La sicurezza della filiera di Internet in Italia: rischi, resilienza e fragilità

Il Salotto di MIX, principale evento organizzato ogni anno dal Milan Internet Exchange, si è occupato quest'anno dei temi della sicurezza. Lo spunto era stato dato da alcuni articoli apparsi quest'estate sui quotidiani che ponevano l'attenzione sugli Internet Exchange Point (IXP) italiani. È certamente una buona cosa che venga evidenziato il ruolo degli IXP all'interno della filiera dell'Internet italiana: molto spesso, infatti, ci si dimentica del ruolo strategico di facilitatori che questi svolgono sia nei confronti degli operatori, che possono interconnettersi tra loro riducendo i costi e migliorando la qualità del servizio offerto ai propri clienti), sia nei confronti degli utenti finali, individui ed organizzazioni, che godono di una migliore "*user experience*". Entrando poi nel tema della sicurezza, tramite un IXP gli utenti hanno anche la garanzia che i loro dati seguano percorsi interamente all'interno del nostro Paese e siano gestiti da operatori sempre soggetti alle leggi nazionali.
Il tema regolamentare è particolarmente significativo, anche perché è stato il Garante della Privacy che per primo ha messo sotto osservazione gli IXP, sollevando anche il problema del loro status nel contesto della normativa italiana. Il problema esiste e proprio in questi giorni viene affrontato, ma in modo scevro da allarmismi e titoli scandalistici, andando concretamente alla base della questione.

Il sottotitolo dell'evento, provocatoriamente "Lo sai o lo pensi", vuole proprio sottolineare come certe affermazioni false passino di bocca in bocca o circolino in rete senza che nessuno le abbia mai davvero verificate. Ad esempio, non è vero che tutte le telefonate degli italiani passano per il MIX o comunque attraverso gli IXP italiani: per quanto la tecnologia IP sia diventata pervasiva anche per la telefonia, l'interconnessione tra operatori di telefonia ha regolamentazione a sé e modalità tecniche distinte da Internet. Per quanto riguarda il traffico Internet in genere, comprese le e-mail degli italiani, certamente una parte viaggia attraverso MIX, che con 230 Gbps di picco di traffico scambiato, costituisce una significativa componente del traffico Internet tra soggetti operanti in Italia, e quote più piccole sono veicolate attraverso gli altri IXP. Ma non si tratta certamente della "totalità del traffico", sia perché alcuni grandi operatori preferiscono ancora diversificare le proprie infrastrutture di interconnessione, gestendo una combinazione di interconnessioni dirette con altri operatori consimili (meno efficienti e più soggette a problemi di pianificazione degli upgrade) insieme all'interconnessione presso alcuni IXP per tutte le altre opportunità di peering (con operatori consimili e con content provider e OTT, presenti in modo sempre più significativo presso MIX).
Come ho avuto modo di sottolineare nel Salotto, il traffico che passa attraverso un IXP deve essere sempre inteso come una ottimizzazione del percorso seguito, perché, per la definizione stessa di IXP, ogni operatore deve disporre di percorsi verso la Big Internet che siano alternativi a quelli che attraverso lo specifico IXP. Si tratta di un punto importante: i servizi di IXP sono in libero mercato ed ogni cliente decide autonomamente se e quanto vuole usufruirne; quindi, sempre in termini di libero mercato, è interesse di un IXP garantire ai suoi clienti la massima affidabilità delle infrastrutture, pena l'emarginazione del suo business.

Mi si consenta di sottolineare che, se negli ultimi 2 anni MIX è cresciuto, sia in numero di clienti che in banda trasmissiva veicolata, più della media dei principali IXP d'Europa, è segno che questa affidabilità viene riconosciuta.
Un analogo discorso può essere fatto per quanto riguarda la sicurezza informatica delle infrastrutture di un IXP. Intanto occorre premettere che si tratta di sistemi ICT relativamente semplici rispetto alla complessità dell'Internet dei nostri giorni; in secondo luogo si tratta di una questione di reputazione: in un mondo dove le notizie viaggiano istantaneamente, anche il solo sospetto di non garantire l'integrità e la riservatezza dei flussi di dato in transito attraverso gli apparati dello IXP provocherebbe l'immediata reazione degli operatori clienti che potrebbero scegliere di spostare altrove il traffico di interscambio, alla velocità del cambio di una configurazione software.
Questo per quanto attiene alla sostanza. Ma questo non implica che non debba esserci un ruolo di vigilanza e di verifica da parte delle autorità preposte, sia pure tenendo conto del ruolo specifico degli IXP. Infatti questi sono operatori atipici, sia per questo ruolo di facilitatori, sia perché non hanno una forte connotazione "for profit" (molti di loro hanno natura consortile, ad esempio), sia per l'esclusività geografica che ognuno di essi, di fatto, possiede.
Al termine del convegno è stata sottolineata, da parte dei rappresentanti delle autorità pubbliche presenti (nello specifico: il Ministero dello Sviluppo Economico, il Garante della Privacy ed il Centro nazionale anticrimine informatico per la protezione delle infrastrutture critiche, CNAIPIC) la scelta di un percorso collaborativo, volto prima a conoscere e capire e poi, solo in seguito, a normare ed eventualmente sanzionare. Un primo frutto di questo approccio è la stesura di un Codice di Autoregolamentazione degli IXP italiani, sollecitato dal MISE e la cui bozza è stata finalizzata e sottoscritta da MIX, NAMEX e TOPIX proprio in questi giorni.

Il Salotto di MIX è stata anche l'occasione per riflettere sugli aspetti di sicurezza di Internet nel senso più ampio. È stata sottolineata la pervasività della Rete in tutti gli aspetti della nostra vita, non ultimo come infrastruttura sottostante delle comunicazioni di ogni genere, tanto che anche per una diversa infrastruttura critica nazionale, la rete gas di SNAM, presente all'evento come esempio di quello che avviene in contesti diversi da quello ICT, è stato verificato che la componente di comunicazione ed interconnessione telematica finisce per essere uno degli snodi critici.
La sempre più pervasiva dipendenza dalla Rete per qualsiasi aspetto della nostra vita porta ad alcune considerazioni di scenario.
Il flusso dei dati via Internet. Dopo Snowden ed il Datagate è cresciuta molto la preoccupazione, e talvolta la paranoia, circa la possibilità che qualche soggetto possa intercettare il traffico Internet in modo massivo, estraendo informazioni critiche e costruendo archivi di dati sensibili da analizzare secondo le metodologie dei "Big Data". In Germania, ad esempio, è attiva un'iniziativa per confinare l'interscambio tra soggetti nazionali all'interno del Paese. In ogni caso, è ovvio che il grado di trust che si può avere nei confronti di un operatore che sia soggetto alle leggi nazionali è molto più alto di una lunga filiera di operatori, dei quali solo quelli terminali operano nel Paese, mentre quelli intermedi sono soggetti internazionali aventi sedi magari fuori dall'Europa; per non parlare dei casi in cui, come riportato dagli esperti di sicurezza presenti al Salotto, il traffico Internet viene dirottato, per un errore di configurazione del "*routing*" di Internet - o per un'azione illegale volontaria - attraverso un paese terzo di dubbia reputazione.
"Mantenere il traffico locale sempre locale" è un comandamento che attiene alla sicurezza e non solo all'ottimizzazione dei flussi trasmissivi. E quindi fa un specie che qualche operatore di accesso con grande forza di mercato neghi l'interconnessione diretta ad altri operatori, forse non altrettanto grandi, imponendo di fatto tortuosi percorsi che viaggiano attraverso tutto il mondo per consentire ad utenti italiani di accedere servizi e contenuti italiani. Uno scenario preoccupante, specie quando i dati veicolati

sono sensibili, o strategici, ed in ogni caso ogni volta che questo flusso riguarda la Pubblica Amministrazione.

I sistemi di posta elettronica. È stato fatto osservare che, mentre il Garante delle Privacy si preoccupa, giustamente, che tutti gli operatori di telecomunicazione, ed ora anche gli IXP, soddisfino requisiti di sicurezza informatica previsti dalle leggi, nessuno segnala come sia sempre più diffusa l'adozione di sistemi di posta elettronica, GMail è un esempio, che contrattualmente hanno diritto a leggere ed estrarre informazioni dalle mail scambiate. Non è solo un problema di cultura e conoscenza della Rete da parte dei singoli utenti: sono stati segnalati casi in cui sono soggetti pubblici, come le Università, che scelgono di andar dietro a questa moda, adducendo ragioni economiche che appaiono molto miopi.

Grandi flussi di dati o analisi dei piccoli segnali. All'apertura del Salotto è stato proiettato l'intervento che pochi giorni prima Geoff Houston, grande esperto della Rete e CTP di APNIC, aveva tenuto alla Conferenza di RIPE. Nella presentazione Geoff mostra come, da un'analisi di piccole anomalie (1 su 400) negli accessi ad un server Web gestito da APNIC, era stato possibile risalire ad un "pattern" ben chiaro che mostrava che un grande numero di sistemi, in tutto il mondo, era stato compromesso attraverso un'azione sistematica, e che c'era evidenza - lo "*smoking gun*" - che la centrale di gestione di tutto il meccanismo fosse in Cina. Nessun segreto industriale era coinvolto, ma la consapevolezza che possa esserci qualcuno che è in grado di tener traccia di qualunque sito web venga visitato dal mio PC, senza aver bisogno di interagire con i doppini in rame, le fibre ottiche e gli apparati trasmissivi direttamente coinvolti, è davvero allarmante.

In conclusione, la complessità e pervasività di Internet in tutti gli aspetti della nostra vita è un fatto ormai conclamato; quando, 6 anni fa, sempre al Salotto del MIX si parlò di sicurezza, poteva essere un tema da addetti ai lavori, ma oggi fa parte della vita di tutti noi. Come dice il detto "Ogni problema complesso ha una soluzione semplice e totalmente sbagliata": non ci sono ricette facili o scorciatoie per la sicurezza, ogni elemento dell'infrastruttura è più o meno critico o strategico, ma tutti sono importanti ed anche nelle pieghe più recondite della Rete si può celare un pericolo.

La sicurezza informatica richiede vigilanza continua, con la consapevolezza che molto si può fare, ma nulla può essere reso totalmente sicuro. Alla fine delle fini sarà sempre una questione di equilibrio, di *trade-off*, tra rischi, costi e fruibilità.

Joy Marino
Presidente MIX