Informatica

Gioie e dolori della posta elettronica

di Nicola Bortolotti

Cosa portereste con voi e con il vostro business sulla classica "isola deserta"? Quasi certamente il computer, ma se - in aggiunta - vi fosse chiesto di scegliere un solo servizio Internet fra tutti quelli disponibili, la palma dell'"irrinunciabile" probabilmente spetterebbe proprio alla posta elettronica, la "E-Mail" grazie alla quale avete ricevuto anche questo numero de "I Servizi Funerari".
Detto per inciso, l'impatto di "world-wide-web" e navigazione ipertestuale è stato e rimarrà sicuramente indelebile neI tempo, tanto che i più accorti potrebbero astutamente scegliere come servizio proprio questo, giocando sul fatto che ormai quasi tutti i providers offrono anche la cosiddetta "interfaccia web" per la gestione della propria posta elettronica.
Ma rimane il fatto che l'E-Mail può vantare una storia più ricca ed ha modificato tempi e modi di lavoro in maniera ancor più rilevante di quanto non abbia fatto in passato il fax, altra grande rivoluzione operativa nella vita d'ufficio del secolo appena trascorso.
Non a caso il bisogno più sentito - quando si ritorna in sede in crisi da astinenza da connettività Internet - è proprio quello di "scaricare la posta".

La lunga e fulgida storia dell'RFC821

C'è spesso un qualcosa di bizzarro e curioso nel rileggere la storia della tecnologia. Come il far notare, a quasi ventun'anni dalla comparsa del fondamentale protocollo SMTP per il trasferimento della posta utilizzato ancor oggi, che il celebre documento RFC 821 da tempo passato alla storia di Internet (www.ietf.org/rfc/rfc821.txt) porta la firma di J.B. *Postel*, un nome quasi profetico.
Al di là delle singolari assonanze e coincidenze, va rilevato come il nucleo base delle specifiche ivi racchiuse per la spedizione dei messaggi sia - in buona parte - rimasto il medesimo anche oggi, un po' come è accaduto allo standard del fax, ormai mummificatosi con i suoi pregi e i suoi numerosi difetti. Un sicuro sintomo di grandissima capacità e lungimiranza tecnica, ma anche un percorso di inevitabili compromessi in nome della compatibilità e del "preesistente", un insieme di limitazioni che - prima o poi - inevitabilmente iniziano a cozzare con le accresciute esigenze dell'utenza.

Sicurezza e flessibilità vo' cercando...

L'immediatezza e versatilità d'uso della posta elettronica ne nascondono - spesso - le molte lacune sotto il profilo della sicurezza. Storicamente - infatti - l'evoluzione dell'informatica è spesso stata fortemente orientata verso la protezione dei dati ma - parimenti - verso la diffusione e condivisione dei servizi. Così, se da un lato è possibile apprezzare "file system" longevi ma "blindati" come quello di Unix (enormemente più avanzato rispetto a quello di Windows 9x, ad esempio), dall'altro non si può non notare come un protocollo vitale quale l'SMTP - che permette la trasmissione della posta elettronica

Figura 1

- sia intrinsecamente assai "debole" sotto il profilo della sicurezza.
È un discutibile merito dei virus, ad esempio, l'avere svelato a tutti gli utenti quanto sia facile spedire posta sotto "mentite spoglie". A chi non è capitato di ricevere una mail da un utente amico (e ignaro) che conteneva un virus e scoprire poi che non era stato l'amico ad inviarla ma - semplicemente - qualcuno che aveva il suo indirizzo E-Mail in rubrica? O - viceversa - ricevere segnalazione di avere inviato un messaggio infetto mentre il proprio PC era perfettamente "sano"?
Non occorre un virus sofisticato per fare ciò e - anzi - qualunque utente può divertirsi a camuffare in pochi secondi la propria identità E-Mail alterando i settaggi del proprio client (figura 1).
D in quanto eccessivamente ardua.
Con l'esponenziale crescita di Internet, dunque, si è continuato ad utilizzare i protocolli originali per la posta elettronica per ragioni di robustezza, efficienza, flessibilità e compatibilità ma è fuor di dubbio che l'intero castello si fondi oggi su dei presupposti di "buona fede" difficilmente sostenibili in sede di contenzioso.
Un primo passo potrebbe essere - quantomeno - quello di imporre la propria "autenticazione" al server SMTP (anche se questo non viene di norma richiesto - assai discutibilmente - se si utilizza il server del provider al quale si è collegati) mediante la selezione dell'apposito checkbox che - ad esempio - in Outlook Express è situato nel menu Strumenti - Account - Proprietà - Server (figura 2). Questo consente almeno di far figurare nell'"header" dei messaggi ricevuti un - seppur minimo - attestato di autenticità (ad esempio: "authenticated as xxx@yyyyyy.it"); un'attestazione - peraltro non standardizzata - che tuttavia rimane sostanzialmente invisibile alla maggior parte degli utenti e degli applicativi e può talora essere utile solo in caso di contenzioso.

Figura 2

Ancora troppo poco, insomma, per potere riporre nello strumento E-Mail l'elevatissimo livello di fiducia che invece potrebbe meritare.

L'esigenza di una posta elettronica certificata

L'affermarsi della crittografia a chiave pubblica, cuore della cosiddetta "firma digitale", ha di colpo reso assai meno pressante l'esigenza di irrobustire gli stessi protocolli di posta elettronica, in quanto è possibile aggirare il problema assicurando la paternità del contenuto, firmandolo digitalmente, pur rimanendo nella sostanza incerto il mittente.
Sulle vicissitudini normative della "digital signature" ci si è soffermati nel numero scorso della rivista e su questi temi si ritornerà nei prossimi mesi, in quanto mai "parto" tecnologico fu più travagliato - dovendo miscelare e armonizzare tematiche diversissime, che spaziano dal diritto internazionale (passando per la burocrazia europea) alle prassi e protocolli informatico/telematici; a ciò si aggiunga la serie imbarazzante di bug procedurali ed effettivi di recente manifestatisi, fatto questo assai grave perché in grado di minare sul nascere la fiducia degli utenti - già scarsamente informati e consapevoli - in uno strumento realmente affidabile e rivoluzionario.
Tralasciando per un attimo la firma digitale in senso stretto, è bene sottolineare il fatto che una "posta elettronica certificata" non si limita alla digital signature; col termine "certificata" si intende infatti "un servizio basato sulla posta elettronica, come definito dallo standard SMTP e sue estensioni, che consenta la trasmissione di documenti prodotti mediante strumenti informatici *nel rispetto dell'articolo 14 del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445* [ossia il Testo unico delle disposizioni legislative e regolamentari in materia di documentazione amministrativa]". È dunque bene riportare integralmente il citato articolo 14:

"Sezione III - Trasmissione di documenti - Articolo 14 (R) Trasmissione del documento informatico.
1. Il documento informatico trasmesso per via telematica si intende inviato e pervenuto al destinatario, se trasmesso all'indirizzo elettronico da questi dichiarato.
2. La data e l'ora di formazione, di trasmissione o di ricezione di un documento informatico, redatto in conformità alle disposizioni del presente testo unico e alle regole tecniche di cui agli articoli 8, comma 2 e 9, comma 4, sono opponibili ai terzi.
3. La trasmissione del documento informatico per via telematica, con modalità che assicurino l'avvenuta consegna, equivale alla notificazione per mezzo della posta nei casi consentiti dalla legge."

Cosa questo implichi effettivamente sotto l'aspetto tecnico e procedurale è stato stabilito con notevole dettaglio dalle "Linee guida del servizio di trasmissione di documenti informatici mediante posta elettronica certificata" - licenziate in prima edizione il 3 Febbraio 2003 - e dall'allegato tecnico, entrambi facilmente rintracciabili all'indirizzo del Centro Tecnico della Presidenza del Consiglio dei Ministri www.ctrupa.it/RETE-RUPA/Posta-Elet/index.htm (figura 3).

Figura 3

Legalmail, la soluzione di Infocamere

In sintesi, con la posta elettronica certificata si ha un reale e ben più potente sostituto della classica "raccomandata a.r.", pur potendo continuare ad utilizzare i normali e più diffusi programmi di gestione dell'E-Mail (come Outlook Express 5.x e 6.x, Netscape 7.01, Mozilla 1.0.2, Lotus Notes client 6.0, Opera 5.02, Eudora 5.2) ma anche una comune interfaccia web (la sicurezza è in questo caso assicurata dall'utilizzo della "smart card" contenente la propria firma digitale).

In particolare - come recita la homepage dedicata all'argomento da uno dei due operatori di posta certificata accreditati sino al momento della stesura di questo articolo - ossia InfoCamere s.c.p.a. (l'altro è EDS PA s.p.a.) - sono garantite "l'identificazione del mittente, l'integrità e confidenzialità del messaggio, ma anche di attestare il recapito del messaggio stesso" (figura 4, all'indirizzo Internet www.legalmail.it).

Una soluzione di questo tipo, oltre all'immediatezza propria della posta elettronica, comporta ulteriori aspetti migliorativi rispetto all'equivalente cartaceo, specie se lo scambio avviene con altri utenti di posta certificata. In particolare, non esiste un solo "avviso di riscossione": come illustrato nel sito Legalmail, dedicato da Infocamere al tema, "il mittente riceve dal proprio server una prima ricevuta di presa in carico, con attestazione temporale (come un timbro postale). Poi riceve dal server destinatario una ricevuta di consegna del messaggio nella casella di arrivo; anche questa ricevuta comprende un'attestazione temporale. Il mittente ottiene, con la ricevuta di avvenuta consegna, un'attestazione su tutto il contenuto inviato nel messaggio; *questa ricevuta, firmata dal server che ha effettuato la consegna, rappresenta un'attestazione decisamente più dettagliata rispetto alla ricevuta di una raccomandata cartacea.* Inoltre, tutte le operazioni vengono registrate e conservate nel tempo. L'interoperabilità con gli altri fornitori di posta certificata garantisce invio e ricezione di messaggi certificati a/da qualsiasi utente di posta certificata. Legalmail fornisce anche la possibilità di richiedere la 'notifica di

Figura 4

accesso' marcata temporalmente per certificare l'accesso del destinatario al messaggio".
In sostanza, con la posta certificata è possibile un tracciamento pressoché totale dei propri messaggi E-Mail.
Si noti che la posta certificata protegge l'utente anche da se stesso e dai possibili malfunzionamenti dei propri computer. Nelle linee guida si può leggere - infatti - che "i gestori devono mantenere traccia delle operazioni svolte su un apposito registro. *I dati contenuti nel suddetto registro devono essere conservati per un periodo di almeno due anni* e devono essere disponibili ed accessibili per la consultazione a fini ispettivi, da parte del Centro Tecnico, o in caso di contenzioso dai soggetti individuati per tale compito. (...) *Nel caso in cui il mittente non abbia più la disponibilità delle ricevute dei messaggi inviati, le informazioni presenti nei registri degli operatori coinvolti nell'invio sono opponibili ai terzi* ai sensi dell'articolo 14, comma 2, del decreto del Presidente della Repubblica 28 dicembre 2000, n. 445".

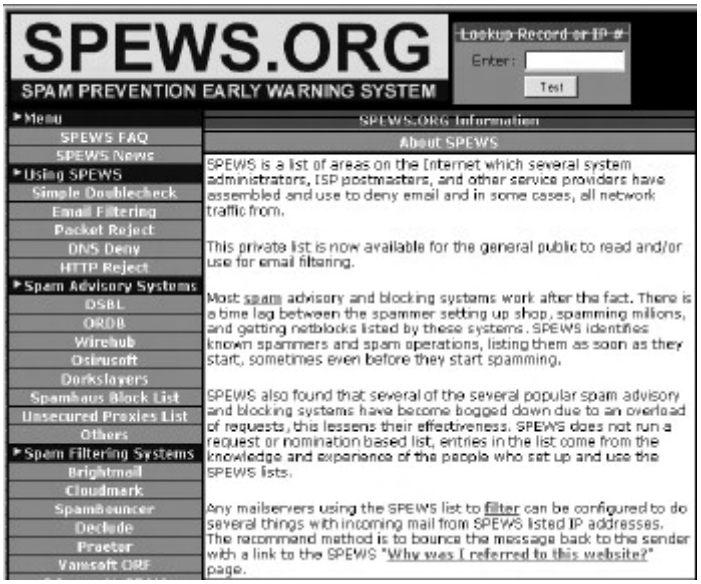

Figura 5

La minaccia dello spam
La posta elettronica - che con la certificazione sarà ora finalmente in grado di sostituire a tutti gli effetti legali l'equivalente cartaceo - fra tante gioie comporta tuttavia anche qualche dolore, il principale dei quali è sicuramente il cosiddetto "spam", ossia l'essere bersagliati da posta indesiderata, tipicamente di carattere commerciale.
Lo spam rappresenta un vero e proprio costo aziendale, che uno studio dell'Unione Europea pubblicato nel gennaio 2001 e intitolato "Unsolicited Commercial Communications and Data Protection" tentò anche di quantificare giungendo ad una cifra astronomica: ben dieci miliardi di euro all'anno.
La stima - riportata alla pagina 67 delle 145 che costituiscono il corposo studio - è in realtà limitata ai costi di connessione necessari agli utenti finali per scaricare messaggi non voluti. Oggi, alla luce delle tante offerte di connessione "flat" - il cui costo non dipende dal tempo di connessione, tale stima non appare più così appropriata ma ridiventa oltremodo attuale qualora si pensi che una parte del costo della connettività è destinato a spostarsi dal fisso al mobile (che - come il GPRS - è prevalentemente tariffato "a traffico", ossia in base ai Kbyte scaricati) e che anche il "flat" - prima o poi - verrà probabilmente indicizzato in base al volume di dati scaricati così come avviene già oggi per molti contratti aziendali ad elevata velocità.
Vi è tuttavia un secondo e ben più importante aspetto da considerare: se - infatti - spendere 20 euro per scaricare la propria posta infestata dallo spamming con il telefonino può apparire un caso infrequente (ancorché assai irritante nonché inaccettabile se ripetuto), è invece un dato evidente e quantificabile il tempo perso dai dipendenti per selezionare la posta importante da quella pubblicitaria, con la conseguente successiva eliminazione. Il rapporto UE riporta uno studio di Schwartz e Garfinkel dove si afferma che - nell'ipotesi di ricevere sei messaggi spam al giorno - si perderanno due ore di lavoro all'anno semplicemente nel premere il tasto del mouse per cancellarli. Tale stima - in realtà - appare assai ottimistica. Il principale effetto collaterale dello spam consiste infatti nel far perdere concentrazione giacché non è sempre così scontato distinguere lo spam dalla posta "utile".

Una lotta vana?
Lo spamming rappresenta un fenomeno così diffuso e così sgradito tanto che - da anni - vi è una mobilitazione generale per contrastarlo. I risultati - tuttavia - sono generalmente deludenti e, spesso, decisamente più agri che dolci.
La strategia comune consiste infatti nell'identificare chi spedisce spam e bloccarlo, se possibile, prima che il messaggio indesiderato giunga nella casella di posta del destinatario. Il problema sta proprio nell'identificazione del mittente visto che - come

già fatto notare - il protocollo SMTP consente con elementare facilità di alterare la propria identità quante volte si desideri, anche in maniera automatizzata e pseudo casuale.
Un metodo solo apparentemente migliore - in quanto è spesso inattuabile in quanto "getta via il bambino con l'acqua sporca" - consiste nel bloccare tout-court l'indirizzo Internet (IP) del server mittente: si tenga infatti presente che imporre un filtro con maglie troppo strette implica un rimedio assai peggiore del male, ossia il rifiutare come spam anche messaggi E-Mail "utili".
Ne sanno qualcosa Libero/Inwind/IOL/Blu, ad esempio, che - per avere adottato una lista antispam pubblica internazionalmente nota come SPEWS (www.spews.org, figura 5), che aveva improvvisamente inserito l'IP Address di Yahoo nella sua "blacklist" - si sono viste sommergere dai messaggi di protesta dei propri utenti impossibilitati a ricevere i messaggi (fortemente voluti!) delle mailing list che costituiscono l'asse portante dei numerosissimi "gruppi" di utenti ospitati da Yahoo; una protesta *anti-antispam* che ha persino sollevato l'attenzione della stampa specializzata (figura 6).

Figura 6

Figura 7

La via migliore per combattere lo spam

Senza affidarsi a blacklist troppo restrittive, la via migliore per combattere lo spam rimane quindi quella di gestire una propria "lista nera". Tutti i client di posta elettronica consentono di dirottare automaticamente nel cestino i messaggi provenienti da mittenti non graditi (per esemplificare, in Outlook Express esiste all'uopo l'"Elenco mittenti bloccati" alla voce "Regole messaggi"). Ma si può fare assai di meglio, ossia identificare e bloccare i messaggi *prima* di scaricarli sul proprio PC per poi cancellarli direttamente sul server del provider, risparmiando quindi tempo prezioso.
Software cosiddetti "spam-killer" di questo tipo ne esistono molteplici, ma è opportuno segnalare l'ottimo prodotto - italiano e gratuito - Spam Terminator reperibile e liberamente scaricabile all'indirizzo www.sertel.net/terminator.
Spam Terminator è dotato di flessibili e sofisticate opzioni (utili anche per prevenire taluni virus), nonché di una blacklist già pronta all'uso ma sicuramente troppo ricca e selettiva per un utilizzo professionale, per cui il consiglio è di ignorarla (il problema è sempre il medesimo: si rischierebbe di gettare via messaggi di interesse) e di crearne invece una personale, progressivamente ritagliata sulle proprie esigenze. La regola aurea deve essere sempre la stessa: meglio tollerare uno spam di troppo piuttosto che correre il rischio di scartare erroneamente un messaggio utile.