Aria Nuova in ICT

Sommario:

Gli ultimi avvenimenti nell'ambito della sicurezza ICT portano a fare alcune riflessioni sul suo sviluppo negli ultimi anni nell'ottica di capire le tendenze per il prossimo futuro ed i principali rischi che potremmo incontrare.

Il titolo potrebbe trarre in inganno il lettore in quanto potrebbe aspettarsi che questo articolo presenti qualche gustosa novità tecnologica. Invece questo articolo vuole presentare alcune considerazioni ad alto livello sugli ultimi avvenimenti in ICT, visti comunque da un professionista di sicurezza, anche per stimolare alcune riflessioni personali del lettore che non è detto sia d'accordo con le conclusioni che trarremo.

Prima di tutto, non è un caso l'utilizzo in questo articolo del termine 'ICT' invece del più comune 'IT'. La 'C' in ICT sta per Comunicazione, ed oggi questo è probabilmente l'aspetto principale da tenere in considerazione.

Ma andiamo con ordine.

Considerazioni Tecnologiche

Negli ultimi 10 anni molti è cambiato in ICT. Considerando le più recenti e significative novità, potremmo riassumerle in

- Web 2.0 (e 3.0)
- Mobile computing
- Social networking.

Dal punto di vista tecnologico, questo si declina in varie componenti di cui elenchiamo i principali. Per primo vi è stato un impressionante aumento della velocità di connessione alla rete dei client siano essi

PC via Adsl, che terminali mobili via UMTS, WiFi ecc. Poi l'aumento di potenza con contestuale riduzione di consumi e dimensioni dell'HW, dalle CPU alle memorie ecc., per cui la potenza computazionale di un telefonino oggi è superiore a quella di un PC di qualche anno fa e di un super-computer di tre decadi fa. Infine l'emergere di nuove tecnologie per lo sviluppo di applicazioni 'Web-based'.

Quest'ultimo punto richiede qualche ulteriore commento in quanto la storia degli ultimi 20 anni è abbastanza interessante. Il modello client-server ha subito infatti molte modifiche: siamo partiti dal terminale 'dumb' connesso ad un mainframe; siamo poi passati a terminali 'intelligenti' connessi a mini-computer (anche noti come Server, tanto per confondere le idee); arrivati al PC come Personal mini-Computer indipendente ove il server è un sito Web (o simile) molto remoto che fornisce informazioni poco strutturate in pagine statiche; al Web 1.0, ove le informazioni tornano al server ed il terminale è al contempo 'dumb' per quanto riguarda le interazioni con il server, ma un PC per i dati locali; al Web 2.0, ove il terminale/PC diventa 'rich' ed esegue parte delle elaborazioni a lui demandate dal server permettendo al contempo di alleggerire il server di elaborazioni, diminuire il traffico in rete e condividere più dati tra client e server; ed infine alla visione prossima ventura ed in parte già presente (Web 3.0, Google computing ecc.) ove il terminale non è più un computer (seppure Personal) ma è una 'rich interface', ove i dati risiedono sul server ed il client è incaricato della rappresentazione delle informazioni nel formato adatto al proprio HW.

Facendo un cortocircuito tra gli albori dell'ICT e l'oggi/domani, la storia si può riassumere dicendo che siamo partiti da un modello 'client-dumb' <=> 'server', per arrivare ad un modello 'client-rich' <=> 'server' passando per il 'Personal Computing'.

La storia alle volte è proprio strana!

Considerazioni sull'utilizzo e gli utilizzatori

Se le principali novità tecnologiche sono state il Web 2.0 (e 3.0), il Mobile computing ed il Social networking, quello che è cambiato per gli utilizzatori è praticamente tutto.

Siamo passati da un situazione ove bisognava essere degli esperti dotati di strumenti (HW/SW) appositi per poter utilizzare queste tecnologie, alla situazione attuale ove chiunque vi ha accesso con strumenti disponibili in qualunque supermercato e che spesso si ottengono facilmente con i punti fedeltà dei ne-

gozi. Gli aspetti principali che hanno permesso ciò sono:

- la riduzione del costo degli apparati
- la riduzione delle dimensioni e la migliore maneggevolezza dell'HW
- la fruibilità degli applicativi.

In particolare la facilità di uso, oltre ovviamente ad altre usuali condizioni, è uno degli ingredienti fondamentali del successo di Facebook, Twitter, Flickr, Linkedin, solo per citare i più comuni.

Infatti anche solo un wiki o blog richiede in realtà un qualche tipo di conoscenza e livello di competenza per poter essere utilizzato, mentre strumenti quali twitter sono così semplici, ovviamente dal nostro punto di vista anche limitati, che possono essere intuitivamente utilizzati da chiunque. Associando alla semplicità d'uso

- la immediatezza della comunicazione
- la ubiquità degli strumenti e degli utilizzatori
- la facilità di memorizzazione e ricerca delle informazioni

si ottengono strumenti (semplici) che superano od eliminano le passate barriere spazio/temporali nella diffusione delle informazioni. Essere in contatto 'ora' con le persone che ci interessano indipendentemente dallo spazio e dal tempo, unito alla possibilità di trovare 'ora' le informazioni cercate, è una rivoluzione per il genere umano forse paragonabile all'avvento della stampa o del telegrafo/telefono.

Da questo punto di vista è anche abbastanza ovvio che strumenti che forniscono all'individuo questi servizi derivino dal cellulare piuttosto che dal PC. Il cellulare è lo strumento che oltre alla sua mobilità, offre una facilità d'uso che lo rende universale. Il PC anche se molto diffuso, rimane uno strumento troppo tecnico per i più, utilizzabile veramente solo dagli esperti.

Informazioni e Privacy

Lo scenario, da un certo punto di vista apocalittico, che ci si sta palesando è quello di un mondo ove una esorbitante quantità di informazioni personali di ciascuno di noi è archiviata in tempo reale in molteplici server/archivi distribuiti sul globo terrestre così da essere immediatamente disponibile ai nostri

amici o a chi ne abbia comunque accesso, intenzionalmente autorizzato o meno.

Già ora cominciamo a vedere le prime novità dovute a questo. Ad esempio, sempre più indicatori segnalano come nella vita politica delle nazioni avanzate, dagli USA alla nostra stessa Italia, il ruolo dei social network diventi sempre più importante spesso a scapito della stampa e della televisione. Ma forse più eclatante è il ruolo svolto da queste tecnologie nelle recenti vicende politiche dei paesi del nord Africa e medio Oriente, od anche di nazioni del terzo mondo ove l'accesso ad un cellulare può letteralmente cambiare la vita. Questo è ulteriormente evidenziato dal fatto che in situazioni di grave conflitto politico recentemente sta diventando frequente il tentativo di bloccare l'accesso e l'utilizzo di questi strumenti.

In queste situazioni poter comunicare liberamente ed avere accesso alle informazioni è sicuramente un fatto positivo. Ma vi sono almeno due fattori negativi da valutare attentamente.

Il primo è che è molto spesso difficile se non impossibile essere certi della fonte di informazioni. Nelle comunicazioni personali dirette, si ha a che fare con una persona ed ognuno di noi è in grado di valutare con in qualche maniera l'attendibilità della stessa. Almeno abbiamo una storia milionaria di imbroglino e millantatori. Per le informazioni che otteniamo da libri, radio e televisioni, giornali ecc. possiamo farci un'idea di chi gestisce le informazioni e di quanto sia attendibile.

Il mondo dei social network, con la sua totale de-localizzazione e la possibilità di comunicazione non filtrata, in tempo reale molti-a-molti, rende in pratica impossibile ogni valutazione sulla attendibilità delle informazioni. E' molto facile costruire informazioni totalmente fasulle, come recentemente dimostrato ad esempio dal caso di Amina [1]. Il rischio è grande!

Il secondo fattore da valutare va generalmente sotto il nome di Privacy.

Finché faccio delle chiacchiere al bar con amici, ho un numero limitato di interlocutori che tipicamente conosco e che per lo più non si ricorderanno quello che ho detto. Le informazioni scambiate diventeranno con il tempo sempre più vaghe (alle volte deformate e ingannevoli) e scompariranno. Nella incertezza delle chiacchiere sarà comunque sempre possibile negare di aver detto qualche cosa o sostenere un malinteso. Tutte queste condizioni non valgono nel mondo dei social network:

- le informazioni sono normalmente attribuibili (a meno che non si prendano misure per mascherare la propria identità, tecniche normalmente non accessibili ai più, od in casi di furti di identi-

tà)

- le informazioni non sono cancellabili né modificabili, anzi spesso non sono più neanche di tua proprietà!
- È impossibile controllare chi può avere accesso alle informazioni.

Riassumendo, due parole al bar possono suscitare una grassa risata, le stesse parole su un social network possono rovinarti la vita, per sempre.

Purtroppo ben pochi sono coscienti di questi rischi.

ICT e sicurezza

In questo scenario, come già notato da alcuni punti di vista apocalittico, molte responsabilità ricadono sulle spalle di chi gestisce l'ICT. In particolare la centralizzazione delle informazioni pone un enorme fardello sulle nostre spalle. Siamo in grado di portarlo e di rispondere alle sfide di oggi e domani?

Il primo aspetto da valutare è l'integrità morale di persone ed aziende dell'ICT. Per ovvi motivi lasciamo al lettore fare le proprie considerazioni personali su questo aspetto.

Per quanto riguarda l'aspetto tecnologico, molto è cambiato negli ultimi 10 anni, ma al contempo ben poco è cambiato nell'approccio alla sicurezza da parte delle aziende ICT. Sono decenni che gli esperti di sicurezza predicano un approccio pro-attivo e olistico alla sicurezza in ICT. E' vero che in alcuni casi questo è stato adottato, ma la filosofia generale rimane tipicamente:

- non considerare la sicurezza, o alcuni aspetti di sicurezza, sino a che non sia veramente necessario, quindi a-posteriori
- quando si verificano i primi problemi, negare e sperare che scompaiano da se
- se proprio non si può fare altrimenti, fare quello che si sarebbe dovuto fare sin dall'inizio.

E' probabile che questo approccio abbia senso dal punto di vista economico, ovvero che l'introduzione a priori della sicurezza non sia giustificato in termini di ROI sino a che non vi siano sufficienti 'incidenti' da renderla necessaria. Basta seguire un attimo le più recenti vicende dei più grandi produttori/fornitori di ICT, da Microsoft a Apple, RSA, Sony ecc. [2,3,4,5] per farsi un quadro di come viene gestita

usualmente la sicurezza ICT.

D'altra parte, se la sicurezza non è ancora, e forse non lo sarà mai, pro-attiva e olistica, sicuramente negli ultimi 10 anni molti passi avanti sono stati fatti dal punto di vista della reattività. Molti sono i segnali a questo proposito e vale la pena citarne alcuni:

- la recente eliminazione dell'auto-run da parte di Microsoft [3]
- il recente take-down del botnet Rustock [4]
- la fiorente industria degli anti-virus, anti-spam, anti-spyware, anti-adware ecc. ora non solo per i PC con S.O. Microsoft ma anche per altri S.O. e piattaforme mobili
- il mercato dei firewall, proxy, (web-) application firewall ecc.
- le politiche e normative sulla comunicazione riguardante gli incidenti di sicurezza informatica (soprattutto negli USA)
- la normativa sulla Privacy Europea
- l'effetto delle normative di settore quali PCI-DSS ecc.

Tutto ciò è venuto per lo più come una continua corsa a guardie e ladri, ove le guardie rincorrono quasi sempre i ladri e poche volte si trovano davanti a loro.

Se 15 anni fa il 'cracking' era per lo più fatto per diletto, sfida e poche volte come atto criminale, negli anni 2000 la criminalità ha preso il controllo delle attività illecite in ICT portandoci lo spam, i botnet, i trojan modulari ed acquistabili sul mercato, ed attività sempre più mirate al guadagno finanziario, ovvero la truffa ed il furto online.

L'industria ICT, dopo un po' di tentennamenti, ha risposto migliorando la qualità del software, introducendo procedure di disclosure e aggiornamento automatico tant'è che oggi la malavita si rivolge sempre più alla truffa verso l'utilizzatore finale piuttosto che all'attacco tecnologico che sfrutta vulnerabilità del software. Infatti negli ultimi tempi si è visto un aumento dei finti anti-virus, in realtà malware, e finti servizi che cercano di aggirare la fiducia dell'utente piuttosto che la tecnologia da lui usata.

Ma questo ci pone un problema ancora più grande: disegnare le applicazioni in modo che risulti molto arduo truffare l'utente che le utilizza è una missione in pratica impossibile visto che ha a che vedere più

con l'aspetto umano che con l'aspetto tecnologico. Come faremo?

La rinascita degli script-kiddies

Infine, ricollegandoci a quando descritto inizialmente, è molto interessante considerare il ruolo e significato di alcuni fenomeni strettamente legati alla situazione attuale dell'ICT e le cui conseguenze non sono ancora chiare.

Ci riferiamo principalmente ai casi Wikileaks, Anonymous [7] e Lulzsec [8], che ci segnalano dei nuovi sviluppi nel mondo dell'underground ma intrinsecamente legati al social networking ed alla sicurezza ICT.

Tutti siamo a conoscenza delle vicende di Wikileaks ove il social networking è stato allo stesso tempo la sorgente delle informazioni e il mezzo per la loro diffusione. Come già detto, la chiacchiera la bar una volta scritta nel mondo virtuale diventa incontrollabile e può avere conseguenze imprevedibili come ben le diplomazie di molti paesi hanno visto.

Rimane da capire se qualcuno abbia imparato qualcosa da tutto ciò e quali siano le lezioni ed i provvedimenti da adottare. Per ora nulla sembra cambiato.

L'evento Wikileaks ha però molto probabilmente funzionato anche da catalizzatore di alcuni movimenti già attivi ma scoordinati nel mondo del social networking. Si tratta molto probabilmente per lo più di giovani, alcuni con notevoli capacità tecniche, altri per lo più con motivazioni che potremmo classificare in senso lato come 'politiche', che vogliono dimostrare il loro dissenso, disaffezione ed insoddisfazione per vari e diversi motivi tra cui alcuni che abbiamo citato anche noi in questo articolo. Ovviamente le principali motivazioni delle loro azioni vanno dall'esperienza ludica, alla bravata dimostrativa alla 'vendetta' personale. Sembrerebbe di essere tornati ai tempi degli script-kiddies, ma la situazione è molto diversa.

Le dimostrazioni, gli atti di sabotaggio ed intrusione degli Anonymous e Lulzsec, suonano come un vero e ultimo campanello d'allarme verso sia gli utilizzatori sia i gestori dei sistemi ICT, dei rischi del “social networking always-on” associato alle attuali pratiche di sicurezza ICT. Se il Denial-of-Service è oggi facile da implementare è addirittura imbarazzante [9] la facilità con cui questi gruppi riescono ad accedere agli elenchi degli utenti dei servizi online da loro attaccati ottenendone credenziali, indirizzi

di posta elettronica, informazioni personali ecc. che poi rendono pubbliche per lo più ad onta del fornitore dei servizi (anche se questo può danneggiare direttamente anche gli utenti titolari delle informazioni).

A questo punto è forse meglio lasciare al lettore fare le proprie riflessioni e trarne le proprie conclusioni. Da parte nostra ci piacerebbe solo che queste considerazioni agiscano da stimolo per lo sviluppo di un ICT più sicuro nel segno del social networking.

Andrea Pasquinucci (PhD CISA CISSP, socio AIEA) è un consulente freelance in sicurezza informatica. Si occupa prevalentemente di progetti di sicurezza ICT, audit, compliance, governance e formazione ICT per il management ed il personale tecnico. In particolare è esperto di sicurezza delle reti e dei servizi web, dei sistemi operativi e di crittografia.

Riferimenti

[1] Si veda ad esempio http://27esimaora.corriere.it/articolo/amicizie-online-con-persone-mai-viste-ma-sappiamo-davvero-chi-ci-sta-davanti/

[2] http://punto-informatico.it/3149929/PI/News/macdefender-finto-antivirus-mac.aspx

[3] http://punto-informatico.it/3086044/PI/News/microsoft-come-eliminare-autorun.aspx

[4] http://punto-informatico.it/3112596/PI/News/microsoft-attacco-alla-botnet.aspx

[5] http://punto-informatico.it/3125285/PI/News/rsa-anatomia-un-attacco.aspx

[6] http://punto-informatico.it/3146073/PI/News/psn-grosso-guaio-sony-town.aspx

[7] Si veda ad esempio: http://nakedsecurity.sophos.com/2011/02/07/hbgary-federal-hacked-and-exposed-by-anonymous/

[8] Si veda ad esempio: http://www.theregister.co.uk/2011/06/15/lulzsec_eve_online/ , http://www.theregister.co.uk/2011/06/17/lulzsec_release_aus_data/

[9] Si noti la contraddizione con le affermazioni della sezione precedente, anche se probabilmente non vi è valenza economica diretta in questo caso e quindi l'interesse da parte della criminalità per questo tipo di attacchi, per lo più molto evidenti e facilmente individuabili, è praticamente assente.