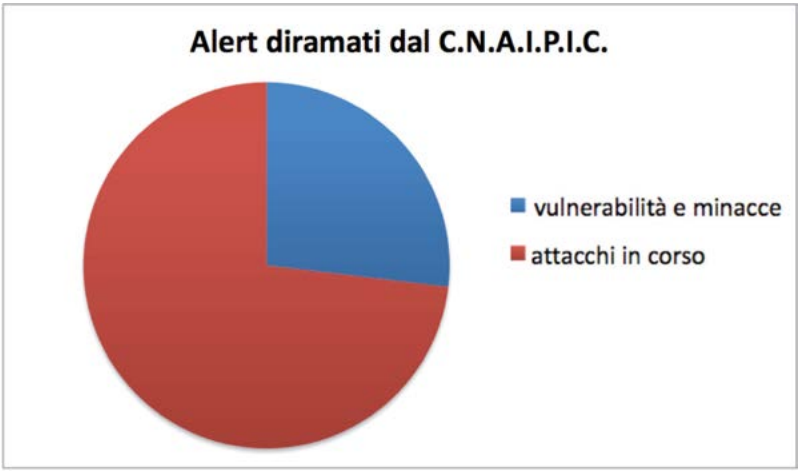
Nell'ambito della sua attività di prevenzione e contrasto al crimine informatico, il Centro nel periodo di riferimento ha gestito attraverso la Sala Operativa: 1.151 attacchi informatici di cui 161 di tipo defacement, 50 di tipo DDoS o di altra natura nei confronti di servizi internet relativi a siti istituzionali e infrastrutture critiche informatizzate di interesse nazionale; tra questi vi sono 64 intrusioni e accessi abusivi a sistemi informatici relativi ad infrastrutture critiche e 187 compromissioni da malware nei confronti di enti istituzionali e imprese private.



È in questo scenario che il C.N.A.I.P.I.C. ha avviato 208 indagini per attacchi informatici perpetrati direttamente ai danni di enti pubblici e 487 nei confronti di imprese private; nell'ambito di tali attività 114 persone sono state deferite presso l'Autorità Giudiziaria.



Particolare attenzione è stata posta alla rilevazione e segnalazione di nuove vulnerabilità e minacce. In particolare sono state rilevate dal Centro 154 potenziali vulnerabilità per i sistemi informatici di infrastrutture critiche e 148 potenziali attacchi, mentre sono stati diramati verso le infrastrutture critiche 1.552 alert dei quali 417 per vulnerabilità e minacce rilevate e 1135 per attacchi in corso.



Nello svolgimento delle sue attività, come previsto dalla stessa legge istitutiva del Centro il C.N.A.I.P.I.C ha attivato diverse convenzioni istituzionali con infrastrutture critiche nazionali. Particolarmente positiva è la collaborazione con quelle realtà del settore privato che, grazie al loro DNA digitale, affrontano le minacce informatiche più di altri. Uno di questi casi ad esempio è quello di Poste Italiane, il cui rapporto con la Polizia Postale è collaudato e di lunga tradizione.

Il CERT di Poste Italiane, infatti, affronta alcune delle problematiche afferenti l'area di interesse del C.N.A.I.P.I.C. come lo dimostrano i dati sottostanti:

- 3.414 segnalazioni di sicurezza gestite
- 14.271 server appartenenti a reti botnet monitorati
- 8 attacchi di tipo DDoS gestiti
- 63 bollettini di Early Warning in riferimento all'identificazione, l'analisi e la definizione delle contromisure necessarie per la loro mitigazione di vulnerabilità e minacce tecnologiche emergenti; tra le principali vulnerabilità sono state analizzate Hearthbleed, NTP Amplification, Eubury rootkit, Shellshock e Poodle sslv3;
- 1300 campioni di malware analizzati nel Cyber-Lab in collaborazione con enti istituzionali;
- 10 casi di illeciti o presunti illeciti gestiti in collaborazione con la Polizia Postale e delle Comunicazioni (es. falsi annunci online fatti a nome e per conto di Poste Italiane, analisi di e-mail con sospetto malware allegato, etc.);
- 7800 siti di phishing attraverso il monitoraggio dei siti cloni e l'attuazione delle relative procedure di shutdown;
- monitoraggio di canali digitali e chiusura di 29 pagine Facebook, 6 pagine Twitter, 60 pagine Pastebin ed 1 blog contenenti informazioni lesive per l'immagine di Poste Italiane;
- rilevamento e blocco di oltre 10.000 credenziali di utenti di Poste Italiane e 12.000 carte Postepay compromesse, attraverso attività di security intelligence ed Information Sharing;
- monitoraggio continuo di 146 applicazioni mobili di Poste Italiane o ad essa riconducibili presenti su 22 application market, con la rimozione di 2 "app" rinvenute malevoli a fronte dell'analisi effettuata.

Collaborazione Internazionale e nazionale

La Polizia Postale ha riconosciuto da subito l'importanza della collaborazione sia in ambito nazionale sia in ambito internazionale per il contrasto dei crimini informatici. Il cyber spazio non ha confini, è pertanto necessario stringere alleanze e collaborazioni con altre realtà transfrontaliere per difendere i propri cittadini dall'"abuso" che taluni fanno delle risorse informatiche.

La Polizia Postale partecipa al Sottogruppo High Tech Crime del G8 e al Comitato per la Politica dell'Informatica e delle Comunicazioni (I.C.C.P.) dell'Organizzazione per la Cooperazione e lo Sviluppo Economico (O.C.S.E.).

Inoltre, il Servizio è anche il punto di riferimento per le emergenze informatiche all'interno delle Reti istituite nel G8 e nel Consiglio d'Europa.

Ulteriori gruppi di lavoro in cui la Polizia Postale e delle Comunicazioni è coinvolta attivamente per il contrasto sono: la Electronic Crime Task Force (ECTF); la European Financial Coalition (EFC); la Virtual Global Task Force (VGT); l'European Working Party on Information Technology Crime; il Comitato High Tech Crime dell'Europol e di alcuni tavoli di lavoro tematici della Commissione Europea.

A livello nazionale, la Polizia Postale è rappresentata su più tavoli di lavoro istituzionali. In questo contesto, forse è più utile invece focalizzarsi su alcune delle iniziative pubblico-private a cui la Polizia ha dato impulso creativo per rendere più incisivo il contrasto al crimine informatico sia a livello strategico sia a livello operativo.
Le iniziative sviluppate sono di information sharing. La prima è l'iniziativa European Electronic Crime Task Force (EECTF) che ha un respiro più strategico, mentre la seconda è nata da un progetto co-finanziato dalla Commissione Europea: Online Fraud Cyber Center and Expert Network (OF2CEN). Quest'ultima ha un respiro più operativo di scambio dati fra istituti bancari e Polizia Postale.

L'European Electronic Crime Task Force

L' European Electronic Crime Task Force è stata costituita nel **giugno del 2009** a seguito di un **accordo di collaborazione** sottoscritto dalla Polizia Postale e delle Comunicazioni, l'United States Secret Service e Poste Italiane. L'iniziativa di cooperazione, inizialmente circoscritta alla partecipazione dei soli Membri Fondatori, è stata successivamente estesa ad un selezionato network di partner, operanti anche a livello internazionale, con competenze specialistiche nel settore della prevenzione e del contrasto alla criminalità elettronica. L'ampliamento del circuito partecipativo e relazionale, articolato su più livelli di interlocuzione tecnica e istituzionale, ha assicurato sia l'estensione del bacino di analisi e raccolta delle informazioni, sia il consolidamento e la condivisione delle best practice di protezione e contrasto di fenomeni di criminalità elettronica rilevati a livello europeo. In tale quadro, si è delineato un qualificato consesso, altamente rappresentativo di professionisti attivi nel settore della cyber security, con l'obiettivo di **rafforzare la collaborazione cross-settoriale tra entità pubbliche e organizzazioni private, al fine di costituire un fronte omogeneo ed univoco di risposta, analisi e prevenzione delle più significative ed emergenti forme di criminalità elettronica**. La Task Force, avvalendosi dei contributi partecipativi periodicamente forniti dai partecipanti, ha altresì avviato un percorso progettuale orientato alla costituzione di un polo europeo di eccellenza - a forte propulsione anche da parte di enti del settore privato - per la valorizzazione dello scambio di informazioni tecniche e operative nonché per la valutazione dei rischi e l'evoluzione delle minacce correlate alla continua evoluzione de fenomeni di *electronic crime*.
Con tale terminologia ci si riferisce a tutte le fattispecie d'illecito informatico formalmente riconducibile alle disposizioni contenute, a livello comunitario, nella nota Convenzione di Budapest del 2001, recepita in Italia con legge dello Stato nel 2008. L'obiettivo di analisi tecnica e di scenario, così come quello di aggregazione di competenze e expertise della Task Force devono intendersi pertanto necessariamente trasversali rispetto ai segmenti produttivi interessati da tali fenomeni criminali, così come rispetto ai Paesi coinvolti nei possibili percorsi fraudolenti. La Task Force si propone altresì come momento di aggregazione strategica, espresso a livello europeo, tra istituzioni pubbliche, forze di polizia, mondo accademico, magistratura ed aziende private altamente tecnologiche, a beneficio dell'intera community di riferimento. In particolare le attività condotte dall'EECTF si articolano oggi

lungo tre prioritarie direttrici di intervento, di seguito sintetizzate:

- **ANALISI:** con riferimento allo sviluppo di approfondimenti dedicati alle nuove minacce che vengono identificate dai partner nei rispettivi ambiti di competenza e operatività, sia in modo congiunto su specifiche iniziative comuni che in un'ottica di condivisione degli studi realizzati al proprio interno. In questo contesto si inserisce anche la partecipazione di Poste Italiane, in qualità di rappresentante della EECTF, a numerose proposte di progetti finanziati dalla Comunità Europea in materia di sicurezza delle informazioni e di collaborazione intersettoriale e cross-country;
- **NETWORK**: con riferimento alla costruzione di una rete di collaborazioni e di scambio informazioni sempre più fitta ed efficace, sia con partner istituzionali attivi a livello nazionale, che nel contesto di iniziative di più ampio respiro. Si inserisce in tale quadro, a mero titolo di esempio, la partecipazione al gruppo dell'ENISA denominato FI-ISAC, Financial Institutions Information Sharing and Analysis Center, che raggruppa in un contesto unico i rappresentanti di istituzioni finanziarie, CERT nazionali europei e Forze dell'Ordine, per facilitare lo scambio di informazioni in materia di sicurezza informatica dei servizi bancari e di prevenzione delle frodi.
- **COMMUNICATION**: con riferimento alla realizzazione di iniziative di comunicazione, siano esse dedicate a una platea ristretta, come nel caso di incontri tecnici a porte chiuse denominati Expert Group, o rivolte a una platea più ampia, come nel caso dei tre Plenary Meeting per anno, o la newsletter CyberNews.

In virtù di una rappresentatività molto consistente del panorama di contrasto del cyber crime a livello nazionale, la EECTF ha stabilito nel tempo importanti relazioni istituzionali con le controparti pubbliche di maggiore rilievo:

- **il Ministero dell'Interno**, non solo attraverso la presenza continuativa e la collaborazione operativa da parte della Polizia Postale e delle Comunicazioni, ma anche mediante la partecipazione alla Community dei rappresentanti delle altre Forze dell'Ordine;
- **il Ministero dell'Economia e delle Finanze**, sia per tramite dell'articolazione dell'U-CAMP (Ufficio Centrale Anticrimine sui Mezzi di Pagamento, con il quale è allo studio un protocollo d'intesa) che di Consip, il cui centro operativo di sicurezza è considerato una best practice nazionale;
- **il Ministero per lo Sviluppo Economico**, attraverso l'**ISCOM** (Istituto Superiore delle Comunicazioni e delle Tecnologie dell'Informazione), anche nel loro ruolo di supporto alla definizione dell'Agenda Digitale Italiana;
- **l'Autorità Garante per la Protezione dei Dati Personali;**
- **Banca d'Italia;**
- **l'Associazione Bancaria Italiana**, per tramite di **ABI Lab**.

Un altro aspetto sul quale si sviluppa ulteriormente l'azione della Task Force e il valore di ritorno per i partecipanti è certamente quello delle cooperazioni internazionali. Sono stati consolidati contatti permanenti con numerose realtà di alto profilo istituzionale che sviluppano percorsi analoghi e che condividono le finalità della EECTF:

- **l'ENISA**, anche attraverso i gruppi di lavoro specifici FI-ISAC (Financial Institutions Information Sharing and Analysis Center) e EP3R (European Public-Private-Partnership for Resilience);
- **Europol**, con riferimento allo European Cyber Crime Center (EC3) e a canali di collaborazione operativa sui temi di criminalità elettronica;
- lo **European Payments Council**;
- il **CERT-EU**;
- **EuroJust**;
- **l'AntiPhishing Working Group**;
- il **Digital Crimes Consortium**;
- **ulteriori gruppi ad accesso riservato altamente qualificati e vendor-independent**, che hanno consentito negli anni di costruire relazioni operative con centri di sicurezza di importanti organizzazioni private. In questo contesto è attivo il contatto con i principali CERT nazionali europei, oltre che con USA e Australia.

Il progetto OF2CEN

Da qualche decennio è in corso un sostanziale cambiamento del modello di erogazione dei servizi da parte delle imprese pubbliche e private verso la propria Clientela; se ad esempio fino a qualche anno fa era necessario presentarsi fisicamente presso lo sportello di un istituto bancario per la gestione del proprio conto corrente, oggi tutto questo è fattibile con una semplice e veloce interazione via web. La "rete Internet" è diventata un vero e proprio canale per il business, dove si facilita l'incontro tra la domanda e l'offerta. Se da una parte tutto ciò ha portato a dei vantaggi considerevoli nella vita delle persone e nello sviluppo delle imprese, dall'altra parte li ha esposti a nuove forme di rischio subito sfruttate dal settore criminale per aumentare i propri guadagni illeciti, tra l'altro spesso favoriti dal vuoto normativo che spesso caratterizza la rete Internet. Sono nati così diversi fenomeni legati al settore del cyber crime con lo scopo principale di sottrarre illegalmente dei soldi agli utenti attraverso meccanismi di raggiro nel tempo sempre più sofisticati (ad es. phishing).

Gioco forza, l'evoluzione tecnologica che ha modificato i comportamenti sociali delle persone negli ultimi anni e ha determinato l'insorgere di nuove forme di pericolo per i cittadini e le imprese, ha richiesto alle forze di Polizia di adeguare i propri metodi d'indagine e di approccio al fenomeno criminale. Nuove esigenze sono nate, fra cui quella di raccogliere e divulgare in modo sistematico informazioni riguardanti le transazioni fraudolente che avvenivano online.

Al riguardo la Polizia Postale e delle Comunicazioni ha iniziato, da qualche anno, un processo di sensibilizzazione nei confronti del settore bancario, tra i più critici e appetibili da parte dei criminali informatici, al fine di convincerli dell'importanza di condividere le informazioni relative a fenomeni di frodi online che andavano a colpire i propri Clienti. Per superare l'approccio classico di scambio delle informazioni basato su comunicazioni di diversa natura, email e telefoniche *in primis*, la Polizia Postale e delle Comunicazioni ha formato un consorzio di organizzazioni appartenenti al mondo pubblico e privato in grado

di supportarla nella realizzazione di una piattaforma di information sharing per il contrasto avanzato ai crimini informatici che interessano in particolare il settore bancario.
Il consorzio vede coinvolte altre Forze di Polizia europee come l'Ispettorato Generale della Polizia Romena la National Crime Agency britannica, istituti di ricerca come la Fondazione GCSEC di Poste Italiane, l'Abi Lab, istituti di credito come Unicredit e società di consulenza come Booz & Company. Con questi partner, è stato realizzato il progetto OF2CEN (Online Fraud Cyber Center and Experts Network), finanziato dall'Unione europea, attraverso il programma di prevenzione e lotta contro la criminalità (Isec). OF2CEN con la sua piattaforma di scambio informazioni, raccoglie le segnalazioni di operazioni sospette che vengono comunicate alla polizia dalle banche che hanno aderito ad un protocollo firmato con Abi Lab, facilita lo scambio di informazioni di indirizzi IP e di dati bancari fraudolenti attraverso canali sicuri. In aggiunta la polizia postale rileva e condivide informazioni degli "early warning", relativi a possibili attività criminose, mettendo in atto un'efficace prevenzione del cyber-crime.
Nella tabella che segue sono riportati alcuni dei risultati ottenuti dalla Polizia Postale e delle Comunicazioni nel contrasto del fenomeno del phihing, del furto di identità e di truffe online. Parte di questi risultati sono stati ottenuti grazie alla nuova piattaforma OF2CEN.

Denunce	**91.460**
Arresti	**31**
Deferimenti presso l'Autorità Giudiziaria	**4.927**
Somme sottratte	**€ 15.470.666**
Somme Recuperate (solo Phishing OF2CEN)	**€ 1.900.000**

Tabella 1 - Phishing, Furto d'Identità, Monetica e truffe online

Il progetto OF2CEN è da considerarsi rilevante nel panorama di quelli realizzati nel dominio della cyber security perché, oltre a realizzare un importante strumento di lavoro per gli analisti di sicurezza, pone in primo piano la reale volontà da parte delle istituzioni pubbliche e private di collaborare contro una minaccia di natura trasversale. Nel 2015 è stato presentato un progetto di sviluppo ulteriore della piattaforma. L'obiettivo è di fornire lo strumento anche alle altre Forze di Polizia europee per creare un network europeo di scambio informazioni con le banche e con l'EUROPOL. L'aggregazione dei dati che verranno raccolti dalle varie piattaforme permetteranno agli stessi Stati Membri di comprendere quali siano le dinamiche delle frodi online e dove si debba maggiormente investire in termini di investimento e contrasto.

Il Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza e il contrasto alle attività illecite su Internet

In questo contributo inedito, il Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza descrive i fenomeni criminosi a cui si trova confrontata e le attività di controllo e contrasto di cui si occupa.

Ruolo di polizia economico-finanziaria della guardia di finanza a contrasto del cybercrime

La presa di coscienza delle gravi minacce derivanti dall'utilizzo illegale delle nuove tecnologie ha evidenziato la necessità di rafforzare il contrasto a conseguenti fenomenologie criminali in continua evoluzione. Tali fenomenologie interessano soprattutto le reti telematiche, in particolare la rete mondiale Internet, da cui l'economia nazionale ed europea dipendono fortemente e sulle quali sono compiuti illeciti il cui contrasto rientra a pieno diritto nei compiti d'Istituto della Guardia di Finanza.

Il Corpo, in ogni sua espressione operativa, si muove sempre trasversalmente nell'ambito della missione istituzionale che gli è affidata quale polizia finanziaria sui fronti della lotta all'evasione e del controllo delle uscite, ovvero quale polizia economica nella tutela del mercato dei capitali e di quello dei beni e servizi, oltreché nel contrasto alla criminalità organizzata, soprattutto sotto il versante patrimoniale.

In linea con tale approccio, anche nel contrasto agli illeciti di carattere economico e finanziario realizzati in Internet, ovvero attraverso le cd. nuove tecnologie, interviene attraverso due direttrici che sono in continuo contatto funzionale tra loro:

- la rete dei Reparti territoriali, capillarmente distribuiti sul territorio nazionale, con il compito di assicurare, nei rispettivi ambiti, l'efficiente tutela di tali funzioni. Tra questi i Nuclei di Polizia Tributaria si pongono come Unità investigative di punta;
- i Reparti Speciali che si affiancano ai primi e che, istituiti per l'investigazione in specifiche materie, sono incaricati di realizzare direttamente, ovvero con azioni di supporto alle Unità operative, moduli investigativi connotati da elevati standard qualitativi per i Reparti territoriali.

I moduli d'azione, anche nelle investigazioni che impattano con il mondo digitale sono, quindi, contestualmente orientati:

- al controllo economico del territorio virtuale, attraverso il monitoraggio della rete telematica, per verificare l'esistenza di sacche d'illegalità;
- ad intercettare i flussi finanziari "sospetti" mediante la tecnica cd. "follow the money";
- a verificare la posizione fiscale dei soggetti investigati per l'eventuale tassazione dei proventi leciti ed illeciti sottratti all'imposizione;
- ad intervenire, trasversalmente, su altri profili di rilievo, quali, ad esempio, quelli in materia di reati contro la Pubblica Amministrazione, valuta e mezzi di pagamento, privativa intellettuale, concorrenza e mercato, privacy e sicurezza delle comunicazioni.

Negli ultimi anni, infatti, la nascita di ulteriori insidie derivanti dall'utilizzo illegale delle reti telematiche e delle nuove tecnologie ed il ruolo che queste hanno assunto nelle dinamiche dei sistemi produttivi e finanziari internazionali, hanno comportato la necessità per il Corpo di rafforzare il contrasto a tali fenomenologie che consentono a soggetti (in Rete assolutamente anonimi) di commettere ogni forma di illecito, ivi compresi quelli rientranti nella sfera di competenza della polizia economico-finanziaria.
Si tratta di un ambito di intervento sempre più all'attenzione delle Istituzioni e Autorità nazionali e internazionali in ragione dello sviluppo della Rete, soprattutto di quelle che sono le sue intrinseche componenti (tecnologiche e/o economiche), quale opportunità di crescita e di trasformazione per un sistema socio-economico maturo, che sempre più spesso viene messa in discussione proprio da comportamenti della specie, capaci di minare irrimediabilmente il rapporto di fiducia tra operatori economici e cittadini/utenti.

In tale contesto, al Nucleo Speciale Frodi Tecnologiche, inquadrato nell'ambito delle Unità Speciali del Corpo, sono affidati, a livello nazionale, compiti di polizia giudiziaria, di analisi, di supporto, di studio e formazione, nonché responsabilità nelle relazioni istituzionali di tipo operativo con gli Organi centrali.
L'attività di servizio è sviluppata nel solco dei citati compiti di polizia economico/finanziaria e, in un'ottica di efficace sinergia interforze, nei comparti di specializzazione o, comunque, nei settori d'intervento rimessi alla competenza del Corpo dal decreto del Ministro dell'Interno approvato il 28 aprile del 2006. Ci si riferisce, in particolare, alla tutela dei movimenti dei capitali e dei mezzi di pagamento, nonché alla salvaguardia dei marchi, dei brevetti e della proprietà intellettuale.
Il Corpo, negli ultimi anni, ha, inoltre, rinforzato le capacità operative che nel comparto informatico esprimono le proprie Unità territoriali e le varie componenti dei Reparti Speciali, attraverso l'avvio di iniziative di formazione specifica nei settori precedentemente nonché in materia di Digital Forensics e la creazione di una rete di specialisti sempre più in coordinamento funzionale con le Unità Speciali del Corpo, secondo una logica che, con riferimento ad indagini caratterizzate da elevato spessore tecnologico, oltreché multidistrettualità e/o sovranazionalità, pone queste ultime come punto di riferimento dei terminali sul territorio.

Criminalità e cybercrime

In campo economico/finanziario gli interessi del *cyber-crime* sono particolarmente elevati verso settori quali le frodi bancarie, il furto di identità e di informazioni, la contraffazione, l'evasione fiscale sul commercio elettronico, la pirateria digitale ed i giochi e le scommesse on line. Ciò provoca danni patrimoniali ingenti ai privati, in termini di minore occupazione, alle aziende, minandone la capacità reddituale, ed all'economia pubblica riducendo la base imponibile delle imposte dirette e indirette e, quindi, il gettito fiscale complessivo del Paese.
Sul punto, si riporta dapprima un breve cenno su due tra le fenomenologie illecite sull'*online* più insidiose: contraffazione ed il *gambling* illegale.

Il primo, infatti, che non coinvolge solo *fashion* e *luxury goods* – si pensi alla vendita attraverso questi canali di pezzi di ricambio per automezzi ed elettrodomestici, a quella di giocattoli o di prodotti la cui commercializzazione è riservata a canali regolamentati (come i farmaci) – produce conseguenze particolarmente gravi sia per l'affidabilità delle transazioni, sia per i titolari dei diritti di proprietà industriale violati, sia, soprattutto, per la sicurezza e la salute degli utenti.
Rispetto ai contraffattori tradizionali, i siti *Internet* di commercio elettronico, e specialmente quelli che si limitano a commerciare *online*, senza spazi fisici accessibili dai consumatori, rendono più difficile distinguere i prodotti veri da quelli falsi, spesso semplicemente riprodotti con immagini "ufficiali", tratte dai cataloghi del produttore.
In tale ambito il Corpo ha messo in campo il S.I.A.C., Sistema Informativo Anti Contraffazione, piattaforma *web* che si articola in una serie di funzioni, alcune delle quali riservate alle Unità operative del Corpo ed alla collaborazione con le forze di polizia e gli altri Organismi che agiscono sul fronte anti-contraffazione.
Le funzionalità in argomento consentono la raccolta strutturata dei dati delle operazioni di servizio effettuate sul territorio, allo scopo di agevolare le analisi di rischio sulle modalità di attuazione delle condotte illecite e sulle dinamiche dei fenomeni, per meglio orientare gli interventi di contrasto e da canali di distribuzione merci on-line.
Con riferimento al secondo settore citato sulla rete vi è una proliferazione di siti che, proponendosi come veri e propri casinò virtuali, consentono agli utenti di accedere alle più disparate offerte di gioco, in assenza di qualsiasi autorizzazione. Si tratta di risorse *web* solitamente allocate su "*server*" ubicati in territorio estero.
Noto a tutti, al riguardo, è il forte interesse che la criminalità organizzata ha manifestato, sin dall'inizio, nel controllo di queste filiere di gioco clandestino in virtù dei guadagni "esentasse" che il gioco illecito consente e della possibilità di reinvestire denaro di dubbia provenienza.

Infine, relativamente ai dispositivi *target* preferiti dai cyber-criminali, si assiste al concentrarsi delle attività di questi ultimi, sempre più sofisticate ed aggressive, verso gli apparati cd. "*mobile*", dal momento che oltre ad avere ormai potenza di calcolo e di connettività di tutto rilievo, nella maggior parte dei casi non dispongono di protezioni anti-*malware* efficaci, anzi, spesso, sono gli stessi utenti a manometterli per sbloccarne alcune funzionalità avanzate, rendendoli ancora più vulnerabili.
Quasi sempre, tali dispositivi, spesso definiti "intelligenti", sono vissuti dagli utilizzatori come semplici "gadget", ma, invece, consentono agli attaccanti di sfruttarne le avanzate caratteristiche peculiari (geolocalizzazione sopra tutte) per compiere nuovi tipi di crimini, anche molto insidiosi. In questo contesto, è opportuno sottolineare come l'elevata diffusione di tali *device*, tra i giovani ed i giovanissimi, ha portato inevitabilmente ad un aumento dei reati perpetrati contro questa fascia di popolazione.
La portabilità e la comodità proprie di questi oggetti rendono, inoltre, sempre più diffusi i casi di "*dual use*", cioè di utilizzo ibrido dello stesso dispositivo, tipicamente in ambito pri-

© Clusit 2015

vato e business, introducendo vulnerabilità nuove e particolarmente complesse da gestire all'interno delle organizzazioni di tipo imprenditoriale e, di conseguenza, nelle relazioni di tipo economico.
Va aggiunto, poi, che il processo di educazione digitale dei cittadini appare ancora difficoltoso, mentre lo stesso non si può dire per i Cyber criminali che escogitano, invece, metodi di offesa sempre più sofisticati ed aggressivi, in grado di influenzare i comportamenti degli utenti anche dal punto di vista psicologico, con danni apprezzabili per l'Internet economy nazionale.
Un esempio emblematico di come queste forme di criminalità possano influenzare il comportamento degli utenti è rappresentato dai virus conosciuti come "*ransomware*" capaci di ingannare l'utente.
L'osservazione della realtà esterna ci permette, inoltre, di osservare come le più recenti sfide del crimine informatico siano rivolte anche al mondo dei Social Network, che spingono l'utente ad esporre eccessivamente la propria identità digitale. Tale rischio aumenta in maniera esponenziale nei confronti degli utilizzatori di dispositivi mobili, posto che è più difficile distinguere una pagina web contraffatta su uno schermo di ridotte dimensioni.

Esperienze operative

Entrando nel vivo dell'argomento, va innanzitutto ricordato come, da almeno due decenni, l'affacciarsi delle nuove tecnologie, abbia consentito alle organizzazioni criminali di realizzare ulteriori ingenti profitti illeciti. I fenomeni relativi hanno ormai assunto dimensioni di rilievo anche sotto l'aspetto digitale.
Ciò provoca danni patrimoniali ingenti ai privati, in termini di minore occupazione, alle aziende, minandone la capacità reddituale ed all'economia pubblica riducendo la base imponibile delle imposte dirette e indirette e, quindi, il gettito fiscale complessivo del Paese.

Pirateria digitale

Dall'osservazione del contesto esterno di riferimento è emerso chiaro come le metodologie utilizzate per immettere in consumo contenuti digitali in violazione alle norme sul Diritto d'autore stiano gradualmente mutando.
A prescindere, comunque, dall'applicativo utilizzato per effettuare la condivisione di *files*, ancora oggi è possibile rendersi praticamente anonimi utilizzando tecniche non più appannaggio di utenti esperti. Recentemente, le abitudini dei cosiddetti «pirati» si stanno spostando dai tipici *peer to peer* o Torrent verso altre metodologie, ad esempio quella del *cyberlocker*, che non comporta una condivisione immediata dei *files*, essendo invece un servizio di archiviazione su Internet appositamente progettato per caricare contenuti che possono, poi, essere scaricati da altri utenti per mezzo di un indirizzo *web*.
In alcuni casi tali siti raccolgono donazioni, allo scopo dichiarato di poter sostenere le spese di mantenimento del dominio e dell'infrastruttura che lo ospita. Spesso, invece, i gestori dei siti in parola guadagnano attraverso il cd. *advertsing* ovvero la presenza di banner pub-

blicitari all'interno delle pagine *web* e si servono di false identità e di imprese di facciata per introitare i proventi illeciti.
Centinaia di migliaia di utenti accedono, anche tramite i più noti motori di ricerca e social network, direttamente a tali piattaforme senza alcun obbligo di registrazione e identificazione, e le usano regolarmente ogni giorno per scaricare in altissima definizione e qualità digitale musica, film, videogiochi e *software*.
I siti possono anche presentarsi come forum, finalizzati alla raccolta, indicizzazione e diffusione di materiale tutelato mediante diverse modalità che vanno dal classico *link* ai già citati *cyberlockers*, alla fruizione in *streaming* di palinsesti e contenuti cinematografici o musicali, fino alla condivisione di collegamenti utili alle piattaforme *peer to peer* e torrent.
Le attività di contrasto a tali condotte illecite manifesta delle interessanti particolarità sotto il profilo tecnico e un elevato livello di trasversalità, essendo sviluppati contestualmente aspetti relativi alla violazione del diritto d'autore, tematiche connesse con la violazione della privacy (anche a causa della presenza di *malware*) e fenomeni di evasione fiscale.
Sotto l'aspetto della privacy, inoltre, talvolta le indagini consentono di appurare come una ulteriore fonte di guadagno rappresenti la fornitura, dietro compenso, ad imprese operanti nel settore pubblicitario di database di utenti iscritti ai siti pirata, mettendo a disposizione i dati forniti in sede di registrazione, le e-mail e gli indirizzi IP, senza aver preventivamente acquisito il loro consenso e in violazione alle disposizioni previste a tutela della privacy.
Nel 2014, attraverso l'operazione della Guardia di Finanza denominata "Italian Black Out" per la prima volta in Italia è stato possibile dimostrare un collegamento diretto tra un sito web "vetrina" ed un *cyberlocker*. I creatori dei contenuti diffusi illecitamente attraverso il *cyberlocker* e pubblicizzati sul sito vetrina ricevevano denaro commisurato al numero di download richiesti comportanti l'apertura e visualizzazione di banner pubblicitari.
Altre operazioni, sempre in materia di pirateria digitale, tra le quali quella denominata "Publifilm" hanno permesso di individuare e sequestrare siti *web*, tutti situati su server all'estero, aventi milioni di contatti giornalieri, che ottenevano enormi profitti attraverso sia il cosiddetto sistema del "pay per click" sia tramite *banner* e *pop up* pubblicitari .
La struttura di questi siti *web* consente con estrema facilità, attraverso motori di ricerca interni, di trovare contenuti illegali e visualizzarli su qualsiasi piattaforma.

Contraffazione online

Attraverso il monitoraggio della Rete spesso è stato possibile identificare, oltre ai tradizionali siti vetrina di prodotti contraffatti, collegamenti a negozi virtuali dedicati alla vendita di merci contraffatte con marchi riconducibili a note case di moda internazionali all'interno di siti *web* con dominio di primo livello ".it" violati per mezzo di tecniche di *link building* e *defacement* (inserimento di una nuova pagina all'interno della struttura del sito). Questa tecnica permette alle organizzazioni criminali di aumentare il *page rank* dei loro siti *web* illegali e di direzionare gli utenti di motori di ricerca online verso le piattaforme illecite.

© Clusit 2015

Truffe sulle piattaforme di e-commerce

Attraverso specifiche attività investigative relativamente a siti, intestati a falsi nominativi, presso i quali viene proposta la commercializzazione di beni di vario tipo a prezzi estremamente vantaggiosi si appura, in alcuni casi, al di là delle apparenti finalità di vendita di prodotti, che i negozi virtuali in parola, in realtà, sono concepiti e realizzati per indurre i potenziali clienti a rilasciare le credenziali delle proprie carte di credito, al fine, poi, di acquisirle illecitamente.

I responsabili degli illeciti, facendo leva, ad esempio nel caso di vendita di prodotti da fumo, sulla naturale reticenza che sorge in capo alle vittime una volta che queste scoprono di essere state ingannate, riescono a protrarre le attività delittuose attraverso il finto negozio virtuale per lunghi periodi.

Gambling

Le operazioni della Guardia di Finanza, in questo ambito, hanno permesso negli ultimi anni, attraverso il sequestro di agenzie di gioco e punti scommesse gestite dalla criminalità organizzata in diverse regioni del territorio nazionale di portare alla luce vaste reti telematiche di scommesse su eventi sportivi di qualsiasi genere, parallele a quella legalmente autorizzata, completamente efficienti e in grado di pagare ingenti somme di denaro anche oltre la soglia prevista antiriciclaggio, senza lasciare apparentemente traccia.
Inoltre, i gestori di tali sistemi, al fine di aumentare ulteriormente gli illeciti guadagni, all'esito dei risultati, attraverso l'alterazione di giocate precedentemente effettuate, simulano l'esistenza di più vincitori rispetto a quelli reali riducendo in modo fittizio la consistenza del montepremi visibile sulla rete, in tal modo truffando gli abusivi giocatori risultati effettivamente vincitori.
In alcuni casi, anche i sistemi di gioco autorizzati possono essere utilizzate per riciclare i proventi di un'attività criminosa. Alcuni soggetti in modo fraudolento, carpiscono ad ignari cyber utenti le credenziali dei mezzi pagamento elettronico e, poi, le utilizzano per alimentare conti di gioco, sostituendosi all'identità informatica dei legittimi titolari di centinaia di carte di credito (mediante il cosiddetto "furto dell'identità digitale").
In seguito i "borsellini elettronici", utilizzati per giocare *online* e per effettuare scommesse su Internet, vengono di fatto "svuotati" prelevando con carte prepagate attivate ad hoc o attraverso bonifici bancari, le somme di denaro indebitamente sottratte, in precedenza, agli intestatari delle carte di pagamento.

Conclusioni

In questi anni abbiamo assistito ad una rapida evoluzione nell'utilizzo delle tecnologie collegate ad Internet che ha prodotto un costante aggiornamento dei modelli di interazione e, conseguentemente, di acquisizione di servizi e beni da parte dei cittadini, delle imprese e delle Pubbliche Amministrazioni. Si è affermato, così, un nuovo modo di vivere, organizzare l'impresa, lavorare e governare la *res pubblica*.

Siamo di fronte ad una vera e propria esplosione sociale e culturale, oltre che tecnologica, di determinati fenomeni legati all'accesso on-line ai servizi.

Il *cybercrime* che, ovviamente, riguarda sia reati "endemici" del *web*, che reati tradizionali, per la realizzazione dei quali i primi ed il *web* sono soltanto uno strumento, sta diventando anche una delle espressioni della criminalità economica.

In questo contesto il Corpo, quale Forza di Polizia specializzata nel settore economico-finanziario, persegue, attraverso i propri reparti, il primario obiettivo di intensificare l'aggressione della ricchezza accumulata indebitamente dalle consorterie criminali che operano nei vari campi di interesse, in quanto costituente il frutto ovvero il reimpiego di proventi di attività illecite.

Tale azione di impulso ha comportato una maggiore reattività delle articolazioni operative della Guardia di Finanza che oggi, ogni qual volta da indagini di Polizia Giudiziaria concluse e in corso di svolgimento o dal controllo del territorio emergono indizi di reato costituenti presupposto per l'applicazione di misure ablative, propongono sistematicamente alle locali autorità giudiziarie provvedimenti quali il sequestro preventivo finalizzato alla confisca per equivalente ed il sequestro per sproporzione.

Internet, in ogni caso, come tutte le tecnologie innovative, è una realtà incontestabile in termini di progresso e di democrazia. Basti pensare, ad esempio, alla quantità di informazioni che oggi troviamo liberamente sulla rete, anche di carattere giuridico, tecnico, societario, finanziario etc. etc.. La ricerca di queste informazioni fino ai primi anni '90 impegnava molta parte del nostro tempo ed era anche molto costosa visto che comportava l'impiego di risorse umane e finanziarie. Un altro innegabile vantaggio si ritrova nella estrema facilità di comunicare e scambiarsi, in piena legalità, notizie, documenti o immagini. Come sempre, allora, la patologia risiede nell'utilizzo illegale della tecnologia e non nelle capacità che questa ci offre.

Internet come fonte aperta rappresenta, inoltre, un'opportunità per gli Organismi di *Law enforcement*; non sono rari, infatti, i casi investigativi risolti attraverso elementi trovati sulla rete.

Le nuove tecnologie sono, in sostanza, un formidabile ausilio per combattere i fenomeni criminali che infestano la Rete, a patto che, tra gli attori che operano nella legalità e per la legalità, si mantengano strette forme di collaborazione e cooperazione.

Ecco perché il Corpo, mantiene, da sempre, una linea di collaborazione con gli Enti nazionali ed internazionali che hanno compiti di controllo, regolamentazione e prevenzione, nei vari comparti della missione istituzionale, oltreché con le maggiori associazioni di categoria, come testimoniato anche dai numerosi Protocolli d'intesa in atto.

© Clusit 2015

I Reparti del Corpo si avvalgono, così, nell'ambito della loro azione di ricerca, prevenzione e repressione degli illeciti di polizia economico/finanziaria commessi nel mondo virtuale, ovvero attraverso le nuove tecnologie, della conoscenza "dall'interno" che su tali fenomeni hanno i Soggetti che operano istituzionalmente nel settore a tutela dei cittadini, delle imprese e dell'economia nazionale ed europea.
Il compito di un Corpo di Polizia economico-finanziaria, quale è la Guardia di Finanza, è quello di garantire, anche nel contesto virtuale, il rispetto delle regole per fornire un fattivo contributo allo sviluppo dell'Italia ed un concreto sostegno all'imprenditoria onesta.

Rapporto Clusit 2015 – FOCUS ON

Questa sezione del Rapporto 2015 è dedicata a delle aree di particolare rilevanza per la sicurezza ICT in Italia.
Abbiamo chiesto ad alcuni dei maggiori esperti italiani, nelle singole materie, di approfondire i seguenti temi:

- Internet of (Hacked) Things, ovvero come la sicurezza degli oggetti di uso quotidiano impatterà sulla vita di ognuno di noi e delle aziende in cui lavoriamo.
- M-Commerce, cioè attività di commercio elettronico svolte attraverso dispositivi mobili collegati a Internet, che introduce nuovi fattori di rischio, dove il comportameto degli utenti è il primo fronte di intervento.
- Bitcoin, aspetti tecnici e legali della criptovaluta. Con questo Focus On si intende fare il punto sugli aspetti tecnici e legali che hanno spinto milioni di investitori a puntare sulla criptomoneta e un gran numero di giornalisti a decretarne un giorno il successo e il giorno dopo la morte (per oltre 30 volte dalla sua nascita).
- Doppia autenticazione per l'accesso ai servizi di posta elettronica. Vediamo sempre più che i grossi operatori di Internet a livello mondiale, offrono servizi di posta con doppia autenticazione. Dal punto di vista tecnologico non c'è nulla di veramente nuovo, ma a livello di comportamento consapevole da parte degli utenti è una vera rivoluzione.
- Lo stato della sicurezza dei siti web della pubblica amministrazione.
  Lo studio offre una panoramica generale dello stato attuale della sicurezza dei siti web delle Pubbliche Amministrazioni ed offre spunti di analisi in merito agli accorgimenti che possono essere adottati per migliorare il livello di sicurezza .
- Il Regolamento generale sulla protezione dei dati: novità per i cittadini, le imprese e le istituzioni. Se le istituzioni europee sapranno evitare un compromesso al ribasso, il Regolamento potrà migliorare sensibilmente la protezione dei dati e al contempo stimolare il mercato digitale.
- Cloud e sicurezza: profili legali. Lo sviluppo dei servizi di cloud computing appare inarrestabile. La sicurezza è elemento essenziale da cui non si può prescindere. Per questo motivo a livello normativo esistono precisi vincoli da tenere in considerazione. Anche alla luce delle nuove ISO 27018 appare quindi quanto mai utile fare il punto sullo scenario attuale e sulle prospettive evolutive.
- Return on Security Investment. Uno strumento utile a chi in azienda deve compiere, e quindi giustificare, investimenti in sicurezza IT, ma anche un supporto per la valutazione di processi e sistemi esistenti.
- L'impatto della Direttiva 263/agg.15 di Banca d'Italia sugli operatori del settore bancario.
  Per chi si occupa di sicurezza, nessuno degli obiettivi posti dalla Direttiva è una vera novità, ma è significativo lo sforzo nell'incardinare nelle logiche di sistema gli aspetti di sicurezza che sono irrinunciabili. Il recepimento di queste e delle future Raccomandazioni aumenterà di molto il livello medio di sicurezza dei servizi bancari e delle transazioni online, costituendo una base importante per lo sviluppo e la diffusione di questo tipo di servizi.

Internet of (Hacked) Things

Ovvero come la sicurezza degli oggetti di uso quotidiano impatterà sulla vita di ognuno di noi e delle aziende in cui lavoriamo.

A cura di Alessio L.R. Pennasilico

Molto, troppo marketing in questo periodo usa, spesso in modo inappropriato, il termine Internet of Things, che per brevità chiameremo IoT.
Si immagina un mondo di oggetti connessi ad Internet che interagiscono tra loro e con noi, scatenando azioni automatiche ed aggregando dati per permettere a software e/o persone di prendere decisioni.
Il mercato consumer è letteralmente inondato di oggetti che si fregiano di aggettivi quali "*smart*", proprio per raccontare quel livello di interconnessione appena descritto. Da qualche anno oramai si trovano, ad esempio, le "*smart*" TV in ogni negozio di elettrodomestici. Addirittura, oggi, è difficile trovare una TV che *smart* non sia. Altri elettrodomestici fanno oggi sorridere se nominati come *smart*, o connessi ad Internet, quando a dire il vero sono già in commercio: dal frigo alla lavatrice.

Ma gli oggetti *smart* che già utilizziamo sono ben di più: dai cellulari che sono diventati *smart* Phone, agli orologi .che sono diventati *smart* Watch alle chiavi per entrare in auto in modo più semplice, definite *smart* Key. Pensiamo poi alla domotica con tutti gli allarmi, impianti di videosorvegliaza, riscaldamento, condizionamento, gestione dei pannelli solari… la lista sarebbe ancora molto lunga.

Non sempre, ovviamente, tali oggetti sono già connessi ad Internet.
Si pensi ad elettrodomestici che già sono nelle nostre case, che conservano informazioni che riguardano in modo puntuale. Mi raccontava l'amico Marco Calamari del tecnico della lavatrice in grado di dire con che frequenza viene fatta la lavatrice del bianco, quando vengono lavate le lenzuola o le tende. Che la centrifuga viene usata troppo spesso in modo troppo aggressivo. Tutto grazie ad un connettore dentro alla lavatrice al quale il tecnico si collega. Connettore che domani sarà una porta ethernet. Ed i dati saranno visualizzati attraverso una comoda interfaccia web.
Si pensi ad oggetti come la *smart* Key di alcune auto: anche in questo caso, a ben guardare, le evoluzioni sono veloci e portano ad oggetti sempre più connessi: se oggi la chiave serve a riconoscere il guidatore e mettere il sedile nella sua posizione preferita, domani le auto potranno decidere la playlist della musica, le impostazioni del navigatore, le mail da mostrare sul display e molto altro ancora.
Parliamo di IoT oggi, ma questi oggetti sono già parte della nostra vita quotidiana oramai da tempo. Le auto, ad esempio, sono molto spesso già connesse ad Internet. I produttori hanno già iniziato a gestirle da remoto. Si pensi a BMW che recentemente ha inviato a molte delle

proprie auto un aggiornamento software[1].
Per non parlare delle auto che hanno addirittura delle App per controllarle[2].

"I sistemi sia di infotainment che di funzionamento del veicolo sono sempre più connessi"

In ambito aziendale questo è ancor più vero: qui non si parla più solo della *smart* TV della sala riunioni o dello *smart* Projector, il proiettore connesso e comandato via IP della sala conferenze. Soprattutto in ambito industriale si parla di sensori, macchinari, PLC ed altra componentistica che permette di tenere sotto controllo una rete complessa, una rete di Automazione e Controllo. Reti che, anche se impropriamente, per capirci, possiamo definire SCADA. Anche in questo caso gli oggetti sono molti, moltissimi, sempre di più, soprattutto però, presenti già da molto tempo. Se negli anni '90 questi oggetti erano connessi esclusivamente tra loro, oggi l'interazione con l'IP, con i Servizi Informativi (IT) e con Internet è sempre maggiore.

Viviamo in un mondo meraviglioso (di Leibniziana memoria) dove gli oggetti sono sempre più intelligenti, più smart, e ci aiutano sempre meglio a governare situazioni complesse tanto a casa quanto in ufficio o in fabbrica.

Viviamo nel migliore dei mondi possibili. Oppure no?

Se pensiamo che la risposta sia si rischiamo di passare per il Candido di Voltaire. Spesso, infatti, mi dichiaro "preoccupato" delle cose che vedo attorno a me. Molti, troppi degli articoli che leggo da mesi oramai riguardano, infatti, questo tema.

Viviamo in un mondo meraviglioso… in realtà ci vivremmo se tutti fossero preoccupati quanto me.
Il costo di sviluppo di un prodotto *smart* è molto diverso dal costo di sviluppo di un prodotto

1 http://www.securityweek.com/bmw-patches-security-flaw-let-hackers-open-doors

2 http://www.computerweekly.com/news/2240239247/Ford-Lincoln-announces-remote-control-car-app-as-BMW-issues-security-patch

© Clusit 2015

"smart & secure". Vengono troppo spesso privilegiate variabili quali il Time to market, il contenere il costo di Ricerca e Sviluppo o il Costo industriale del prodotto, rispetto alla sicurezza del prodotto.
Progettare un prodotto sicuro costa denaro, molto più denaro che progettarne uno senza curarsi di questo aspetto. Mantenere un prodotto sicuro costa denaro. Per questa ragione, non essendoci specifiche leggi in proposito, non tutti, non abbastanza produttori si preoccupano del problema.

Immaginatelo su temi più noti rispetto alla sicurezza IT: in un mondo in cui non sia obbligatorio certificare la conformità del prodotto alla rete elettrica ed un suo adeguato livello di sicurezza e qualità (si pensi al marchio CE banalmente), quanti lo farebbero?
Quanti lo farebbero, ben conoscendo problemi che quel settore dell'industria, oramai maturo, conosce da anni.
Ecco, in un contesto come quello degli oggetti *smart* il problema diventa ancora più grave: oltre al problema **economico**, infatti, vi è anche un problema di **consapevolezza** e di **percezione**.

Il problema **economico** è rendersi conto che progettare un prodotto senza pensare alla security costa molto meno. Ma non rendersi conto che renderlo sicuro in un secondo momento, dover far fronte ad eventuali responsabilità o richieste di danni, oltre al market share perso a causa di eventuali incidenti o violazioni, costa molto di più che progettare un prodotto sicuro. Chiedete ad una casa automobilistica quanto costa richiamare qualche milioni di automobili a causa di un errore di progettazione/implementazione. Nel settore dell'informatica questo problema diventerà noto solo quando le software house diventeranno legalmente responsabili dei danni che causano vendendo software scritto senza rispettare le più note e comunemente accettate best practice. Fino a che nessuno sarà responsabile di alcunché, temo, l'industria continuerà a non trovare un buon motivo per investire in modo adeguato in *smart security.*
Consapevolezza perché oggi molti dei rischi che tali oggetti introducono sono noti a pochi esperti, visti come dei pazzi che urlano nel deserto, salvo poi scoprire che in realtà si trattava di maledette Cassandre che prevedevano un futuro non troppo lontano, che puntualmente si avvera. Basta seguire media generalisti, senza addentrarsi nelle pubblicazioni specialistiche. Non passa settimana senza che vengano annunciati nuovi incidenti, vulnerabilità o esaltati prodotti che all'esperto fanno venire i brividi. Leggevo su Facebook un conoscente scrivere "ecco una foto del mio nuovo citofono IP! Sono a Parigi e posso vedere chi suona a casa mia ed aprire la porta". Meraviglioso. Fino a che non inizio a chiedermi chi altri potrà aprire la porta oltre a me, tramite Internet. A volte anche solo per errori di configurazione, senza che siano note vulnerabilità gravi dell'oggetto. Potenza del Plug&Play: mia madre può comprare un oggetto elettronico al supermercato, assieme a riso ed all'ananas, tornare a casa e collegare in autonomia il nuovo oggetto con tutte le sue mirabolanti funzioni smart semplicemente collegando un cavo ethernet. "Collegati sempre, ovunque, dovunque" dice

la brochure. Non vedo scritto da nessuna parte "solo tu". Senza pensare a quanti frigoriferi mal configurati ci sono nel mondo, basti pensare a quanti access-point wireless (oggetto con il quale abbiamo confidenza da 15 anni) sono nelle case e nelle aziende di decine di milioni di persone, con tutte le configurazioni di default, password comprese o mal configurati, tanto da poter essere violati in pochi minuti da una ragazzina[3].

Percezione perché questi oggetti vengono presentati nel modo errato, distorcendo profondamente la loro natura. Mi sono già scagliato contro questo problema in altri articoli e conferenze: l'odio per la parola *smart*, che molti altri, come me, condividono.
Quando mi presentano la *smart* TV io mi immagino una TV anni '80 con il tubo catodico, che la tecnologia ha fatto evolvere in un oggetto esteticamente più gradevole, fatto di schermi piatti poiché il tubo catodico non serve più e più intelligente perché connessa ad Internet. Bugia. Inganno.

"In quanti film abbiamo visto "hacker" attaccare e modificare i famosi pannelli sulla Quinta strada?"

L'oggetto che sto guardando non ha nulla a che vedere con una TV anni '80. Hanno progettato una cosa da zero: hanno preso un PC, piccolo, poco potente per i nostri standard, ma potentissimo per quel che deve fare, un computer che nasce collegato ad Internet ed ad essa integrato, gli hanno saldato sopra un ricevitore di segnale televisivo ed hanno saldato tutto su uno schermo per PC molto grande. Non stiamo quindi parlando di *smart* TV, ma di idiot PC. Non è l'evoluzione della TV, ma la riduzione del computer per un uso semplificato da persone meno avvezze. Per questo io sono preoccupato: guardiamo gli oggetti che colleghiamo ad Internet, gli oggetti in cui inseriamo le nostre credenziali ed i nostri dati e ci sentiamo sicuri tanto quanto ci sentivamo sicuri con i vecchi oggetti di uso quotidiano.
Dimentichiamo completamente di considerare e gestire tutti i nuovi rischi che questi dispositivi introducono.
Come già detto: statisticamente parlando, non sappiamo configurare correttamente un access-point, oggetto non riconducibile a nulla di noto e rassicurante, oggetto al quale anche

[3] http://www.tripwire.com/state-of-security/latest-security-news/seven-year-old-hacks-public-wifi-in-under-11-minutes/

© Clusit 2015

per sola "ansia per il non noto" dovremmo applicare tutta la nostra attenzione. Figuriamoci quanta attenzione poniamo nel configurare e gestire questi oggetti…

Per questo sono preoccupato, perché sento parlare di smart City e di smart Industry.
Tutti questi elementi mi convincono che sempre più spesso sentiremo parlare non di Internet of Things (#IoT) ma di Internet of Hacked Things (#IoHT).

"C'è ma non si vede. Già oggi le aziende che usano tecnologia SCADA sono moltissime e troppe sono già a rischio, come dimostra il motore di ricerca Shodan"

Purtroppo non è solo preoccupazione, ma la certezza di un futuro di cui abbiamo già visto delle anteprime. Già al Security Summit di Milano del Marzo 2014 si parlò di questo tema[4]. Un frigorifero *smart*, con un controller basato su Linux era stato infettato da un Worm. Ed aveva iniziato a spedire phishing, come qualsiasi altro PC infetto.

Questo è quel che temo per il futuro: un'industria che poco si preoccupa di progettare device sicuri "by design", che quando se ne preoccupa si invischia in problemi burocratici o di budget interni, associati ad un'utenza che adotta strumenti di cui non conosce i rischi. Ed organizzazioni criminali che sanno perfettamente come sfruttare le falle "dimenticate" e come monetizzarle, con truffe più o meno tecnologicamente all'avanguardia. Forse meno che più, visto che troppo spesso la competenza necessaria è davvero ridicola.

Temo un futuro, che purtroppo è già presente, in cui esista un motore di ricerca come Shodan[5] che permetta a chiunque, anche ai nostri figli curiosi e poco esperti di IT Security, di individuare reti industriali non protette, accederci in modo semplice ed intuitivo per causare danni incalcolabili.

Sono molto preoccupato per un futuro in cui verranno coniugate truffe note con "nuove" falle e tecnologie. Immagino un futuro in cui i nostri device "*smart*" verranno contagiati da malware tipo Cryptolocker. Quest'ultimo è molto noto visto l'enorme numero di vittime mietute nel 2014 ed in questo inizio di 2015. Numero di vittime in costante aumento. Si

[4] https://www.securitysummit.it/milano-2014/percorso-gestione-sicurezza/talk-52/

[5] http://www.shodanhq.com/

riceve una mail in cui vengono utilizzate le scuse più diverse (la fattura da pagare, il pacco da ritirare, il rimborso da ricevere) per convincere l'utente a cliccare l'allegato. Allegato che se cliccato avvia un programma che cripta tutti i dati sia sul PC locale che sui server di rete a cui quel PC accede. Bella l'encryption, da anni voi esperti ne parlate bene, giusto? Si, peccato che in questo caso la password per accedere di nuovo ai dati la possegga solo il criminale. E che chieda un compenso per comunicarcela. Un riscatto. Per questo questa categoria di malware si chiama Ransomware: o paghi, o hai perso per sempre i tuoi dati[6].
Capito che il modello di business funziona molto bene e presenta un ROI elevato[7], i criminali hanno già iniziato a declinarlo. È già uscita la variante per Android. "Vuoi utilizzare di nuovo il tuo smartphone? Paga il riscatto!".
È già uscita la versione che colpisce i siti web. Non cripta il proprio PC, ma rende inutilizzabile il sito web non particolarmente curato dal punto di vista della sicurezza. "Sito inaccessibile. Paga il riscatto per renderlo di nuovo operativo". Ne ridevo all'Internet Festival a Pisa, dove sono andato a trattare questi temi a nome di Clusit. Assieme a me c'era l'amico Andrea Zapparoli Manzoni, con il quale abbiamo riso per un pomeriggio di questi scenari, ipotizzando cose che potrebbero accadere ogni giorno a chiunque in futuro. Ho coniato in quell'occasione un hashtag che sto usando in diversi articoli, sui social network e in diverse conferenze oramai da mesi per descrivere il problema. #1bitcoin. Ricordate Benigni e Troisi in "Non ci resta che piangere"? ecco. Questo è il mio, il nostro, timore. Un futuro dove un doganiere-criminale ci chieda un riscatto di 1 bitcoin ogni volta che vogliamo fare qualcosa. Abbiamo già avuto esempi in ambito "consumer" non solo *smart* Phone, TV e frigoriferi che potevano essere violati, ma anche automobili, pacemaker, pompe per l'insulina, telecamere dei circuiti di videosorveglianza. Questo mi preoccupa. Un futuro in cui qualcuno possa bloccare la mia auto. "Vuoi andare in ufficio oggi? 1 Bitcoin!".

Un futuro in cui tutte le attrezzature ospedaliere saranno connesse (già oggi molte lo sono), in cui i semafori saranno IP, in cui l'accesso ad Internet in aereo sarà all'ordine del giorno, ma potrebbe permettere di accedere ai comandi dell'aereo stesso[8].

Tutto questo mentre i giornali di automobilismo acclamano la self-driving-car come il futuro. Magnifico. Basta solo essere concordi su chi intendiamo per "self".

---

[6] Salvo potersi permettere di buttare tutto e ripristinare un backup o utilizzare altre tecniche più fantasiose o che sfruttano errori dei criminali.

[7] Su una campagna di 10 milioni di e-mail inviate, nei primi 5 giorni si sono infettati ed hanno pagato il riscatto 12mila computer. Essendo il riscatto di $ 750, sono circa 9 milioni di dollari di ricavo. Nei primi 5 giorni. Faccia il lettore il conto del ricavo a fronte di una redemption ridicola tipo il 5%.

[8] Consiglio di partire dal giustamente più scettico Bruce Schneier, che molti di voi hanno conosciuto al Security Summit, https://www.schneier.com/blog/archives/2008/01/hacking_the_boe.html per leggere poi l'articolo della FAA che lui cita nel suo post.

© Clusit 2015

Ovviamente una preoccupazione ancora più grande va al mondo dell'industria. Cosa succederà quando qualcuno prenderà il controllo di una pressa o di un altoforno e chiederà il riscatto? Di una diga? Di una centrale elettrica? Fantascienza in effetti. Se non fosse che correva l'anno 2000 quando successe a Gazprom, un'azienda le cui misure di sicurezza sono "un po' più complesse" di quelle di una azienda comunale…[9]
Non credete alle mie parole: provate ad utilizzare Shodan per una decina di minuti e poi ditemi cosa siete riusciti a spegnere dove.

Fantascienza. Vorrei che fosse fantascienza, alla Die Hard, mentre abbiamo già visto succedere questo dietro casa nostra, quando il cryptolocker prima citato ha "rapito" i dati dell'anagrafe di molti comuni italiani. Che per riappropriarsi dei dati hanno fatto l'unica cosa che restava da fare: pagare. E lo vedremo succedere per chi pubblica su Internet il proprio impianto di generazione solare di energia, per chi per evidenti ragioni di "interconnessione" fa interagire sempre più spesso i propri sistemi con quelli di terzi. Senza verificare quanto questi terzi siano affidabili. Come nell'attacco subito da Target[10].

L'ho già detto: sono preoccupato. Lo sono perché usiamo inconsapevolmente, sempre di più, sempre più spesso oggetti di cui non conosciamo e di cui non ci preoccupiamo del livello di sicurezza.

Sarò retrogrado e paranoico, ma dovendo scegliere dove abitare preferirei la più noiosa ed affidabile "*secure* City" alla più idolatrata e sbrillucicante "*smart*" City. Non ho abbastanza bitcoin per permettermi di vivere nella seconda. Non ho abbastanza bitcoin neppure per fare impresa nella seconda città.

Per questa ragione credo sia compito di tutti noi, dagli esperti di security fino ai curiosi che hanno capito il problema, informare le persone che ci circondano di fare attenzione. Di richiedere prodotti sicuri.

Possiamo farlo. Oppure, per scoprire quanti incidenti come quelli descritti sono diventati problemi quotidiani, possiamo aspettare di poter leggere il Rapporto CLUSIT 2017. Dopo aver pagato qualche bitcoin per sbloccare il device sul quale lo vorremo leggere.

---

[9] Nel caso citato era coinvolto un dipendente infedele, la tecnologia era un po' diversa… ma pensate a che tecnologia utilizzavate 15 anni fa!

[10] Sul Rapporto Clusit 2014 è descritto con dovizia di particolari l'incidente. La catena di negozi ha subito una violazione perpetrata grazie alla rete insicura di una azienda che manuteneva i loro frigoriferi.

M-COMMERCE

a cura di Fabio Guasconi

M-commerce in Italia

Chiariamo innanzitutto cosa si intende con il termine "mobile commerce" e con la sua più colloquiale forma contratta "**m-commerce**" che useremo nel seguito. Questo termine è stato coniato nel 1997 da Kevin Duffey alla cerimonia iniziale del Mobile Commerce Forum con l'accezione di: "conferimento della facoltà di effettuare attività di commercio elettronico direttamente tra le mani del consumatore, ovunque si trovi, attraverso tecnologie wireless". Tradotto in termini pratici stiamo parlando di contratti di vendita stipulati attraverso dispositivi mobili collegati a Internet, che svincolano il consumatore non solo dalla presenza fisica nel luogo d'acquisto ma anche dall'impiego di una postazione fissa o a portabilità limitata.

L'amore degli Italiani verso i dispositivi per la telefonia mobile è noto da lungo tempo e costituisce uno di quei campi in cui a livello europeo possiamo vantare un primo posto positivo nella classifica. Sorprende quindi fino a un certo punto assistere a significativi incrementi d'uso del neonato paradigma di m-commerce nel nostro paese se non fosse che, secondo il consorzio Netcomm[1], stiamo parlando di cifre da capogiro nell'ordine di **+289%** nel 2013 e di ulteriori **+85%** nel 2014.

M-commerce è cresciuto in Italia del 289% nel 2013 e dell'85% nel 2014

Il più vasto fenomeno dell'e-commerce, che include l'm-commerce ma che vi aggiunge tutte le attività efettuate anche da computer di tipo fisso e portatile, continua a crescere a doppia cifra nel nostro paese ma i volumi restano ancora contenuti rispetto al resto del mondo. Sul fronte del m-commerce invece, soprattutto grazie al sopracitato amore per i dispositivi per la telefonia mobile ormai irrimediabilmente avviati ad essere in gran parte smartphone (sono utilizzati da oltre il **40% della popolazione**), i numeri di cui sopra testimoniano una performance decisamente sopra la media. Il personal computer resta comunque **lo strumento preferenziale per l'accesso a Internet nel nostro paese ma la sua diffusione è sostanzialmente ferma a p**oco meno del **60% della popolazione**, mentre la tendenza all'uso di dispositivi mobili (comprensivi di smartphone e di tablet) sta salendo ininterrottamente negli ultimi anni.

Il fenomeno esplosivo del m-commerce sarà quindi in grado di far recuperare all'Italia il ritardo accumulato sul fronte dell'e-commerce? Forse è presto per dirlo ma come si può vedere sono molti i segnali che vanno in questa direzione come ad esempio Audiweb[2], che

[1] http://www.consorzionetcomm.it/

[2] http://www.audiweb.it/

© Clusit 2015

riporta già dal 2014 una prevalenza di fruizione dei contenuti digitali da dispositivi mobili piuttosto che da personal computer.

Quanto è sicuro l'm-commerce

Come ben sanno gli esperti di sicurezza informatica, che ora è molto più "alla moda" chiamare cybersecurity, quasi tutte le nuove tecnologie e gli annessi paradigmi d'uso innovativi sono tradizionalmente lontani dall'avere da subito un livello di sicurezza definibile come soddisfacente. L'm-commerce non fa particolare eccezione in questo senso e, per quanto sia in grado di mutuare molte misure di sicurezza dal più consolidato mondo dell'e-commerce, introduce una serie di nuovi fattori di rischio legati alla sua stessa facilità d'uso tra cui principalmente:

- la **facilità di smarrimento/sottrazione** dei dispositivi mobili collegata alle loro ridotte dimensioni e amplificata dallo scarso impiego di misure di blocco dello schermo o del dispositivo;
- la **limitata potenza di calcolo** dei dispositivi mobili dovuta a ragioni di peso e ingombro, in progressivo superamento con l'uscita dei più recenti modelli multi-core;
- la **disomogeneità dei sistemi operativi** utilizzati sui dispositivi mobili, con numerose release differenti da manutenere da parte dei produttori, acuita dalla carenza di funzionalità di sicurezza utilizzabili da parte dell'utente;
- l'**abbondanza di informazioni e funzionalità** sui dispositivi mobili che ne permettono un impiego sempre più rapido e versatile anche in sostituzione di altri oggetti più o meno tecnologici (navigatori satellitari, orologi, agende, riproduttori di musica etc.);
- la possibilità d'**impiego di app**(plicazioni) diverse dai browser e scarsamente controllate dai gestori degli "store" per effettuare transazioni;
- l'**uso di protocolli di trasmissione radio** (dal GPRS all'LTE ma anche WiFi e Bluetooth) che sono per loro natura non riservati e condivisi in luoghi pubblici con altri utenti attraverso funzionalità spesso lasciate attive dagli utenti.

Questi fattori di rischio, opportunamente sfruttati da un attaccante, possono generare molteplici problemi legati alla sicurezza delle informazioni utilizzate per effettuare le transazioni di m-commerce o semplicemente memorizzate sui dispositivi mobili. Numerosi esempi in questo senso possono essere reperiti sui più popolari studi statistici di settore, che tuttavia tendono a sottovalutare il fenomeno in quanto è poco spesso una causa di perdite dirette e significative per le aziende. La principale motivazione di ciò è che il nuovo elemento vulnerabile sono proprio i dispositivi mobili e le tecnologie da essi impiegate, cosa che rende **i clienti finali bersagli di questi nuovi attacchi**, molto più che le aziende o i fornitori di servizi di m-commerce.

I clienti finali sono i nuovi bersagli degli attacchi al m-commerce

Le principali minacce che sfruttano i fattori di rischio precedentemente elencati sono il **malware sviluppato per il mondo mobile**, che si stima coinvolga oltre 16 milioni di dispositivi nel 2014 con un tasso di crescita di nuovi malware del +83% rispetto al 2013[3] e le **app contraffatte**. Queste due minacce sono spesso collegate tra loro in quanto, diversamente da quanto avviene per i malware su personal computer, sui dispositivi mobili l'infezione si diffonde prevalentemente tramite installazione manuale dell'utente che è indotto a credere di aggiungere una normale applicazione. L'abitudine a non impiegare un software anti-malware sui dispositivi mobili, inizialmente motivata da rallentamenti delle prestazioni ma sempre meno sostenibile, combinata con l'installazione di app contraffatte e l'apertura di link o contenuti appositamente confezionati da attaccanti preparati sono gli elementi alla base dell'elevata diffusione del malware registrata sui dispositivi mobili. Mentre i malware più diffusi solitamente raccolgono dati personali generali dell'utente (oltre eventualmente quelli generati dalle funzionalità attive, come ad esempio la geolocalizzazione), cercando di inviargli messaggi pubblicitari, le app contraffatte possono essere più mirate e cercare di riprodurre dei software esistenti o anche inesistenti per sottrarre i legittimi dati di accesso degli utenti a quel servizio specifico o, ancora peggio, di modificare le informazioni scambiate a fini malevoli. È successo in passato a soggetti come la popolare Netflix americana ma anche ad una banca italiana che non offriva alcuna app per l'accesso al conto dei propri correntisti. Persino quando sono legittime, le stesse app possono soffrire di una serie di problemi di sicurezza del tutto simili a quelli esistenti per le applicazioni web e già ben indirizzati da anni dal lavoro di gruppi di interesse, quali ad esempio OWASP, e che acquisiscono ulteriore rilevanza in questo contesto come ad esempio la necessità di cifratura delle informazioni scambiate attraverso protocolli radio.

Considerando poi gli altri fattori di rischio, molte app permettono di memorizzare i propri dati personali in un profilo, tra cui anche i dati di pagamento (carta di credito o wallet elettronico che sia) e lo smarrimento o il furto di un dispositivo non bloccato possono quindi permettere un loro reimpiego non autorizzato in modo molto semplice. L'abbondanza di funzionalità attive sui dispositivi mobili e il loro uso in zone pubbliche permette anche l'effettuazione di attività quali il **bluesnarfing** che utilizza delle vulnerabilità del protocollo wireless Bluetooth, se attivato, per accedere in modo non autorizzato a informazioni memorizzate sul dispositivo.

In questo scenario purtroppo non vengono più di tanto in aiuto i sistemi operativi sviluppati per piattaforme mobile che, dovendo supportare hardware molto variegato e in continua evoluzione, si ramificano in numerose release rendendo complesso per i produttori mantenere sotto controllo le vulnerabilità. Ulteriore aggravante è il fatto che le funzionalità di sicurezza offerte dal sistema operativo sono spesso ridotte all'osso per favorire le performance dei dispositivi.

---

[3] Kindsight Security Labs H1 2014 Malware Report

© Clusit 2015

Per riassumere, è possibile collegare visivamente i fattori di rischio rilevanti per la sicurezza del m-commerce e i problemi che possono emergere dallo sfruttamento degli stessi.

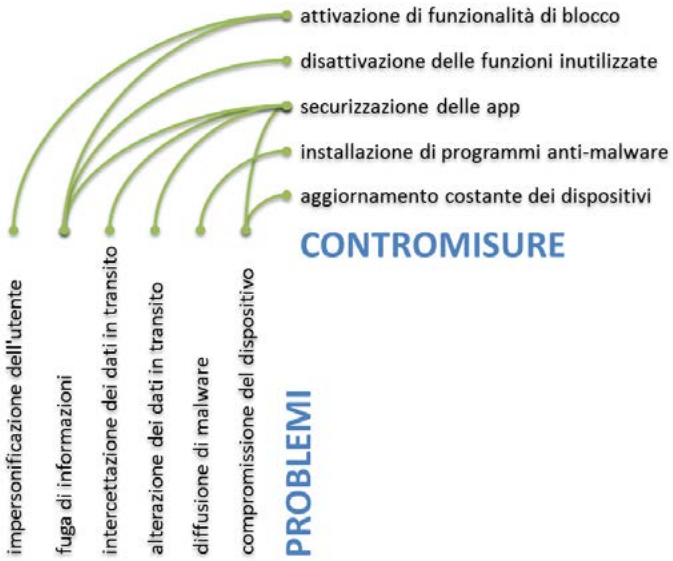
Come rendere l'm-commerce più sicuro

Per migliorare il livello di sicurezza offerto dai sistemi di m-commerce vi sono fondamentalmente due attori che devono intervenire, ciascuno nel suo ambito. Il più importante ma contemporaneamente il più difficile di questi siamo tutti noi, **gli utenti dei dispositivi mobili**, mentre l'altro sono il variegato insieme di **gestori dei servizi e delle infrastrutture** abilitanti del m-commerce, con in prima fila gli sviluppatori delle app.

La sicurezza del m-commerce dipende da utenti e gestori dei servizi

Cosa ciascuno di questi attori debba fare è abbastanza evidente prendendo spunto dalla situazione illustrata poc'anzi ed è riassunto visivamente nello schema sottostante. Gli utenti dovrebbero attuare un insieme minimo di semplici **misure di "igiene" dei propri dispositivi mobili** che includono il blocco automatico in caso di inattività (con uno sblocco che prevede un'autenticazione complessa e sicura naturalmente!), la disattivazione delle funzionalità non utilizzate quando non necessarie (collegamenti di rete, individuazione della posizione) e il loro non impiego quando non necessario (soprattutto per la memorizzazione di dati di pagamento all'interno dei profili), l'installazione di software per la protezione dal malware (ve ne sono molti di gratuiti per uso personale), l'installazione periodica degli aggiornamenti messi a disposizione dai produttori ma soprattutto cautela e discernimento nell'installazione di app verificandone l'attendibilità ed eventualmente rinunciando in caso

di dubbio. I gestori dei servizi, oltre a curare in maniera completa la sicurezza dei sistemi informativi che utilizzano come richiesto da norme tecniche quali la ISO/IEC 27001 o PCI-DSS, massimamente applicabile in questo contesto, dovrebbero concentrare la loro attenzione sul nuovo aspetto di **sicurezza delle app**. Che siano sviluppate internamente o che vengano fornite da terze parti, dovrebbero imporre al loro interno dei requisiti di sicurezza avanzati, adottando tecniche sicure di sviluppo e sottoponendole infine a verifica prima della loro messa a disposizione verso il pubblico, come peraltro già da tempo suggerito da gruppi autorevoli[4].



Pur essendo generalmente chiare le azioni da intraprendere quello che manca da entrambi i lati è purtroppo la leva della motivazione. Per quanto riguarda gli utenti, fintanto che oltre il 50% di noi[5] non solo non attiverà ma addirittura disabiliterà le funzioni di sicurezza presenti sul proprio dispositivo per poterlo usare più liberamente, la difficoltà di quest'impresa rimarrà paragonabile a uno scenario in cui agli automobilisti è concesso di guidare senza allacciare la cintura di sicurezza. I gestori dei servizi sono, per parte loro, limitatamente interessati a investire per migliorare la sicurezza dell'm-commerce in quanto non sono essi stessi ad essere frodati ma possono al peggio ricevere dei danni indiretti (d'immagine e per cause legali relative all'assenza di quella che il mondo anglosassone chiama "due diligence").

[4] https://www.owasp.org/index.php/OWASP_Mobile_Security_Project

[5] Cyber Defense Labs, 2013

Gli incentivi per migliorare la sicurezza del m-commerce languono

Di certo **il primo punto su cui è importante intervenire è la cultura**, nell'ottica di rendere consapevoli dei rischi tutti i soggetti coinvolti, soprattutto gli utenti finali che hanno il diritto di non essere degli esperti di sicurezza informatica e di non doverlo essere per proteggersi adeguatamente.

La cultura sulla cybersecurity degli utenti è il primo fronte d'intervento

Un elemento attorno al quale potrebbe crearsi l'occasione favorevole per diffondere una corretta cultura sul tema potrebbe essere un "bollino" europeo riconosciuto da (e imposto a, in maniera incentivante piuttosto che penalizzante) tutti gli attori che sia largamente sponsorizzato nei suoi principi, ivi incluso il corretto comportamento degli utenti, da istituzioni e associazioni rilevanti. Qualche passo in questo senso è stato mosso in passato ma ancora molto vi è da fare, soprattutto per quanto riguarda la sicurezza delle informazioni, troppo spesso dimenticata a favore di altri aspetti più tangibili ma purtroppo meno rilevanti.

Alcune azioni che potrebbero avere dei risvolti benefici sulla sicurezza del m-commerce sono ad esempio state recentemente portate avanti per tutelare i cosiddetti m-payments e il mobile banking, entrambi allo stesso modo dipendenti dalla sicurezza dei dispositivi mobili e delle applicazioni da essi utilizzate. Anche il Garante per la protezione dei dati personali è intervenuto su questo nell'ottica di garantire i trattamenti di informazioni legate alle firme grafometriche effettuate con dispositivi mobili.

Purtroppo però in tutti questi casi ci si è rivolti ai gestori dei servizi cui sono state indicate misure di carattere generico, operando in modo limitato verso un aumento della cultura degli utenti.

Resta da sperare che l'aumento della diffusione dell'impiego dei dispositivi mobili (è notizia recente ad esempio la loro sperimentazione per ospitare un'app sostitutiva di una patente fisica negli USA) possa innescare una maggiore attenzione in questo contesto e che quindi altri attori, oltre naturalmente a CLUSIT, possano raccogliere la sfida e le numerose opportunità rappresentate da un incremento della **cultura per la sicurezza delle informazioni o cybersecurity** che dir si voglia nel nostro Paese, legata sì al m-commerce ma non solo ad esso …

Bitcoin, aspetti tecnici e legali della criptovaluta

a cura di Giuseppe Vaciago e Paolo Dal Checco

Il 2014 è stato l'anno caratterizzato dal boom della cosiddetta "criptomoneta", una valuta decentralizzata la cui implementazione si basa sui principi della crittografia a chiave pubblica, detta anche asimmetrica. Pur essendo stati censiti oltre 500 tipi di valute elettroniche soltanto dieci possiedono una capitalizzazione di mercato che supera i 10 milioni di dollari e di una si è parlato costantemente, per motivi diversi che vedremo a breve, durante tutto l'arco del 2014: il Bitcoin. Il presente focus-on mira a fare il punto sugli aspetti tecnici e legali che hanno spinto milioni di investitori a puntare sulla criptomoneta e un gran numero di giornalisti a decretarne un giorno il successo e il giorno dopo la morte (per oltre 30 volte dalla sua nascita).

Il sistema Bitcoin

Bitcoin – con l'iniziale maiuscola si intende la rete e il protocollo, con la minuscola la valuta in sé – è un'unità di scambio progettata nel 2009 da un uno sviluppatore che si cela dietro lo pseudonimo di Satoshi Nakamoto. L'idea delle criptovalute non era comunque nuova, già dal 1998 erano in circolazione progetti di monete digitali decentralizzate basate sulle proprietà crittografiche e su pubblici registri.

A differenza delle valute tradizionali, nessuna autorità riconosciuta si occupa di coniare, regolamentare e distribuire i bitcoin. Ogni nodo del sistema, infatti, possiede una copia del database chiamato "blockchain" che contiene lo storico di tutte le transazioni avvenute tramite la criptomoneta. Le transazioni attestano il trasferimento di bitcoin tra ciò che potremmo paragonare ai nostri IBAN, cioè gli indirizzi bitcoin, pseudonimi che indicano appunto un contenitore nel quale matematicamente viene inserita della moneta e dal quale può essere estratta per migrare verso altri contenitori. Un indirizzo Bitcoin è un numero di 160 bit che può essere rappresentato in diversi formati: quello standard inizia con un "1" o un "3" e possiede numeri e lettere 'O', '0', 'I' e 'l' per evitare confusione, come notiamo nell'indirizzo "*1883gY1csW3J7RytYXmfc9JSC6RnQuckjg*". Legati al concetto di indirizzi ci sono i *wallet*: contenitori più grandi che raccolgono insieme diversi indirizzi in modo che possano essere utilizzati più facilmente.

Due aspetti intrinsecamente legati sono alla base del funzionamento del Bitcoin: la generazione di nuova moneta e lo scambio di quella in circolazione. Senza entrare nei dettagli, illustriamoli brevemente per fornire a chi non conosce le basi del sistema il modo di capirne il funzionamento e le motivazioni che l'hanno reso la criptomoneta del 2014.

La valuta bitcoin non viene coniata nella maniera tradizionale, ma tramite un processo chiamato *mining* (*mine* in inglese significa minare) da parte di nodi della rete che vengono definiti *miners*, cioè minatori. Minare bitcoin significa – e qui ci si riconduce all'aspetto relativo alle transazioni – raccogliere insieme un certo numero di scambi di criptomoneta in

© Clusit 2015

corso e aggiungerli alla blockchain, che come abbiamo visto costituisce il registro pubblico di tutte le transazioni. La difficoltà del lavoro svolto dai minatori, che viene costantemente adattata in modo da rendere necessari circa 10 minuti per minare ogni blocco, fa sì che i minatori che riescono ad "agganciarsi" con successo alla *blockchain* ottengano un certo numero di bitcoin che possono versare su un proprio indirizzo, utilizzando una transazione del blocco stesso che hanno minato. Oltre al premio fornito dal sistema, i minatori ricevono una commissione variabile anche da tutti coloro che hanno eseguito transazioni inserite all'interno del blocco stesso.
Il premio elargito ai minatori viene dimezzato per protocollo ogni quattro anni, questo fa sì che ne 2140 il numero di bitcoin in circolazione raggiungerà i 21 milioni e lì rimarrà costante.
L'utilizzo della rete Bitcoin è in rapido aumento, così come la sua popolarità. Non è facile stimare le cifre di questa ascesa, ma possiamo usufruire di alcuni indici piuttosto significativi per farci un'idea di come il 2014 sia stato un anno intenso per la criptomoneta.
Il primo indice è quello del numero di transazioni giornaliere, ricavato direttamente dai dati pubblici presenti nella blockchain. Il 2014, come si nota nella grafica, ha ripreso la tendenza di crescita del 2013 raggiungendo picchi di oltre 100.000 transazioni giornaliere.

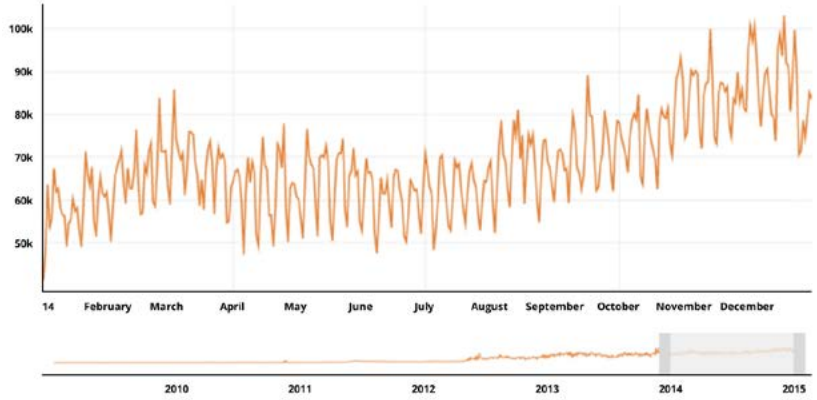


Figura 1: numero di transazioni giornaliere in bitcoin (fonte: blockchain.info)

Mentre il numero di transazioni fornisce stime confortanti, meno rassicurante è il grafico del controvalore attribuito in dollari al bitcoin, che nel 2014 ha fatto rabbrividire per la discesa costante (in netto contrasto con la rapidissima salita di fine 2013) buona parte di chi ha tentato di utilizzare il Bitcoin per speculare sul tasso di cambio.

Figura 2: controvalore in dollari del bitcoin (fonte: blockchain.info)

Dagli oltre 1.000 dollari di gennaio 2014 il bitcoin è sceso a 400 dollari, per riprendersi per alcuni mesi e poi precipitare fino a 300, perdendo il 70% del proprio valore.
Nonostante questa discesa, numerosi sono stati gli eventi positivi per il Bitcoin nel corso del 2014. Ai primi di maggio la Federal Electron Commission ha annunciato l'approvazione dei bitcon come valuta per le donazioni elettorali. Poche settimane dopo è il turno di Paypal, colosso statunitense che conta oltre 300 milioni di utenti e circa 150 miliardi di dollari di transazioni l'anno, che ha dichiarato pubblicamente per voce dell'A.D. Ebay Inc. John Donahoe l'intenzione di includere i bitcoin nei metodi di pagamento accettati.
A dicembre Microsoft USA, grazie ad un accordo con BitPay, ha iniziato a offrire il pagamento tramite bitcoin per l'acquisto delle App per smartphone. Questa novità ha ricevuto commenti entusiasti della community, la quale non ha perso tempo nell'aggiungere il gigante di Redmond alla già ricca lista che vede Expedia, Dish, Dell Computer, Virgin e Overstock attivi già da tempo nel settore.
Il 2014 è l'anno in cui l'Italia ha visto i primi bancomat per Bitcoin, nelle città di Roma e Milano, novità per noi ma strumento già sdoganato in decine di paesi dove questi ATM vengono utilizzati per prelevare o depositare criptomoneta. Per chi preferisce operare online, sempre nel 2014 sono nati alcuni servizi basati in Italia, come PosteBit e CoinBit, che permettono in pochi minuti di acquistare bitcoin pagando tramite bonifico, carta SuperFlash o versamento PostePay.

Natura giuridica e profili fiscali della criptovaluta

Da un punto di vista giuridico, una criptovaluta potrebbe rientrare nella definizione di software fornita dalla WIPO (World Intellectual Property Organization).
Ciò che rileva, tuttavia, è l'inquadramento giuridico della criptovaluta come unità di conto,

© Clusit 2015

in quanto da questo tipo di classificazione ne derivano delle conseguenze giuridiche da un punto di vista fiscale.
Sotto questo profilo, alcuni esperti della materia (Capaccioli, Burlone, De Caria, Aranguena) hanno concluso che la criptovaluta può essere considerata moneta a corso legale, ma in questo caso la mancata accettazione di tale strumento di pagamento a livello statale ne fa perdere un requisito essenziale. Stessa sorta subisce la definizione di critpovaluta come strumento finanziario in quanto, in Italia, il Testo Unico sulla Finanza espressamente esclude i sistemi di pagamento dal suo ambito di applicazione.
Rimane quindi la possibilità di far rientrare la criptovaluta nella definizione di bene che possiede, esattamente come l'oro o l'argento, un valore che perdura fintantoché le persone e le aziende sul mercato decidono liberamente di attribuirglielo.
Da un punto di vista tributario, la criptovaluta può subire un trattamento diverso a seconda di quale classificazione giuridica le venga data. Se venisse considerata una moneta fiat, il miner non sarebbe assimilabile al soggetto emittente, mentre l'utilizzatore che spesso svolge un'attività speculativa rientrerebbe nella normativa in materia di imposte dirette sul reddito delle persone fisiche se la sua attività speculativa superasse l'importo di euro 51.645,69 per almeno sette giorni lavorativi continui. Se, invece, fosse considerata uno strumento finanziario verrebbe assoggettato solo il reddito di capitale, ossia i frutti prodotti sotto forma di interessi attivi o dividendi o di profitto in caso di cessione.
Se, infine, venisse considerata come bene immateriale, si generebbe una situazione ancora più complessa, in quanto se il miner svolgesse l'attività in modo professionale e continuativo sarebbe da considerare un imprenditore soggetto all'obbligo di iscrizione al Registro delle imprese (ex art. 2195 c.c.), con tutti gli adempimenti civilistici e tributari che ne potrebbero derivare. Sotto il profilo dell'assoggettamento a regime IVA, l'operazione di cessione della criptovaluta dovrebbe quindi essere assoggettata alla penalizzante aliquota IVA del 22% prevista dal D.P.R. n. 633/72, mentre l'utilizzatore ricadrebbe nella stessa disciplina del miner nel momento in cui la sua attività di cessione della criptovaluta avesse uno scopo dichiaratamente speculativo.
Un'ultima categoria di soggetti che va presa in considerazione dal punto di vista tributario è sicuramente quella degli intermediari che svolgono l'attività di promozione e negoziazione di criptovaluta. La normativa bancaria tedesca (Kreditwesengesetz, o KWG) ha disciplinato quattro tipologie di intermediari in base al mercato di riferimento in cui essi operano (broking services, multilateral trading system, contract broking e proprietary trading) prevedendo la possibilità che la loro attività sia sottoposta ad autorizzazione da parte della preposta autorità di vigilanza. Nel resto del mondo, invece, tale figura non è stata disciplinata e normalmente opera senza una licenza specifica.
In conclusione la natura virtuale e immateriale della criptovaluta che la differenzia considerevolmente dalla moneta elettronica come definita dalla Direttiva 2009/110/CE, genera dubbi interpretativi che rischia anche di portare a delle valutazioni giuridiche non sempre corrette.

Sicurezza del sistema bitcoin

L'utente medio che si avvicina al mondo Bitcoin ragiona in termini di *wallet* (portafoglio) e password necessaria per custodire il *wallet*. Che sia online, in locale sul proprio PC oppure un ibrido, il sistema tradizionale di gestione dei propri bitcoin prevede un portafoglio e una parola chiave che ne protegga i segreti. Segreti che sono, in realtà, le chiavi private corrispondenti agli indirizzi sui quali sono stati riversati i propri bitcoin.

Questo aspetto ci fa capire che la sicurezza del sistema coinvolge la riservatezza delle chiavi private (o del wallet se sono in esso custodite) e l'integrità del sistema stesso, dal punto di vista matematico. Il sistema Bitcoin si basa sul principio delle chiavi private e pubbliche e della firma elettronica, in particolare fa uso dell'algoritmo ECDSA, una variante dell'algoritmo DSA basato sulle curve ellittiche. Matematicamente, i principi fondamentali sono considerati sicuri e nessuno è ancora riuscito a violare l'algoritmo, se ben utilizzato, quindi non ci concentreremo in questa sede sulla questione matematica pura, ma sulle implicazioni che ha poi sulla sicurezza delle chiavi e dei wallet.

Per ogni indirizzo Bitcoin esiste una chiave privata che, se custodita al sicuro, protegge i bitcoin contenuti e ne impedisce il trasferimento da parte di terzi. La chiave privata non è altro che un numero di 256 bit, che può essere rappresentato in diversi formati: la chiave "*5K9kuq6RmRJoxGdLrmf37LNEcEf1MjUacvbC56bzWjzQYo1se11*" per esempio è relativa all'indirizzo Bitcoin mostrato nel primo paragrafo e tramite essa è possibile controllare i fondi ivi presenti. Per chi è curioso di come sia stata generata, la chiave dell'esempio deriva dalla parola "clusit" elaborata tramite il meccanismo dei cosiddetti *brain wallet*: metodi comodi per ricordare a memoria la propria chiave, vivamente sconsigliati perché la rendono debole quanto la frase scelta come riferimento mnemonico.

Chi desidera utilizzare bitcoin può scegliere se installare un client in locale oppure avvalersi di servizi web. Nel primo caso la sicurezza del proprio patrimonio è garantita dalla riservatezza della parola chiave che protegge il proprio wallet, oltre che dall'integrità del proprio PC. Che si tratti di client "pesanti" (che scaricano in locale tutta la *blockchain* che a oggi occupa quasi 40 GB) o "leggeri" (che utilizzano servizi web per verificare le transazioni senza bisogno di avere copia della *blockchain*) l'utente deve essere consapevole del fatto che la password del suo wallet protegge tutti i suoi bitcoin. Non è un caso che mentre nel 2013 si è vista – come riportato dal Rapporto Clusit 2014 – l'ascesa dei trojan che utilizzavano risorse delle vittime per minare bitcoin, nel 2014 ci sia stata la svolta dei malware che invece rubano le credenziali dei wallet, cosa ben più redditizia. Trojan come "CoinThief" o "Pony" hanno infettato migliaia di vittime rubando le credenziali per accedere ai loro wallet su client locali ma anche su servizi web come BlockChain.info o BTC-E. Una nota di colore: anche modificando la password del proprio wallet, non si può impedire gli effetti di un'infezione che ne abbia acquisito le chiavi private a meno che non lo si svuoti il prima possibile trasferendo i fondi su un nuovo indirizzo o su un nuovo wallet.

E' evidente che mai come nel mondo Bitcoin, la sicurezza viene riposta nelle mani dell'utente. Abituato a *token* O-Key, autenticazione a due fattori, conferme di bonifico via SMS, fondo interbancario, l'utilizzatore del Bitcoin deve dimenticare queste tutele e imparare a

© Clusit 2015

gestire con cura le proprie credenziali e il proprio computer, la cassaforte dei suoi risparmi. Un'alternativa da considerare sono i wallet online, servizi web che stanno acquisendo sempre di più la forma di banche e tutelano la sicurezza dei fondi a livelli dei *web banking* nostrani. Sistemi come Greenaddress adottano strumenti di verifica dell'utente basati su PIN inviati via SMS o tramite Google Authenticator, oltre che proteggere gli indirizzi tramite *multisig*, cioè firme congiunte che fanno sì che il gestore non sia in grado di utilizzare le criptovalute senza l'intervento dell'utente. Inoltre, diversi servizi online permettono all'utente di scaricare in locale il proprio wallet, così da ridurre il rischio di perdita del proprio capitale, riconducendo però nuovamente il tutto alla sicurezza locale, sempre che il gestore non finisca comunque per chiudere.
Basti pensare all'exchange MTGox, nato nel 2010 e cresciuto al punto da gestire nel 2013 oltre il 70% delle transazioni in bitcoin. A febbraio del 2014 la società, con sede a Tokyo, ha dichiarato bancarotta informando i clienti della scomparsa di 750.000 dei loro bitcoin, per un controvalore di 450 milioni di euro di allora. MTGox non è l'unico exchange ad aver chiuso i battenti lasciando a piedi i clienti: di recente BitStamp ha subito la perdita di oltre 18.000 bitcoin ed è noto come anche i mercati di scambio nel *dark web* – si pensi al famoso Sheep Marketplace – abbiano avuto guai simili in passato.
Questi avvenimenti evidenziano i rischi che corrono tutt'oggi gli utenti meno tecnologicamente avanzati, coloro che non sanno nulla di sistemi di *cold storage* o di *multi signature*, che aprono allegati di email ricevute da sconosciuti, cliccano su qualunque banner con su scritto "download" e non installano antivirus né antispyware.

I bitcoin e il cybercrime: ransomware, Deep Web e Silk Road

La stampa tende sempre più spesso a identificare il mondo dei bitcoin con quello del cybercrime e del deep/dark web, in quanto nel 2014 i bitcoin sono stati utilizzati in diversi episodi criminosi che li hanno portati a conoscenza del grande pubblico sotto un'accezione ben poco positiva. Tuttavia, va ricordato che quasi tutti i mezzi di pagamento sono uno strumento fisiologico per la commissione di illeciti e quindi è sicuramente da evitare una demonizzazione aprioristica dei bitcoin che, spesso, vengono considerati la causa del comportamento illecito.
Il motivo principale di tali critiche è che il Bitcoin è un sistema che garantisce un sostanziale anonimato circa i proprietari dei wallet/indirizzi e gli autori delle transazioni. Altro elemento a favore di un utilizzo "alternativo" è il fatto che – a differenza dei conti bancari – un indirizzo Bitcoin non può essere sequestrato, pignorato o chiuso, a patto ovviamente che la chiave privata sia al sicuro. Se aggiungiamo che con i bitcoin è possibile ripulire il denaro in modo efficiente, economico e sicuro e capiamo perché i criminali amino particolarmente le criptovalute. Non parliamo soltanto dei servizi di *money laundering* presenti nel deep web o di siti di gioco come il noto *SatoshiDice*, ma anche di funzioni offerte direttamente dagli exchange, alla luce del sole. Chiunque può ad esempio aprire un wallet su Blockchain.info e osservare come nell'area dedicata al trasferimento di bitcoin è presente un'opzione chiamata *shared coin*. Nata con il nome di *coinjoin*, questa modalità di trasferimento permette

– in cambio di una piccola commissione aggiuntiva – di mescolare ripetutamente la propria transazione con quella di altri utenti facendo così perdere le tracce della valuta anche a un'attenta *taint analysis*, cioé l'analisi di correlazione tra indirizzi Bitcoin.
A proposito di correlazione, il 2014 ha visto la pubblicazione di articoli accademici che sostengono che l'anonimato dei client Bitcoin può facilmente essere messo a rischio con alcuni accorgimenti. Biryukov parla in un suo paper di come sia in grado di deanonimizzare dal 60% (su rete di test) all'11% (sulla rete reale) dei client, a patto di isolare la rete Bitcoin dalla rete Tor con un espediente. Sempre Biryukov arriva a sconsigliare, in un altro scritto, di utilizzare la rete anonima Tor per gestire i propri indirizzi bitcoin ed eseguire transazioni, paventando la possibilità di attacchi di tipo *man-in-the-middle* oltre che di *fingerprinting* per riconoscere i client nel momento in cui dovessero uscire dalla rete Tor.
Riteniamo che queste considerazioni – per quanto condivisibili dal punto di vista puramente teorico e probabilmente motivate anche dal fatto che in qualche modo possano giovare all'integrità del sistema Bitcoin scoraggiando potenziali malintenzionati – siano ancora inapplicabili al mondo reale. La realtà è che i *wallet* online come Blockchain.info forniscono persino indirizzi *onion* per potervi accedere in totale sicurezza e anonimato dietro rete Tor, senza richiedere un indirizzo email di riferimento (che comunque servirebbe a poco) e permettendo di eseguire transazioni che rendono difficile la tracciabilità. Senza considerare i cosiddetti *mixing services*, pensati proprio per ripulire il denaro mescolando i bitcoin e retituendone persino di nuovi (appena minati) in cambio di una somma aggiuntiva. Attenzione soltanto ai siti di *money laundering* falsi, in genere pubblicati su indirizzi onion della rete Tor, che fingendosi servizi veri incassano i bitcoin senza restituirli. Per i tradizionalisti poi, come nella vita reale ci sono sempre i siti di gioco online, che permettono di caricare un credito in bitcoin, giocare e riversare la somma vinta o ciò che ne è rimasto su un conto esterno. Chi ha dimestichezza può tentare un'analisi di correlazione sull'indirizzo bitcoin di esempio riportato sopra, constatando come sia impossibile rilevare la provenienza e la destinazione del centibitcoin ivi contenuto.
Per una casistica di utilizzo illecito dei bitcoin basti pensare alle diverse ondate di ransomware come "CryptoLocker", "TorrentLocker" o "CTB-Locker", i noti trojan che infettano il PC delle vittime e cifrano tutti i loro dati, chiedendo poi un riscatto. Il bottino viene richiesto in bitcoin e il motivo dovrebbe ormai essere chiaro. Quando a ottobre 2014 il trojan si è diffuso nelle reti di numerosi Uffici Comunali italiani, in poche settimane i criminali hanno racimolato centinaia di migliaia di dollari, solo in Italia e solo nella decina di giorni successivi all'infezione. Ciò che ha fatto scalpore in questo caso è il fatto che i dipendenti comunali si sono ritrovati a dover pagare il riscatto raccogliendo il denaro tramite colletta, non trovando il modo di giustificare a bilancio la somma in bitcoin necessaria. A fine 2014 il malware si è evoluto dedicando per ogni vittima un indirizzo bitcoin unico su cui eseguire il versamento, così da impedire analisi sugli indirizzi e quindi valutazioni sull'entità del fenomeno. Si consideri, inoltre, che in questi casi non sono presenti, a differenza del tradizionale circuito bancario, diritti al rimborso o altre tutele per gli utenti danneggiati.
E' poi noto come, nel deep e dark web, la moneta di scambio si sia consolidata nel bitcoin,

per le proprietà sopra riportate. Servizi che consentivano il traffico di stupefacenti come Silk Road e i vari marketplace di oggetti o servizi di dubbia legalità ospitati dietro la rete anonima Tor si basano sullo scambio di valuta in bitcoin o comunque di criptovalute alternative, che garantiscono anonimato a chi spende e a chi incassa.
Nonostante le proprietà di anonimato, nel noto caso giudiziario che ha visto la chiusura del sito Silk Road grazie a una lunga e articolata indagine compiuta dall'FBI, è stato possibile effettuare delle interessanti analisi sul patrimonio di Ross Ulbricht, uno dei presunti fondatori del servizio per lo spaccio di stupefacenti nel deep web.
Durante il processo che è iniziato nel 2014, Nicholas Weaver, ricercatore di sicurezza per l'International Computer Science Institute di Berkeley, è riuscito a individuare come Ulbricht abbia ricevuto circa 29 mila bitcoin (del valore attuale di circa 6 milioni di Euro) da Silk Road tra il 5 luglio ed il 21 agosto 2013.
La semplicità deduttiva con cui questo ricercatore ha identificato la provenienza del denaro fa comprendere come la preparazione tecnica e l'intuito investigativo siano gli unici strumenti in grado di superare l'ostacolo dell'anonimato.

La regolamentazione giuridica dei bitcoin

I bitcoin sia a livello internazionale che nazionale non sono ancora stati oggetto di una regolamentazione giuridica, fatto salvo per la Germania che li ha ufficialmente riconosciuti come "unità di scambio" per le transazioni private. Nel resto del mondo le criptovalute, salvo qualche eccezione (ad esempio, Cina, Thailandia e Corea del Sud), sono generamente tollerate in attesa di una disciplina specifica nel settore.
Al di là dei profili fiscali già analizzati, un altro tema sicuramente importante che i legislatori di tutto il mondo dovranno affrontare nei prossimi anni è quello connesso alle caratteristiche di immaterialità e anonimato dei bitcoin.
L'immaterialità delle criptovalute fa sorgere immediatamente una riflessione sulla configurabilità del reato di furto di bitcoin, in quanto esso implica la presenza di una "cosa mobile altrui" tra cui non può essere ricompresa una moneta virtuale.
Tuttavia, è importante rilevare che il furto di criptovaluta comporta la sottrazione della chiave privata al fine di disporre della stessa per iscrivere la transazione nella blockchain. Di conseguenza sono ipotizzabili diverse fattispecie di reato che possono comprendere alternativamente o congiuntamente la truffa (640 c.p.), la frode informatica (640-ter c.p.) e il reato di accesso abusivo a sistema telematico (615-bis c.p.). In sostanza, l'ordinamento giuridico esistente, come è già accaduto nel caso del phishing, è in grado di sopperire al problema generato dalla natura immateriale dei bitcoin attraverso la creazione di una fattispecie complessa modulabile rispetto al caso concreto..
La caratteristica dell'anominato dei bitcoin può essere di estrema utilità per la commissione del reato di riciclaggio. A questa caratteristica si unisce il fatto che la criptovaluta consente un trasferimento immediato in diverse giurisdizioni.
Tuttavia, come osservato da alcuni autori (Capaccioli), è importante chiarire che l'anonimato non è una caratteristica intrinseca dei bitcoin, in quanto la blockchain consente di

tracciare pubblicamente tutti i passaggi di denaro effettuati. Tuttavia, lo scambio di bitcoin avviene molto spesso attraverso l'utilizzo di Tor che, come chiarito in precedenza, consente di proteggere l'identità degli utenti. Questo chiarimento è importante per evitare facili demonizzazioni verso uno strumento che, ove efficacemete regolamentato, ha di per sé delle caratteristiche tecniche di particolare utilità per lo scambio di beni e servizi in un mondo sempre più globalizzato.

Da un punto di vista normativo, a livello nazionale, il d.lgs. 231/07 impone obblighi in materia di antiriclaggio a determinate categorie di soggetti individuate dagli art. 10 e seguenti della norma. Tali obblighi ricomprendono la necessità di effettuare controlli che permettano la piena conoscenza del cliente, la tracciabilità delle transazioni finanziarie e l'individuazione delle operazioni sospette di riciclaggio. Allo stato nessuno dei soggetti che operano nel settore delle criptovalute rientra in modo evidente nelle categorie previste dal d.lgs. 231/07. Di conseguenza, è chiaro che, in assenza di una normativa ad hoc, il fenomeno del riciclaggio attraverso l'utilizzo delle critpovalute sta rapidamente proliferando attraverso l'utilizzo di casinò on line o altre forme di offuscamento del denaro proveniente da attività illecita.

Il furto di bitcoin e il reato di riciclaggio rappresentanto indubbiamente due profili patologici connessi alla crescita esponenziale dei bitcoin e di tutte le altre critpovalute. Tuttavia, il caso Silk Road ha dimostrato come le tecniche investigative più evolute supportate dal costante rispetto delle best practices della digital forensics sono e saranno sempre più in grado di contrastare anche queste nuove forme di criminalità.

Dall'altro lato, è opportuno osservare che fin dal 2012 la Banca Centrale Europea ha espresso preoccupazione per il fenomeno delle monete virtuali in quanto possono rappresenta una "sfida" per le autorità pubbliche dato lo stato di incertezza legale del fenomeno che può essere sfruttato per compiere un'attività illecita.

A distanza di tre anni, lo scenario non è molto differente, mentre il fenomeno della criptovaluta ha avuto indubitabilmente una crescita esponenziale. La speranza è che, dopo tre anni di attesa, sia arrivato il momento di pensare seriamente ad una regolamentazione giuridica che sia in grado di non frenare la crescita del fenomeno bitocoin, ma che, allo stesso tempo, ne limiti il potenziale d'utilizzo illecito.

© Clusit 2015

Doppia autenticazione per l'accesso ai servizi di posta elettronica

A cura di Manuela Santini

Introduzione

"Vediamo sempre più che i grossi operatori di Internet a livello mondiale, quali Google, Facebook, Apple e Microsoft, offrono servizi di posta con doppia autenticazione. Dal punto di vista tecnologico non c'è nulla di veramente nuovo, dato che è in definitiva quanto hanno fatto le banche oltre dieci anni fa per l'accesso ai sistemi di home-banking, ma a livello di comportamento consapevole da parte degli utenti è una vera rivoluzione, che può contribuire ad innalzare in modo significativo il livello di sicurezza delle comunicazioni online. Per approfondire il discorso abbiamo chiesto ai responsabili della sicurezza di Italiaonline, prima internet company italiana, di raccontarci l'evoluzione della sicurezza nei servizi di posta elettronica: il passato, la situazione attuale e le tendenze per il futuro. Nel focus on ci illustreranno quindi i vantaggi e le eventuali criticità della doppia autenticazione. Abbiamo infine chiesto di raccontarci la loro esperienza nell'implementazione di un tale servizio a favore di una massa così rilevante di utenti."

(P. Giudice, segretario generale Clusit)

Dopo la navigazione web, la posta elettronica è una delle applicazioni Internet più conosciute e utilizzate. Nata nel 1971, per scambiare messaggi fra le varie università, si è in seguito evoluta fino a diventare uno strumento per tutti.

Nel 1994, nasce Libero.it, col nome Italia On Line (chiamato anche "iOL", prima comparsa del nome dell'attuale gruppo), come sito di assistenza agli utenti nella navigazione internet (allora a pagamento) e nella configurazione della posta elettronica.

Nel 1995 nasce Virgilio.it, primo portale italiano, motore di ricerca e web directory che si è via via evoluto come portale generalista che tratta contenuti di vario genere, offrendo ai propri utenti servizi di webmail, search, chat e community.

Nel 2013, dalla fusione delle società proprietarie dei due portali nasce Italiaonline, il più grande gruppo digitale italiano, prima internet company nazionale e terzo player del mercato web in Italia dopo Google e Facebook.

Oggi la piattaforma webmail che fa capo a Italiaonline (@iol.it, @libero.it, @virgilio.it, @giallo.it, @blu.it, @inwind.it) conta più di 11 milioni di caselle di posta attive.

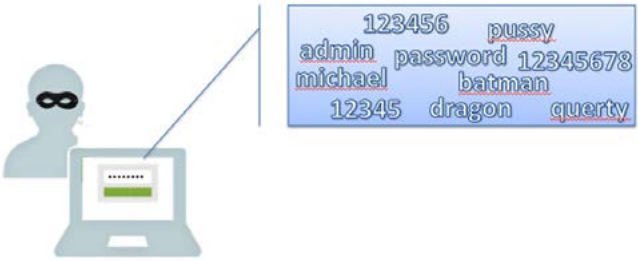
Ogni settimana sui server di Italiaonline vengono scambiati 700 milioni di messaggi, per un totale di 3 miliardi ogni mese.

Alla piattaforma di webmail, Italiaonline ha aggiunto il servizio Libero PEC (Posta Elettronica Certificata). Con la vigente normativa (DPR 11 Febbraio 2005 n.68) la PEC ha assunto valore legale ed è quindi equiparata alla raccomandata con ricevuta di ritorno.

Ad oggi, la posta elettronica rappresenta quindi la controparte digitale della posta ordinaria e cartacea.

A differenza della posta cartacea, in entrambe le versioni (standard e PEC), la consegna del messaggio, avviene normalmente con un ritardo di pochi secondi/minuti, anche se alcune eccezioni possono ritardare la consegna di qualche ora.
Con la Legge 23 dicembre 1993, n. 547 (G. U. n. 305 del 30 dicembre 1993), il legislatore ha esteso il concetto di "corrispondenza" anche a quella informatica o telematica estendendolo cioè ad ogni forma di comunicazione a distanza imponendo la medesima tutela della posta ordinaria a quella telematica.
Sempre nella medesima legge il legislatore ha voluto anche definire il concetto di "domicilio informatico" in quanto i sistemi informatici e telematici costituiscono un'espansione virtuale della propria area personale e riservata che, a differenza del domicilio fisico, non ha confini ben visibili ma sono delineati da una serie di dati/informazioni che permettono di creare all'interno di un unico grande spazio tanti spazi privati.
Non è solo la legislazione che ha dovuto evolversi per far fronte a questo nuovo modo di comunicare ma anche i fornitori di servizi di posta elettronica hanno dovuto imparare ad adeguarsi al sempre più crescente utilizzo di tali sistemi di comunicazione.
Se la posta elettronica e lo spazio ove essa è contenuta è così importante per la legislazione, come può non esserlo per chi fa di quelle applicazioni il fattore abilitante del proprio business? Sin dalle prime versioni si è mostrato indispensabile proteggere tali spazi con una seppur minima misura di sicurezza che potesse mitigare i rischi di un accesso non autorizzato al proprio spazio web.
L'abitudinarietà degli utenti, l'aumento delle applicazioni e la continua innovazione tecnologica (e con essa delle tecniche di attacco dei cybercriminali) combinata all'esigenza dei provider di e-mail di rendere semplice ed intuitivo l'utilizzo dei propri servizi, in modo tale da incrementare reach ed audience , ha provocato in buona parte degli utenti fruitori di questi servizi internet una scarsa consapevolezza sull'importanza di proteggere adeguatamente il proprio domicilio informatico, con azioni mirate consapevoli (come cambiare frequentemente la password od usare una password robusta), che invece sono spesso considerate una inutile perdita di tempo. Da ciò negli anni è derivato, grazie anche all'affinamento delle tecniche cybercriminali di hacking e cracking, che un elevato numero di informazioni facenti parte del proprio domicilio informatico possano essere rese disponibili, a causa di condotte sprovvedute degli utenti, per intenti cybercriminali. Anche i meno esperti, facendo qualche ricerca in internet possono potenzialmente creare il loro "dizionario" di parole chiave da poter usare per entrare in possesso di un account.

© Clusit 2015



Quindi, come i provider di posta elettronica possono aiutare gli utenti a proteggersi?

Dal punto di vista dei fornitori di servizi la prima cosa da identificare, nel contesto in esame, è un possibile scenario di attacco al fine di individuare i parametri fondamentali per una corretta analisi del rischio:

- identificazione delle minacce/vulnerabilità;
- tipologia di attaccante (interno e/o esterno);
- identificazione degli asset interessati e dunque dell'infrastruttura tecnologica del servizio e delle relazioni con altri servizi interni;
- identificazione del livello di sicurezza "intrinseco" degli ambienti costituenti lo scenario in esame.

Lo scenario sarà quindi simile a quello in Fig. 2

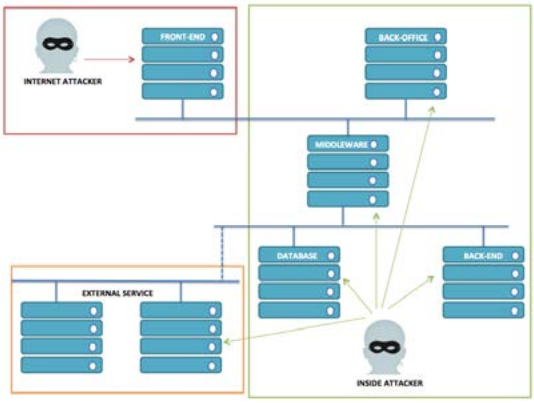


Fig.2

Rispetto allo scenario in Fig. 2 l'attività di analisi deve essere svolta sia dal punto di vista dell'attaccante esterno, agendo esclusivamente sul sito "pubblico", sia sulle componenti di amministrazione interne sia sulle interazioni con altri servizi del service provider.

Per proteggersi da eventuali attacchi provenienti dall'interno della propria rete è necessario implementare misure tecniche ed organizzative adeguate al rischio esistente al fine di garantire la protezione dei dati archiviati o trasmessi da una serie di eventi quali distruzione, perdita, alterazione (anche accidentali), archiviazione, trattamento, accesso o divulgazione non autorizzati o illeciti e quindi è necessaria l'attuazione di una "politica di sicurezza".
Analogamente a quanto fatto per proteggersi dagli attacchi interni è possibile proteggersi mediante le medesime misure anche da attacchi esterni volti ad individuare i codici di accesso.
Perché quindi non permettere agli utenti di:

- visualizzare gli accessi al proprio spazio web
- accedere tramite "Strong Authentication
- fornire dei "profili di autorizzazione" basati sui dispositivi utilizzati
- attivare degli alert a fronte di determinati eventi?

Libero Mail ha iniziato questo percorso diversi anni fa, infatti funzioni quali "dettaglio degli ultimi accessi", scadenza password dopo 180 giorni, limitazioni sull'utilizzo di vecchie password, mail secondaria/sms per recuperare la password, inserimento di un codice di verifica (CAPTCHA) alla login, sono solo alcune delle misure di sicurezza messe a disposizione per i suoi utenti.
Recentemente Libero Mail ha implementato la funzionalità di "2-step authentication" per proteggere ulteriormente i propri account attraverso un doppio controllo: **la password della propria casella di posta** e **un codice di verifica inviato sul cellulare**. **Questo nuovo servizio, reso disponibile su base opzionale a tutti gli utenti di Libero Mail, ha preso il nome di "Password Sicura".**

Fig.3

Le banche utilizzano da anni questo meccanismo fornendo ai propri utenti dei meccanismi per la generazione di "One Time Password".
Ma quante operazioni si fanno in banca? Quante invece sul proprio spazio web o sulla propria casella di posta?

Per un provider di posta elettronica velocità ed affidabilità sono fattori chiave per il successo del proprio sistema di posta elettronica così come lo è la sicurezza.
La "2-step authentication" si basa su un doppio controllo al momento dell'accesso alla mail: alla password che l'utente usa abitualmente viene associato un "codice di verifica" generato dal sistema e inviato all'utente tramite un altro canale (ad es. SMS sul cellulare). La dinamica è ben sintetizzata dal concetto: "qualcosa che so, qualcosa che ho".
Per non penalizzare la facilità di accesso in termini di user experience il sistema consente all'utente di "validare" dopo il primo utilizzo il computer e i dispositivi che usa abitualmente e fare in modo che non gli venga più richiesto di inserire i codici di verifica.
Il secondo fattore di autenticazione, quello che rappresenta il "qualcosa che ho" è un elemento di identificazione che può essere un token o un codice spedito ad una mail secondaria dell'utente o sul suo telefonino (tramite SMS) oppure qualcosa che l'utente si è precedentemente salvato/stampato.
Libero Mail implementa la "2-step authentication" richiedendo di inserire, oltre alla password, un codice numerico di verifica che viene inviato sul telefono dell'utente via SMS, qualora lo stesso acceda al proprio account da un dispositivo o da una posizione sconosciuti.

Fig.4

In questo modo se un malintenzionato entrato indebitamente in possesso della password corretta cercasse di accedere alla casella di posta sarebbe impossibilitato a farlo perché privo del necessario codice di verifica.
In Fig. 5 è rappresentato un macro sequence diagram di come Libero Mail ha progettato il proprio sistema di "2-step authentication".

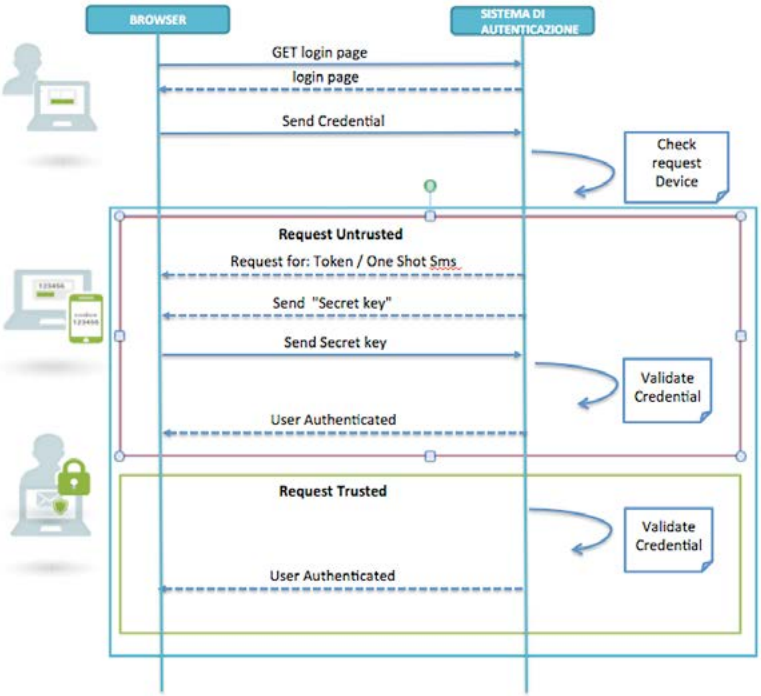


Fig. 5

Ogni richiesta proveniente da un sistema client/web è sempre correlata da informazioni nascoste che permettono di identificare il dispositivo chiamante. Queste informazioni, nominate fingerprint, sono utilizzate per identificare la richiesta come "trusted" o "untrusted". Questi dati vengono collezionati e spediti automaticamente contestualmente alla richiesta di autenticazione. Il loro utilizzo permette di identificare il device anche nelle successive richieste.

Libero Mail ha posto molta attenzione nella gestione dei codici di verifica per i seguenti motivi:

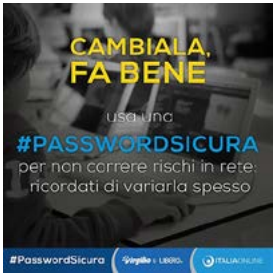
- L'identificazione del codice di verifica è potenzialmente possibile anche se molto oneroso per un attaccante, sia in termini di risorse informatiche che di effort.
- Un codice di verifica solitamente è deterministico, cioè è spesso formato da sempre lo stesso numero di caratteri, da una precisa sequenza (solo numeri, solo lettere, etc.), ed i sistemi che lo devono recepire spesso permettono un numero elevato di tentativi, permettendo di fatto l'utilizzo di programmi per l'identificazione del codice; è stato perciò importante costruire un'architettura che permettesse un numero massimo di tentativi e che durante gli stessi proponesse un codice captcha (test fatto di una o più domande e risposte per determinare se l'utente sia un umano) che diminuisca le possibilità di automazione della ricerca del codice segreto.

© Clusit 2015

- Le configurazioni dei dispositivi di "load balancer" così come la gestione delle sessioni rivestono un punto molto importante nella costruzione di un sistema di "2-step authentication". Nel caso in cui il numero di richieste arrivasse a rallentare i sistemi, è importante che la sicurezza prenda il sopravvento rispetto alle "page view". L'applicazione deve prevedere, quindi, adeguati sistemi di gestione degli errori, al fine di impedire accessi non "certificati".

Indispensabile è stato anche porre molta attenzione su come si è sviluppato il sistema che permette l'attivazione e la gestione della funzionalità di "2-step athentication". Se il codice di sicurezza utilizzato è sicuro (e l'unico codice veramente sicuro è quello generato dal nostro corpo, unico ed irripetibile) ma non lo è il sistema che utilizza, vi è comunque una possibilità che qualcuno possa entrare in possesso delle informazioni private.
Libero Mail per garantire un adeguato livello di sicurezza del servizio "2-step authentication" esegue ciclicamente attività di analisi del codice sorgente "secure code review", Security Assessment quali Vulnerability Assessment, Penetration Test ed Ethical Hacking che hanno permesso di escludere diverse vulnerabilità quali ad esempio Cross-Site Request Forgery (CSRF) che forza utenze già autenticate ad effettuare operazioni arbitrarie (a loro insaputa) all'interno del portale (disabilitare l'autenticazione a due fattori, modificare il numero di cellulare per l'invio del codice di verifica, etc.).

Nonostante i TOP player di mercato abbiano adottato la "2-step authentication" e l'abbiano resa disponibile con adozione opzionale, ad oggi il suo utilizzo è poco diffuso, a causa dell'abitudinarietà degli utenti, di una certa avversione alla novità ed inoltre perché è una misura di protezione da molti percepita ad uso "bancario".



E proprio per contrastare l'avversione degli utenti alle novità, Libero Mail, come molti altri social, sta implementando dei sistemi per agevolare l'utilizzo della "2-step authentication" semplificando anche le modalità di recupero dei codici di verifica (ad esempio tramite l'utilizzo di app per la generazione dei codici) e la gestione dello smarrimento dei dispositivi mobili a cui viene inviato l'sms che li contiene.
In attesa che l'utilizzo di queste nuove misure di sicurezza vengano sempre più utilizzate, Italionline tramite apposite campagne comunicative sui propri siti e sui social media continua a raccomandare agli utenti di utilizzare password complesse e non banali e di sfruttare la protezione offerta dalla "2-step authentication".

© Clusit 2015

Lo stato della sicurezza dei siti web della pubblica amministrazione.

A cura di Michele Iaselli, Antonio Parata e Sylvio Verrecchia

Normativa dei siti web della P.A.

La diffusione di Internet nel settore della P.A. porta un elemento nuovo e per certi versi rivoluzionario nel rapporto delle stesse con i cittadini. Al fine di consentire un migliore sfruttamento del Web da parte della Pubblica Amministrazione è stato necessario promuovere ed introdurre forme nuove di utilizzo allo scopo di realizzare una migliore soddisfazione dei cittadini e delle imprese.

Nel 2002 il Ministero per l'Innovazione e le Tecnologie con il Ministro Stanca ha acquisito un nuovo dominio di secondo livello "gov.it", da intendersi come suffisso di tutti quei siti dell'amministrazione centrale e periferica che possiedano determinati requisiti di qualità e sicurezza. La direttiva del Presidente del Consiglio dei Ministri, datata 30 maggio 2002, in linea con quanto fissato dalla circolare del 13 marzo 2001 n. 3, ha definito i criteri di accessibilità, usabilità ed efficacia ai quali i siti della P.A. devono attenersi per conseguire il nuovo suffisso e che sono richiamati anche nella disposizione in esame.

Secondo la direttiva, ciascuna amministrazione doveva individuare strutture di coordinamento esistenti o istituire specifiche strutture o gruppi di lavoro cui affidare l'attuazione della normativa inerente la conoscenza e l'uso del dominio internet "gov.it" e l'efficace interazione del portale nazionale "italia.gov.it" con le pubbliche amministrazioni e le loro diramazioni territoriali.

L'obiettivo era e continua ad essere quello di avere veri e propri portali della pubblica amministrazione utilizzabili per consultare leggi e decreti, reperire moduli e certificati, ottenere le autorizzazioni richieste alle imprese, cercare di mettere insieme domanda e offerta di lavoro, fornire veri e propri servizi.

Stante le difficoltà e l'evidente distanza dai risultati, il 9 Marzo 2010 il Ministero per la Pubblica Amministrazione e l'Innovazione ha pubblicato le "Linee guida per i siti web della PA[1], come previste dalla Direttiva 8/2009[2]: il documento (più volte rinnovato negli anni successivi) ha l'obiettivo di indicare gli strumenti da usare per il miglioramento della qualità dei siti web pubblici, per la loro gestione e l'aggiornamento dei contenuti. Uno spazio di notevole rilevanza viene destinato al requisito della sicurezza, che definisce le caratteristiche idonee che i siti devono possedere per fornire transazioni e dati affidabili, gestiti con adeguati livelli di sicurezza. Ciò si accompagna ad altri aspetti delle Linee Guida che hanno certamente sofferto di influenza nelle scelte degli strumenti, delle regole e delle modalità di comunicazione adottate:

[1] http://www.funzionepubblica.gov.it/media/835828/linee_guida_siti_web_delle_pa_2011.pdf

[2] http://www.agid.gov.it/agenda-digitale/pubblica-amministrazione/registrazione-al-dominio-govit

- l'eventuale rilascio attraverso licenze d'uso che ne favoriscano la diffusione verso cittadini e incoraggino il loro riutilizzo presso le imprese;
- l'utilizzo di Internet come canale di comunicazione primario, in quanto il più accessibile e meno oneroso, attraverso il quale diffondere i flussi informativi, nel rispetto però di quanto prescritto dalla deliberazione n. 13 del 1 marzo 2007 del Garante per la Protezione dei dati personali e dalla Direttiva n. 2/2009 del Ministero per la Pubblica Amministrazione;
- l'utilizzo di formati aperti, standardizzati e interoperabili.

In tale sede appare anche opportuno un richiamo al Decreto legislativo 30 giugno 2003, n. 196 "Codice in materia di protezione dei dati personali", in particolare per quanto concerne le misure minime ed idonee di sicurezza agli artt. 31 e seguenti.
Con il Codice dell'Amministrazione Digitale (CAD), ancor prima di regolamentare i siti web, agli art. 50-bis e 51 il legislatore si è occupato anche della sicurezza dei dati nell'ambito dei sistemi e delle infrastrutture della P.A., auspicando l'intervento di ulteriori regole tecniche che, in coerenza con la disciplina in materia di tutela della privacy, introducano elementi utili per riconoscere l'esattezza, la disponibilità, l'integrità e per verificare l'accessibilità e la riservatezza dei dati.
Di fondamentale importanza per i siti della P.A. è anche l'art. 54 del Codice dell'Amministrazione Digitale, poi sostituito dall' art. 52, comma 3, D.Lgs. 14 marzo 2013, n. 33, che ha introdotto per la prima volta nel nostro ordinamento in termini generali gli obblighi di pubblicità, trasparenza e diffusione di informazioni da parte delle pubbliche amministrazioni.

Le informazioni e i documenti oggetto di pubblicazione obbligatoria ai sensi della normativa in argomento sono piuttosto numerosi ed essendo generati e gestiti dalla Pubblica Amministrazione devono essere tutelati secondo i principi di disponibilità, affidabilità, integrità e sicurezza. I siti devono quindi possedere caratteristiche idonee a fornire transazioni e dati affidabili e gestiti con adeguati livelli di protezione.

Analisi e valutazioni tecniche

Il presente studio offre una panoramica generale delle caratteristiche realizzative dei siti web delle Pubbliche Amministrazioni, per trarre una serie di spunti di analisi in merito ai possibili accorgimenti che possono essere adottati per assicurare un adeguato livello di sicurezza . I dati[3] sono stati ottenuti da fonti pubbliche (esempio: ricerche sul web, Open Data[4]) e dal sito Ancitel[5].
Al fine di poter fornire una ricerca coerente e supportata da dati concreti,è stata effettuata l'analisi di 8414 siti web della Pubblica Amministrazione, cosi suddivisi:

- 218 Enti Governativi (Governo, Ministeri, Agenzie, Istituzioni e Consorzi vari);
- 20 Amministrazioni Regionali;

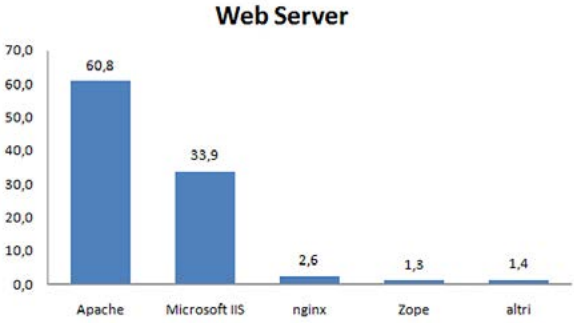
[3] Dati utilizzati con licenza CC BY-SA 3.0, scaricati da http://siamogeek.com/statistiche-web-pa/

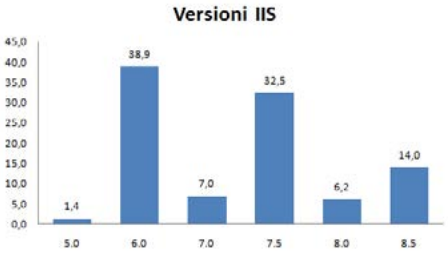
[4] http://www.lineaamica.gov.it/opendata

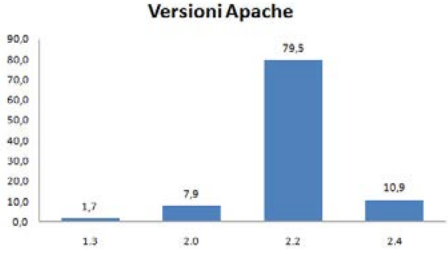
[5] http://www.ancitel.it/link/siti/index.cfm

- 109 Amministrazioni Provinciali;
- 8067 Enti Locali (tutti i Comuni d'Italia e Consorzi vari).

Un sito risiede su un server web ,il quale è fondamentale che sia ben configurato ed aggiornato in modo da garantirne un adeguato livello di sicurezza, tenuto conto che un server vulnerabile può compromettere numerosi siti web in esso contenuto.
I server web della nostra Pubblica Amministrazione sono configurati nella maggioranza con Apache (60,8%) seguito da Microsoft IIS (33,9%). Nell'analizzare le rispettive versioni si evince che molte amministrazioni utilizzano ancora versioni obsolete, come ad esempio il 38,9% utilizzano la versione IIS 6.0 e solo il 14% si sono aggiornati alla versione IIS 8.5. L'utilizzo di versioni obsolete potrebbero in alcuni casi esporre i server a rischi di intrusioni con relative perdita di dati, per cui risulta importante tenere conto del ciclo di vita del prodotto in modo da essere supportati ai service pack e al rilascio di nuove patch[6].







[6] http://support.microsoft.com/lifecycle?sort=PN&qid=&alpha=Microsoft+Windows+Server+2003&Filter=FilterNO

Un sito web può essere realizzato con diversi linguaggi di programmazione, ad esempio in HTML, in PHP o in ASP e necessita obbligatoriamente di conoscenze specifiche. Oggi, rispetto al passato, i siti sono dinamici e contengono grandi quantità di informazioni, per cui spesso si utilizzano per la loro gestione i CMS.
Il CMS (Content Management System)[7] è un sistema di gestione dei contenuti web, ovvero è uno strumento software, installato su un server web, il cui compito è facilitare l'inserimento, la modifica e la cancellazione dei contenuti. Con esso è possibile creare ed aggiornare un sito web senza necessità di scrivere una riga di codice, senza conoscere alcun linguaggio di programmazione o conoscere come amministrare un database.

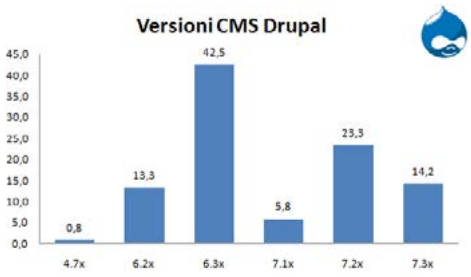
La ricerca è stata condotta tramite un rilevamento statistico di informazioni pubblicamente disponibili, relative al tipo di CMS ed al numero di versione. Ulteriori valutazioni, come la presenza di misure di sicurezza ulteriori, lo stato di aggiornamento delle librerie di sistema ed usate dal CMS, non sono nello scope dell'analisi. Lo studio è stato inoltre limitato ai soli CMS Drupal[8], Joomla![9] e Wordpress[10] in quanto i più diffusi.

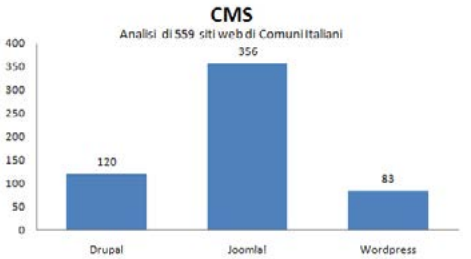
L'analisi ha messo in evidenza che le Pubbliche Amministrazioni sempre più adottano i CMS Open Source in quanto:
1 consentono un notevole risparmio economico;
2 si ha accesso al codice sorgente;
3 possibilità di analizzare il codice (comunità di sviluppatori intenti a migliorare il prodotto);
4 aggiornamenti gratuiti;
5 accesso a componenti, template grafici e plugin reperibili in rete;
6 l'utilizzo di software libero è sostenuto dal D.Lgs 82/2005 Codice dell'Amministrazione Digitale.
7 garanzia di accessibilità (con l'utilizzo di standard aperti);
8 garanzia di usabilità come descritto dalla Legge Stanca;

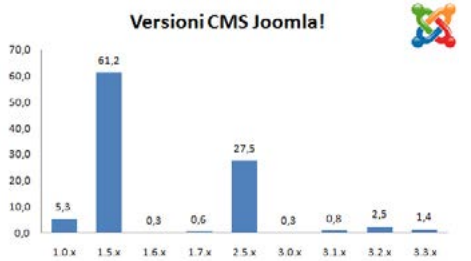
Le informazioni raccolte hanno riguardato la totalità dei siti web dei comuni italiani (dal 1° gennaio 2015 il numero ufficiale dei comuni italiani è pari a 8.048 unità amministrative[11]) e verificato l'appartenenza ai CMS più diffusi, con la relativa versione ed escludendo i siti realizzati con altre applicazioni, abbiamo così classificato 559 Comuni.

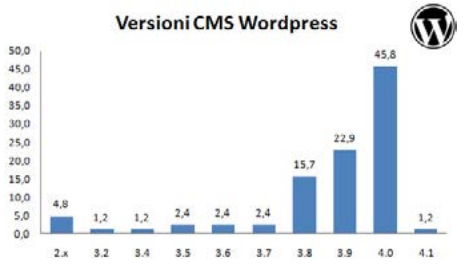
7 http://it.wikipedia.org/wiki/Content_Management_System
8 http://it.wikipedia.org/wiki/Drupal
9 http://it.wikipedia.org/wiki/Joomla!
10 http://it.wikipedia.org/wiki/WordPress
11 Fonte Istat (http://www.istat.it/it/archivio/6789)

© Clusit 2015









Dall'analisi si evidenzia che il CMS Open Source più diffuso nella pubblica amministrazione è Joomla!, seguito a distanza da Drupal e Wordpress.

Relativamente a Joomla! il grafico mostra che più della metà dei siti (61,2%) sono ancora sviluppati con la versione **1.5**. Questa versione è nata nel 2008 e ha conquistato gli utilizzatori di Joomla! grazie al grande numero di template ed estensioni/componenti disponibili ed al lungo periodo di supporto (4 anni) terminato nel Settembre 2012. La versione **2.5** segue con una percentuale del 27,5% ed il suo periodo di supporto è terminato il 31 Dicembre 2014 e a tale data non presenta vulnerabilità note.

La procedura di migrazione dalla 1.5 ad una versione aggiornata non è delle più semplici e questo potrebbe spiegare almeno in parte i molti siti che ancora utilizzano Joomla! 1.5. Ancora un 5,3% di Comuni Italiani utilizzano la versione 1.0 e come evidenziato dalla tabella delle Versioni di Joomla! tutte le vecchie versioni non sono più supportate. Non è stato possibile, in questa analisi, verificare la sussistenza di altre misure di sicurezza messe in atto dalle pubbliche amministrazioni, tuttavia l'assenza di un supporto sulla piattaforma può essere interpretato come un indice di maggiore rischio per i gravi bug di sicurezza che a mano a mano sono stati individuati su tali piattaforme.

Versioni di Joomla

	1.0	1.5	1.6	1.7	2.5	3.0	3.1	3.2	3.3	3.4
Rilasciata nel	Set. 2005	Gen. 2008	Gen. 2011	Lug. 2011	Gen. 2012	Set. 2012	Apr. 2013	Nov. 2013	Apr. 2014	Fine 2014
Supporto ufficiale	✖	✖	✖	✖	✖	✖	✖	✖	✔	-
Termina nel	Lug. 2009	Set. 2012	Ago. 2011	Feb. 2012	Dic. 2014	Mag. 2013	Dic. 2013	Ott. 2014	alla 3.4	alla 3.5
Ultima stabile	1.0.15	1.5.26	1.6.6	1.7.5	2.5.28	3.0.4	3.1.6	3.2.7	**3.3.6**	-
Possibili nuovi aggiornamenti?	✖	✖	✖	✖	✖	✖	✖	✖	✔	-
Presenza Bug di sicurezza noti?	SI	SI	SI	SI	NO	SI	SI	NO	NO	-

Tabella Versioni di Joomla!
http://www.joomla.it/notizie/7564-statistiche-2014-sulla-diffusione-delle-versioni-di-joomla.html

Per le applicazioni web implementate tramite Drupal, esse risultano in maggioranza, ovvero il 42,5%, appartenere alla versione 6.3x, contro il 14,2% appartenente alla 7.3x. Anche in questo caso, ciò rappresenta potenzialmente uno svantaggio, in quanto tale versione si porta dietro un numero di vulnerabilità note non indifferenti.
Da segnalare al contrario che la versione maggiormente installata del CMS Wordpress risulta essere non troppo datata, infatti è la 4.0 mentre l'ultima versione rilasciata al momento della scrittura dell'articolo risulta essere la 4.1. Ciò può imputarsi con buona probabilità alla presenza di una feature di aggiornamento automatico del framework, aspetto che potrebbe essere valutato dalle Pubbliche Amministrazioni nella scelta futura dei prodotti da utilizzare. Una tale funzionalità evidentemente costituisce un ausilio al mantenimento del livello di sicurezza definito in fase di prima installazione della piattaforma web, come i dati dimostrano.
Inoltre le vulnerabilità possono essere presenti anche nei plugin, nelle estensioni e nei componenti realizzati da terze parti ed anche per essi valgono le medesime considerazioni su vulnerabilità e rischi[12].
I siti web subiscono spesso attacchi informatici, talvolta con effetti eclatanti che portano alla luce il problema, come in caso di defacement[13], ovvero quando la pagina principale del sito web è stata cambiata, modificata o sostituita in modo illecito. In realtà gli attacchi possono essere di diverso tipo e sono spesso invisibili, vengono portati a segno se esistono vulnerabilità presenti nel software di gestione del sito oppure nei sistemi operativi del server web e hanno l'obiettivo di carpire dati importanti come le password ftp, le password mail, i documenti ed il contenuto dei database.

[12] http://www.ilsecoloxix.it/p/magazine/2014/12/16/ARGTmvtC-soaksoak_wordpress_terrore.shtml

[13] http://it.wikipedia.org/wiki/Defacing

I ricercatori di Cisco confermano che i principali bersagli dei più recenti tentativi di accesso brute-force sono proprio le piattaforme CMS. In alcuni casi, la compromissione può consentire di arrivare fino al server host per impossessarsene, sovente sfruttando le vulnerabilità dei vari plugin installati[14].

A titolo esemplificativo, si riportano di seguito alcuni casi di attacchi reali, che hanno interessato le pubbliche amministrazioni locali, raccolte da fonte pubbliche quali zone-h e quotidiani online.

Regione	1° attacco	2° attacco	3° attacco
Abruzzo	16/05/2014		
Calabria	10/09/2014		
Campania	05/05/2014	09/09/2014	
Puglia	12/03/2014	22/05/2014	16/10/2014
Veneto	29/07/2014	15/10/2014	

Sono state classificate 5 regioni che hanno subito attacchi nel 2014, questo significa il 25% dei siti web regionali e sono Abruzzo, Calabria, Campania, Puglia e Veneto.

Fonte http://www.zone-h.org/archive

In data 29/07/2014: Regione Veneto.

Anonymous viola i server e vengono pubblicati su Internet le email dei Consiglieri manifestando la loro contrarietà ad un'opera come il Mose[15].

In data 16/10/2014: Regione Puglia.

La Comunità di hacker Anonymous ha annunciato sul suo blog[16] di aver modificato la home page del sito della Regione Puglia per tenere alta l'attenzione sui danni all'ambiente causati dall'Ilva di Taranto[17].

[14] www.cisco.com/assets/global/IT/pdfs/executive_security/sc-01casr2014_cte_lig_it_35330.pdf

[15] http://corrieredelveneto.corriere.it/veneto/notizie/cronaca/2014/29-luglio-2014/anonymous-viola-server-regione-rete-mail-consiglieri-veneto-223650403330.shtml

[16] http://anon-news.blogspot.it/2014/10/regione-puglia-hacked-by-anonymous.html

[17] http://www.foggiacittaaperta.it/news/hackerato-il-sito-web-della-regione-puglia.asp

Provincia	1° attacco	2° attacco	3° attacco
Arezzo	27/10/2014	28/10/2014	
Avellino	04/03/2014		
Brindisi	10/10/2014	13/10/2014	
Cosenza	13/03/2014	11/09/2014	
Firenze	27/10/2014	28/10/2014	29/10/2014
Grossetto	28/10/2014		
Latina	10/09/2014		
Livorno	28/10/2014		
Lucca	03/05/2014	28/10/2014	08/11/2014
Milano	27/10/2014		
Napoli	11/11/2014		
Pescara	07/01/2014		
Pistoia	15/12/2014		
Roma	12/05/2014		
Treviso	10/11/2014		
Venezia	31/07/2014		

Fonte http://www.zone-h.org/archive

Invece le Province classificate che hanno avuto nel 2014 una compromissione del proprio sito web rappresentano il 14,7% del totale. Notiamo che alcune di esse hanno subito più attacchi, in date diverse.

In data 07/01/2014: Provincia di Pescara.

Il sito istituzionale della Provincia di Pescara ha subito un attacco esterno da uno o più hacker.

I tecnici dell'ente stanno provvedendo a riparare i danni. Alcune cartelle sono state svuotate del loro contenuto che quindi non risulta più disponibile. I disguidi sono stati segnalati alla Provincia da cittadini che non riuscivano ad accedere a documenti e bandi[18].

In data 16/10/2014: Provincia di Lucca.

La home page del sito istituzionale è stata resa inaccessibile ed al suo posto è apparsa una pagina con l'immagine di un uomo, di spalle, che imbraccia due fucili, firmata da RatHack e con una scritta inequivocalbile: "La sicurezza è solo un'illusione"[19].

[18] http://ilcentro.gelocal.it/pescara/cronaca/2014/01/08/news/pescara-attacco-hacker-al-sito-della-provincia-1.8431012

[19] http://iltirreno.gelocal.it/lucca/cronaca/2014/11/09/news/il-sito-della-provincia-oscurato-dagli-hacker-1.10275849

Invece i comuni che nel 2014 hanno subito attacchi ai propri siti web[20] rappresentano l'8,5%, ovvero 681 comuni classificati su un totale di 8048.

In data 12/02/2014: Comune di Sarzana.

La home page del Comune di Sarzana è stata sostituita nella notte da una serie di rivendicazioni firmate da "Albanian Hackers Terrorist" con la scritta "Niente può fermarci". Il gruppo di hacker aveva già colpito in passato altri siti istituzionali, soprattutto piccoli comuni, con riferimenti legati alla guerra in Kosovo[21].

In data 14/05/2014: il Comando unità speciali della Gdf individua 53 siti alterati.

Un gruppo di hacker ha trasformato 53 siti, tra cui Comuni e Scuole, in negozi virtuali di merci contraffatte[22].

In data 22/09/2014: Mass Defacement[23] Attack, 213 siti di comuni alterati in un unico attacco.

Dalla nostra analisi si evince che su un unico IP di un noto provider è stato effettuato un attacco da un cracker sfruttando una vulnerabilità su server IIS 6.0 e sistema operativo Windows 2003. Tutti i siti compromessi sono realizzati in ASP. I siti sono stati infettati tramite una backdoor che ha consentito all'autore dell'attacco di caricare dei moduli "lato server" dannosi. La compromissione ha consentito il defacement in tempo reale dei siti web ospitati. Tra questi il comune di Cuorgnè (To)[24].

[20] Fonte http://www.zone-h.org/archive

[21] http://www.cittadellaspezia.com/Sarzana/Sarzana-Val-di-Magra/Sito-del-Comune-hackerato-dai-151888.aspx

[22] http://www.ilsole24ore.com/art/notizie/2014-05-14/gdf-hacker-truccano-53-siti-trasformandoli-negozi-virtuali-merci-contraffatte-104339.shtml?uuid=AB7Qj7HB

[23] http://www.kaspersky.com/it/about/news/virus/2010/Mass_Defacement_di_siti_web_il_divertimento_degli_hacker_che_minaccia_il_business

[24] http://lasentinella.gelocal.it/ivrea/cronaca/2014/09/29/news/cuorgne-sito-blindato-dopo-l-attacco-degli-hacker-1.10024161

In data 04/11/2014: Comune di Spoleto.

Sulla home page è comparsa la scritta: "Perché abbiamo hackerato il sito? Per mandare un messaggio al mondo: fermate la distruzione di Gaza. Noi non dimentichiamo". I tecnici del Municipio sono subito intervenuti per rimuovere la scritta[25].

Conclusioni

Esistono leggi e normative riguardante la protezione delle informazioni e vanno applicate. Essendo i dati trattati dei cittadini, a cui la P.A. fornisce i servizi tramite i loro portali web, vanno tutelati con adeguati sistemi di sicurezza.

Come evidenziato da questo studio, tali attacchi non dipendono dalla piattaforma specifica (i siti web possono essere realizzati sotto piattaforma Linux o Windows, utilizzare applicazioni Open Source o proprietari), la causa è piuttosto da imputare alla mancanza di consapevolezza alle problematiche evidenziate e alla mancanza di personale con competenza tecnica in materia. Rivolgersi a professionisti ed esperti in sicurezza informatica risulta fondamentale per affrontare il problema.

Appare ovvio che la Pubblica Amministrazione sia di fronte ad una sfida complessa ed estremamente impegnativa specie nel contesto di scarsità di risorse disponibili che caratterizza questo periodo di crisi. Inoltre, come spesso accade nei piccoli comuni, essi non hanno internamente il personale che possa essere dedicato ad attività di programmazione e sicurezza web, né tali competenze sono sempre disponibili sul territorio. Dovendo essi affidarsi a ditte esterne, ci si potrebbe legittimamente chiedere quali siano i **criteri di scelta** dei provider, delle web-agency e delle **software house** incaricati della gestione dei servizi informatici statali. E in nome della **trasparenza** il cittadino-utente dovrebbe poterne verificare agevolmente **l'affidabilità**, nonché quanto sia costato il sito web e quanto il suo ripristino in caso di compromissione[26].

Il legislatore sta comunque lavorando e gli obiettivi sono stati ridefiniti nel tempo. Vi sono segnali importanti di consapevolezza ed è di questi giorni (11 Febbraio 2015) la notizia che attribuisce allo Stato competenza esclusiva in materia di sistemi informativi della P.A.. Siamo di fronte ad un cambiamento estremamente importante: ciò consentirà di superare la frammentazione, gli ostacoli all'interoperabilità e la sovrabbondanza di piattaforme tecnologiche sviluppate negli anni dalle Regioni e dai Comuni, che impedisce la completa digitalizzazione, lo sviluppo e la competitività del nostro paese[27].

[25] http://www.perugiaonline.net/cronaca/hackerato-sito-comune-spoleto-8670/

[26] http://www.ilfattoquotidiano.it/2014/06/18/pa-2-0-siti-web-attaccabili-gestiti-a-nostre-spese/1031738/

[27] http://www.agendadigitale.eu/egov/1346_ecco-che-cosa-cambia-con-la-centralizzazione-delle-competenze-it-della-pa.htm

© Clusit 2015

Il Regolamento generale sulla protezione dei dati: novità per i cittadini, le imprese e le istituzioni[1]

A cura di Maria Grazia Porcedda

Sono trascorsi tre anni da quando la Commissione Europea ha pubblicato la proposta di Regolamento generale sulla protezione dei dati, ma l'attenzione del pubblico sulla bozza non è per questo diminuita. Da un lato, le motivazioni che spingono ad abrogare la Direttiva 95/46/CE sono sempre più pressanti. Dall'altro, l'iter legislativo è assediato (e rallentato) dai contrapposti interessi in gioco. La complessità del testo, che consta di 92 articoli e 192 considerando, interviene a parziale giustificazione dei ritardi.

La complessità del testo giustifica anche il taglio di questo *focus on,* dedicato agli aspetti salienti della proposta per i cittadini, le imprese e le istituzioni, con particolare attenzione al settore della sicurezza informatica. Prima di analizzare in dettaglio la proposta come emendata dal Parlamento Europeo (PE), mi soffermo sulle ragioni e le tappe della riforma.

A. Ragioni e tappe della riforma

La proposta di Regolamento risponde alla palese incapacità della Direttiva 95/46/CE di regolare il crescente flusso (transfrontaliero) dei dati, e conciliarlo con l'esigenza di tutela della persona. In effetti, sebbene la Direttiva sia stata scritta con un linguaggio "tecnologicamente neutrale", non ha retto la prova della rapida evoluzione tecnologica successiva alla sua entrata in vigore: il successo della ragnatela globale e lo sviluppo di Internet, il *cloud computing*, l'uso quotidiano di tecnologie "intelligenti" dotate di microprocessori e programmi sofisticati (*smartphones*, droni, applicazioni biometriche…), il c.d. *Internet of Things*, fino alle tecniche di analisi che permettono di sfruttare i *big data*.

Questo ha portato all'incapacità del tessuto normativo di salvaguardare gli interessi tanto dei cittadini quanto delle imprese affamate di dati, definiti "il nuovo petrolio" [2]
. Inoltre, la protezione dei dati di carattere personale è assurta al livello di diritto fondamentale, sancito dall'articolo 8 della Carta dei Diritti Fondamentali dell'Unione Europea, resa giuridicamente vincolante dal Trattato di Lisbona. Lo stesso Trattato ha poi imposto al legislatore europeo di adottare regole consone alla tutela del nuovo diritto[3].

[1] Si ringrazia la dott.ssa Federica Casarosa (Istituto Universitario Europeo, Centre for Judicial Cooperation), per gli utilissimi commenti e la revisione del testo.

[2] Neelie Kroes, The big Data Revolution, Discorso tenuto presso l'EIT Foundation Annual Innovation Forum, 26 marzo 2013: http://europa.eu/rapid/press-release_SPEECH-13-261_en.htm (accesso effettuato il 31/01/2015).

[3] Si tratta dell'art. 16.1 del Trattato sul Funzionamento dell'Unione Europea, base giuridica del Regolamento.

Alle ragioni di mercato e di diritto si sono aggiunte quelle politiche, in particolare la necessità dell'Unione di stabilire le proprie regole del gioco prima di affrontare negoziati internazionali sullo scambio di dati, come i dibattuti accordi PNR (*passengers name record*), SWIFT, ecc.

È per far fronte a queste necessità che la Commissione Europea ha proposto un Regolamento, invece che una Direttiva. Le sue caratteristiche giuridiche (applicazione diretta e vincolante in ogni sua parte) dovrebbero ovviare al problema dell'applicazione difforme negli Stati Membri, contribuendo alla certezza giuridica e innalzando il livello di protezione.

Il regolamento segue l'iter della procedura legislativa ordinaria (art. 294 TFUE), rallentato dalle elezioni del PE e della nuova Commissione Europea. Agli emendamenti proposti dal PE e parzialmente accolti dalla Commissione durante il 2014 [4], il Consiglio ha risposto con un "approccio generale parziale", [5] basato sulla proposta originaria della Commissione, che potrebbe preludere alla volontà di adottare il testo in prima lettura[6] (sulle tre disponibili).

In linea generale, gli emendamenti del PE rafforzano le tutele accordate ai dati personali, mentre le proposte del Consiglio mirano ad appianare gli ostacoli al raggiungimento del mercato unico digitale, e ad arginare la perdita di potere degli Stati Membri, di cui il Consiglio è espressione, riservando loro aree di autonomia legislativa più vaste di quelle previste dalla proposta[7].

Tuttavia, lo scontro tra il PE e il Consiglio non è l'unico scatenato da quest'iniziativa. Già prima della sua pubblicazione apparvero numerosi commenti alla riforma da parte di lobbisti, tra cui esponenti del governo statunitense [8], che auspicavano interventi particolari.

B. Innovazioni salienti

In queste pagine mi soffermo sulle proposte più innovative[9] e interessanti per il pubblico italiano, introdotte dalla Commissione Europea per far fronte alle sfide alla Direttiva 95/46/

[4] Documenti disponibili in inglese e francese: http://www.europarl.europa.eu/oeil/popups/ficheprocedure.do?lang=en&reference=2012/0011(OLP)#tab-0 (accesso effettuato il 31/01/2015).

[5] Il testo dell'approccio generale parziale non è stato pubblicato, ma una versione trapelata è disponibile sul sito dell'ONG Statewatch: http://www.statewatch.org/news/2014/dec/eu-council-dp-reg-15395-14.pdf (accesso effettuato il 31/01/2015).

[6] Si veda: http://www.europarl.europa.eu/aboutparliament/it/0081f4b3c7/Law-making-procedures-in-detail.html (accesso effettuato il 31/01/2015).

[7] Si veda, ad esempio, la posizione del Consiglio sull'articolo 1.

[8] Si veda l'articolo scritto da European Digital Rights il 22/12/2011: https://edri.org/US-DPR/ (accesso effettuato il 31/01/2015).

[9] Molte innovazioni della riforma codificano le interpretazioni date negli anni alla Direttiva 95/46/CE, per es. dalla Corte di Giustizia dell'UE o dal Gruppo di Lavoro dell'Articolo 29.

CE descritte nella Comunicazione che anticipava la proposta di Regolamento[10].
Si tratta di misure atte a tutelare il diritto alla protezione dei dati, anche a fronte delle sfide globali, completare il mercato interno, e migliorare l'assetto istituzionale, dunque misure indirizzate rispettivamente ai cittadini, alle imprese e ai garanti.

B.1 Innovazioni a favore dei cittadini: un diritto efficace

In ossequio all'articolo 8 della Carta dei Diritti, il Regolamento ribadisce che la tutela della persona con riguardo al trattamento dei suoi dati personali è un diritto fondamentale. Per tutelare meglio la persona fisica, il Regolamento estende la rosa dei dati sensibili (art. 9) ai dati genetici e, secondo il PE, alle informazioni biometriche e alle sanzioni amministrative. Inoltre, il Regolamento dedica norme specifiche alla protezione dei minori cui sono offerti servizi (in rete) o prodotti, riconoscendo la loro maggiore vulnerabilità (artt. 8 e 11).

Nonostante la Direttiva sottolinei l'importanza dell'informazione per un efficace esercizio del diritto (il consenso informato), ha fallito nell'imporre misure incisive in questo senso: quanti si soffermano a decifrare le impenetrabili informative dei servizi offerti in rete? Il Regolamento affianca al diritto di accesso il principio di trasparenza del trattamento (art. 11) e obbliga il responsabile a offrire un'informativa chiara e intelligibile, secondo moduli standard (art. 14 e 13(a) nella versione emendata dal PE). Ai sensi della Direttiva, il consenso dovrebbe poi essere espresso liberamente, ma la pratica è spesso diversa. Il Regolamento cerca di ovviare invalidando il consenso dato in caso di notevole squilibrio tra l'interessato e il responsabile, e imponendo a quest'ultimo l'onere di dimostrare che l'interessato abbia espresso il consenso ("accountability") (artt. 7 e 22).

Perché l'esercizio del diritto sia effettivo, il cittadino riceve nuovi diritti in materia di rettifica, cancellazione e opposizione. Innanzitutto, un aspetto particolarmente sentito dai cittadini (come dimostra il grafico in fig. 1[11]), il diritto alla portabilità dei dati, che permette all'interessato di 'trasportare' i propri dati da un servizio elettronico a un altro (art. 18, 15.2a nella versione emendata dal PE). Poi, il tanto discusso diritto all'oblio, che rende la richiesta di cancellazione dei dati personali vincolante anche per i terzi: il responsabile che ha reso i dati dell'interessato pubblici, per motivi diversi da quelli che rendono il trattamento necessario, deve assicurarsi che eventuali terze parti autorizzate a successiva divulgazione cancellino link, copie o riproduzione dei medesimi (art. 17).

L'art. 19 del Regolamento prevede la possibilità di opporsi con mezzi tecnici al trattamento dei propri dati, per esempio a scopo di profilazione, da parte dei servizi della società dell'in-

[10] Comunicazione della Commissione, COM(2010) 609 finale, 4 novembre 2010, Bruxelles.

[11] Sondaggio Speciale dell'Eurobarometro n. 359 (2011), Atteggiamento nei confronti della protezione dei dati e dell'identità elettronica nell'Unione europea, Risultati per l'Italia: http://ec.europa.eu/public_opinion/archives/ebs/ebs_359_fact_it_it.pdf (accesso effettuato il 31/01/2015).

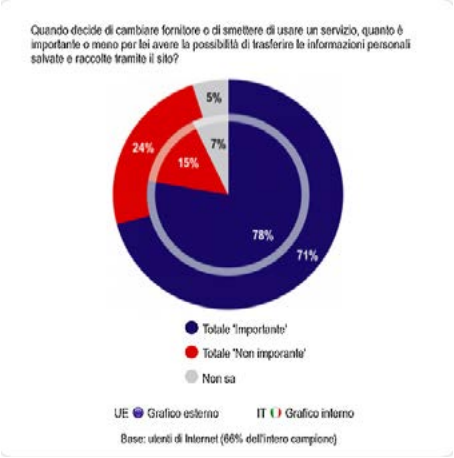


Figura 1: L'importanza della portabilità dei dati in Italia. Fonte: Eurobarometro (2011)

formazione (commercio elettronico, social networks etc.).
Inoltre, riconoscendo l'importanza crescente e sempre più discussa [12] del ruolo svolto dagli algoritmi nella vita quotidiana, se la profilazione conduce alla produzione di effetti giuridici (trattamento automatizzato), diventa obbligatorio affiancare misure di salvaguardia dei diritti, tra cui l'intervento umano (art. 20).

Il Regolamento impone che il responsabile del trattamento risponda entro quaranta giorni e gratuitamente alle richieste dell'interessato (art. 12 e 19), che potrà presentare reclamo presso qualunque autorità di controllo competente in Europa, anche tramite associazioni e organizzazioni non governative, che comunque possono fare ricorso indipendentemente dall'interessato (art. 73).

I (co)responsabili che non ottemperano agli obblighi sono esposti a sanzioni amministrative proporzionali e crescenti, fino, per le violazioni più gravi, a cento milioni di euro, o il 5% del fatturato globale dell'azienda (artt. 78 e 79). E questo ci porta alle novità per le imprese.

B.2 Novità per i responsabili del trattamento e delle imprese

Se è vero che ai diritti dei cittadini corrispondono doveri per i responsabili del trattamento, il Regolamento non prevede solo misure "lacrime e sangue". L'obiettivo è garantire la certezza giuridica, offrendo condizioni uniformi per il trattamento dei dati in tutta l'Unione (e dunque l'area Schengen) grazie all'uso del Regolamento al posto della Direttiva, in ultima analisi rimuovendo oneri amministrativi e finanziari. Gli stati membri possono adottare provvedimenti specifici in alcuni campi (punto su cui si sta battendo il Consiglio), ad es. il trattamento dei dati nell'ambito dei rapporti di lavoro e in ambito sanitario.

Innanzitutto il regolamento chiarisce l'ambito di applicazione della normativa. Nel caso dell'ambito territoriale, la normativa vigente si applica se il trattamento è effettuato da un

[12] Si veda la lettera aperta pubblicata dal Future of Life Institute contro un approccio sregolato all'Intelligenza Artificiale: http://www.repubblica.it/tecnologia/2015/01/14/news/intelligenza_artificiale_va_regolata_l_appello_firmato_anche_da_hawking_e_musk-104916286/ (accesso effettuato il 31/01/2015).

soggetto stabilito nel territorio dell'Unione o che, se stabilito altrove, impiega 'strumenti' situati nel territorio dell'Unione. L'uso crescente del cloud [13] (adottato da un quinto delle imprese europee, figura2 [14]) ha seriamente minato la validità del secondo criterio, che scompare nella proposta. Il PE propone che la normativa si applichi quando il responsabile offre beni e servizi, anche gratuiti, o monitori individui nell'Unione, a prescindere da dove sia stabilito e dove effettui materialmente il trattamento (art 3).

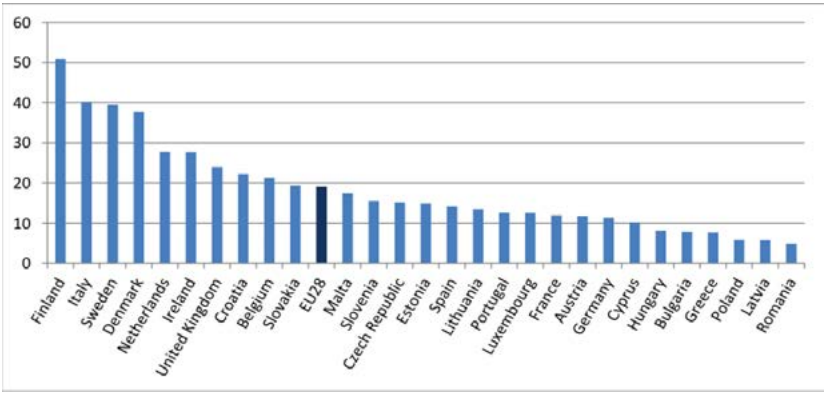


Figura 2: Percentuale di imprese che usano il cloud negli Stati Membri dell'UE (% imprese). Fonte: Eurostat (2014)

Non solo la nuova normativa sarà (quasi) uniforme: il meccanismo del "one-stop-shop" permetterà a responsabili operanti in più paesi dell'UE di rimettersi alle sole decisioni dell'autorità garante del paese in cui ha stabilito la sede principale (art. 51, 54 nella versione emendata dal PE).

A vantaggio delle imprese sparisce l'onere di notificazione, sostituito dall'obbligo di conservare la documentazione del trattamento (art. 28) e da meccanismi come valutazioni d'impatto del trattamento, autorizzazioni e consultazioni preventive (artt. 33 e 34). La proposta poi incoraggia iniziative di autoregolazione, come codici di condotta e certificazioni (artt. 38 e 39).

[13] Sull'uso del cloud nell'Unione Europea si vedano le recenti statistiche elaborate da Eurostat per i cittadini (http://ec.europa.eu/eurostat/documents/2995521/6343581/4-16122014-BP-EN.pdf/b4f07b2a-5aee-4b91-b017-65bcb6d95daa) e le imprese (http://ec.europa.eu/eurostat/statistics-explained/index.php/Cloud_computing_-_statistics_on_the_use_by_enterprises) (accesso effettuato il 31/01/2015).

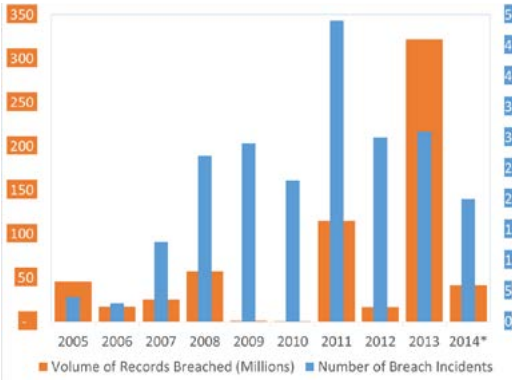
[14] Eurostat News Release, Cloud computing services used by one out of every five enterprises in the EU28, 189/2014 - 9 December 2014: http://ec.europa.eu/eurostat/documents/2995521/6208098/4-09122014-AP-EN.pdf/627ddf4f-730a-46ca-856b-32532d8325c5 (accesso effettuato il 31/01/2015).

Il Regolamento prevede inoltre norme diverse in base alla dimensione dell'impresa. Le imprese che trattano dati concernenti meno di 5000 interessati in un periodo di 12 mesi sono esentate da alcuni obblighi (come quello di designare un responsabile aziendale del trattamento); allo stesso modo, la Commissione ha il compito e potere di adottare norme specifiche per le piccole e medie imprese.

B.2.1 Novità con impatto positivo sulla sicurezza informatica

Il regolamento, come già la Direttiva, obbliga il responsabile ad adottare misure tecniche e organizzative, in linea con i costi e l'evoluzione tecnica, adeguate per il tipo di dati e il trattamento svolto (art. 30). Quest'onere però funge anche da incentivo, perché porta a investire nella prevenzione, con guadagno notevole per la protezione dei dati e la sicurezza informatica.

Innanzitutto, a fronte del numero crescente dei cosiddetti *data breaches* (figura 3[15]), il Regolamento estende l'obbligo di notificazione delle violazioni dei dati introdotto dalla Direttiva relativa alla vita privata e alle comunicazioni elettroniche (2002/58/CE) a tutti, inclusi i servizi della società dell'informazione (art. 31 e 32). Il responsabile deve notificare in breve tempo (72 ore per il PE, considerando 67) eventuali perdite di dati alle autorità di controllo e agli interessati (salvo aver messo in atto misure tali da prevenire il danno), pena una pesante ammenda e, ovviamente, conseguenze per la propria reputazione.



*Include il terzo trimestre del 2014

Figura 3: Variazione del volume e numero delle violazioni dei dati nell'Unione Europea dal 2005 al 2014. Fonte: CEU (2014)

Un'altra misura che rafforza la sicurezza informatica è la privacy fin dalla progettazione ("privacy by design"), concetto promosso originariamente dalla Garante dell'Ontario[16], che significa tutelare i dati, e quindi la loro sicurezza, sin dalle prime fasi di progettazione di un sistema di trattamento e per tutta la durata del ciclo di vita (art. 23). L'operazione dovrebbe essere facilitata dall'obbligo di designare un responsabile del trattamento (*data protection*

[15] Philip N. Howard and Orsolya Gulyas (2014) Data Breaches in Europe: Reported Breaches of Compromised Personal Records in Europe, 2005-2014, CMDS Working Paper 2014.1, Central European University, p. 8.

[16] Si veda il sito internet dedicato: http://privacybydesign.ca (accesso effettuato il 31/01/2015).

©Clusit 2015

officer), anche congiuntamente con altre imprese (artt. 35-37), incaricato di assicurare la sicurezza dei dati, e dunque dei sistemi che li contengono e con cui si elaborano.

Allo stesso modo, le valutazioni d'impatto del trattamento, e l'adozione di certificati sulla privacy, possono produrre un incentivo a combinare le politiche di tutela dei dati e di sicurezza informatica (il cui stato dell'arte è riportato nella figura 4[17]), a vantaggio di entrambe.

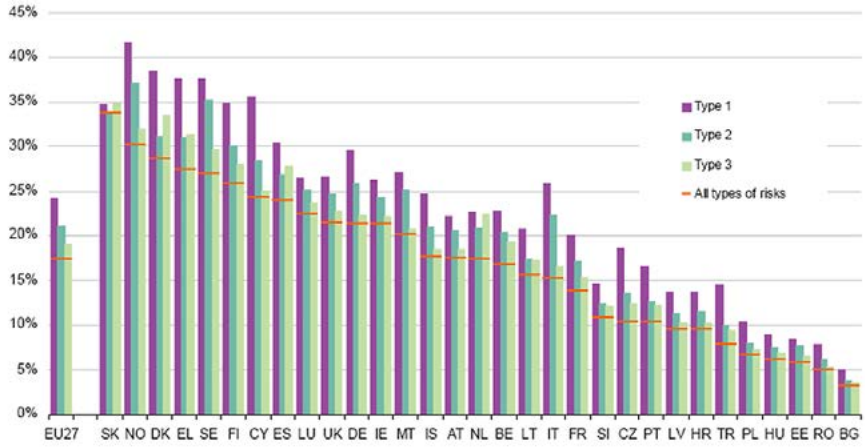


Figura 4: Percentuale di imprese dotate di una policy sulla sicurezza informatica per paese e tipo di rischio. Fonte: Eurostat (2010)

B.3 Novità per le autorità di controllo

Oltre a comportare un aggiustamento delle normative nazionali, la proposta di Regolamento introduce novità importanti per le autorità di controllo. Se ciò da un lato modificherà le procedure esistenti, dall'altro ridurrà la duplicazione degli sforzi in un quadro di cronica carenza di fondi e di personale[18].

Il Regolamento evidenzia l'importanza dell'indipendenza e adeguatezza del personale dell'autorità di controllo, così come la disponibilità di risorse sufficienti (artt. 46-50). Il meccanismo del "one-stop-shop" (art. 51, 54 nella versione emendata dal PE) affida all'au-

[17] Grafico disponibile alla pagina: http://ec.europa.eu/eurostat/statistics-explained/index.php/ICT_security_in_enterprises. Type 1 significa distruzione o corruzione dei dati a causa di un attacco o incidente imprevisto; type 2 consiste nella perdita (disclosure) di dati riservati a causa di violazione, pharming o phishing; type 3 significa l'indisponibilità dei servizi TIC a causa di un attacco esterno.

[18] Sul punto, si veda lo studio comparato dell'agenzia dell'Unione Europea per i Diritti Fondamentali: http://fra.europa.eu/sites/default/files/fra_uploads/815-Data-protection_en.pdf (accesso effettuato il 31/01/2015).

torità garante del paese in cui il responsabile ha stabilito la sua sede principale, il compito di controllare il trattamento che il responsabile effettua in qualsiasi stato dell'Unione. Ovviamente, questo presume la necessità di cooperazione tra le autorità europee, che appunto avranno l'obbligo di prestarsi assistenza reciproca, anche tramite operazioni congiunte (art. 55 e 56), conformandosi al principio di coerenza (art. 57-63), coadiuvate in questo dal "Comitato Europeo per la protezione dei dati" che sostituirà il Gruppo di Lavoro dell'Articolo 29 (art. 64-72), e dalla Commissione.

C. Conclusione

Le novità discusse in questo focus on sono solo una parte di quelle contenute nel Regolamento, che include ad es. nuove misure sui flussi transfrontalieri dei dati, i trattamenti particolari, il margine di manovra della Commissione nell'adottare atti delegati e di esecuzione. Tuttavia, un esame approfondito richiederebbe un contributo ben più ampio.

Quando ci si può aspettare una pubblicazione del documento? Durante il suo intervento nel corso del Convegno Computers, Privacy and Data Protection (tenutosi a fine gennaio 2015), il relatore della proposta per il PE, Jan Albrecht (Verdi), si è detto fiducioso, reputando possibile che la proposta diventi legge entro l'anno. Contrapposizioni sui punti salienti, però, potrebbero far slittare i tempi (la precedente Direttiva 95/46/EC divenne legge dopo cinque anni di accesi dibattiti).

Se le istituzioni europee sapranno evitare un compromesso al ribasso, il testo potrà migliorare sensibilmente la protezione dei dati e al contempo stimolare il mercato digitale, sempre che la neutralità tecnologica non sia sconvolta da un'innovazione di cui ancora non si comprenda la portata. Una valutazione concreta si potrà fare solo col tempo, mettendo a confronto il Regolamento con le regole che disciplinano l'uso dei dati personali in ambiti specifici, come quelle attualmente in fase di discussione[19], così come le proposte che la Commissione intende pubblicare a breve sulla revisione della Direttiva 2002/58/CE, della Direttiva sulla conservazione dei dati, e del Regolamento sulla protezione dei dati da parte delle istituzioni europee.

[19] Si tratta della proposta di Direttiva concernente la tutela delle persone fisiche con riguardo al trattamento dei dati personali da parte delle autorità competenti a fini di prevenzione, indagine, accertamento e perseguimento di reati o esecuzione di sanzioni penali, e la libera circolazione di tali dati, la proposta di Direttiva recante misure volte a garantire un livello comune elevato di sicurezza delle reti e dell'informazione nell'Unione, e la revisione della Convenzione n. 108 del Consiglio d'Europa.

© Clusit 2015

Cloud e sicurezza: profili legali

A cura di Gabriele Faggioli

A fronte degli innegabili vantaggi che in termini di flessibilità, scalabilità, accesso ai dati in mobilità ed abbattimento dei costi legati all'implementazione e alla gestione dell'infrastruttura hardware e software, potrebbero derivare, tanto alle imprese quanto alla pubblica amministrazione, dal ricorso a servizi di cloud computing, tale nuova modalità di fruizione di risorse e applicazioni informatiche presenta altrettante criticità che devono essere adeguatamente analizzate in sede di valutazione circa l'opportunità di ricorrere alla "nuvola".
I principali rischi potenziali connessi al trasferimento dei dati da sistemi informatici posti nella materiale disponibilità del titolare dei dati da allocare a sistemi remoti di titolarità di un fornitore terzo possono essere fondamentalmente ricondotti alle tre seguenti aree problematiche:
riservatezza ed integrità dei dati e delle applicazioni;
disponibilità dei dati e delle risorse da parte del titolare degli stessi;
esigenze di compliance normativa legate anche alla normativa sulla protezione dei dati personali, in particolare a causa della frequentissima ipotesi di flusso transfrontaliero degli stessi.

Sotto il primo dei tre profili sopra indicati, il rischio che venga compromessa la confidenzialità del patrimonio informativo allocato sulla "nuvola" rappresenta una delle principali remore rispetto all'adozione dei servizi di cloud computing.
Tale minaccia è tipicamente legata a una serie di fattori – quali eventuali comportamenti dolosi o colposi del service provider o di terzi, eventi distruttivi, black-out o malfunzionamenti del sistema informatico – che, in ottica di valutazione e gestione del rischio, dovranno essere opportunamente verificati attraverso la predisposizione di adeguate misure e protocolli di sicurezza.
Ove si consideri che i dati aziendali, il know-how e le esperienze tecnico-industriali che, in quanto segrete, abbiano uno specifico valore economico, costituiscono un vero e proprio asset aziendale – per di più oggetto di specifica tutela giuridica avverso l'indebita appropriazione ed utilizzazione, ai sensi dell'art. 98 Codice della proprietà industriale – è evidente che eventuali falle dei sistemi di sicurezza predisposti dal cloud provider potrebbero comportare il deprezzamento di beni aziendali e la perdita di competitività sul mercato.
Sotto il diverso profilo della disponibilità dei dati, occorre considerare che l'accesso agli stessi da parte dell'utente potrebbe essere reso difficoltoso da elevati picchi di traffico sulla rete o addirittura interdetto in presenza di eventi anomalie, guasti, attacchi informatici, calamità naturali, ecc. Sarebbe, pertanto, opportuno che le imprese valutassero anticipatamente l'impatto e i costi di un eventuale, più o meno prolungata, indisponibilità del servizio, concordando in anticipo con il cloud provider idonee procedure di business continuity e disaster recovery, che garantiscano la continuità operativa in caso di emergenza ed il recu-

pero dei dati persi o distrutti in conseguenza di eventi eccezionali che compromettano il funzionamento dei data center.
Per altro verso, un livello ottimale di servizio dovrebbe prevedere l'adozione di formati e standard aperti, che garantiscano la replicabilità dell'ambiente applicativo presso diversi fornitori di servizi, così facilitando la portabilità (migrazione da un sistema cloud ad altro, gestito da diverso fornitore) e la interoperabilità (possibilità di fruizione e condivisione delle risorse cloud da parte di utenti afferenti a due o più fornitori diversi) dei dati gestiti in cloud.
In ultimo, per quanto concerne il terzo dei profili di rischio summenzionati, basti considerare che la conservazione dei dati in luoghi geografici differenti (sempre più frequentemente in Paesi extra UE) ha riflessi immediati non solo sulla normativa applicabile in caso di eventuale contenzioso tra fornitore ed utente, ma anche e soprattutto sugli obblighi di legge inerenti il trattamento e la sicurezza dei dati personali; obblighi la cui violazione potrebbe esporre in prima persona l'utente cloud a rilevanti sanzione di carattere amministrativo e, in talune ipotesi, perfino penale. E' bene, infatti, sottolineare che l'adozione di servizi esternalizzati e la migrazione di dati da sistemi locali posti sotto il diretto controllo dell'utente a sistemi remoti soggetti all'esclusivo controllo del fornitore non esime le imprese e la pubblica amministrazione, che di tali servizi si avvalgono per la gestione del proprio patrimonio informativo, dalle responsabilità che ad esse derivano dalla normativa in materia di protezione dei dati personali.
In relazione al riparto, tra le diverse parti del trattamento, di obblighi e responsabilità previsti dalla normativa privacy, sono intervenute anche le Autorità Garanti per la protezione dei dati personali, le quali, tanto a livello nazionale, quanto a livello europeo, hanno più volte evidenziato come l'utente di un servizio cloud debba essere considerato quale "titolare del trattamento" ai sensi della normativa dettata dal Codice Privacy (D. Lgs. 196/2003) e, in quanto tale, abbia l'obbligo di designare il cloud provider quale "responsabile del trattamento", con conseguente potere/dovere di controllo nei confronti di quest'ultimo, in relazione alla corretta esecuzione degli adempimenti normativi previsti in relazione ai dati trattati.
In caso di violazioni commesse dal provider, infatti, anche il titolare del trattamento sarà chiamato a rispondere dell'eventuale illecito. E a questo proposito, le Autorità Garanti hanno sottolineato che, all'utente/titolare dei dati trattai, non sarà sufficiente, per giustificare un'eventuale violazione, affermare di non aver avuto la possibilità di negoziare clausole contrattuali adeguatamente tutelanti o modalità di controllo sufficientemente stringenti, potendo pur sempre rivolgersi ad altro fornitori che offrano maggiori garanzie circa il rispetto della normativa sulla protezione dei dati personali.
Un ulteriore aspetto di fondamentale importanza di cui occorre tener conto in sede di adempimento della normativa privacy riguarda la problematica del flusso transfrontaliero dei dati caricati sulla "nuvola", fenomeno che in tale settore costituisce praticamente la regola. Infatti, tanto la disciplina comunitaria, quanto il Codice Privacy italiano che la recepisce, definiscono regole particolarmente restrittive in ordine al trasferimento dei dati personali al di fuori dell'Unione Europea, in linea di principio vietando il trasferimento "anche temporaneo" verso uno Stato extraeuropeo, a meno che l'ordinamento giuridico del Paese

© Clusit 2015

di destinazione o di quello di transito dei dati non garantisca un livello di protezione adeguato (art. 25 comma 1, direttiva 96/46/CE – art. 45 Codice Privacy). Anche sotto questo profilo, pertanto, il fruitore di servizi cloud dovrà conoscere e tenere in debito conto il luogo in cui risiedono i dati di propria titolarità e le normative previste dai Paesi extra UE per il trattamento degli stessi. Ciò reso difficoltoso tanto dal fatto che non sempre il fornitore rende l'utente in grado di conoscere l'ubicazione dei data center utilizzati, quanto dal fatto che sovente il servizio prescelto viene fornito attraverso le prestazioni di subfornitori diversi da service provider con cui l'utente ha stipulato il contratto di servizio; di conseguenza, a fronte di complesse filiere di responsabilità, l'utente non sempre è in condizione di conoscere l'identità dei gestori intermedi del servizio che hanno accesso ai dati di sua titolarità. Con il dichiarato obbiettivo di promuovere una riflessione sulle penetranti forme di tutela dei dati personali previste dall'attuale legislazione e di fornire, al contempo, una serie di utili indicazioni atte a favorire un'adozione consapevole e responsabile dei servizi cloud, il Garante Privacy italiano, nel giugno 2012, ha pubblicato un vademecum informativo intitolato "*Proteggere i dati per non cadere dalle nuvole*", ove ha stilato un vero e proprio decalogo volto a facilitare la valutazione del rapporto rischi/cisti/benefici in sede preventiva rispetto all'adozione di tecnologie di cloud computing.

Brevemente, di seguito le indicazioni del Garante:

Il decalogo del Garante
Effettuare una verifica sull'affidabilità del fornitore. Gli utenti dovrebbero accertare: - **l'esperienza, la capacità e l'affidabilità del fornitore**; - la struttura societaria del fornitore, le referenze, le garanzie di legge offerte in ordine alla confidenzialità dei dati e alle misure adottate per assicurare la continuità operativa a fronte di eventuali e imprevisti malfunzionamenti; - Gli utenti dovrebbero valutare, inoltre, le **caratteristiche qualitative dei servizi di connettività di cui si avvale il fornitore in termini di capacità e affidabilità;** - Il cliente deve valutare **l'impiego da parte del fornitore di personale qualificato, l'adeguatezza delle sue infrastrutture informatiche e di comunicazione, la disponibilità ad assumersi una responsabilità risarcitoria in caso di eventuali falle nel sistema di sicurezza o di interruzioni del servizio**
Privilegiare i **servizi che favoriscono la portabilità dei dati**. In particolare, è consigliabile ricorrere a servizi di cloud computing privilegiando quelli basati su formati e standard aperti, che facilitino la transizione da un sistema cloud ad un altro, anche se gestiti da fornitori diversi.
Assicurarsi la **disponibilità dei dati in caso di necessità**. È opportuno chiedere che nel contratto con il fornitore siano ben specificate adeguate garanzie sulla disponibilità e sulle prestazioni dei servizi cloud.

Il decalogo del Garante
Selezionare i dati da inserire nella nuvola
Non perdere di vista i dati. È sempre opportuno che l'utente valuti accuratamente il tipo di servizio offerto, anche **verificando se i dati rimarranno nella disponibilità fisica dell'operatore con cui è stato stipulato il contratto oppure se questi svolga un ruolo di intermediario**, ovvero offra un servizio basato sulle tecnologie messe a disposizione da un operatore terzo
Informarsi su **dove risiederanno concretamente i dati**. È importante per l'utente sapere se i propri dati vengono trasferiti ed elaborati da server in Italia, in Europa o in un Paese extraeuropeo.
Attenzione alle clausole contrattuali. È importante valutare l'idoneità delle condizioni contrattuali per l'erogazione del servizio di cloud con particolare riferimento agli **obblighi e alle responsabilità in caso di perdita e di illecita diffusione dei dati custoditi nella "nuvola", nonché alle eventuali modalità per il recesso dal servizio e il passaggio ad altro fornitore**. Un elemento da privilegiare è senz'altro la **previsione di garanzie di qualità chiare, corredate da penali**, che pongano a carico del fornitore le eventuali inadempienze o le conseguenze di determinati eventi.
Verificare tempi e modalità di conservazione dei dati. In fase di acquisizione del servizio cloud è opportuno approfondire e prevedere nel contratto le politiche adottate dal fornitore riguardo ai tempi di conservazione dei dati.
Esigere adeguate misure di sicurezza. **In generale si raccomanda di privilegiare i fornitori che utilizzino modalità di archiviazione e trasmissione sicure, mediante tecniche crittografiche** (specialmente quando i dati trattati sono particolarmente delicati), **accompagnate da robusti meccanismi di identificazione dei soggetti autorizzati all'accesso.**
Informare adeguatamente il personale. Il personale, sia quello del cliente che quello del fornitore, incaricato del trattamento dei dati mediante servizi di cloud computing dovrebbe essere appositamente formato, al fine di limitare rischi di accesso illecito, di perdita di dati o, più in generale, di trattamento non consentito.

In piena rispondenza con le indicazioni del Garante Privacy, interessanti spunti di riflessione sui rischi connessi all'adozione di tecnologie cloud e sulle contromisure necessarie a prevenirli sono stati formulati dal Gruppo di Lavoro per la tutela dei dati personali ex art. 29 (organismo consultivo e indipendente, istituito dall'art. 29 della Direttiva 95/46/CEE, composto da un rappresentante delle autorità di protezione dei dati personali designate da ciascuno Stato membro, dal Garante europeo della protezione dei dati, nonché da un rappresentante della Commissione; d'ora innanzi: Art. 29 WP) con il parere n. 5 del 2012. In particolare, con riferimento agli obblighi di protezione dei dati nella relazione cliente/fornitore, l'Art. 29 WP ha posto l'attenzione sui seguenti aspetti:

- Trasparenza: costituisce uno dei principi fondamentali idonei a garantire equità e legittimità del trattamento dei dati. Di esso deve informarsi tanto il rapporto tra cliente cloud ed eventuali interessati – che per legge hanno diritto a conoscere l'identità del titolare, le finalità del trattamento e i destinatario o le categorie di destinatari dei dati, che possono

© Clusit 2015

comprendere incaricati e subincaricati del trattamento medesimo – tanto il rapporto tra cliente cloud, cloud provider ed eventuali ulteriori subcontraenti. Sotto tale ultimo profilo, il provider sarà tenuto a fornire un'informativa dettagliata e completa che comprenda, tra le altre cose, l'elenco dei responsabili e dei sub-responsabili, l'indicazione dei luoghi in cui i dati risiedono o possono essere trattati, nonché precise informazioni circa la comunicazione dei dati a terzi e il trasferimento dei dati in paesi fuori dall'Unione Europea.

- Specificazione e limitazione delle finalità del trattamento: i dati personali dovranno essere raccolti per finalità determinate, esplicite e legittime e successivamente trattati in modo non incompatibile e non eccedente rispetto a tali finalità.
- Conservazione e cancellazione dei dati: i dati personali dovranno essere conservati in modo da consentire l'identificazione degli interessati per un arco temporale non superiore a quello strettamente necessario al conseguimento delle finalità per le quali sono rilevati o successivamente trattati. I dati personali non più necessari dovranno essere cancellati o resi anonimi. Ove la cancellazione non sia possibile stante l'esistenza di precise norme di legge che impongono la conservazione (es. normative fiscali), l'accesso a tali dati dovrà essere bloccato. E' comunque responsabilità del cliente garantire ai soggetti interessati la cancellazione dei dati da parte del fornitore e dei sub-responsabili, ed il contratto tra cloud provider e cliente dovrà prevedere idonei meccanismi di cancellazione, quali la distruzione, la smagnetizzazione o la sovrascrittura.
- Tutele contrattuali nel rapporto tra titolare e responsabile del trattamento. Sotto questo profilo, l'Art. 29 WP elenca una serie di aspetti che dovranno essere disciplinato al minimo negli accordi predisposti dai cloud provider. Tra questi ricordiamo: SLA oggetti e misurabili corredati da effettive sanzioni; portata, modalità, finalità ed orizzonte temporale del trattamento; obbligo di riservatezza; obbligo del fornitore di indicare tutti i subcontraenti autorizzati e i luoghi ove risiederanno i dati, garantendo al contempo che gli accordi di subfornitura stipulati rispecchino i contenuti contrattuali dell'accordo sottoscritto con il cloud consumer; obbligo del fornitore di comunicare al cliente eventuali violazioni che possano costituire un rischio per i suoi dati.
- Adozione di adeguate misure tecniche ed organizzative. In relazione a tale aspetto, Ai sensi dell'arit. 17, par. 2, Direttiva 95/46/Ce, il cliente cloud, in qualità di titolare del trattamento, ha la piena responsabilità della scelta di fornitori che adottino misure di sicurezza tecniche ed organizzative adeguate a proteggere i dati personali, garantendone:
  - **la disponibilità**, cioè la garanzia di accesso tempestivo ed affidabile, approntando ogni misura idonea e necessaria a prevenire o mitigare le conseguenza di eventi come perdita accidentale di connettività, attacchi informatici, guasti accidentali dell'*hardware* e dei sistemi cloud di trattamento dati e altri problemi infrastrutturali;
  - **l'integrità**, cioè la garanzia in relazione all'impossibilità di alterazione volontaria o accidentale dei dati durante le operazioni di trattamento, archiviazione o trasmissione. L'autenticità dei dati può essere assicurata tramite meccanismi di autenticazione crittografica, quali codici di autenticazione di messaggi o firme;
  - **la riservatezza**, tramite il criptaggio dei dati, la predisposizione di meccanismi di au-

torizzazione ed autenticazione, la previsione di clausole contrattuali che impongano obblighi di riservatezza ai dipendenti del cliente, del fornitore e degli eventuali subfornitori;
- **l'isolamento**, inteso quale "limitazione della finalità" e prevenzione del rischio di divulgazione e trattamento dati per scopi illegittimi. Tale obbiettivo dovrebbe essere perseguito attraverso un'adeguata *governance* dei diritti e dei ruoli per l'accesso ai dati personali. Sotto questo profilo, andrebbe salvaguardato il c.d. "principio del privilegio minimo", in base al quale amministratori ed utenti devono poter accedere esclusivamente alle informazioni necessarie per le loro finalità legittime, restando invece preclusa la possibilità, anche solo per pochi di essi, di accedere all'intero sistema cloud.
- **la portabilità**, cioè la possibilità di migrare a nuovo fornitore, trasferendo sui suoi sistemi i dati precedentemente detenuti presso altro e diverso fornitore. Tale obbiettivo, volto a prevenire il fenomeno del c.d. *vendor lock-in*, dovrebbe essere perseguito tramite l'adozione di formati di dati standard ed interfacce che facilitano l'interoperabilità.

• Legittimità e sicurezza dei trasferimenti transfrontralieri di dati, la cui verifica è onere che incombe – come già detto – sul cliente cloud in quanto titolare del trattamento.

Come evidenziato dalle stesso Art. 29 WP, una certificazione indipendente effettuata da un terzo affidabile può essere un valido e credibile strumento sia dal punto di vista del fornitore – agevolato nel dimostrare la conformità dei propri servizi agli obblighi normativi vigenti in materia – sia dal punto di vista dell'utente – facilitato nel processo di comparazione tra le diverse offerte esistenti sul mercato.
Sotto questo profilo, accanto agli standard ISO/IEC 27001 e ISO/IEC 27002 in materia di gestione della sicurezza delle informazioni, degna di menzione è la recente pubblicazione, da parte dell'International Organization for Standardization, di una nuova certificazione – l'ISO/IEC 27018:2014 – specificamente diretta ai service providers di public cloud.
La finalità dichiaratamente perseguita da tale Standard *è quella di creare un set di regole, procedure e controlli attraverso cui i fornitori di servizi* cloud che, ai sensi della normativa europea in materia di privacy, agiscano in qualità di "data processor", possano garantire il rispetto degli obblighi di legge in materia di trattamento dei dati personali, fornendo al tempo stesso ai potenziali cloud service consumers un utile strumento comparativo per esercitare i propri diritti di verifica ed audit rispetto ai livelli di compliance normativa assicurati dal fornitore.
L'ISO 27018 richiama e specifica le best pactices già enucleate dall'ISO 27002 in materia di security policy, sicurezza organizzativa, fisica ed ambientale, gestione della continuità operativa, controllo degli accessi e sicurezza del personale, stabilendo inoltre, in aggiunta a queste, una serie di misure e controlli ulteriori non necessariamente destinati a tradursi in clausole contrattuali (la trasposizione dei contenuti dello Standard è, infatti, rimessa all'iniziativa del cloud provider che vi aderisce, trattandosi di misure non cogenti, ma destinate a trovare applicazione su base volontaria); ciò nondimeno è ragionevole prevedere che l'adesione alla Certificazione in commento costituirà un surplus distintivo rispetto alla generalità

© Clusit 2015

dei servizi offerti sul mercato, contribuendo alla diffusione prassi contrattuali e commerciali "virtuose" e conformi alla normativa di legge.
Tra le misure innovative enucleate dall'ISO 27018, da segnalare in particolare le seguenti:

ISO 27018
Il fornitore, in qualità di Responsabile del trattamento, deve prevedere strumenti idonei a consentire e facilitare l'esercizio, da parte dell'interessato, dei propri diritti di accesso, rettifica e cancellazione nei confronti del Titolare del trattamento (tipicamente, il cloud consumer)
In relazione alle finalità del trattamento, il fornitore deve garantire la rispondenza del trattamento alle sole finalità rese note al cliente in sede di contrattualizzazione del servizio, in particolare assicurando che i dati non verranno trattati per finalità che esulano quelle indicate dal cliente, né per finalità di marketing diretto o pubblicitarie, salvo che non vi sia esplicito consenso dell'interessato; consenso che, in ogni caso, non potrà mai costituire una condicio sine qua non imposta dal fornitore per la fruizione del servizio
Salvo eventuale divieto previsto per legge, la richiesta di divulgazione di dati personali proveniente da autorità amministrative o giudiziarie deve essere tempestivamente notificata al cloud service consumer
Relativamente alla materia del subappalto, lo Standard prevede, in maniera particolarmente incisiva, il diritto del cliente a conoscere, ancor prima di iniziare a fruire del servizio, l'intera catena degli eventuali subfornitori, i Paesi ove essi sono stabiliti, la localizzazione dei data center da essi utilizzati nonché gli obblighi degli stessi in relazione al trattamento dei dati. E', inoltre, riconosciuto al cliente il diritto di opporsi ad eventuali codifiche della catena dei subfornitori, ovvero di risolvere il contratto
Il fornitore deve tempestivamente notificare al cliente ogni violazione di dati personali da cui si derivata una perdita, distruzione, alterazione, divulgazione o accesso abusivo, al fine di consentire al Titolare ed eventualmente agli interessati di darne a loro volta notizia alle Autorità di controllo, nel rispetto dei tempi previsti dalla legge
Il contratto di servizio dovrà approntare una policy di transfer back che dettagli le modalità di restituzione, trasferimento e/o cancellazione dei dati detenuti dal fornitore alla cessazione degli effetti del contratto medesimo
In relazione alle misure di sicurezza delle informazioni, sarebbe opportuno che tutto il personale del fornitore e degli eventuali subfornitori fosse vincolato da specifici accordi di riservatezza, ricevesse adeguata formazione, accedesse ai dati mediante specifiche operazioni di autenticazione e logging

Return on Security Investment

A cura di Alessandro Vallega

Un tema centrale per comprendere le prospettive della Sicurezza ICT in Italia e nel mondo, è relativo alla comprensione delle logiche di investimento aziendale, al modo in cui si valuta il ritorno (ROI) dei progetti e alle difficoltà di ricondurre gli investimenti in sicurezza a tali logiche, ovvero alla difficoltà di farne un calcolo matematico. Nella maggior parte dei casi essa viene assimilata ad un costo senza alcun ritorno e quindi, nella normale logica del Business, da evitare o ridurre il più possibile. Capire questi aspetti è importante per molti motivi. E' importante per il responsabile della Sicurezza ICT (il cosidetto CISO - Chief Security Information Officer) affinché possa definire delle strategie ed obiettivi coerenti e quindi sostenibili e raggiungibili; è importante per il Top Management affinché possa superare i limiti degli approcci attuali e, infine, è importante per i revisori, i sindaci, gli analisti, il pubblico e il mercato, che spesso vedono o subiscono i nefasti effetti della mancanza di sicurezza e dovrebbero agire o influire per cambiare lo status quo.

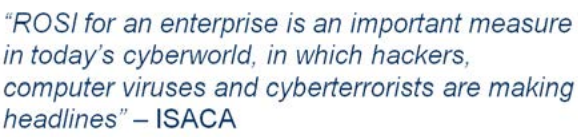


Figura 1: Return On Security Investment[1]

In questi ultimi anni osserviamo un ampio ridisegno dei sistemi informativi dovuto all'adozione di nuovi modelli di business o di go to market. Le aziende rinnovano i canali e sfruttando la tecnologia mobile, social, big data, cloud fanno utili in nuovi modi. Si parla di trasformazione digitale. In questi casi tali servizi dovrebbero essere sicuri per definizione: ad esempio sarebbe inammissibile, oggi, rendere disponibile una Payment App insicura. In tali casi il ROI viene calcolato sull'investimento complessivo e il costo della sicurezza concorre solamente a definire il montante dei costi. In pratica non viene fatta l'analisi del ROI della nuova App senza la sicurezza.

Il problema del ROSI si pone quindi nei casi in cui l'investimento in sicurezza non può essere direttamente relazionato alla trasformazione digitale. Ma questi casi sono numerosi e importanti. Il problema è che gli attuali sistemi sono ampiamente insicuri, essendo stati creati in un periodo di forte e convulsa innovazione tecnologica e nel quale il pericolo cyber non era ancora reale. Infine a ben vedere anche la trasformazione digitale non avviene nel vuoto ma i nuovi servizi si appoggiano agli attuali sistemi informativi e li accrescono; non

[1] Da G41 Return on Security Investment (ROSI) Effective 1 May 2010

sarebbe saggio costruire su delle scarse fondamenta, ma è sicuramente difficile attribuire al prossimo singolo progetto di trasformazione digitale tutto il costo necessario a sanare la scarsa qualità dell'intero sistema informativo.
Fatta questa premessa, ed escluso il fortunato caso della trasformazione digitale, proviamo ad approfondire le logiche di calcolo del ROSI.
Quando si parla di investimenti ci si pone il problema di calcolarne il ritorno per poter valutare le diverse alternative. In linea di principio conviene scegliere la cosa che ha un maggiore e più rapido ritorno econonico. Una delle formule più utilizzate è quella del Return on Investment (ROI) che compara il margine con il costo necessario per realizzarlo e quindi sottrae i costi dal ricavo e divide il risultato per il costo. L'imprenditore o il manager possono quindi più facilmente decidere se effettuare una scelta A oppure B, se rinnovare la catena di montaggio oppure se realizzare il nuovo sito di eCommerce.

$$ROI = \frac{\text{Expected Return} - \text{Cost of Investment}}{\text{Cost of Investment}}$$

Figura 2: formula del ROI

Purtroppo nello specifico caso degli investimenti in Sicurezza ICT la difficoltà sta nel valorizzare i ricavi. Installare una soluzione di data loss prevention che beneficio porterà? Sicuramente non un ricavo ma semmai la riduzione di un possibile danno. Qui le cose si complicano perché è difficile calcolare tre fattori chiave: il valore del danno possibile, la probabilità di incorrervi senza la soluzione di data loss prevention e la probabilità residua ovvero quella di incorrervi ugualmente nonostante la nuova tecnologia.
Nell'esperienza degli esperti interpellati, nel 2009 (all'epoca del primo Security Summit) le aziende non calcolavano il ROI della Sicurezza, non lo facevano nel 2012 (primo Rapporto Clusit) e non lo fanno tuttora. Tutti però concordano che sarebbe utile disporre di un metodo per poterlo fare e in Internet e presso le associazioni professionali si trovano numerosi paper e guidelines. Tra gli altri segnalo una nostra pubblicazione in italiano (AIEA, Clusit, Deloitte, Ernst & Young, KPMG, Oracle e PricewaterhouseCoopers – http://rosi.clusit.it) del 2011 che ha avuto il merito di evidenziare le difficoltà e di dare qualche suggerimento comportamentale al CISO[2].
Che criterio usa allora l'azienda per decidere gli investimenti in sicurezza? Ed è utile insistere nel tentativo di calcolare il ROSI?

[2] ROSI Return on Security Investments: un approccio pratico. Come ottenere Commitment sulla Security http://rosi.clusit.it/views/Homepage.html

Le motivazioni per le quali un'azienda investe in Sicurezza ICT si possono ricondurre ad un mix di queste quattro:
1 Ridurre il Rischio
2 Garantire la Compliance
3 Proteggere il Brand
4 Ridurre i costi dei controlli

Ridurre il Rischio

Si investe per ridurre la possibilità o le conseguenze di un attacco o incidente informatico avendo la consapevolezza del valore per se e per gli altri dei beni da custodire. Quindi un investimento oculato dovrebbe essere preceduto da un'analisi del rischio, una classificazione dei dati e dall'inventario degli asset[3], tutte attività sicuramente utili ma che richiedono un salto culturale e un investimento non semplice da attuare.

In azienda i dirigenti più interessati da questo aspetto dovrebbero essere il Chief Financial Officer (CFO – direttore finanziario), il Chief Risk Manager (CRM – responsabile dei rischi) e i vari direttori di funzione, ognuno per la propria area (CxO).

Alcuni metodi per il calcolo del ROSI considerano che gli incidenti informatici siano numerosi ma nel contempo non producano singolarmente molti danni e quindi tali metodi possono permettersi di moltiplicare la probabilità di incidente con il danno causato con e senza l'investimento di sicurezza. Purtroppo essi prestano il fianco al grande evento nefasto e poco probabile[4] che produce un danno multimilionario e che **è** in grado di compromettere la sussistenza stessa dell'azienda[5].

Inoltre il concetto di probabilità va bene quando ci si rapporta a certe categorie di eventi, come per esempio alla probabilità di fare ambo giocando al Lotto, ma presenta dei seri limiti quando dall'altra parte c'è un attaccante che mette in gioco la sua intelligenza contro le nostre contromisure. In tale situazione sarebbe utile valutare la probabilità di essere violati anche in funzione (dello skill dell'attaccante e) del suo impegno contro di noi visto come una funzione dell'appetibilità dei nostri asset[6].

---

3 I primi 100 giorni del Responsabile della Sicurezza delle Informazioni; http://100giorni.clusit.it/views/Homepage.html

4 Una lettura interessante è quella del "Il cigno nero. Come l'improbabile governa la nostra vita" di Taleb Nassim N.

5 Numerosi degli attacchi presentati nel Rapporto Clusit degli anni passati sono costati più di 100 milioni di euro solo come danno diretto. Quale azienda italiana è in grado di permetterseli? Inoltre tendono ad essere pubblici solo quelli che compromettono i diritti di terzi (ad esempio i cittadini dei quali viene trafugata la carta di credito), mentre la perdita di segreti commerciali a favore della concorrenza (ad esempio la lista dei clienti più profittevoli) e quelli industriali (progetti, piani, altri segreti) rimangono più facilmente sconosciuti e quindi non sono stati pubblicati nel Rapporto Clusit.

6 Ringrazio Sergio Fumagalli – Zeropiù e Andrea Longhi - ConsAL per i loro commenti e rimando ad una interessante lettura di Bruce Schneier http://bit.ly/ROSIBRUCE

© Clusit 2015

Normalmente chi investe in sicurezza per ridurre il rischio lo fa senza appoggiarsi ad un'analisi formale dello stesso, senza alcuna data classification e senza un inventario degli asset, con la sola marginale eccezione di qualche istituto bancario che piano piano vi ci si avvicina. Inoltre si tende a proteggere la parte più esposta ad internet dell'infrastruttura IT, in quanto questi incidenti sono molto visibili e più facilmente comprensibili dal management e quindi ricevono più facilmente le risorse necessarie, ma ciò lascia l'azienda vulnerabile agli attacchi che partono (o che transitano) dall'interno.

Garantire la Compliance

Si investe in specifiche misure di sicurezza per obblighi imposti da terzi. Questi possono essere gli Stati tramite le leggi, varie autorità locali o internazionali come quella per la Protezione dei Dati Personali (la Privacy), l'Unione Europea tramite la definizione di regolamenti e direttive da declinare localmente in modi differenti, oppure tra soggetti economici collegati con regole concordate o forzate commercialmente (ad esempio quelle sulla protezione delle carte di credito). Inoltre possono essere obblighi auto-imposti, per esempio dalla capogruppo oppure per scelta di business per ottenere alcuni vantaggi come quelli legati ad una certificazione ISO. Limitando queste considerazioni al primo caso (obblighi esterni), si osservano due cose: la prima è che normalmente le compliance tendono a definire regole per proteggere i diritti di terzi che interagiscono con l'azienda. E' il caso della Privacy che definisce come proteggere i dati personali dei propri clienti, delle regole sull'accesso ai sistemi di controllo delle infrastrutture critiche per evitare danni ai cittadini e sulla qualità dei crediti della banca per proteggere il sistema economico intero. Questo implica che la compliance non si preoccupa della salute di un'azienda in quanto tale, ma che si limita a proteggere i soggetti con i quali l'azienda interagisce e quindi **è normale** che alcuni aspetti di sicurezza molto importanti siano lasciati alla discrezionalità del management, che deve o dovrebbe preoccuparsene (per ridurre il rischio).

La seconda cosa osservata **è che** fortunatamente le compliance stanno lentamente migliorando nella loro formulazione grazie ad un certo grado di concertazione effettuato tramite le consultazioni pubbliche, i forum industriali, i gruppi di interesse e il riferimento alle best practice internazionali. Compliance scritte all'inizio degli anni 2000 includevano prescrizioni del tipo "La parola chiave, quando è prevista dal sistema di autenticazione, è composta da almeno otto caratteri oppure, nel caso in cui lo strumento elettronico non lo permetta, da un numero di caratteri pari al massimo consentito" mentre quelle più moderne possono recitare "progettando, sviluppando e manutenendo i servizi di pagamento via internet, i fornitori (...) dovrebbero prestare attenzione speciale ad una adeguata separazione (dei compiti) degli ambienti IT di sviluppo, test e produzione e ad una precisa implementazione del principio del minimo privilegio alla base di una robusta gestione delle identità e dell'accesso"[7].

[7] http://www.ecb.europa.eu/pub/pdf/other/recommendationsforthesecurityofinternetpaymentsen.pdf?d9d3c572d5484d0767b39d8d84c7d2c9

Queste nuove formulazioni possono consentire ad una azienda di trasformare un obbligo in opportunità, ovvero di poter utilizzare, con un minimo sforzo aggiuntivo, le stesse misure adottate per obblighi di compliance (diritti di terzi) con quelle adottabili per considerazioni di rischio operativo (diritti propri). Una ricerca realizzata l'anno scorso dal PMI-NIC (Project Management Institute, Northern Italy Chapter) e da Clusit, già riportata nel Rapporto Clusit 2014 indicava che il 48% degli investimenti in Sicurezza IT[8] viene realizzato per motivazioni di compliance e che il 47,7% per motivazioni di rischio. Questo indica che si fa ancora molto sulla compliance e che vale la pena approfittarne.

Il calcolo del ROSI nella compliance potrebbe interessare al Chief Executive Officer (CEO – direttore generale) e al Chief Compliance Manager (CCM) e dovrebbe considerare gli effetti negativi della mancanza di compliance (valore economico delle multe comminabili, effetti personali sugli individui apicali, effetti sull'azienda in forza della responsabilità delle persone giuridiche per il decreto legislativo 231/01 ed infine sull'immagine aziendale) ed eventualmente anche quelli positivi diretti (poter dichiarare il rispetto di una compliance aumenta la fiducia dei propri interlocutori e l'immagine aziendale). Essere certificati ISO 27001 può costituire un vantaggio competitivo e ridurre i costi derivanti dagli audit interni e/o di terze parti.

Negli anni passati, in Italia, numerosi investimenti in sicurezza ICT sono stati guidati dall'operosa produzione dell'Autorità Garante dei Dati Personali di Provvedimenti o Linee Guida generali (ad esempio Amministratori di Sistema[9]) o di industry (ad esempio FSE[10] e Tracciamento operazioni bancarie[11]). Negli ultimi due anni sono state dedicate molte attenzioni da parte delle banche al quindicesimo aggiornamento della circolare 263 della Banca d'Italia che recita nella premessa "A tal proposito, le banche valutano l'opportunità di avvalersi degli standard e best practices definiti a livello internazionale in materia di governo, gestione, sicurezza e controllo del sistema informativo." Il settore finanziario sarà in futuro ancora oggetto di accresciute compliances generali o specifiche che avranno un forte impatto sui sistemi informativi. Per tutti i settori industriali, invece, siamo in attesa del nuovo Regolamento europeo sulla Privacy che, tra altre importanti cose, nella corrente formulazione, pone molta enfasi sulla Privacy by Design e sulla notifica obbligatoria agli interessati dei data breach (fughe di dati). Infine i grandi temi legati alla mobilità (e ai pagamenti in mobilità), al (public) cloud, ai big data, ai social e all'internet delle cose, saranno affrontati dal legislatore e dalle aziende con nuove compliance e con nuove regole contrattuali.
La compliance accompagnerà per molti anni gli investimenti IT nell'industria.

---

8 In Italia, secondo i 286 project manager certificati che hanno risposto. Risposta singola.

9 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1577499

10 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1634116 e http://fse.clusit.it/views/Homepage.html

11 http://www.garanteprivacy.it/web/guest/home/docweb/-/docweb-display/docweb/1813953

Proteggere il Brand

Si investe in certe misure di sicurezza per proteggere il marchio, la fama della propria azienda e aumentare o mantenere la fiducia che i consumatori o i clienti hanno verso la stessa. Le aziende italiane, secondo l'esperienza diretta e la sopra citata ricerca PMI-NIC / Clusit, non sono quasi interessate a proteggere il proprio brand tramite la sicurezza ICT. Il nesso tra le due cose non è ancora stato da loro pienamente compreso. E' però probabile che la situazione in futuro cambi e la cosa possa interessare sia al Chief Executive Officer (CEO – direttore generale) sia al Chief Marketing Officer (CMO) per via degli effetti della nuova Privacy europea menzionata in precedenza, unitamente ad un generale aumento delle capacità relazionali globali dell'azienda (per via di un incremento dell'eCommerce e dell'uso del canale Social-Mobile per attrarre clienti). In diversi settori industriali, in presenza di una riduzione costante della marginalità, è infatti necessario creare i presupposti di fiducia nel brand per poter attuare strategie di upsell e cosell. Un eventuale calcolo del ROSI dovrebbe riuscire a dare un valore economico al danno di immagine a fronte di un incidente di sicurezza ICT considerando la probabilità che tale incidente diventi di pubblico dominio e stimando la reazione (spontanea o meno[12]) dei consumatori e di altri attori su Internet.

Ridurre i costi dei controlli

In quest'ultima categoria si includono quegli investimenti in sicurezza tesi a ridurre il costo dei controlli o per aumentare la qualità e l'efficacia degli stessi. Si pensi per esempio alla produzione manuale di report di audit in cui devono essere censiti tutti gli utenti abilitati ad accedere ad un certo insieme di sistemi informativi verificandone nel dettaglio i privilegi e le incompatibilità (segregation of duties). Quanto lavoro si è disposti a pagare per ottenere una certa qualità dei controlli?

Per il primo aspetto, ovvero quello della riduzione del costo, il ROSI è facile da calcolare utilizzando la classica definizione del ROI (***Figura 2: formula del ROI***); per il secondo, le cose si complicano nuovamente.

1. Ognuna delle quattro motivazioni all'investimento presenta caratteristiche e problematiche diverse di calcolo del ROSI. Raccogliere e definire gli elementi per il calcolo è molto complesso.
2. Ogni motivazione interessa un diverso insieme di attori aziendali e ciò complica l'approvazione degli investimenti perchè non c'è un singolo budget dal quale attingere per i progetti più impegnativi
3. Fortunatamente, soprattutto grazie ad una compliance più matura, le misure di sicurezza stanno convergendo portando valore in più punti

[12] Un modello completo dovrebbe tenere conto anche dei comportamenti dei concorrenti e delle autorità.

Valutare il risparmio di costo è interessante per chi normalmente lo deve sostenere e in quest'area di solito si pensa al Chief Information Officer (CIO – il responsabile dei sistemi informativi) o al CEO (Direttore Generale) e al CFO (Direttore Finanziario). Quest'ultimo in particolare quando, come capita, i controlli siano relativi all'area contabile e amministrativa sulla quale insistono alcune compliance (per le aziende quotate in borsa) e dove maggiore è il rischio di frode legata direttamente al denaro. Esiste purtroppo, nella grande maggioranza dei casi, una netta sproporzione tra il costo del progetto (licenze software, forza lavoro e manutenzione) e il suo ritorno economico e raramente un'azienda trova conveniente investire solamente per questa motivazione.

Considerazioni finali

Vista la complessità del calcolo, è difficile investire in Sicurezza ICT sulla base di sole considerazioni economiche come talvolta viene chiesto dal Top Management. Le aziende che investono in sicurezza lo fanno per un accresciuta consapevolezza di quello che può avvenire senza sicurezza. In questi anni la crescente interconnessione dei sistemi informativi, la scomparsa del perimetro aziendale e la consumerizzazione hanno sottoposto le nostre aziende a nuove sfide di sicurezza. Purtroppo a volte esse sono state danneggiate senza neanche essersene accorte, come quando hanno subito un furto di segreti e di proprietà intellettuale. Ormai nessuno dovrebbe più credere "a me non capita", "i miei dati non sono interessanti per un attaccante".

Utilizzando un approccio pratico, invece che calcolare matematicamente il ROSI dei singoli investimenti in sicurezza sarebbe meglio definire dei criteri per l'ottimizzazione nel lungo periodo, per capire quali sono le aree maggiormente vulnerabili e dove destinare un budget che deve essere sicuramente incrementato. Ovvero trovare dei criteri per allocare in maniera intelligente le risorse disponibili nel breve e nel medio-lungo periodo.

E' molto importante capire che bisogna implementare un ecosistema organizzativo e tecnologico in grado di proteggere l'azienda dagli attacchi e dagli incidenti che possono comprometterne la disponibilità (abbastanza riconosciuti perchè sono molto visibili, ad esempio un distributed denial of service), ma anche l'integrità (una frode condotta utlizzando in maniera illecita un'applicazione) e la riservatezza (la più difficile da scoprire; data breach, furto di segreti industriali) e che le misure per proteggere e monitorare le risorse vanno distribuite in profondità, dal perimetro di rete, ai dispositivi, i server, lo storage, le basi dati e i file system, i sistemi operativi, le App e le applicazioni...

Non credo che le aziende agiscano per motivazioni esclusivamente razionali ed esclusivamente economiche. In realtà il comportamento del soggetto collettivo è frutto dell'interazione di molteplici interessi e convinzioni da parte dei dipendenti e di altri stakeholder. E' quindi necessario continuare a parlare del ROSI[13]: il ritorno sarà che l'azienda potrà continuare ad operare nel mercato, rispettata e attenta ad impedire che altri possano danneggiare le terze parti collegate.

[13] http://bit.ly/ROSIALE

L'impatto della Direttiva 263/agg.15 di Banca d'Italia sugli operatori del settore bancario

A cura di Luca Bechelli, Luca Boselli e Claudio Telmon

Premessa

Nell'estate del 2013, Banca d'Italia ha emesso un aggiornamento alla Circolare n. 263/2006 «Nuove disposizioni di vigilanza prudenziale per le banche» (Aggiornamento n. 15 del 2 Luglio 2013). La Circolare è un riferimento fondamentale per le banche: oltre a fornire indicazioni specifiche rispetto alle aree oggetto di verifica ispettiva, i contenuti del documento si configurano anche come possibili linee guida di indirizzo su diversi ambiti. L'aggiornamento n. 15 integra il Titolo V della Circolare con tre nuovi capitoli, dedicati rispettivamente al sistema dei controlli interni (Capitolo 7), al sistema informativo (Capitolo 8), ed alla continuità operativa (Capitolo 9).

Per quanto riguarda il contesto della sicurezza informatica, si possono individuare due punti di rilievo:

- l'introduzione del concetto di gestione del rischio come cardine nella gestione dell'operatività della banca, in particolare allineandosi con valutazioni complessive e strategiche di più alto livello come la "propensione al rischio " della banca stessa;
- l'ulteriore riconoscimento dell'importanza dei sistemi informativi nell'operatività bancaria, che richiede conseguentemente una gestione dei rischi IT in generale, e dei rischi di sicurezza IT in particolare, allineata alla gestione degli altri rischi operativi.

Il Capitolo 8, sul quale ci focalizziamo (il Capitolo 9 razionalizza un insieme di misure già da tempo indirizzate in modo settoriale), si può idealmente considerare che affronti il tema sotto due aspetti:

- un insieme di controlli obbligatori che costituiscono una sorta di "baseline" o di "misure minime" che devono essere necessariamente implementate, come quelle previste nell'ambito dei pagamenti elettronici;
- un'indicazione dell'adozione di logiche di gestione del rischio per quanto riguarda i rischi IT in generale, e quindi anche per quanto non specificamente coperto dai controlli obbligatori di cui sopra, la cui selezione e implementazione segue peraltro comunque logiche di gestione del rischio.

La gestione del rischio IT

All'interno delle disposizioni sul sistema informativo (Capitolo 8), **l'analisi del rischio informatico** costituisce un aspetto chiave, in cui il tema della sicurezza e della protezione delle risorse ICT assume una valenza non solo operativa ma anche strategica: la normativa stessa sottolinea come un sistema informativo sicuro consenta di sfruttare le opportunità offerte dalla tecnologia per ampliare e migliorare i prodotti e servizi per la clientela, e l'analisi dei rischi è lo strumento a garanzia dell'efficacia e dell'efficienza delle misure di protezione delle risorse ICT.

Alla luce delle date previste da Banca d'Italia per le attività di adeguamento, nei prossimi mesi è ragionevole attendersi un consolidamento ed un affinamento di quanto predisposto in questi ultimi anni in termini di processi, metodologie e strumenti.
In quest'ottica, con riferimento all'insieme dei requisiti previsti per l'attività di analisi del rischio, è possibile perciò evidenziare alcuni aspetti la cui evoluzione sarà da monitorare con attenzione:

- **Integrazione con il modello generale di valutazione e gestione dei rischi**: gli approcci metodologici adottati dalla banche per l'analisi dei rischi informatici dovranno essere in grado di raccordarsi con gli altri processi aziendali di valutazione integrata dei rischi aziendali, ed in particolare con il modello di Risk Appetite Framework previsto dalla Circolare. Assumono perciò rilevanza alcuni aspetti legati alle metodologie di analisi dei rischi adottate dalle banche:
  - *Il tipo di approccio metodologico per la valutazione del rischio potenziale e del rischio residuo*, ed in particolare i benefici e le difficoltà legati all'adozione di approcci quantitativi o qualitativi. E' ipotizzabile come inizialmente sia necessario basare le proprie valutazioni del rischio su stime di natura qualitativa, laddove spesso non risultino disponibili basi informative quantitative su cui basare il processo di analisi (ad esempio, le modalità di raccolta e analisi delle informazioni relative agli incidenti di sicurezza informatica non sempre consentono di far leva su indicatori quantitativi per stimare con maggiore precisione le probabilità di accadimento di determinati eventi ed i relativi impatti). Tuttavia, poiché l'analisi dei rischi dovrà consentire di graduare le misure di mitigazione ed i relativi investimenti in funzione del profilo di rischio, diventerà fondamentale poter disporre di informazioni che consentano agli organi decisionali della banca (in particolare, all'organo con funzione di supervisione strategica ed all'organo con funzione di gestione, così come previsti dalla normativa) di stimare la propensione al rischio informatico e di attuare politiche di trattamento integrate e coerenti rispetto alle più ampie strategie aziendali.
  - *La qualità delle informazioni raccolte nel processo di analisi dei rischi*. Così come avviene all'interno di processi di controllo più maturi (si pensi, ad esempio, all'ambito dei rischi operativi), sarà necessario garantire al management di disporre di informazioni dettagliate, pertinenti e aggiornate per l'assunzione di decisioni consapevoli.
- **Implementazione operativa del processo di valutazione e gestione del rischio:** la "messa a regime" del processo rappresenterà una sfida significativa, alla luce di una serie di aspetti da considerare preventivamente:
  - *Complessità organizzativa del processo*. La normativa richiede espressamente il coinvolgimento di diversi attori all'interno del processo di valutazione e gestione del rischio (utente responsabile, personale ICT, funzioni di controllo, ecc.). Se da una parte ciò consente alla sicurezza di uscire dai confini di un mondo puramente tecnologico, dall'altra occorrerà garantire adeguate modalità di coordinamento, comunicazione e di validazione delle informazioni e delle stime raccolte. Questo elemento di complessità dovrà essere perciò gestito attentamente, al fine di sfruttare al meglio l'occasione di

© Clusit 2015

stimolare la diffusione di una maggiore sensibilità sul tema della sicurezza.

- *Impegno operativo.* Benché esistano situazioni molto differenti in termini di maturità degli attuali processi di analisi e gestione del rischio informatico, è facilmente ipotizzabile come sarà richiesto un impegno consistente nell'effettuazione delle attività di analisi sull'intero perimetro dei sistemi informativi aziendali. Inoltre, trattandosi di attività da ripetersi periodicamente, sarà necessario dotarsi di una struttura adeguata rispetto al contesto (risorse, competenze, strumenti di supporto, ecc.).
- *Modalità di rappresentazione e comunicazione dei risultati delle analisi dei rischi.* Le banche dovranno definire una serie di passaggi formali che prevedono il coinvolgimento attivo di referenti che spesso non hanno avuto modo in passato di acquisire dimestichezza con specifiche tematiche di sicurezza informatica: a tal proposito, basti pensare all'attività di accettazione formale di un eventuale rischio residuo dell'utente responsabile, oppure alla definizione della propensione al rischio o all'approvazione annuale del rapporto sintetico sulla situazione del rischio informatico da parte dell'organo di supervisione strategica. Diverrà perciò fondamentale attuare delle specifiche attività di sensibilizzazione nonché adottare approcci e modalità di comunicazione adeguati che consentano, ad esempio, di tradurre eventuali criticità di sicurezza tecnologica in un linguaggio quanto più vicino a quello del business.

La gestione della sicurezza informatica

La particolarità della Circolare rispetto ad altre normative generali e di settore può essere individuata nel fatto che essa è meno incentrata sull'elencazione di misure "minime" da adottare, quanto piuttosto nel definire un modello di gestione del sistema informativo che riconosce la centralità della sicurezza ICT. Nell'omonima sezione "Gestione della sicurezza informatica" si definisce l'obiettivo di "preservare la sicurezza delle informazioni e dei beni aziendali, a garantire a ciascuna risorsa informatica una protezione, in termini di riservatezza, integrità, disponibilità, verificabilità e accountability, appropriata e coerente lungo l'intero ciclo di vita" e "contribuire alla conformità del sistema informativo".

La stessa gestione del rischio informatico diventa lo strumento centrale di decisione e gestione del sistema informativo, con un perimetro che comprende evidentemente anche i rischi di sicurezza ICT, i cui risultati sono portati tanto all'Organo con Funzione di Gestione (OFG; in genere, il Direttore Generale) che all'Organo con Funzione di Supervisione Strategica (OFSS; in genere, il Consiglio di Amministrazione) con frequenza almeno annuale.

La gestione del rischio informatico **è alimentata anche dal Processo di Gestione degli Incidenti, con lo scopo di contestualizzare la valutazione di impatti e probabilità. La gestione degli incidenti a sua volta si raccorda con il monitoraggio di sistemi, accessi e operazioni** nonché con la gestione dei malfunzionamenti e delle segnalazioni di problemi, per individuare le possibili iniziative di prevenzione. Peraltro, è significativo che i gravi incidenti di sicurezza informatica diventano oggetto di reporting alle figure apicali della Banca, o addirittura alla stessa Banca d'Italia.

Non stupisce, pertanto, rilevare come la Policy di Sicurezza Informatica diventi un docu-

mento soggetto all'approvazione dell'OFSS, per altro assieme alla metodologia di analisi del rischio informatico, evidentemente con finalità di maggior commitment e consapevolezza degli organi apicali su una tematica di così ampia rilevanza. Di tale policy la Circolare definisce i principali contenuti, richiamando la "propensione al rischio informatico" come strumento per definire gli obiettivi aziendali di sicurezza.
Dal punto di vista organizzativo, si afferma il principio di "indipendenza di giudizio rispetto alle funzioni operative" della funzione di sicurezza informatica, tramite "un'adeguata collocazione organizzativa". Se, da un lato, tale funzione non è del tutto chiaramente identificata, in quanto nella maggior parte delle organizzazioni le responsabilità definite dalla Circolare sono attribuite a più soggetti (es: "segue la redazione delle policy di sicurezza" e "segue lo svolgimento dei test di sicurezza prima dell'avvio in produzione di un nuovo sistema"), dall'altro è evidente lo scopo del Regolatore di assicurare che tali responsabilità siano correttamente collocate, anche se distribuite, nell'organizzazione interna.
L'approccio orientato alla gestione della sicurezza è ancora più evidente nell'ambito del processo di gestione dei cambiamenti: esso è normato nella sezione "Gestione della sicurezza informatica", quasi a ribadire il legame stretto delle ricadute di una buona gestione nella protezione degli asset aziendali: infatti, in questo ambito le misure da adottare potrebbero benissimo essere tratte sia da un manuale di IT Service Management sia da una best practice di sicurezza. Lo stesso si può dire della sezione relativa alla "disponibilità delle informazioni e delle risorse ICT", che oltre a trattare dei backup, della progettazione e realizzazione di architetture prive di SPOF, disaster ricovery etc…, non manca di ribadire l'importanza del capacity planning.
Riguardo alle misure di sicurezza vere e proprie, si rimanda il lettore al testo della Circolare: esse sono una sintesi degli obiettivi di protezione che sono evidentemente ispirati ai principali standard e best practice di settore, pur comprendendo alcune misure puntuali riconducibili a tematiche di particolare rilevanza per il contesto bancario. Nella maggior parte dei casi, la Circolare non definisce "l'intensità dei presidi da porre in atto" che dovranno dipendere "dalle risultanze del processo di analisi dei rischi". Faranno piacere agli esperti del settore i richiami ai concetti di "difesa in profondità", oltre ai più classici "need to know", "minimo privilegio", "separazione degli ambienti" e "separazione dei compiti", che devono essere attuati anche nell'ambito delle procedure operative. Di nota sono l'uso di account univoci, la segmentazione della rete ed il controllo dei flussi, misure di contrasto ai *denial of service* distribuiti, l'adozione di metodologie e tecniche per lo sviluppo sicuro, il monitoraggio continuativo delle minacce e le regole di tracciabilità delle azioni svolte a supporto di verifiche ex post, nonché requisiti puntuali sulle applicazioni di informatica utente.
Solo, infine, ad una lettura approfondita non sfuggirà al lettore della Circolare l'intensità della relazione tra sicurezza e qualità dei dati a cui tende il Regolatore nei requisiti definiti per la c.d. Data Governance, che ha tra gli obiettivi assicurare "nel continuo l'integrità, completezza e correttezza dei dati conservati e delle informazioni rappresentate;"(…) e garantire " l'accountability e l'agevole verificabilità delle operazioni registrate". Insomma: data quality, certamente, ma anche sicurezza dell'informazione a tutto tondo.

© Clusit 2015

Le Raccomandazioni della Banca Centrale Europea

All'interno del Capitolo 8, la Circolare integra in modo molto sintetico[1] le Raccomandazioni della BCE "sulla sicurezza dei pagamenti via Internet".

Le Raccomandazioni vanno inquadrate nell'integrazione in corso a livello europeo nell'ambito della vigilanza bancaria. Alla data di emissione dell'Aggiornamento alla Circolare, la Banca Centrale Europea aveva in carico competenze in base alle quali aveva emesso le succitate Raccomandazioni, ed aveva in programma l'emissione di due ulteriori Raccomandazioni: una relativa ai pagamenti via *mobile*, l'altra relativa ai "*payment account access services*"[2]. La materia è complessa, particolarmente per l'ultimo caso, ed in effetti finora le Raccomandazioni sulla sicurezza dei pagamenti via Internet sono le uniche che abbiano visto la luce. Nel frattempo, la competenza è passata all'European Banking Authority. L'EBA quindi, ha pubblicato delle nuove raccomandazioni, senza variazioni sostanziali ma prevedendo la possibilità di una successiva integrazione, anche in considerazione di un prossimo aggiornamento della Direttiva Europea sui servizi di pagamento[3] (PSD2). Come si vede, il quadro normativo è in evoluzione, e le banche devono adeguarsi ad indicazioni anche puntuali (e non sempre chiarissime) tenendo conto di questa fluidità, per evitare di fare investimenti che non risultino poi adeguati a fronte di nuovi requisiti posti anche a breve distanza temporale da quelli appena soddisfatti.

Le Raccomandazioni della BCE integrate nella Circolare sono riferite all'ambito specifico dei pagamenti via Internet, escludendo quindi ad esempio le "App" per smartphone, ma includendo per contro l'accesso da smartphone via browser. Il discriminante è quindi il tipo di front-end del servizio o, se vogliamo, il tipo di client. L'ambito non è quindi di facile perimetrazione per molte banche, che hanno un'offerta di servizi online estremamente integrata fra i diversi canali (Internet, mobile, smart TV o altro). L'adeguamento alle Raccomandazioni potrebbe quindi andare a toccare ambiti che saranno presumibilmente oggetto di requisiti posti dalle norme di prossima emanazione (ad esempio, sui pagamenti via *mobile*), requisiti che saranno sperabilmente integrativi e non incompatibili, ma che comunque richiedono di valutare i progetti di adeguamento in una prospettiva un po' più ampia che non di semplice conformità alla normativa finora emessa. Il perimetro dei pagamenti via Internet suggerisce anche un altro aspetto, e cioè che le Raccomandazioni affrontano una tipologia di servizio la cui sicurezza è rilevante per il cliente, anche se non risulta essere di particolare impatto per la banca: l'impatto economico degli eventi di phishing, ad esempio, nell'economia complessiva di una banca è piuttosto marginale, mentre invece è molto rile-

---

1 L'integrazione avviene, oltre che tramite la citazione delle Raccomandazioni fra le fonti normative, attraverso una semplice nota a pié di pagina che recita: "Con riferimento ai servizi di pagamento tramite internet si applicano le già citate *Recommendations for the security of internet payments*. emanate dalla BCE". L'integrazione avviene quindi, fra l'altro, senza una traduzione in italiano che fornisca un'interpretazione "autentica" di alcuni termini o concetti espressi in inglese.

2 Servizi di accesso ai conti, http://www.ecb.europa.eu/press/pr/date/2013/html/pr130131_1_response.en.html

3 http://ec.europa.eu/finance/payments/framework/index_en.htm

vante per i singoli clienti che li subiscono. Questo tipo di eventi inoltre, a prescindere da chi poi subisca materialmente il danno (banca o cliente), minano la fiducia dei cittadini negli strumenti di pagamento elettronici.
Anche le Raccomandazioni affrontano il tema della sicurezza in un'ottica di gestione del rischio, ma comprendono una parte importante di controlli specificamente richiesti, in logica baseline, come ad esempio l'utilizzo di strumenti di strong authentication e di cifratura end-to-end nell'accesso da parte dei clienti. Nel complesso, i controlli richiesti dalle raccomandazioni non prevedono niente di particolarmente nuovo rispetto alle best practice della sicurezza dei servizi online in generale. Nonostante questo, l'adeguamento ha richiesto per la maggior parte delle banche l'avvio di progetti di adeguamento significativi, anche se di impatto meno esteso di quelli richiesti dall'Aggiornamento alla Circolare nel suo complesso, che tocca aree di molto maggiore impatto per le banche. Certamente comunque, il recepimento di queste e delle future Raccomandazioni (a quel punto, dell'EBA e non più della BCE), aumenterà di molto il livello medio di sicurezza dei servizi bancari e delle transazioni online, costituendo una base importante per lo sviluppo e la diffusione di questo tipo di servizi.

Conclusioni

Il Capitolo 8 della Circolare non può essere letto ed attuato in modo settoriale nell'ambito dell'organizzazione della Banca; gli obiettivi e le finalità espresse, quanto meno dal punto di vista della sicurezza informatica, sostanziano il dispiegamento di un sistema di gestione piuttosto che alimentare uno statico insieme di regole e politiche che le Banche possono pensare di implementare per poi passare oltre, in attesa del prossimo, sedicesimo, aggiornamento. Anche laddove le misure siano identificate in modo più puntuale, come per esempio nel caso dei pagamenti elettronici, abbiamo visto come in ambito europeo i regolamenti siano in evoluzione, così come sarà da attendersi una estensione del perimetro da parte dell'EBA a nuovi ambiti (es: pagamenti mobili).
Tutto questo è in linea con una direzione tracciata già da tempo da Basilea II, ma è significativo lo sforzo a livello locale (Banca d'Italia) e Europeo (BCE/EBA) nell'incardinare nelle logiche di sistema gli aspetti di sicurezza che sono irrinunciabili. Per chi si occupa di sicurezza, nessuno degli obiettivi posti è una vera novità, ma interessante è il cambio di prospettiva rispetto alle normative finalizzate maggiormente a definire "baseline" di sicurezza.
Infatti, l'attuazione della Circolare, la cui efficacia è richiesta dallo scorso febbraio 2015, prevedrà necessariamente un approccio progressivo, di miglioramento crescente. Questo sia in considerazione della richiesta di realizzare un "modello di gestione", sia perché l'attuazione della Circolare richiede un coinvolgimento ed una consapevolezza diffusa in tutti gli ambiti organizzativi delle Banche, da quelli operativi IT, a quelli di business (l'"utente responsabile" individuato nell'ambito della gestione del rischio informatico) fino alle figure apicali, essendo OFG e OFSS coinvolti nell'approvazione della propensione al rischio informatico, delle policy di sicurezza, nel reporting del rischio informatico, degli incidenti, dei cambiamenti rilevanti, eccetera.

© Clusit 2015

Gli autori del Rapporto Clusit 2015

Antonio Apruzzese, Dirigente Superiore della Polizia di Stato, è Direttore del Servizio di Polizia Postale e delle Comunicazioni, articolazione della Polizia di Stato specializzata in cybercrime. Con una pregressa pluriennale esperienza nel contrasto della criminalità comune ed organizzata ha coordinato complesse attività info-investigative nel contrasto del crimine informatico, della pedofilia on-line e degli attacchi ai servizi bancari on line e ai sistemi di carte di credito. Il Dott. Apruzzese è attivamente impegnato nella realizzazione di mirate strategie per la prevenzione di attacchi alle reti informatiche ed alle infrastrutture critiche informatiche nazionali. Specializzato in Criminologia è autore di numerose pubblicazioni scientifiche ed ha svolto pluriennali incarichi di insegnamento presso Università e scuole di polizia.

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

Gianluca Bocci, laureato in Ingegneria nel 1996, certificato CISM, CISA, Lead Auditor ISO/IEC 27001:2013, Lead Auditor ISO/IEC 22301:2012, CSA STAR Auditor e ITIL Foundation v3, ha maturato un'esperienza pluriennale nel settore della Sicurezza Informatica in qualità di Security Solution Architect presso multinazionali di rilevanza nel settore dell'ICT e della Sicurezza Informatica. Attualmente in Poste Italiane in qualità di Security Professional Master nella funzione "Sicurezza delle Informazioni" supporta le attività del CERT di Poste Italiane e partecipa alla realizzazione del Distretto Tecnologico di Cyber Security previsto nell'ambito delle iniziative del Programma Operativo Nazionale (PON) in qualità di referente tecnico scientifico del progetto "End User Protection". Dal Gennaio 2015 è membro del Comitato Tecnico Scientifico del Clusit.

Luca Boselli, 39 anni, laureato in economia aziendale presso l'Università L.Bocconi di Milano, è Associate Partner di KPMG Advisory S.p.A. Dal 2001 in KPMG, è attualmente responsabile dei servizi di Information Protection & Business Resilience, e ha maturato esperienze significative in progetti complessi presso aziende appartenenti a differenti settori su tematiche di Information Security, IT Audit, IT Governance, IT Risk & Compliance, Business Continuity/Disaster Recovery. E' membro del consiglio direttivo dell'AIEA, socio CLUSIT, ed ha ottenuto una serie di certificazioni professionali di settore (CISA, CISM, CRISC, Lead Auditor ISO27001). Ha collaborato inoltre alla redazione di varie pubblicazioni ed ha partecipato come relatore a convegni e seminari su diverse tematiche di IT Security e Compliance.

Paolo Bufarini, Head of Security Sales for Mediterranean Region Akamai Italia. Paolo, 51 anni, entra in Akamai a maggio 2014 con l'incarico di guidare le operazioni della divisione security della multinazionale in Italia, Grecia, Turchia, Israele e Medio Oriente. Con oltre 26anni di esperienza in qualità di Sales Manager in Europa e nel Medio Oriente, Paolo Bufarini vanta numerose esperienze maturate in diversi settori dell'Information Technology tra cui Security, Networking ed Enterprise Software. Prima di entrare in Akamai, Bufarini ha lavorato presso Imperva, dove si è occupato dell'espansione del business dell'azienda multinazionale in Italia e nei Balcani, oltre ad aver precedentemente ricoperto incarichi di responsabilità presso Hewlett-Packard, McAfee, Citrix Systems, Wall Data, Dataware Technology, Fulcrum, Bull SA, Itway e Sentrigo. Paolo Bufarini ha iniziato la sua carriera nell'Esercito Italiano, con il grado di Tenente nel dipartimento ICT ed Intelligence.

Stefano Buttiglione, Lead Enterprise Architect, Akamai Technologies. Da dieci anni lavora nel settore della sicurezza informatica per società in ambito tecnologico. Attualmente gestisce il team europeo che si occupa di implementazione, consulenza ed educazione delle soluzioni di sicurezza Akamai.

Paolo Dal Checco svolge attività di Consulente Informatico Forense collaborando con Procure, Tribunali e Forze dell'Ordine oltre che con aziende, privati e Avvocati. Dopo la Laurea in informatica ha conseguito il Dottorato e svolto un periodo di ricerca nel campo della crittografia e sicurezza. Dopo aver lavorato alcuni anni nell'ambito della sicurezza delle comunicazioni, ha fondato insieme al collega Giuseppe Dezzani lo Studio di consulenza informatica forense "Digital Forensics Bureau" tramite il quale ogni anno vengono gestiti centinaia di fascicoli, parte dei quali di rilevanza nazionale. Lo Studio gestisce quotidianamente perizie su computer, cellulari reti, dispositivi elettronici, web, OSINT, audio

© Clusit 2015

e video forensics. Recentemente si è avvicinato al mondo delle criptovalute, dal punto di vista matematico e investigativo più che fiscale ed economico, focalizzando l'attenzione sulle questioni relative ad anonimato, riciclaggio e sicurezza. Relatore in numerosi convegni e docente in corsi e seminari, è tra i fondatori dell'associazione DEFT - che gratuitamente sviluppa e distribuisce una piattaforma open source per le indagini digitali utilizzata da Forze dell'Ordine e consulenti tecnici di tutto il mondo - e dell'Osservatorio Nazionale d'Informatica Forense.

Davide Del Vecchio, conosciuto in rete con il nickname "Dante", da sempre appassionato di sicurezza informatica, ha firmato parecchie ricerche in quest'ambito. È il responsabile del Security Operation Center di FASTWEB da cui vengono erogati i servizi di sicurezza gestita per migliaia di Clienti. Scrive sporadicamente per Wired ed altre testate ed è tra i fondatori del Centro Hermes per la Trasparenza e i Diritti Umani Digitali. Ha collaborato con diverse università e ha partecipato come relatore a numerosi congressi nazionali e internazionali. Nel 2014 è entrato a far parte del comitato direttivo del Clusit.

Gabriele Faggioli, legale, è Presidente del Clusit (Associazione Italiana per la Sicurezza Informatica) e docente del MIP – Politecnico di Milano. È membro del Gruppo di Esperti sui contratti di cloud computing della Commissione Europea. È specializzato in contrattualistica informatica e telematica, in information & telecommunication law, nel diritto della proprietà intellettuale e industriale e negli aspetti legali della sicurezza informatica, in progetti inerenti l'applicazione delle normative inerenti la responsabilità amminstrativa degli enti e nel diritto dell'editoria e del marketing. Ha pubblicato diversi libri fra cui, da ultimo, "I contratti per l'acquisto di servizi informatici" (Franco Angeli), "Computer Forensics" (Apogeo), "Privacy per posta elettronica e internet in azienda" (Cesi Multimedia) oltre ad innumerevoli articoli sui temi di competenza ed è stato relatore a molti seminari e convegni.

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

Corrado Giustozzi, Consulente e docente di sicurezza delle informazioni, divulgatore scientifico. Membro per i mandati 2010-2012 e 2012-2015 del Permanent Stakeholders' Group dell'Agenzia dell'Unione Europea per la Sicurezza delle Reti e delle Informazioni (ENISA), membro del Comitato Direttivo di Clusit. Ha iniziato ad occuparsi di network and information security nel 1985, quando partecipò alla progettazione, messa in linea ed esercizio del primo pioneristico sistema telematico professionale italiano, poi divenuto uno dei primi ISP nazionali. Dal 1999, come direttore di divisione o di business unit, è stato responsabile dell'erogazione dei servizi di consulenza sulla sicurezza delle informazioni presso diverse aziende nazionali e multinazionali; in tale ruolo ha condotto importanti progetti di audit ed assessment di sicurezza logica, e progettato infrastrutture di sicurezza e trust, presso grandi aziende e pubbliche amministrazioni. Collabora da oltre quindici anni con il Reparto Indagini Tecniche del Raggruppamento Operativo Speciale dell'Arma dei Carabinieri nello svolgimento di attività investigative e di contrasto del cybercrime e del cyberterrorismo; fa parte del Comitato Scientifico dell'Unità di Analisi del Crimine Informatico della Polizia delle Telecomunicazioni; è Perito del Tribunale Penale di Roma in materia di criminalità informatica. Fa parte del "Expert Roster" della International Telecommunications Union (ITU) per la cybersecurity e ha collaborato con l'Ufficio delle Nazioni Unite per il Controllo della Droga e la Prevenzione del Crimine (UNODC) su progetti internazionali di contrasto alla cybercriminalità ed al cyberterrorismo. È componente del Consiglio Didattico Scientifico del Master Universitario di II livello in Gestione della Sicurezza Informatica per l'impresa e la Pubblica Amministrazione della Sapienza Università di Roma, e come professore a contratto insegna i temi della cybersecurity e del contrasto al cybercrime in diversi corsi di Laurea e di Master presso varie università italiane. Giornalista pubblicista e membro dell'Unione Giornalisti Italiani Scientifici (UGIS), svolge da sempre un'intensa attività di divulgazione culturale sui problemi tecnici, sociali e legali della sicurezza delle informazioni. Ha al suo attivo oltre mille articoli e quattro libri.

© Clusit 2015

Fabio Guasconi, Laureato in Informatica, opera da 10+ anni nella consulenza sulla sicurezza delle informazioni, con focus sui temi di analisi del rischio, di organizzazione della sicurezza e di conformità a norme internazionali, cui contribuisce direttamente. Certificato CISA, CISM, ITIL e ISFS, è auditor ISO 9001 e ISO/IEC 27001, di cui ha curato le traduzioni in italiano. Coautore del quaderno CLUSIT sulle certificazioni professionali e sullo standard PCI-DSS, è un QSA, partecipa regolarmente ad eventi e pubblicazioni sulla sicurezza. E' membro del direttivo di CLUSIT, presiede il comitato italiano ISO/IEC SC27 in UNINFO e ne partecipa al direttivo. E' co-fondatore e presidente dell'azienda di consulenza BL4CKSWAN S.r.l.

Michele Iaselli è Vicedirigente del Ministero della Difesa presso il 10° Reparto Infrastrutture con incarico di Capo Ufficio Demanio e Servitù Militari a Napoli.
Collaboratore della cattedra di logica ed informatica giuridica presso l'Università degli Studi di Napoli Federico II.
Docente a contratto di informatica giuridica alla LUISS – facoltà di giurisprudenza. Specializzato presso l'Università degli Studi di Napoli Federico II in "Tecniche e Metodologie informatiche giuridiche".
Presidente dell'Associazione Nazionale per la Difesa della Privacy (ANDIP).
Relatore di numerosi convegni, ha pubblicato diverse monografie e contribuito ad opere collettanee in materia di informatica giuridica e diritto dell'informatica con le principali case editrici.

Rocco Mammoliti, nato nel 1968, ha studiato Ingegneria Elettronica presso l'Università di Pisa e ha conseguito un Master in sicurezza presso il Ministero della Difesa - Centro Alti Studi. Ha svolto per diversi anni attivita' di ricerca scientifica presso il CNR. E' autore di diverse pubblicazioni scientifiche su temi legati alla modellistica, data mining, sicurezza ICT oltre che su temi di innovazione e nuove tecnologie. Ha lavorato per aziende di rilevante importanza nel campo dell'IT ed industrie TLC quali Ericsson, Bull e Telecom Italia, ricoprendo in quest'ultima il ruolo di Responsabile della Funzione di Information Security. Ha svolto attivita' di consulenza per diverse società nel settore ICT e Telecomunicazioni. E' membro di associazioni professionali internazionali tra cui l'IEEE e la Computer Society. Le sue principali aree di competenza sono afferenti ai domini nel Network & Information Security, creazione e gestione di Security Operation Center e Computer Emergency Response Team, Abuse & Cybercrime Prevention, Child Online Protection, etc. Attualmente è Responsabile della funzione Sicurezza delle Informazioni di Poste Italiane S.p.A., del CERT di Poste Italiane, del Distretto di Cyber Security di Cosenza e Direttore Generale della Fondazione GCSEC (Global Cyber Security Center) di cui Poste Italiane è fondatore.

Antonio Parata è ingegnere informatico con la passione per lo sviluppo e la software security. Parte del board di OWASP Italy con il quale ha collaborato alla stesura della OWASP Testing Guide v2 e v3. Collabora inoltre con il capitolo italiano di CSA. Ha partecipato come relatore ad importanti congressi di sicurezza e ha pubblicato articoli in ambito scientifico. La passione per gli aspetti tecnici lo porta spesso a scrivere nuovi tool di analisi di sicurezza, come ad esempio il tool Nebula. Attualmente ricopre il ruolo di responsabile del gruppo R&D di Reply Communication Valley con il quale porta avanti, tra le altre cose,l'attività di ricerca e sviluppo in ambito anti-frode e analisi di nuovi malware.

© Clusit 2015

Alessio L.R. Pennasilico, Security Evangelist in Obiectivo Technology, 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 Comitato Direttivo e del Comitato Tecnico Scientifico di Clusit, del Comitato Direttivo Nazionale dell'Associazione Informatici Professionisti (AIP) oltre che essere Membro del Comitato di Salvaguardia per l'Imparzialità di LRQA e membro del Comitato di schema UNI 11506:2013 per Kiwa-Cermet.

Maria Grazia Porcedda è ricercatrice presso il Dipartimento di Legge dell'Istituto Universitario Europeo. Lavora per i progetti europei (FP7) SURVEILLE e SurPRISE sulla relazione tra sicurezza, privacy e sorveglianza, e sta completando la tesi di dottorato in giurisprudenza sulla complementarietà tra protezione dei dati di carattere personale e prevenzione della criminalità informatica. Ha pubblicato diversi articoli in lingua inglese sul tema. Appassionata di protezione dei dati personali e sicurezza informatica da quando, nel 2007, ha partecipato al Silicon Valley Study Tour (La Storia nel Futuro e SVIEC), Maria Grazia lavora nel settore dal 2009. È stata ricercatrice presso il Centre de Recherche Informatique et Droit (CRID, Università di Namur) su temi di privacy e cloud computing, e tirocinante presso l'Organizzazione per la Cooperazione e lo Sviluppo Economico (OCSE), unità di privacy e sicurezza informatica, e il Garante Europeo per la Protezione dei Dati Personali (EDPS). Maria Grazia si è laureata con lode sia in Relazioni Internazionali (specialistica, Università di Bologna) che in Scienze Politiche (triennale, Università di Cagliari). Ha inoltre conseguito la licenza del Collegio Superiore (Università di Bologna) e un master in Diritto Europeo e Internazionale (LLM) presso l'Istituto Universitario Europeo. Le ricerche condotte nell'ambito del master sono state premiate dall'Accademia Nazionale dei Lincei (Premio Ruffini) e dal CLUSIT, di cui è membro dal 2012.

Domenico Raguseo è Manager del team europeo di Technical Sales per IBM Security. Ha 15 anni di esperienza manageriale in diverse aree. Domenico collabora con alcune università nell'insegnamento del Service Management e del Cloud Computing. Dal 2010 Domenico è membro del comitato scientifico del Master in IT Governance dell'Università di Roma. Domenico è IBM Master inventor grazie a una moltitudine di brevetti e pubblicazioni in diverse discipline (Business Processes, ROI, Messages and Collaborations, Networking). Infine, è stato speaker di Sicurezza delle Informazioni, Service Management, Cloud computing, Energy Optimization e Smarter Planet in eventi nazionali e internazionali.

Col. t. ISSMI **Alberto Reda** è laureato in Giurisprudenza e in Scienze della Sicurezza Economica e Finanziaria, con 30 anni di servizio. Dopo diversi incarichi, è stato Comandante Provinciale Guardia di Finanza di Reggio Calabria e, poi, Vice Comandante operativo dello SCICO. Dal luglio 2012, ha il Comando del Nucleo Speciale Frodi Tecnologiche, Unità centrale della Guardia di Finanza la cui missione è il contrasto, anche fornendo supporto ai Reparti territoriali, agli illeciti di natura economico/finanziaria commessi sul web e/o attraverso le tecnologie. Il Nucleo Speciale, quale polo tecnologico di settore per l'intera Guardia di Finanza, collabora, con varie Università ed istituti di ricerca, in importanti progetti, finalizzati alla realizzazione di strumenti da destinare al contrasto al Cyber Crime. Numerose le attività di insegnamento presso la Scuola di Polizia Tributaria, l'Accademia e la Scuola Ispettori del Corpo, su materie professionali e, da ultimo, nel comparto dell'economia digitale e delle investigazioni tecnologiche. Ha partecipato: al Gruppo di Lavoro interistituzionale presso l'Osservatorio socio-economico sulla criminalità del Comitato Nazionale dell'Economia e del Lavoro; al Comitato per la Lotta contro le Frodi Comunitarie presso il Ministero delle Politiche Europee; al Comitato tecnico art. 5 D.M. del n. 44/2003 presso il Ministero delle Politiche Agricole, Alimentari e Forestali. Dal 2013: è stato membro titolare del Nucleo per la Sicurezza Cibernetica istituito presso la Presidenza del Consiglio dei Ministri; è membro dell'Osservatorio Europeo sui diritti di proprietà intellettuale nato a fine 2012 su iniziativa dell'UAMI (Ufficio per l'Armonizzazione del Mercato Interno).

© Clusit 2015

Cap. **Antonio Romano**, laureato con Lode in Ingegneria Elettronica ad indirizzo Telecomunicazioni presso l'Università degli Studi di Napoli, è Ufficiale del Ruolo Tecnico Logistico Amministrativo della Guardia di Finanza. Dal 2012 è in servizio presso il Nucleo Speciale Frodi Tecnologiche e svolge periodicamente attività di docenza in materia di Digital Forensics presso la Scuola di Polizia Tributaria della Guardia di Finanza. I suoi interessi si concentrano soprattutto nel settore della Mobile Forensics e della sicurezza di sistemi telematici.
Prima di essere arruolato nel Corpo, ha lavorato nel settore ferroviario ed in quello aerospaziale. Nel primo, si è occupato di controllo di qualità ed anticontraffazione di componenti elettronici analogici e digitali e di validazione di protocolli di comunicazione sicuri per sistemi safety-critical per le linee ferroviarie ad alta velocità. Nel secondo, invece, ha lavorato nella progettazione di sistemi radar ad apertura sintetica per applicazioni satellitari e di dispositivi affidabili software radio defined di comunicazione terra-bordo per velivoli senza pilota (Unmanned Aerial Vehicles) destinati a scopi civili e militari.

Pier Luigi Rotondo si occupa di soluzioni di sicurezza in IBM Security per clienti sul mercato europeo e del Medio Oriente, contribuendo a numerosi progetti internazionali. Le principali tematiche seguite sono quelle dell'Identity e Access Management, Single Sign-on e della Security Intelligence. Con una laurea in Scienze dell'Informazione presso l'Università degli Studi di Roma "La Sapienza" ricopre incarichi di docenza su temi di Sicurezza delle Informazioni in Master e corsi di Dottorato presso l'Università degli Studi di Roma "La Sapienza", Università degli studi Roma Tre e l'Università degli studi di Perugia. Per conto di IBM viene spesso chiamato ad illustrare la strategia, le soluzioni e i prodotti di sicurezza ai propri clienti, e a divulgare sul mercato italiano i risultati del team X-Force.

Manuela Santini, referente IT Security and Internal Audit prima per Matrix S.p.A. e dal 2013 per Italiaonline S.p.A. si occupa di Information Security Governance and Compliance in conformità a standard/normative di settore e parallelamente alle strategie di business aziendali. Si occupa inoltre di Security Awareness con lo scopo di aumentare la consapevolezza della sicurezza in azienda eseguendo sessioni informative e fornendo supporto alla diverse funzioni aziendali.

Sofia Scozzari si occupa con passione di informatica dall'età di 16 anni. Ha lavorato come consulente di sicurezza presso primarie aziende italiane e multinazionali, curando gli aspetti tecnologici ed organizzativi di numerosi progetti. Chief Executive Officer de iDIALOGHI, negli anni si è occupata di Social Media Security, ICT Security Training e di Servizi di Sicurezza Gestita, quali Vulnerability Management, Mobile Security e Threat Intelligence. Membro di CLUSIT ed Assintel, è autrice di articoli e guide in tema di Social Media Security. È tra gli autori del paper "La Sicurezza nei Social Media" pubblicato nel 2014 dalla Oracle Community for Security. Fin dalla prima edizione contribuisce alla realizzazione del "Rapporto Clusit sulla Sicurezza ICT in Italia" curando l'analisi dei principali attacchi a livello internazionale e nazionale.

Claudio Telmon è consulente freelance nel campo della sicurezza da quasi vent'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 e organizzativi 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. Nell'ambito delle attività dell'associazione è anche responsabile: dei Progetti Europei, dei Progetti per le PMI, del Premio Tesi.

© Clusit 2015

Giuseppe Vaciago è Avvocato, iscritto all'Ordine degli Avvocati di Milano dal 2002. Le aree di specializzazione sono il diritto penale delle nuove tecnologie, il diritto penale societario e la consulenza finalizzata alla redazione dei modelli di organizzazione gestione e controllo ai sensi del D.lgs. 231/01. Ha prestato la sua attività professionale per alcune importanti società nazionali e internazionali nel settore dell'information technology. Ha conseguito un PHD in Digital Forensics all'Università degli Studi di Milano Bicocca ed è docente di informatica giuridica presso l'Università degli Studi dell'Insubria dal 2007. Ha frequentato in qualità di Visiting Scholar la Stanford Law School e la Fordham Law School di New York. Ha partecipato a numerosi convegni presso le più prestigiose Università italiane ed estere. È fellow presso il Nexa Center di Torino e presso il Cybercrime Institute di Colonia. È membro del comitato editoriale della Rivista Digital Investigation edita da Elsevier. È autore di numerose pubblicazioni di carattere universitario tra cui "Computer Crimes" "Digital Forensics" e "Modelli di organizzazione gestione e controllo ai sensi del D.lgs. 231/01". È membro dell'Organismo di Vigilanza di Procter & Gamble Italy S.p.A., Whirlpool S.p.A, e Studio Legale Carnelutti e Fondazione Albero della Vita.

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 per Oracle WCE South. Ha definito ed esportato un approccio per valutare la Security Maturity dei database e per valutare i vantaggi aziendali nell'uso di soluzioni IAM. Inoltre è il fondatore e il coordinatore della Oracle Community for Security. E' coautore, editor o team leader delle pubblicazioni "ROSI Return on Security Investments: un approccio pratico", "Fascicolo Sanitario Elettronico: il ruolo della tecnologia nella tutela della privacy e della sicurezza", "Privacy nel Cloud: le sfide della tecnologia e la tutela dei dati personali per un'azienda italiana", "Mobile Privacy: adempimenti formali e misure di sicurezza per la compliance dei trattamenti di dati personali in ambito aziendale", "I primi 100 giorni del Responsabile della Sicurezza delle Informazioni (Come affrontare il problema della Sicurezza informatica per gradi)", "La Sicurezza nei Social Media - Guida all'utilizzo sicuro dei Social Media per le aziende del Made in Italy", "Le Frodi nella Rete - Il Duplice Ruolo dell'ICT" e, di prossima pubblicazione, Privacy Europea e Mobile Security. Contribuisce fin dal 2012 ai Rapporti Clusit sulla Sicurezza ICT in Italia. E' socio AIEA, CSA Italy e membro del Consiglio Direttivo di Clusit.

Sylvio Verrecchia ha un'esperienza di oltre 15 anni come consulente esperto nel settore Information Technology. Si occupa di Computer Forensics, Sicurezza Informatica e Privacy. E' socio CLUSIT, membro del Comitato Tecnico Scientifico ed incaricato al progetto "Video Clusit". Ha partecipato come relatore al progetto "La sicurezza informatica nelle scuole" e ha pubblicato articoli riguardanti l'information security e la digital forensics. Certificato ITILv3 e PRINCE2 è responsabile della gestione dei servizi e progetti in ambito IT presso varie aziende clienti.

Andrea Zapparoli Manzoni si occupa con passione di ICT dal 1997 e di Information Security dal 2003, mettendo a frutto un background multidisciplinare in Scienze Politiche, Computer Science ed Ethical Hacking. Dal 2012 è membro dei Consiglii Direttivi di Clusit e di Assintel, e Board Advisor del Center for Strategic Cyberspace + Security Science di Londra. E' stato Presidente de iDialoghi per oltre 10 anni, società milanese dedicata alla formazione ed alla consulenza in ambito Cyber Security. Nel gennaio 2015 ha assunto il ruolo di Senior Manager della divisione Information Risk Management di KPMG Advisory. E' spesso chiamato come relatore a conferenze ed a tenere lezioni presso Università, sia in Italia che all'estero. Come docente Clusit tiene corsi di formazione su temi quali Cyber Crime, Mobile Security, Cyber Intelligence e Social Media Security, e partecipa come speaker alle varie edizioni del Security Summit, oltre che alla realizzazione di white papers (FSE, ROSI v2, Social Media) in collaborazione con la Oracle Community for Security. Fin dalla prima edizione del "Rapporto Clusit sulla Sicurezza ICT in Italia" cura la sezione relativa all'analisi dei principali attacchi a livello internazionale, ed alle tendenze per il futuro.

© Clusit 2015

Ringraziamenti

Clusit e Security Summit ringraziano tutti gli autori e le persone che hanno contribuito alla realizzazione del Rapporto Clusit 2015.

Si ringraziano inoltre: Akamai Technologies, Cisco Systems, ENISA, FASTWEB, Nucleo Speciale Frodi Tecnologiche della Guardia di Finanza, HP ES Italia, IBM, Italiaonline, KPMG Advisory, ORACLE, Polizia Postale e delle Comunicazioni, Poste Italiane, Trend Micro, Websense.

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

Gli obiettivi

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

Le attività ed i progetti in corso

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

Il ruolo istituzionale

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

I rapporti internazionali

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

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

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

I docenti e relatori.

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

I partecipanti

Nel corso delle prime 6 edizioni, il Security Summit è stato frequentato da oltre 8.000 persone e sono stati rilasciati circa 5.000 attestati validi per l'attribuzione di 8.500 crediti formativi (CPE) e 900 diplomi.

L'edizione 2015

La settima edizione del Security Summit si tiene a Milano dal 17 al 19 marzo, a Roma il 10 e 11 giugno e a Verona l'1 ottobre.

Informazioni

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

In collaborazione con

www.securitysummit.it