

Sicurezza IT, la sfida delle pubbliche amministrazioni

Il progetto eGovernment possiede uno straordinario potenziale innovativo per i cittadini e per le imprese, ma non potrà decollare se non verrà garantita la sicurezza

ANGELA ROSSONI

La realizzazione di una rete sicura per la totalità delle pubbliche amministrazioni europee, che sfrutti le potenzialità della banda larga e garantisca allo stesso tempo elevate prestazioni e facilità all'uso, costituisce una sfida senza precedenti, che ridefinirà il concetto di sicurezza IT. Il successo del progetto eGovernment, per cui la comunità europea ha previsto imponenti investimenti nel corso dei prossimi tre anni, è legato a doppio filo alla sicurezza: senza di essa il progetto non potrà decollare e sprigionare il proprio potenziale innovativo in termini di servizi on line per imprese e cittadini. Un'organizzazione pubblica in rete possiede infatti una mole imponente di

zioni, delle università e di importanti aziende, fra cui figurano, nel settore ITC, IBM, Schlumberger e Telecom Italia. L'associazione Telecities è stata fondata nel 1996 e raggruppa 126 città digitali d'Europa, che comprendono una quindicina di capoluoghi italiani: Roma e Siena partecipano in qualità di membri nel comitato di direzione. Fra i partner "commerciali" del consorzio si annoverano colossi tecnologici quali Cisco Systems, Microsoft e Oracle.

La eSicurezza costituisce una disciplina estremamente vasta. Dal punto di vista delle tecnologie interessa l'autenticazione, l'identificazione, e l'utilizzo di protocolli Internet. Gli algoritmi di autenticazione e di protezione dei dati attualmente in uso hanno dimostrato di non essere a prova di manomissione. Si stanno per questo motivo svolgendo intense ricerche sugli algoritmi crittografici e in particolare sulla crittografia quantistica, che garantisce l'invulnerabilità sfruttando il principio di indeterminazione di Heisenberg: qualsiasi tentativo di decifrare una chiave quantistica la renderebbe inutilizzabile e lascerebbe una "traccia" del tentativo di manipolazione. Per il momento la sicurezza nelle reti pubbliche è garantita da un'infrastruttura

ra PKI e da una password. La Comunità Europea ha deciso di promuovere l'utilizzo della firma digitale, che potrà essere emessa da autorità di certificazione accreditate, e la distribuzione di una carta d'identità elettronica che conterrà informazioni biometriche (impronte digitali, ed eventualmente iride, profilo del viso e voce). La sperimentazione svolta sulle carte digitali nella città di Siena ha dato risultati positivi: fra le 1500 persone coinvolte, nessuno ha rifiutato di rilasciare le impronte digitali, sebbene fosse facoltativo. Occorreranno dai 5 ai 6 anni per fornire a tutti i cittadini europei la carta d'identità elettronica: essa sarà affiancata da alcune carte dei servizi rilasciate

ture), partito a metà dello scorso anno, che intende migliorare la condivisione delle informazioni fra gruppi di cittadini, aree geografiche o associazioni, informando gli utenti sul grado di vulnerabilità della rete. Il progetto Prelude, inaugurato nell'Aprile del 2002 e con una durata prevista di due anni, intende aiutare le città e altre organizzazioni a instaurare un rapporto di fiducia con gli utenti, creando un'aggregazione a livello europeo. A tal fine sono state individuate nove regioni digitali per la sperimentazione degli strumenti di eSicurezza, fra le quali la Lombardia è stata prescelta per lo sviluppo del sistema sanitario. Particolarmente critica è l'attuazione del programma di "eGiustizia": i criminali usano i database con una familiarità che la pubblica amministrazione non possiede. Esistono già delle reti internazionali per la giustizia, quali EuroJust ed Europol, e una serie di progetti pilota fra le amministrazioni locali, come quello organizzato fra le giurisdizioni delle Alpi Marittime e della Liguria, al fine di sviluppare tool per il controllo dell'immigrazione clandestina. In questo ambito è più che mai forte l'esigenza di disporre di un database e di un motore di ricerca unici, per facilitare le comunicazioni fra i Paesi dell'Unione.

Per realizzare questi ambiziosi progetti una solida partnership fra pubblico e privato, è un imperativo, così come la definizione di requisiti standard per la cooperazione. Occorre creare una sinergia fra città europee, centri di ricerca e aziende, siano esse grandi multinazionali o piccole start-up, per sviluppare nuove tecnologie e applicazioni per la eSicurezza.

Il successo del progetto di eGovernment è legato a doppio filo alla sicurezza

dalle pubbliche amministrazioni. Per implementare la eSicurezza non bastano tuttavia le tecnologie. Occorre innanzitutto elaborare standard che garantiscano un unico processo di identificazione in tutte le città d'Europa, ancora divise dalle legislazioni locali. È inoltre essenziale assicurare un solido servizio di assistenza e promuovere la formazione degli utenti, anche attraverso strumenti di eLearning, creando una cultura della sicurezza. La gestione dei rischi (risk management) infine, disciplina sorta una trentina di anni fa all'interno delle aziende, potrebbe migliorare sensibilmente la gestione della sicurezza all'interno delle pubbliche amministrazioni.

Sono stati attivati diversi progetti paneuropei, quali Cases (Cyberworld Awareness and Security Enhancement Struc-

Occorre creare una sinergia fra le città europee

dati "sensibili", per la privacy e per la sicurezza, ed è esposta ad attacchi continui e in crescita esponenziale. Questo è il messaggio lanciato nel corso del congresso "Telecities AGM&Winter Event", tenutosi a Siena dal 2 al 4 dicembre scorsi, cui hanno preso parte rappresentanti delle pubbliche amministra-

