OLTRE L'AUSTERITY

La Ue investe sul futuro ora i privati

di Raffaele Rovati

Poca enfasi è stata data in settimana a un annuncio cruciale per il futuro di un'Europa che mostra di avere un'agenda non solo da lacrime e sangue. Máire Geoghegan-Quinn, commissario europeo per Ricerca, Innovazione e Scienze, ha presentato il settimo Framework Programme for Research and Technological Development (Fp7), che prevede investimenti per 8,1 miliardi di euro (e dovrebbero arrivarni altri sei dal privato). Sforzo importante della Ue in favore delle attività di ricerca in It, nanotecnologie e non solo, con un raggio d'azione che va dalle *smart city* agli oceani del futuro. I fondi andranno a istituzioni pubbliche, ma anche private. Il programma comunitario non nuovo, visto che dal 2007 ha messo in campo un budget di oltre 55 miliardi di euro, per 19.000 progetti, 79.000 organizzazioni e 55.000 singoli ricercatori. È importante che annunci come questi arrivino in contemporanea a un'austerity senza precedenti nell'Europa degli ultimi anni, perché sono segnali di come non si possa pensare di battere la crisi solo mettendosi a dieta. Fondamentale è investire. Nella speranza che lo sforzo dell'Europa come istituzione faccia da volano anche per l'Europa delle aziende, che devono continuare a credere nel futuro. Si stima che l'Fp7 possa generare 210.000 nuovi posti di lavoro nell'immediato e una crescita economica di 75 miliardi di euro nei prossimi 15 anni. Sembra poca cosa, ma quello che conta è l'effetto contagio. Nella speranza che il virus dell'innovazione continui a invadere il nostro continente. «La nostra azienda plaude ai continui sforzi rappresentati dall'Fp7 - ha detto il chairman di Ibm Europe Harry van Dorenmalen - e confida nell'imminente approvazione del programma Horizon 2020». Grandi aziende, piccole realtà, istituzioni, la sfida della crescita è comune e per vincerla bisogna partire. Bruxelles ha fatto il suo, ora tocca agli altri.

NON SOLO SMARTPHONE CON SAMSUNG LA RIVOLUZIONE MOBILE CONTAMINA LA TV DI CASA

L'app sarà la regina del focolare

ALLEGRA GELLER

Appmania. Fino a un paio di anni fa nessuno avrebbe parlato di *app*, che non è altro che il diminutivo di applicazioni, intese come programmi, software. Oggi, però, con *app* s'intendono soprattutto quei software altamente specializzati (tendenzialmente servono a fare una cosa e solo quella) che sono la principale caratteristica di smartphone e tablet. Da un punto di vista del business, poi, le *app* sono cruciali perché per lo più sono recuperabili solo attraverso gli *store* di pochi grandi *player* (anche se a ruota ogni produttore di hardware ha aperto la sua vetrina digitale di software). Il che ci porta alla solita infinita guerra tra Apple (pioniere di questo modello di business con l'iTunes Store inizialmente limitato alla sola musica per iPod) e Google (con il suo sistema operativo *Android* e il suo *store* che di recente ha assunto il nome di Play, e in cui si compra di tutto, dai libri alle *app* appunto). Ma le *app* non sono solo sui terminali mobili, bensì sono il cuore delle *smart tv*, i televisori intelligenti che stanno gradualmente sostituendo quelli «stupidi» (cioè limitati al *broadcasting*) che hanno caratterizzato decenni di storia del settore.

In questo particolare comparto si distingue Samsung. Prima rivale di Apple nei terminali mobili, rispetto a Cupertino il colosso coreano è un passo avanti nel portare questo rivoluzionario interfaccia nel salotto di casa o, meglio (visto che anche smartphone e tablet stanno conquistando un ruolo importante anche sul divano), sulla parete del salotto di casa. «Il nostro investimento in ricerca e sviluppo - spiega Alberto Strani, Smart Tv Contents & Solutions Manager di Samsung Electronics Italia - per il mercato dei televisori, di cui oggi deteniamo una quota pari al 53% (il dato si riferisce a tutti gli schermi di nuova generazione che comprendono anche i

Led Tv, *ndr*), sta esplorando sempre nuove frontiere di intrattenimento per offrire un'esperienza a 360 gradi attraverso un'interfaccia coinvolgente ricca di applicazioni, servizi e contenuti, e ovviamente interattiva. Fattore che è alla base del successo dei dispositivi mobili. La rivoluzione *smart tv*, che nel 2011 ha visto una vendita di oltre 800.000 unità e si prevede continuerà a crescere nel corso di quest'anno, trasforma in questo modo il ruolo tradizionale del televisore, che diventa il centro della vita famigliare dentro e fuori casa attraverso applicazioni che rispecchiano lo stile di vita moderno, semplificando le attività quotidiane».

Ma se le *app* sono prevalentemente viste come strumento di *entertainment* (per i terminali mobili esistono anche software professionali di tutto rispetto, ma ovviamente la gran massa degli utenti si limita a programmi per musica, giochi e simili), Samsung pone proprio l'accento sull'utilità di queste nella vita quotidiana. Intrattenere sì, ma anche fornire un aiuto per tutte le attività di una persona e ancor più di una famiglia. Le app più innovative su cui Samsung si sta concentrando spaziano da soluzioni che consentono una gestione più oculata del budget familiare (cruciale in tempi di crisi), a quelle che permettono di monitorare salute e benessere in modo semplice e immediato, compatibilmente con uno stile di vita sempre più frenetico che lascia pochissimo tempo per la cura di se stessi. Senza dimenticare l'esigenza di gestire al meglio la vita privata, controllando anche da remoto i vari dispositivi domestici e facendoli dialogare tra loro, per ottimizzare tempo ed efficienza e per arricchire le opportunità di informazione, espressione e condivisione. «Non più solo *gaming* e intrattenimento, quindi, ma anche servizi di qualità, in grado di garantire un reale beneficio al consumatore: dal monitoraggio di salute e benessere alla gestione dell'economia, dal controllo anche da remoto dei dispositivi domestici per ottimizzare tempo ed efficienza fino all'educazione dei più piccoli in modo divertente e interattivo», ricorda Strani.

Da non sottovalutare, poi, l'integrazione tra il mondo delle app che ci portiamo in tasca e quello che sta nella tv di casa. E Samsung, ovviamente, gioca la partita su entrambi i fronti. «Pur essendo focalizzati sullo sviluppo e sulla distribuzione dei nostri prodotti molto amati dai consumatori - spiega Antonio Bosio, Product & Solutions Director di Samsung Electronics Italia - siamo consapevoli che le applicazioni siano un importante completamento dei nostri dispositivi. Abbiamo quindi sviluppato una serie di partnership con primari *content provider* che sono in grado oggi di erogare i propri contenuti e servizi attraverso i nostri dispositivi connessi, smartphone, tablet e *smart tv*. A differenza di quanto altri hanno ritenuto di fare, abbiamo scelto strategicamente di limitare il numero di applicazioni, preoccupandoci molto più della reale utilità e *appeal* di ciascuna di esse piuttosto che del solo dato quantitativo. Lavoriamo costantemente affinché i servizi di ciascuno dei nostri partner siano disponibili su tutti i nostri prodotti e, al tempo stesso, in modalità ottimizzata per ciascun modello in funzione delle dimensioni del display, della presenza di un'interfaccia touch ed eventuali altre caratteristiche. La nuova frontiera è quella dell'interazione di prossimità tra smartphone, tablet e *smart tv*, con la possibilità di guardare il contenuto sul televisore e al tempo stessa accedere alla componente *social* o all'approfondimento con il tablet».

SCENARIO di Rodolfo Falcone*

Quando l'Informatica Diventa Business. Illecito

Nel 2010, l'Fbi ha collaborato a un'operazione a livello mondiale volta a bloccare un atto criminoso che aveva sottratto circa 70 milioni di dollari a banche americane. L'arma scelta dalla gang non era una mitragliatrice o un set di strumenti da scassinatore, si è invece affidata al *trojan* ZeuS per accedere illegalmente ai conti correnti dei clienti. Questo episodio in realtà evidenzia un trend che si sta verificando nel mondo della sicurezza. Sono ormai lontani i giorni in cui la pirateria informatica era finalizzata al puro divertimento o ad atti dimostrativi. Nel mondo del cibercrimine odierno la spinta a commettere reati risiede nella possibilità di acquisire numeri di carte di credito, credenziali, dati di accesso a siti di *home banking* e ogni altra informazione che nel mercato nero possa essere trasformata in denaro sonante.

In questo business delle informazioni ottenute in modo illecito, opera un mix di criminali indipendenti e gruppi organizzati guidati dalla fame di denaro anche se, in alcuni casi, restano le motivazioni politiche. Che a guidare le azioni sia l'*hacktivism* o gli interessi economici della bande criminali, il cui principale obiettivo sono le aziende di brokeraggio, due cose sono certe: questi gruppi hanno modificato la realtà della sicurezza per le aziende. Una consapevolezza fondamentale per combatterli.

Comprendere la struttura di questi gruppi offre agli esperti di sicurezza la possibilità di disturbarli intercettando diversi anelli della catena delle attività di criminalità informatica. Queste azioni possono comprendere dal monitoraggio dei siti in cui vengono vendute le informazioni sulle carte di credito al controllo di *internet service provider* (Isp) noti per la loro «amicizia» con gruppi criminali. È importante ricordare che i gruppi pirati informatici si presentano sotto le più molteplici forme. Alcuni addirittura svolgono operazioni che ci si aspetterebbe di vedere effettuate da aziende legittime. Altri dispongono di membri con competenze di marketing, utilizzate per diffondere minacce e sottrarre informazioni attraverso social network e in generale in siti di community in cui possono promuovere *botnet* (reti di pc infetti, all'insaputa dei proprietari, la cui capacità di calcolo è utilizzata per fini illeciti, *ndr*) e *malware*.

Nella maggior parte dei casi, questi diversi team collaborano in maniera indipendente, con figure centrali che sovrintendono alle attività. Ma non tutti i cibercriminali sono parte di un gruppo. Alcuni stanno da soli e affittano porzioni di *botnet* che hanno assemblato. Altri guadagnano facendo quello in cui sono bravi, come scoprire nuove vulnerabilità di software e realizzare strumenti offensivi per altri cibercriminali. Questi lati deboli, noti nel settore della sicurezza come *zero-day*, potrebbero facilmente rendere ricchi coloro che le individuano e le sfruttano: secondo software e sua affidabilità con *exploit* che possono fruttare 10.000-500.000 dollari sul mercato nero.

ATTACCO A YAHOO!
Di ieri è l'annuncio, da parte di un gruppo sconosciuto di hacker (D33DS Company), del furto dei dati sensibili (*password* comprese) di 450.000 utenti di Yahoo! (che ha ovviamente avviato subito un'indagine interna). I dati sarebbero stati sottratti da un server dell'azienda californiana. D33DS Company avrebbe avuto accesso attraverso un sottodominio del sito di Yahoo! alle informazioni che non sarebbero state crittate. In particolare, sarebbe stato colpito Yahoo! Voices, un servizio Voip dell'azienda Usa.

Sia *gli zero-day* che altri *exploit* spesso vengono inseriti in *toolkit* di attacco disponibili su forum nel Web anche a cifre irrisorie (40 dollari), ma le versioni più sofisticate possono arrivare a costare diverse migliaia di dollari. Questi strumenti tipicamente si affidano al fatto che molti utenti non dispongono delle più recenti versioni del software, e si avvalgono di note vulnerabilità piuttosto che di *zero-day*. In alcuni casi, i criminali compromettono siti legittimi e tentano di reindirizzare gli utenti verso siti malevoli che integrano l'*exploit kit* (il software malevolo, *ndr*).

In generale, l'obiettivo degli assalitori rimangono i dati di valore. Oggi, tuttavia, le informazioni delle carte di credito condividono lo spazio nei negozi virtuali della malavita informatica con di dati di accesso (nome utente e *password*, *ndr*) a Facebook o alle caselle di posta elettronica. Questo è dovuto in parte alle banche che utilizzano diverse forme di autenticazione per verificare le transazioni *online*, il che impone ai criminali di disporre di maggiori informazioni al fine di compromettere un conto corrente. I cibercriminali hanno quindi fatto evolvere il loro *malware*, anche con moduli che cercano informazioni quali il numero Imei (International Mobile Equipment Identity) del cellulare di un individuo di modo che sia possibile contattare il *service provider* dell'utente e ottenere una nuova Sim, con cui diventa più semplice intercettare le comunicazioni tra la banca e il cliente intese a prevenire le frodi.

Non è una sorpresa che maggiori siano le informazioni in mano ai criminali, più mirato sarà l'attacco, e la probabilità di successo. Per esempio, si presta maggiore attenzione a un messaggio indirizzato a noi stessi che non a uno che riporta «all'attenzione di...». Questa tecnica si chiama *spear phishing*, ed è correlata ad alcuni dei più gravi *breach* avvenuti di recente. La lotta al *cybercrime*, in parte, richiede la formazione degli utenti in merito ad alcuni dei segnali necessari a identificare e-mail sospette, a partire da messaggi con richieste inusuali di informazioni o parole chiave che invitano gli utenti a scaricare allegati potenzialmente pericolosi.

Poiché i criminali informatici sono focalizzati sui dati, è fondamentale che le imprese facciamo altrettanto. Le aziende devono identificare i dati critici e salvaguardarli in modo appropriato, con *firewall*, cifratura e tecnologie di monitoraggio. Prendendo in prestito una citazione del noto stratega militare cinese Sun Tzu: «Se non conosci né te stesso né il nemico, sarai sempre in pericolo». Il che è ancora più vero nel ciberspazio.

**Country manager per l'Italia di Check Point Software Technologies, azienda israeliana quotata al Nasdaq specializzata in soluzioni di sicurezza It*