

SPAM: TANTE AREE GRIGIE

Troppe ambiguità nell'interpretazione da parte dei Governi della Direttiva 58 dell'Unione Europea "Electronic Communications and Privacy". Lo rivela uno studio condotto da IviR (Institute for Information Law- www.ivir.nl) di Amsterdam e Sybari Software (www.sybari.com) che ha coinvolto 130 aziende di 15 Paesi europei.

I risultati preliminari dello Studio IviR sullo Spam e sulla Direttiva 58 dell'Unione Europea (entrata in vigore lo scorso 1 novembre) rivelano numerose aree grigie, sia per le imprese che per i governi, riguardo all'interpretazione e all'implementazione di questa nuova legge. Ci sono ambiguità che riguardano, ad esempio, i casi in cui le e-mail commerciali possono essere inviate su una base 'opt out' e quando l'accordo preliminare – 'opt in' – può essere dato.

Altre aree, non correttamente preparate dalla Direttiva, includono la protezione dallo Spam di alcuni gruppi di utilizzatori di e-mail in ambienti professionali, così come i free-lancers, l'uso di comunicazioni elettroniche come 'pop-up's', e la questione dello Spam che si autopropaga.

Una combinazione di norme, meccanismi di applicazione, cooperazione internazionale, prevenzione attraverso la formazione, soluzioni tecniche, cruciale nella battaglia contro lo Spam.

«La battaglia legale contro lo Spam è difficile. - afferma Lodewijk Asscher, senior researcher di IviR - Il campo di battaglia è ancora ricoperto da una densa nebbia di incertezze legali dovute alla tardiva implementazione della Direttiva, meccanismi di applicazione deboli e scappatoie nelle principali norme. La battaglia legale contro lo Spam richiede un approccio multi-focus. Ma il successo di questa Direttiva dipende soprattutto dai meccanismi di applicazione adottati dagli Stati Membri.

Per quanto, la nostra analisi legale dà una piccola speranza di ottenere una grande diminuzione dello Spam come unico risultato della Direttiva 58. La cooperazione internazionale, la promozione dell'informazione da parte dei consumatori e l'informazione dalle società sono i prossimi passi necessari.

Il nostro studio mostra che la Direttiva 58 è l'inizio piuttosto che la conclusione di una soluzione legale dello Spam».

I punti deboli

Lo studio ha evidenziato alcuni punti deboli:

- La legge nell'articolo 13 prevede il cosiddetto 'opt-in' - accordo preliminare - prima di consentire l'invio di posta elettronica commerciale. Tuttavia, l'articolo 13,2 della nuova legge – il quale dichiara che dove un indirizzo di posta elettronica è stato ottenuto nel contesto della vendita di un prodotto o di un servizio, la trasmissione di posta elettronica

commerciale per prodotti o servizi relativi è consentita - lascia aperta una notevole scappatoia per i rapporti esistenti con il cliente, che potrebbe favorire determinati settori più di altri. Ci sono inoltre varie ambiguità quanto a che cosa potrebbe essere considerato "prodotti correlati".

- È poco chiaro se le comunicazioni elettroniche come 'pop-up's' siano coperte dalla Direttiva.

- La protezione contro lo Spam di certi gruppi di utenti di posta elettronica in un ambiente professionale, come i free-lancers, è inoltre ambigua.

- Il rapporto fra lo Spam che si diffonde attraverso un virus e le disposizioni sulla sicurezza dell'Articolo 4 della Direttiva, rimangono vaghi.

L'Articolo 4 obbliga i fornitori a prendere 'misure appropriate' per proteggere la sicurezza delle proprie reti. Questo potrebbe avere implicazioni importanti per la responsabilità dell'ISP.

- Il significato esatto di "misure appropriate" non è definito.

- Poco aiuto è fornito quanto al meccanismo di applicazione necessario per implementare effettivamente le nuove regole.

- Una combinazione di legislazione, meccanismi di applicazione, cooperazione internazionale, prevenzione attraverso la formazione e soluzioni tecniche è cruciale nella lotta contro lo Spam.

- L'efficacia della Direttiva per quanto riguarda la riduzione dello Spam, dipende dalle scelte che gli Stati Membri fanno nella trasposizione della Direttiva nelle proprie leggi nazionali.

- Questa legislazione nazionale dovrebbe in primo luogo chiarire sia ai consumatori che alle aziende, i "do's" e i "don'ts" nell'e-marketing, visto che la Direttiva lascia molto spazio per speculazione.

I risultati dell'indagine

In media, quasi la metà dei partecipanti all'indagine (società che usano e-mail) ritiene che gli Stati Membri (i Paesi dell'Unione Europea) non siano del tutto efficaci nell'applicare la nuova legislazione sullo Spam. Il resto degli intervistati dalla ricerca crede, in media, che i propri governi saranno solo in parte efficaci nell'applicare queste norme. Quasi la metà delle società che hanno partecipato all'indagine sostiene che la legislazione non avrà effetti sull'attuale quantità di Spam ricevuta, con un altro 25% che pensa che si avrà solo un effetto a breve termine.

Più del 70% degli intervistati ha espresso perplessità sulla sanzione massima per gli spammer nel proprio Paese, ma il 93% vorrebbe vedere gli spammer arrivare in giudizio. Solo il 7% degli amministratori IT ritiene che gli spammer debbano andare in prigione. La migliore misura di giustizia (50%) è per gli spammer la penalizzazione finanziaria, con multe e costi addizionali. A meno del 10% interessa la citazione dei dipendenti da parte della propria organizzazione per una mancanza di protezione, e altrettanto poche società pensano di rischiare di essere citate da altre organizzazioni per una inadeguata protezione dei propri sistemi di messaggistica.

«Ciò che stiamo osservando – ha sottolineato Paolo Cavalsassi, Territory Manager Sybari per l'Italia - è che le aziende europee sono favorevoli a una legislazione che combatta lo Spam, ma non credono che sarà capace di far diminuire i costi correnti e i rischi che si stanno affrontando oggi».

«Le società – ha continuato Cavalcassi - non hanno chiaro cosa lo Spam può rappresentare per le proprie organizzazioni e non stanno applicando politiche corporate di utilizzo delle e-mail.

Gli amministratori delle e-mail stanno incrementando il cambiamento verso software che li aiutino a prendere queste decisioni e li rendano capaci di monitorare l'utilizzo delle e-mail da parte dei propri dipendenti, e i rischi a cui i propri dipendenti possono esporre l'organizzazione. Una soluzione software anti-Spam non è efficace se non abbatta i costi correntemente causati dallo Spam e non limita l'esposizione dell'azienda ai rischi».

Gli intervistati credono che ambienti di messaggistica poco sicuri creeranno una perdita di produttività, una perdita di dati aziendali e l'incapacità a comunicare con efficienza utilizzando i mezzi elettronici. La maggior parte degli interpellati affermano di aver aumentato la propria spesa in software come risultato dello Spam, mentre solo una piccola parte di aziende precisa di aver aumentato la spesa in hardware o in contratti con organizzazioni terze parti per risolvere la questione Spam. Il 99% degli intervistati ritiene importante per la propria organizzazione investire, nel futuro, in tecnologia per proteggersi dallo Spam, applicare linee guida sulla gestione delle e-mail e conformarsi con la legislazione. Dall'indagine emergono anche alcune informazioni relative alle politiche aziendali di utilizzo delle e-mail:

- Il 69% delle aziende intervistate precisa che la propria società non possiede una definizione operativa di cosa considerare 'Spam'.
- Il 41% degli intervistati afferma di non avere una definizione corporate di Spam già definita, ma ritiene di doverla formulare.
- Il 55% crede che l'aggiunta di un testo di 'non accettazione' a tutti i messaggi diretti verso l'esterno, non aiuterà l'azienda in termini di esposizione di responsabilità.
- Il 72% degli intervistati crede che, per la propria organizzazione, includere una politica corporate di uso delle e-mail ridurrà l'esposizione di responsabilità dell'organizzazione.
- Il 46% delle aziende intervistate possiede una politica corporate di uso delle e-mail, ma non riceve riconoscimento dagli impiegati di averla ricevuta o compresa.

Dettagli sui risultati dell'indagine sono disponibili
www.solidground.nl/sybari-survey/

CONTENT MANAGEMENT: CONTINUA IL TREND POSITIVO

Nel 2006 il mercato europeo delle applicazioni di Content Management varrà 744 milioni di euro. Il dato è emerso dalla ricerca condotta da IDC (www.idc.it) nel corso del 2003 su un campione di 500 imprese italiane con almeno 20 addetti, con un alto grado di informatizzazione e dotate di accesso internet. L'indagine ha avuto l'obiettivo di analizzare le soluzioni di Content Management presenti nelle aziende italiane e la propensione al loro utilizzo.

Roberto Mastropasqua e Fabio Rizzotto, rispettivamente Research Director e Senior Research Analyst di IDC Italia, hanno messo l'accento sui punti focali, quali la progettualità e le fasi nella catena del Content Management; i portali aziendali. Secondo gli analisti IDC il Content Management è destinato a divenire uno dei principali fronti di investimento delle aziende nel prossimo futuro. Il mercato europeo delle applicazioni di Content Management vale oggi 618 milioni di euro, grazie a una crescita costante e continuata, nel 2006 raggiungerà i 744 milioni di euro.

Negli ultimi anni, la complessità delle informazioni, unita alla necessità di armonizzare siti web e attività on-line, ha spinto le imprese a dotarsi di politiche e strumenti per una gestione corretta e un controllo sempre più attento di documenti e dati critici.

I vantaggi di un trattamento razionale delle informazioni sono ormai evidenti non solo in termini di organizzazione della conoscenza aziendale, ma anche di rapidità nel reperimento dei dati, sicurezza dei contenuti critici e contenimento dei costi dei processi.

«La diffusione di standard aperti e l'affermazione dei Web Services favoriscono infatti una portata sempre più allargata delle tecnologie di Content Management, - ha spiegato Roberto Mastropasqua - I sistemi di ricerca, raccolta e organizzazione, l'analisi di dati e contenuti favoriscono processi di ottimizzazione della gestione di dati, documenti e informazioni sia strutturate che non, con impatti considerevoli in termini di efficienza, come emerge anche dalla ricerca IDC associata al nostro evento».

I risultati.

Nel dettaglio, l'indagine vuole fare il punto sullo stato dell'arte nell'adozione di soluzioni di Content Management e sugli Enterprise Portals, analizzando la relazione che intercorre tra le implementazioni attuali e l'adozione futura di soluzioni di gestione del Digital Content e verificando le aree di opportunità attuali e nel medio termine per i vendor che operano in questo mercato.

Ne risulta un settore rallentato da fattori congiunturali, ma che si prepara ad affrontare le sfide future con consapevolezza, grazie anche ad un'offerta ormai più matura e rispondente alle reali esigenze di business. In questo contesto si aprono diverse opportunità per i vendor, anche se con le dovute differenze tra le aziende di piccole dimensioni e quelle medio grandi.

L'analisi condotta da IDC Italia mostra una buona diffusione di soluzioni per la gestione di documenti e contenuti all'interno del campione intervistato: circa il 28% delle imprese interpellate, infatti, si è già dotata di applicazioni di Content Management, mentre un ulteriore 25% ha in programma investimenti in quest'area entro il 2004.

Il primo obiettivo che le aziende intendono perseguire nell'anno appena iniziato riguarda la creazione di workflow strutturati all'interno dei processi aziendali (30% degli intervistati). Tra gli obiettivi particolarmente sentiti dalle aziende italiane interpellate, una particolare importanza riveste la necessità di armonizzare la mole di archivi e database aziendali in cui risiedono contenuti e informazioni più o meno strutturati (29%).

Il fattore integrazione è al centro dell'attenzione delle imprese a più livelli: nella pianificazione di nuovi investimenti in Content Management, nella creazione di accessi unificati a repository tradizionali e digitali, nell'armonizzazione tra le tecnologie dei portali e quelle dei sistemi di Content Management e tra le soluzioni di Content Management e le altre tipologie di soluzioni presenti in azienda.

«Le conseguenze di una gestione non razionale delle informazioni sono ormai note a tutti: inefficienza, lentezza decisionale e calo della competitività sul mercato. - ha precisato Fabio Rizzotto - Le imprese italiane sono sempre più consapevoli del valore strategico degli strumenti e soluzioni di Content Management e Enterprise Portals.

BANCOMAT: PRELIEVI DALL'AUTO

A Pergine, in provincia di Trento, è possibile raggiungere il bancomat ed effettuare le operazioni bancarie direttamente dall'auto. La Cassa Rurale di Pergine (aderente al sistema della Banca di Credito Cooperativo), ha installato presso il Centro Finanza e l'Agenzia di piazza Serra un innovativo bancomat che permette di effettuare operazioni bancarie, compreso il prelievo di contante, rimanendo comodamente seduti nella propria automobile.

Già molto utilizzato negli Stati Uniti, questo tipo di sportello è risultato particolarmente gradito agli utenti, soprattutto quando piove o in luoghi in cui è difficile parcheggiare; infatti NCR Personas M-Series drive-up consente di operare semplicemente allungando un braccio fuori dal finestrino.

La richiesta di servizi innovativi, sicuri e comodi da utilizzare è in costante crescita e il nuovo dispositivo consente di soddisfare queste esigenze, offrendo un servizio a misura d'uomo, agevolando anche i portatori di handicap che ne apprezzano in particolare il maggior grado di sicurezza in cui si trovano ad operare.

La Banca di Credito cooperativo con Sede a Pergine Valsugana (TN), conta 11 sportelli e 92 dipendenti. È "banca locale" e persegue l'obiettivo di favorire il benessere delle Comunità nelle quali è radicata, anche mediante strumenti e tecnologie di ultima generazione, come quelli utilizzati nella recentissima realizzazione del nuovo Centro Finanza (dove è stato installato NCR drive-up), in grado di assicurare a Soci e Clienti una consulenza a 360 gradi e dotato di ampia zona self service, sala operativa integrata, borsino, apparecchiature collegate con tecnologia Wireless, e ancora servizi di Internet Banking, Trading on line, ecc. a vantaggio di tutti i risparmiatori.

VIRUS SEMPRE IN AGGUATO

Nel corso del mese di gennaio, Trend Micro ha rilevato circa 550 programmi pericolosi come worm, virus, Trojan horse e altre tipologie di codice "malware". Il 30% di tali programmi riguarda la categoria dei worm mentre un'analoga percentuale appartiene alle categoria delle backdoor. Valutando le prime dieci minacce di gennaio i ricercatori hanno osservato che nel 60% di casi si è trattato di worm, che si confermano così come la principale tipologia da affrontare. Nuovi dati indicano tuttavia che la situazione sta divenendo più complessa: sempre più worm, infatti, collocano **backdoor** all'interno dei sistemi che riescono a infettare. Le **backdoor**, al contrario dei virus, non possiedono routine di autopropagazione ma si diffondono per mezzo dei worm. In questo modo le backdoor possono giungere attraverso la posta elettronica, la condivisione di risorse di rete, l'instant messaging e le applicazioni P2P: pertanto, sono in grado di compromettere non solo un determinato computer, bensì la sicurezza di intere reti. Inserirle all'interno dei loro ospiti (i worm), le backdoor possono attaccare un numero cospicuo di sistemi di rete, dimostrando come sia sempre più importante definire efficaci policy di sicurezza per proteggere i network aziendali da minacce in costante evoluzione come queste.

Il futuro

Cosa dobbiamo aspettarci nel futuro? In base alla sua esperienza nella lotta all'attività virale, Trend Micro ha elaborato le seguenti previsioni e osservazioni per il 2004:

- Il ricorso agli attacchi a **tecnica mista** rimarrà la norma.
- Il malware attuale e futuro verrà predisposto per tentare di disabilitare programmi antivirus, firewall e anti-Trojan horse.
- **Software per filtraggio** Web o, almeno, policy per la navigazione Internet, dovranno essere ben presenti nelle aziende al fine di prevenire improvvise intrusioni del malware residente su siti Web.
- Il **filtraggio** degli allegati di posta elettronica continuerà a fornire una protezione ulteriore. Tuttavia, il software di scansione antivirus a livello di gateway è più efficace nell'estirpare i file infetti che transitano nelle reti aziendali, così come nel riconoscere diversi formati di file e archivi.
- **Canali di messaging pubblici** e non moderati come IRC e P2P verranno usati di tanto in tanto a causa della necessità di una veloce comunicazione, dato che il sovraccarico della posta elettronica ostacola le operazioni di ogni giorno.
- Molti report pubblicati nel 2002 hanno stimato che, entro il 2007, il 25% di tutto il contenuto email riguarderà una qualche forma di **spamming commerciale**. In realtà, come scritto da Nucleus Research, AmikaNow!, IDC e dal New York Times, nell'ottobre 2003 l'influenza dello spamming ha raggiunto il 49% e ci si aspetta che mantenga un ritmo di crescita annuo del 7%.
- Gli amministratori di sistema devono **valutare attentamente** la situazione e le necessità di software delle rispettive reti aziendali. Devono perciò assicurarsi che il vendor possa impegnarsi tempestivamente per stabilire le vulnerabilità e offrire l'erogazione di servizi omogenei e affidabili.

- Man mano che le aziende continuano a crescere, il ricorso a **servizi centralmente gestiti** diverrà sempre più importante. Parecchi vendor oggi propongono pacchetti di soluzioni per la gestione dei contenuti. Ma davanti a queste offerte si valutino con cura l'efficienza e la capacità globale di fornire dati collaborativi.
- Con i virus di rete sempre più diffusi, gli amministratori devono dotarsi di **strumenti gestionali** che permettano di isolare settori specifici delle loro reti. Per esempio, scaricare policy per la prevenzione delle infezioni che isolino rapidamente aree vulnerabili o colpite per prevenire l'ulteriore allargamento dell'infezione fino al rilascio del pattern file appropriato.
- **Il costo** legato al ripristino della rete in seguito agli attacchi di virus continuerà a rappresentare un aspetto problematico. Le aziende possono minimizzare le tempistiche e le risorse richieste per ripristinare la rete ricorrendo a profili di pulizia specifici secondo il tipo di dispositivo e l'attacco verificatosi.

PRINCIPALI MINACCE OSSERVATE NEL MESE DI GENNAIO

TROJ_XOMBE.A, apparso agli inizi del mese, è un tipico esempio di mix di tecnologie. Abbiamo già visto hacker e autori di virus lavorare insieme; adesso sembra che siano entrati in gioco anche gli spammer.

Come suggerisce il suo nome, TROJ_XOMBE.A è un Trojan horse (ovvero non possiede routine di autopropagazione nel suo codice); tuttavia molti hanno asserito di aver ricevuto questa minaccia attraverso la posta elettronica, indicando pertanto che si tratti di un messaggio spam contenente "malware" in allegato. Le tecniche di spamming vengono ora impiegate per diffondere codice maligno. Il messaggio confonde inoltre chi lo riceve facendo finta di essere stato originariamente spedito da Microsoft (nome dell'allegato: WINXP_SP1.EXE, Titolo: Windows XP Service Pack 1 (Express) - Critical Update). Val la pena notare che una semplice regola a livello di gateway Internet che blocchi i file con estensione .EXE sia sufficiente per neutralizzare questa minaccia.

WORM_BAGLE.A controlla la data di sistema disattivandosi dal 28 gennaio 2004 in avanti; altrimenti apre la porta 6777 rendendo il sistema vulnerabile agli hacker. Viene così compromessa non solo la sicurezza del sistema infetto, ma potenzialmente anche quella della rete aziendale su cui il sistema risiede (qualora si tratti di una macchina collegata in rete).

Proprio come WORM_SOBIG.F, anche questo nuovo worm estrae il nome di dominio dell'indirizzo del sistema infetto interrogandone il DNS (Domain Name Server) per conoscere il relativo MailBox (MB) server: questo accorgimento può velocizzare la propagazione del worm. Si possono inoltre notare due interessanti caratteristiche:

Questo worm si diffonde utilizzando come allegato un file .EXE.

Molti utenti o ambienti di rete aziendali sono stati colpiti da questo worm, confermando come vi siano ancora aziende prive delle più elementari regole di sicurezza.

Viene da chiedersi se questo codice sia effettivamente nel suo stato definitivo e completo, dato che qualunque autore di virus sa che basta una semplice regola per bloccare un file .EXE. Questa ipotesi è corroborata dal fatto che il codice non è compresso. Gli autori di virus comprimono spesso il loro codice attraverso un algoritmo in modo da scavalcare le soluzioni antivirus meno avanzate; pertanto possiamo supporre che questo codice sia stato rilasciato per errore.

WORM_MYDOOM.A (conosciuto anche come Mimail.R o Novarg.A). Si tratta di un mass-mailing worm che sceglie all'interno di un elenco di frasi per comporre titolo, testo e nome del file allegato dei messaggi di posta che diffonde. Lo

spoofing del nome del mittente serve a far credere che il messaggio provenga da utenti diversi da quelli effettivi, dimostrando così una complessa tecnica di social engineering. Questo worm può propagarsi anche attraverso la rete di file sharing P2P Kazaa.

WORM_MIMAIL.R effettua inoltre un attacco di tipo Denial-of-Service (DoS) contro il sito www.sco.com qualora la data sia uguale o successiva al 1° febbraio 2004 fermando questo attacco e la maggior parte delle sue routine il successivo 12 febbraio. Si suppone che questo attacco possa essere motivato dal fatto che SCO ha intentato, nel novembre 2003, una causa contro importanti distributori Linux.

Questo worm contiene anche una backdoor che appare come il file SHIMGAPI.DLL. Tale backdoor apre la porta 3127 per consentire a utenti remoti di accedere ai sistemi infetti e di manipolarli. Si noti che l'accesso remoto resta attivo anche successivamente alla data del 12 febbraio 2004.

Per avere una situazione in tempo reale dei virus è possibile consultare la mappa all'indirizzo: <http://www.trendmicro.com/map>

E-PROCUREMENT? GARA ONLINE PER ACI

L'Automobile Club d'Italia ha scelto BravoSolution per adottare le soluzioni di e-procurement, per ottimizzare costi e tempi dei processi d'acquisto. 2 ore e 10 minuti, 48 rilanci, 7 aziende fornitrici coinvolte, sono stati necessari per aggiudicare la fornitura a 543.999 Euro, con un risparmio del 5% circa sul precedente prezzo di acquisto risalente a 2 anni fa. Questi i numeri dell'asta organizzata da BravoSolution, società di Italcementi Group, leader in Italia nel settore dell'e-procurement, per inaugurare la piattaforma di servizi di EProcurement sviluppata per soddisfare le esigenze di approvvigionamento dell'ACI (www.acquistionlineaci.it).

Oggetto della negoziazione, la fornitura di 20milioni di stampati a modulo discreto denominati "Certificato di Proprietà - CdP" (formato A4 con applicazione di ologramma a caldo e carta filigranata personalizzata ACI) utilizzati per certificare la proprietà dei beni mobili registrati al Pubblico Registro Automobilistico.

Questa negoziazione sopra la soglia di rilievo comunitario, condotta in aderenza al D.P.R. 101/02, è la prima all'interno di un progetto che ACI ha lanciato con l'obiettivo di acquisire, tra i primi nel panorama degli enti pubblici, soluzioni e competenze all'avanguardia nel campo dell'e-Procurement.

Il progetto di ACI ha come obiettivi la necessità di snellire e di ottimizzare, in termini di tempi e costi, i processi di approvvigionamento e la loro gestione garantendo la massima trasparenza.

In questa prima fase ACI si è dotata dei servizi per l'espletamento delle gare telematiche e per la gestione dell'Albo Fornitori offerti da BravoSolution ed ha velocemente organizzato la presente negoziazione e ne ha già pianificate altre per il 2004.

Grazie al successo di questa prima esperienza di negoziazione on line con BravoSolution, ACI si prefigge di utilizzare in modo sempre più sistematico le metodologie di approvvigionamento telematiche.

I PROFILI DEI NAVIGATORI

Le donne rappresentano circa il 40% del totale, mentre le persone tra i 18 e i 34 anni raggiungono il 50 per cento. L'agenzia Media Slash si propone di fotografarne usi e costumi.

Dopo il successo ottenuto dall'Interactive Media Report (IMR), Osservatorio per lo studio e l'approfondimento delle modalità di comunicazione attraverso i Nuovi Media con un ampio panel di direttori marketing ed operatori del settore, l'Agenzia Media Slash, tramite la propria divisione di ricerche di mercato on-line - QMARK - ha istituito due nuovi Osservatori focalizzati sugli utenti della Rete.

Prendono così il via Interactive Generation Report (IGR) e Interactive Women Report (IWR), indagini a cadenza semestrale che studiano e approfondiscono le modalità di comportamento, degli usi e costumi, delle opinioni, dei consumi, e degli stili di vita dei giovani (dai 18 ai 34 anni) e delle donne che utilizzano Internet.

A tal fine, e grazie ad accordi con editori on-line ed aziende, Slash si avvale oggi di un panel di oltre un milione di giovani on-line e di un panel di oltre 500mila donne on-line.

Nel mese di Luglio sono state condotte le due prime importanti indagini: garantendo la rappresentatività dei campioni attraverso criteri logici, metodologici e statistici sono state poste più di 60 domande ad ogni singolo campione costituito ciascuno da 4mila Internet User, indagando per ciascuno di essi oltre 700 variabili, raccogliendo quasi sei milioni di dati che accreditano le due indagini come un punto di riferimento affidabile in riferimento all'utilizzo della Rete da parte dei due target.

I risultati

La prima wave dell'Osservatorio IGR ha indagato diversi temi:

- Caratteri Socio-demografici dei giovani 18-34enni
- Utilizzo di Internet/Pubblicità Online
- E-commerce/Spesa Online
- Interessi/Intrattenimento/Media
- Informatica/Mobile/Hi-tech

Dall'Osservatorio emerge che il 58,4% dei giovani 18-34enni che utilizzano la rete sono uomini e il 33% è residente al Nord Ovest. Per quanto riguarda il livello di Istruzione si nota che la maggior parte dei giovani hanno un diploma di media superiore (68%) ed il 58% ha già un'occupazione.

Quest'ultimo dato è in contro tendenza con i dati Istat della Popolazione Italiana affermando che solo il 42% degli Italiani è Occupata.

Sulla base dell'utilizzo posto in essere dai giovani 18-34enni in Rete è stata costruita la Mappa IGR.

Tale Mappa ha l'obiettivo di rappresentare, attraverso dei profili, il comportamento e le motivazioni di utilizzo della rete da parte degli stessi e diventa un utile strumento per le aziende per sviluppare, con maggior precisione, adeguate strategie di web marketing e di pubblicità online. La Mappa IGR è stata creata seguendo una rigorosa metodologia statistica che, partendo dall'individuazione delle motivazioni che spingono i giovani 18-34enni ad utilizzare la rete, si è proceduto, in una prima fase nel

ridurre tali variabili in fattori che spiegano tali ragioni mediante tecniche di fattorizzazione.

Si è così arrivati a definire, i sei profili che caratterizzano la Mappa IGR:

- 1. INTERATTIVI (28,3%):** Utilizzano Internet in modo completo. Lo utilizzano sia per informarsi e tenersi aggiornati che per comunicare
- 2. RICREATIVI (18,8%):** Utilizzano Internet maggiormente come strumento per comunicare tramite Chat, SMS, Forum. Dalla rete scaricano sia software che musica
- 3. CONCORRENTI (12,4%):** Utilizzano Internet principalmente per partecipare a promozioni e giochi Online
- 4. INFORMATI (15,7%):** Utilizzano Internet per tenersi aggiornati professionalmente e informati sulla vita quotidiana
- 5. ACQUIRENTI (11,8%):** Utilizzano Internet non solo per acquistare ma anche per confrontare prezzi e per prenotare qualsiasi tipo di biglietto
- 6. EVOLUTI (13%):** Di Internet utilizzano particolarmente tutti quei servizi Online come l'home banking e l'eCommerce.

In particolare, i **Concorrenti** si differenziano dai restanti profili per una spiccata partecipazione a promozioni e concorsi online (42,5%) non tralasciando i propri doveri lavorativi o studenteschi (95%).

La componente aggiornamento è alla base degli **Informati** che dedicato gran parte del loro tempo su internet aggiornandosi professionalmente (41%) e/o informandosi quotidianamente (51%).

L'acquisto inteso come confronto di prezzi, prenotazione e, solo in un secondo tempo, l'acquisto vero è proprio, è ciò che caratterizza gli **Acquirenti**. Questo profilo utilizza la rete maggiormente per prenotare viaggi o biglietti di aerei/treni (50,3%).

L'**Evoluto**, invece, è un profilo decisamente formato da utenti presenti maggiormente nell'ultima fascia d'età, quella compresa tra i 30-34 anni (41%), e quasi il 90% di questi è occupato.

Questo profilo utilizza tutti quei servizi avanzati online come, ad esempio, l'home banking (54%).

Nettamente diverso dal profilo prima citato è il **Ricreativo** che utilizza la rete come strumento per comunicare tramite Chat (53%), SMS (45%), download di file (62%).

Infine, il profilo che un po' racchiude tutti i profili è l'**Interattivo**.

Dell'Interattivo spiccano su internet maggiormente doti comunicative (97%), il desiderio di tenersi sempre aggiornato (92%) non trascurando momenti di svago giocando (77%) o scaricando MP3 (85%).

Maggiori informazioni in merito all'Osservatorio e alle Ricerche di Mercato Online sono disponibili in www.qmark.it