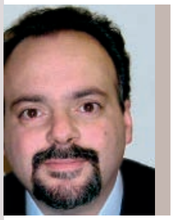
Roberto Ghislandi

# Prevenire è meglio che curare

*Quando la gestione della sicurezza informatica aziendale è affidata ad altri.*

Lunedì mattina ore 9.15 il dottor Edoardo Bianchi arriva in ufficio, accende il computer per controllare la mail ma il programma di posta elettronica si ostina a mostrare una finestra che segnala l'irraggiungibilità del mail server. Bianchi spegne e riaccende il computer ma il messaggio è sempre lo stesso. Sono le 9.22, alle 10.00 ha una importante riunione dove deve presentare il nuovo piano marketing. Gli ultimi ritocchi alla presentazione li ha fatti durante il weekend dal computer di casa e ha spedito il tutto via email in ufficio. Nel fine settimana ha aggiunto una serie di dati interessanti che confermano le sue innovative tesi. Prende il telefono per chiamare l'help desk ma la linea è sempre occupata. Chiede agli altri colleghi se la loro mail funziona ma nessuno riesce ad accedere al server di posta. Sono le 9.32, il tempo stringe. Finalmente alle 9.43 riesce a contattare l'help desk: sabato notte c'è stato un attacco al server aziendale di posta. Attualmente i tecnici stanno cercando di ripristinarlo con i backup di venerdì notte. Ci vorranno almeno due ore e comunque la posta spedita nel fine settimana è andata persa. Fortunatamente a Bianchi viene in mente che su una chiavetta USB ha una copia della presentazione, la carica sul PC (9.55), inserisce in fretta e furia le modifiche che si ricorda (10.02) e si precipita in sala riunioni. Sono le 10.08, è furente e agitato. Si scusa con tutti i presenti per l'inconveniente: massima comprensione da parte di tutti. È comunque nervoso e poco concentrato e durante la presentazione non dà il meglio, continua a tornargli in mente la bellissima presentazione che aveva preparato a casa, quei dati in più che avrebbero fatto la differenza. Il nuovo piano marketing viene giudicato un po' troppo innovativo e rischioso, per il momento viene accantonato.



***Roberto Ghislandi**, laureato in Ingegneria al Politecnico di Milano, ha fondato e lavorato in una software house per 10 anni. Attualmente svolge la sua attività professionale come formatore e consulente per progetti Internet e Intranet nel campo dell'e-commerce e dell'e-mail marketing.*

## Un mondo vulnerabile

Reti aziendali, VPN, mail server ormai fanno parte della vita quotidiana e sono divenuti strumenti di lavoro su cui facciamo affidamento. La rete aziendale ferma per qualche ora, la mancata possibilità di accedere alla mail, la perdita di dati o un virus che blocca il nostro PC sono imprevisti che causano ritardi e perdite di tempo a catena. Le truffe su Internet nell'ultimo anno sono raddoppiate e molte di queste sono state possibili grazie a sistemi informativi non sufficientemente sicuri. Il Symantec Security Update del settembre 2005 riporta come tipo di attacco più diffuso l'SQLExp, un worm che attacca i server su cui gira MS SQL Server 2000 o MSDE 2000 sovraccaricando la macchina sino a comprometterne il funzionamento. Questo genere di attacco viene chiamato DoS (Denial of Service). Nonostante tale worm sia stato individuato per la prima volta il 24 gennaio 2003 e sia Microsoft sia altre aziende come la stessa Symantec abbiano indicato alcune possibili soluzioni, proprio per la cura che va posta nell'adottarle l'SQLExp risulta tutt'ora il tipo di attacco più diffuso (oltre il 30% del totale). Oltre che dall'attacco dai virus la sicurezza informatica ha anche il compito di proteggere dallo spam, un fenomeno che aumenta a dismisura il traffico di e-mail e ci costringe a perdere molto tempo per scartare i messaggi di interesse da quelli spazzatura. Lo spam non è legato, come si è soliti credere, solo alla pornografia o a materiale per adulti, anzi. Secondo il già citato rapporto di Symantec, di tutto lo spam il 26% è relativo alla promozione di prodotti, il 23% a prodotti finanziari, il 12% a prodotti e servizi relativi alla cura della persona, l'11% a servizi Internet e solo al quinto posto, con il 10%, compare il materiale per adulti.

## Che cos'è la sicurezza

L'adozione di politiche per la sicurezza aiuta insomma a «far funzionare al meglio» il sistema informatico proteggendolo da malfunzionamenti, utilizzi impropri e attacchi indesiderati. Prima di addentrarci nella gestione della sicurezza riteniamo utile dare qui una definizione di sicurezza riprendendola liberamente da quella proposta dalla norma ISO 17799: *un sistema informatico viene considerato sicuro quando è in grado di garantire determinati requisiti di sicurezza in termini di disponibilità, integrità, riservatezza e autenticità*. Cosa vuol dire? Il significato è racchiuso nei quattro termini; vediamoli uno alla volta.
**Disponibilità**: il sistema deve garantire la disponibilità delle informazioni a ciascun utente autorizzato nei modi e nei tempi previsti dalle politiche aziendali. In pratica gli utenti autorizzati devono poter accedere con facilità alle informazioni di loro pertinenza.
**Integrità**: il sistema deve impedire e comunque rilevare alterazioni dirette o indirette delle informazioni da parte di utenti o di procedure non autorizzati o causate da eventi accidentali. Il sistema informativo deve quindi non solo permettere l'accesso alle informazioni a chi di dovere ma garantire anche che queste informazioni siano corrette: nel caso siano state manomesse, deve accorgersene e segnalarlo con tempestività.

L'ingresso a un SOC è solitamente protetto da bussole di tipo bancario con eventuale controllo biometrico. Nella figura l'ingresso al SOC di Liscom.

**Riservatezza**: nessun utente deve poter acquisire o dedurre dal sistema informazioni che non è autorizzato a conoscere.
**Autenticità** e non ripudio: il sistema deve poter fornire la certezza che una data informazione appartenga a chi dice di averla generata (autenticità) e chi ha generato una data informazione non deve poter negare di averlo fatto (non ripudio). È questo un punto importante che per esempio su Internet viene spesso disatteso. Tramite i motori di ricerca possiamo reperire qualsiasi informazione ma resta poi a nostro carico capire se l'informazione è affidabile, da chi è stata pubblicata e la sua validità.

## La sicurezza in outsourcing

La sicurezza informatica non è dunque una astrusa serie di regole per mettere in difficoltà il centro Edp o far spendere soldi all'imprenditore ma permette di limitare i danni derivanti dagli incidenti informatici, di proteggere il patrimonio informativo aziendale, di preservarne l'immagine e anche di ottemperare alle normative vigenti (tra cui la tanto famosa 196/2003 con il Dps – Documento programmatico della sicurezza). Gli accorgimenti e le tecnologie da impiegare ai fini della sicurezza sono sempre in evoluzione. Ecco perché è sempre più comune ricorrere all'outsourcing (**Out**side re**sourcing**). Avere personale qualificato che sia in grado di mantenersi aggiornato può essere un costo non sostenibile dalle piccole aziende o si può comunque decidere che non faccia parte del core business dell'azienda e sia inutile avere all'interno le relative competenze.
Un responsabile della sicurezza può costare a una azienda tra i 70 e gli 80 mila euro all'anno senza contare il fatto che non si può pretendere che sia sempre disponibile, 24 ore su 24 sabati, domeniche e festività comprese. Affidarsi all'outsourcing non significa disinteressarsi della sicurezza relegandola a un qualsiasi fornitore ma utilizzare risorse esterne all'azienda. È infatti fondamentale non confondere l'utilizzo di un servizio fornito da terzi con l'outsourcing. Outsourcing significa affidare a un fornitore esterno un **processo aziendale** nella sua interezza. È importante notare la differenza tra Servizio e Processo. Mentre il Servizio è una applicazione con risultati definiti, un Processo è un insieme di applicazioni correlate a una particolare funzione aziendale. Un conto, per esempio, è affidare le pulizie a un'azienda esterna e ben'altra cosa è affidare l'amministrazione dell'ufficio, che oltre alle pulizie prevede la manutenzione ordinaria, straordinaria e preventiva. Quindi non solo la normale pulizia ma anche la gestione di mobili, il rinnovo dell'arredamento ed eventuali operazioni volte, per esempio, a migliorare il prestigio della sede. In questo secondo caso il fornitore diviene a tutti gli effetti un partner che deve **condividere le strategie aziendali** ed essere inoltre **propositivo** nell'indicare gli interventi da effettuare. Il committente da parte sua non può limitarsi al semplice controllo ma deve dialogare con il fornitore, verificare che le strategie siano state ben recepite e coadiuvarlo nella messa in pratica di quanto proposto e approvato. Occorre siglare un accordo in cui il cliente riporta i suoi bisogni e il fornitore indica come intende soddisfarli, specificando anche eventualmente penali nel caso in cui non vengano rispettati gli accordi presi. Nel contratto devono essere previsti anche una serie di report a frequenza prestabilita in cui l'outsourcer illustra gli interventi fatti e quelli in programma. La scelta di unfornitore in outsourcing è dunque assai delicata e va fatta in modo consapevole.

## Pregi e difetti dell'outsourcing

La scelta di un fornitore in outsourcing consente all'azienda di poter contare su personale qualificato e aggiornato che utilizzi sempre la migliore tecnologia presente sul mercato senza dover investire in ricerca in un settore che non fa parte del core business aziendale. La flessibilità e la scalabilità sono inoltre garantite dall'efficienza del fornitore che ha pieno interesse a seguire al meglio il proprio cliente. La scelta dell'outsourcing permette di pagare un canone annuo facilmente inseribile nel budget (costo fisso) invece di dover gestire un vero e proprio centro di costo all'interno dell'azienda che dovrebbe comprendere: l'hardware, il software, il personale qualificato e una serie di altre spese difficilmente prevedibili a priori. Tale canone inoltre si rivela più basso proprio per la possibilità del fornitore di suddividere alcuni costi (per esempio il personale) su più clienti.
D'altra parte il ricorrere all'outsourcing fa perdere competenze all'interno dell'azienda su un settore comunque importante e obbliga a **fidarsi di una struttura esterna**. Oltre quindi a valutare la stabilità finanziaria del partner scelto occorre dedicare parecchie risorse alla stesura di un contratto che soddisfi entrambi e che sia conveniente rispettare. Non si tratta di «strozzare» il fornitore ma di avere un accordo win-win che sia vantaggioso per entrambe le aziende portare avanti nel tempo.
Non è infatti pensabile cambiare ogni sei mesi il fornitore di sicurezza in outsourcing dal momento che nella maggior parte dei casi comporterebbe una riorganizzazione, seppure parziale, dell'intero sistema informativo.
I contratti stipulati in questo caso comprendono anche quello che viene

detto **SLA** (Service Level Agreement), in cui si dettaglia con precisione quando deve essere disponibile il servizio, il tempo di ripristino del servizio, il tempo di risposta ai guasti, come deve essere monitorato il sistema informativo del cliente, come vengono fatte le misurazioni, quando devono essere fatte e come il cliente può accedere a questi dati.

## La scelta dell'MSSP

I fornitori di sicurezza in outsourcing vengo detti **MSSP** (Managed Security Service Provider) e provvedono alla gestione dei dati, dei programmi e a tutti i controlli necessari collegandosi da remoto alla rete del cliente. L'approccio è differente da quello dell'ASP (Application Service Provider) che, al contrario, detiene le applicazioni e i dati sui propri server e permette al cliente il loro utilizzo collegandosi da remoto. Un MSSP opera di solito attraverso un **SOC** (Security Operation Center) dal quale controlla la rete del cliente. Per questioni di sicurezza alcuni operatori utilizzano per il controllo linee dedicate tra il proprio SOC e il cliente riducendo ulteriormente i rischi. È di fondamentale importanza che al SOC possa accedervi solo personale qualificato, presente 24 ore su 24 in tutti i giorni dell'anno. Altrimenti, un malintenzionato, accedendo al SOC potrebbe prendere il controllo delle reti dei clienti dell'MSSP. In quest'ottica, sono da privilegiare gli MSSP che si servono solo di personale qualificato e assunto che può assicurare un turn over minore di una struttura di consulenti. I SOC devono essere dotati di linee sicure e ridondate e devono operare seguendo certificate norme di sicurezza. Attualmente esiste uno standard per la sicurezza descritto dal protocollo **BS 7799** suddiviso in due parti. La prima, ripresa anche dalla norma ISO 17799, fornisce le «best practice» necessarie per implementare la sicurezza. La seconda parte descrive invece come implementare, mantenere e migliorare un sistema di gestione per la sicurezza dell'informazione ed è la parte certificabile della norma.
I migliori MSSP operano secondo la BS 7799 e spesso sono anche in grado di formare il personale del cliente.
La scelta del proprio MSSP deve essere fatta dunque non solo in base al prezzo ma anche alla professionalità e alla sicurezza finanziaria che possono garantire. Affidarsi a un MSSP e scoprire che dopo qualche mese la società viene messa in liquidazione non solo non risolve il problema ma espone a ulteriori rischi.

## Il percorso verso la sicurezza

Prima di poter stendere un contratto è fondamentale una fase di valutazione che l'MSSP svolge in stretta collaborazione con il cliente. Il percorso parte dall'analisi dei possibili rischi, legati all'importanza e alla appetibilità delle informazioni da proteggere, l'analisi del tipo di minacce (Threat) a cui si può essere soggetti (virus, worm, attacchi di hacker, furto da parte di dipendenti, ecc.) e si conclude con l'analisi delle vulnerabilità legate al sistema informativo da proteggere individuando le parti che devono essere rese più sicure, come controllarle e cosa fare in caso di attacchi.
Conclusa questa fase si passa a rafforzare l'intero sistema informativo. Dove necessario si installa un firewall, degli anti virus, sistemi anti spam e di content filtering per Internet, si definiscono le politiche di accesso degli utenti, il sistema di rotazione delle password e si predispone un sistema di monitoraggio che permetta di individuare possibili attacchi o tentativi di attacco.
Il contratto andrà a descrivere tutto ciò specificando anche i tempi di intervento che devono essere garantiti e le eventuali penali nel caso non fossero rispettati.
Nella tabella riportata vengono elencati i principali servizi offerti da un MSSP.

## Glossario

**Audit trail**: nei sistemi di protezione è un record cronologico dell'utilizzo delle risorse del sistema. Questo include il login dell'utente, l'accesso ai file, altre attività e se si sono verificati tentativi o violazioni effettive della protezione.

**Auditing**: la ricerca di lacune nella sicurezza di un sistema. Esistono vari tipi di auditing, da quello di applicazioni a rischio (verifica del codice sorgente o test per identificare le vulnerabilità) a quello delle reti (mediante test di penetrazione, per esempio).

**Back door**: falla nella sicurezza di un sistema di computer lasciata deliberatamente (a volte per gioco, a volte con intenzioni dolose) dai progettisti o dai responsabili della manutenzione.

**BS 7799**: documento di standard realizzato dal British Standards Institute (BSI) che descrive in che modo le organizzazioni possono creare e gestire un efficace programma di protezione delle informazioni. British Standard 7799 è composto da due parti: la prima descrive i concetti di base per programmi di protezione, la seconda descrive un processo di gestione per programmi di protezione. L'approccio di BS 7799 è simile al successivo standard ISO 17799.

**CISA**: Certified Information System Auditor, una certificazione per l'auditing dei sistemi informativi, contiene anche un'ampia parte sulle procedure di sicurezza e di disaster recovery. È supportata dalla Information Systems Audit and Control Association (**ISACA**) [www.isaca.org].

**CISSP**: Certified Information Systems Security Professional, una certificazione tecnica per la sicurezza informatica offerta da **(ISC)2** (International Information Systems Security Certification [www.isc2.org]).

**CLUSIT**: Associazione Italiana Per La Sicurezza Informatica [www.clusit.it]) con sede presso il Dipartimento di Informatica e Comunicazione dell'Università degli Studi di Milano. Lo scopo di Clusit è di promuovere e diffondere nel nostro paese la cultura e la consapevolezza della sicurezza informatica in tutti i suoi aspetti, in collaborazione alle consociate associazioni europee. Clusit inoltre si occupa di fornire supporto alle imprese in materia di sicurezza informatica e proporre raccomandazioni.

**DoS**: Denial of Service, attacco che mira a saturare o comunque disattivare i servizi offerti da una risorsa informatica, allo scopo di impedirne l'utilizzo ai «legittimi utenti». Può significare rendere indisponibile un Web server, per esempio, subissandolo di false richieste, o sovraccaricare una macchina rendendo temporaneamente inutilizzabili i servizi che essa offre.

**DMZ** (DeMilitarized Zone): zona demilitarizzata, indica un'area della rete che non è situata né all'interno né all'esterno del dominio protetto dal firewall. Ai sistemi e ai dispositivi che si trovano nella DMZ viene fornito comunque un certo livello di protezione anche se inferiore a quello interno alla rete aziendale. Web server, proxy server e banchi di modem sono spesso dislocati nella DMZ.

Accanto a quelli base ve ne sono anche di più avanzati, quali la predisposizione di trappole per gli hacker (honey pot), la stesura del documento sulla protezione dei dati (196/2003), la consulenza legale (una serie di servizi atti a evitare: la partecipazione involontaria a attacchi informatici e a azioni di spionaggio, la fruizione illegale di contenuti civilmente e penalmente rilevanti a opera dei dipendenti, la violazione privacy dei dipendenti e dei clienti, la pubblicazione indebita di materiale con copyright, l'applicazione della 196/2003), sino ad arrivare alla forensic analysis con cui si mettono a punto sistemi di registrazioni di possibili intrusioni o relativi tentativi in modo tale che possano essere utilizzati in fase processuale.
Di primaria importanza è l'esecuzione periodica di test per verificare che il sistema operi correttamente e che sia sempre protetto dai rischi e dalle insidie che nascono via via. La scurezza, come si diceva all'inizio, è un processo che va mantenuto vivo nel tempo. Non appena si interrompono le procedure di manutenzione e aggiornamento, viene a cadere tutto il lavoro fatto.
Per essere sempre aggiornati gli MSSP si avvalgono di particolari organizzazioni chiamate CERT che hanno, tra gli altri, il compito di emanare bollettini periodici dove vengono prese in esame le nuove vulnerabilità. Il più famoso CERT è quello che si appoggia al Software Engeneering Istitute della Carnegie Mellon University. In Italia i due principali si appoggiano uno all'università di Milano e l'altro al GARR.

La Centrale di Controllo del gruppo Lis Spa a cui appartiene Liscom. Dalla Centrale è gestita la sicurezza dei mezzi mobili e degli impianti fissi, civili e industriali, di oltre 18.000 clienti.

## Ma quanto mi costi?

Come è facile intuire, il grado di complessità della gestione della sicurezza dipende dalla tipologia di azienda in cui ci si trova e dalla criticità delle informazioni gestite. Più le informazioni sono appetibili più è necessario introdurre provvedimenti stringenti e tenere alta la guardia. Per molte aziende è sufficiente un firewall opportunamente configurato, anti virus, anti spam e magari un accesso da remoto tramite una VPN. Nella tabella abbiamo dunque chiesto ai vari MSSP di descrivere come vengono calcolati i costi e di valutare un semplice esempio comune a tante piccole realtà italiane. Come è possibile vedere le cifre di partenza sono davvero **alla portata di tutti** considerando quanto può costare tenere ferma solo per una giornata una azienda con 10 persone o perdere i dati contenuti su un server.
Per esigenze più complesse è ovviamente fondamentale un'analisi più approfondita.
Oltre alla tabella con le caratteristiche e con i servizi offerti dai principali MSSP operanti in Italia che trovate sul sito www.internetpro.it, per alcuni di questi abbiamo fatto anche una breve intervista via email di cui riportiamo le conclusioni.

- **Honeypot**: attraente bersaglio che viene inserito in un ambiente di rete come esca per gli hacker. Quando l'hacker attacca l'honeypot, viene seguito per controllarne il comportamento.
- **IDS**: Intrusion Detection System, software che ricerca e segnala sintomi di attività anomala in sistema informativo. Si suddividono in host-based e network-based: i primi analizzano una singola macchina cercando anomalie nei file, nell'utilizzo delle risorse ecc. I secondi invece analizzano i dati in transito sulla rete, cercando di ricostruire le impronte di eventuali attacchi. Istruito opportunamente, un IDS può segnalare il problema all'amministratore, o addirittura intervenire in modo automatico cercando di ovviare al danno.
- **IPSEC**: nuova versione del protocollo IP con funzioni di protezione migliorate.
- **ISO 17799**: Questo è il primo vero standard di sicurezza informatica **ISO** [www.iso.ch].
- **MD2, MD4, MDS**: protocolli per la firma elettronica.
- **MPLS**: MultiProtocol Label Switching. Tecnologia per la trasmissione di dati in rete IP riconoscendone il tipo (per esempio: trasmissioni vocali VoIP), oltre alle caratteristiche della rete e quindi consentendo di trattare i diversi contenuti in modo diverso.
- **PKI**: (Public Key Infrastructure) infrastruttura per la gestione di certificati a chiave pubblica.
- **Rainbow series**: gruppo di documenti governativi prodotti dalla National Security Agency americana che descrivono i processi e le procedure per realizzare programmi di protezione efficaci per l'elaborazione d'informazioni delicate o riservate. Viene chiamata «rainbow series» («serie arcobaleno») perché ogni volume ha un colore di copertina differente. Esempi includono l'Orange Book, o libro arancione (Trusted Computer System Evaluation Criteria) e il Green Book, il libro verde (DoD Password Management Guidelines).
- **Social engineering**: tecnica di persuasione che mira a carpire informazioni riservate o a forzare i soggetti a compiere certe azioni attraverso l'uso di calcolate pressioni psicologiche. Gli hacker usano spesso questa tecnica quando sono intenti alla violazione di un sistema, sfruttando la propensione delle persone a rispondere a domande dirette e impreviste o ad aiutare qualcuno che sembra in difficoltà.
- **VPN** (Virtual Private Network): sistema hardware e software utilizzato per creare una rete di dati privata utilizzando un'infrastruttura di telecomunicazioni condivisa. In una rete privata virtuale, non è necessario che le connessioni tra computer siano dedicate o di proprietà dell'organizzazione; tramite tecnologie VPN, è possibile creare una rete privata che può essere utilizzata solo da persone autorizzate all'interno di qualsiasi struttura di rete condivisa, compresa Internet. Le VPN utilizzano tecnologie di crittografia, quali il protocollo di tunneling point-to-point o PPTP, meccanismi di autenticazione e componenti hardware dedicati per creare una rete sicura a un costo inferiore rispetto alle reti dedicate.

## Dimension Data SpA

Fondata nel 1983 e con sede centrale in Sudafrica, Dimension Data è un'azienda specializzata in soluzioni e servizi IT per facilitare la progettazione, la creazione e il supporto di infrastrutture informatiche. Dimension Data si avvale delle conoscenze acquisite nel campo delle tecnologie di networking, sicurezza, ambienti operativi, storage e contact center e della sua lunga esperienza nella consulenza, nell'integrazione e nei servizi gestiti per offrire soluzioni personalizzate. In Italia sono presenti tre sedi – Milano, Roma, Padova – in cui sono impiegate circa cento persone.
Dimension Data, pur rivolgendosi principalmente ad aziende di dimensioni **medio-grandi** e a gruppi multinazionali, ha da sempre uno spiccato interesse anche per le **PMI**, importanti protagoniste del tessuto imprenditoriale italiano.
Abbiamo chiesto a Francesco Testi come affrontano in genere le aziende i problemi riguardanti la sicurezza: «*I responsabili della sicurezza e gli IT manager percepiscono ormai la sicurezza non più solo come tecnologia ma come un insieme di elementi che concorrono ad abbattere i rischi e garantire l'operatività. Il vero problema, ancora oggi, è che invece, spesso, il top management aziendale considera la sicurezza un elemento di costo, una complicazione inutile, relegandola in secondo piano*».
I servizi più richiesti a Dimension Data dipendono dal settore di appartenenza del cliente. Ultimamente per il mondo bancario e finanziario rivestono sempre più interesse soluzioni di anti-fishing, l'analisi delle vulnerabilità accompagnate dai penetration test. Questi ultimi sono stimolati anche dalla necessità di assicurare la conformità alle normative più o meno recenti in vigore e dalle prescrizioni imposte dalle case madri a tutte le sedi locali.
La sicurezza è un elemento che cambia nel tempo con una velocità relativa maggiore degli altri elementi dell'IT. Per il futuro Dimension Data ha deciso di distinguersi dalla concorrenza offrendo ai propri clienti «*un approccio globale rivolto al business del cliente e non alla tecnologia, un approccio che cerca di aiutare il cliente a controllare i suoi costi piuttosto che chiedergli di comprare nuovi sistemi*», afferma Francesco Testi.
In ogni caso che sceglie un MSSP deve prestare attenzione non solo alla preparazione del fornitore ma soprattutto all'aspetto di consulenza che può offrire per sfruttare al meglio il patrimonio informativo aziendale.

## Durante SpA

Durante SpA è uno tra i maggiori e indipendenti system integrator italiani operanti nell'ambito delle **soluzioni a valore aggiunto** di information & communication technology. Nata nel 1962, ha sviluppato nel corso degli anni approfondite competenze nella progettazione e realizzazione di infrastrutture e applicazioni di **comunicazione video**, **voce** e **dati**.
Il mercato di riferimento per la Durante è costituito da quelle aziende che hanno percepito **l'importanza della sicurezza aziendale** come uno dei fattori determinati per la produttività aziendale e sono dunque alla ricerca di un partner affidabile che le svincoli dall'incombenza di mantenere adeguato il livello di sicurezza della propria struttura informatica.
«*Il problema della sicurezza è sempre più sentito dalle aziende*» dice l'ing. Roberto Casari, «*Virus, spam, firewall sono termini ormai conosciuti anche per chi opera in piccole strutture*». Il punto dunque, prosegue Casari, «*è far loro capire che **la sicurezza è un concetto dinamico** che richiede sempre più l'impegno di **personale specializzato e competente***».
Attualmente i servizi gestiti in outsourcing più richiesti a Durante sono quelli di firewalling, i gateway antivirus, i sistemi di intrusion detection/prevention e i content filtering. Il mercato è in continua evoluzione e per il futuro «la migrazione della trasmissione voce/video verso l'utilizzo dell'IP, e in particolare lo sviluppo sempre crescente della connettività wireless, con i problemi di sicurezza che comportano, sono le aree verso le quali puntare per fornire un servizio sempre più specialistico e application-oriented».
La Durante da valore non solo alle soluzioni e ai prodotti adottati, ma in primo luogo alla qualità del servizio erogato ai propri clienti in termini di competenza, affidabilità, reattività e disponibilità. «*Proprio per questo motivo*», sottolinea Casari, «*occorre diffidare da chi offre servizi a costi molto contenuti offrendo prodotti di basso livello spesso accompagnati da una struttura sottodimensionata. Questa soluzione può pagare solamente a breve termine. Un vero servizio di sicurezza lo si ottiene invece rivolgendosi a società di cui si ha fiducia e di riconosciuta competenza*».

## FastWeb SpA

FastWeb è il principale operatore alternativo nelle telecomunicazioni a **larga banda su rete fissa** in Italia. Attraverso una rete «all IP», con accesso in fibra e xDSL, è riuscita a realizzare la convergenza tra **telefonia**, **Internet** e **televisione**. FastWeb si rivolge dunque al mercato residenziale, ai professionisti, alla piccola media impresa e alle grandi aziende.
Abbiamo chiesto a Andrea Bigolin, Product Manager Internet & Security che cosa offre FastWEb per la sicurezza. «*Nelle grandi aziende c'è una notevole sensibilità alla sicurezza delle Intranet: FastWeb ha introdotto per prima le VPN IP su MPLS e oggi ne raccoglie i frutti. La spesa in sicurezza informatica nei collegamenti verso Internet è invece ancora sentita come un costo piuttosto che un investimento. In generale le aziende cominciano a realizzare come l'ampiezza di banda oggi a disposizione possa permettere di ridurre la distanza con il mercato. In tutto questo la sicurezza si appresta a svolgere un ruolo abilitante piuttosto che restare un semplice costo d'infrastruttura*». In questo quadro i servizi più richiesti a FastWeb sono le VPN IP su MPLS per la **sicurezza delle intranet** e la **protezione perimetrale** (firewalling) per l'accesso a Internet. Nell'immediato futuro FastWeb punta a offrire la **protezione a 360 gradi** del gateway di accesso, con servizi integrati di firewalling, antivirus e content filtering. Per differenziarsi dalla concorrenza FastWeb si investe soprattutto sul livello di servizio. Per la scelta di un fornitore di sicurezza in outsourcing «*non bisogna concentrarsi solo sull'aspetto tecnologico della soluzione, bensì sugli sla e sulle procedure proposte dal fornitore*», suggerisce Bigolin che conclude: «*L'economia mondiale si appresta a ripartire e i consumatori sono più attenti e smaliziati. Oggi è prassi diffusa controllare su Internet le caratteristiche del prodotto prima di procedere all'acquisto in maniera tradizionale (per esempio, GDO o B2B); il cliente si aspetta di trovare tutte le informazioni sul sito aziendale, e che siano aggiornate. Per ottenere questo risultato sono condizione necessaria l'alfabetizzazione informatica dei dipendenti e la digitalizzazione dei processi di workflow, e noi crediamo che una banda veramente larga utilizzabile in sicurezza sia il primo step da cui cominciare*».

## I.NET SpA

Il Gruppo I.NET, fondato a Milano nel 1994, fa capo a BT Group Plc e attualmente impiega circa 270 persone, distribuite sulle sedi di Milano, Brescia, Padova, Roma e Torino. Nel corso di più di dieci anni, I.NET è stata caratterizzata da una continua crescita che l'ha portata nell'aprile 2000 alla **quotazione** presso il Nuovo Mercato e nell'aprile 2004 a essere ammessa al segmento titoli ad alti requisiti (oggi allSTAR).

«*La missione di I.NET*», ci dice Mauro Cicognini, «*è garantire la **business continuity** dei clienti attraverso la progettazione e la gestione di infrastrutture ICT arricchite di servizi, attraverso le proprie offerte di managed connectivity e il proprio network di business factory. Questa missione è sostenuta dai servizi a valore aggiunto, che vanno dalla sicurezza delle informazioni alla gestione della messaggistica aziendale, dai servizi di monitoraggio e reporting al back-up dei dati*». I.NET conta alcune migliaia di clienti in tutti i settori d'attività e in tutto il territorio nazionale tra questi prevalgono organizzazioni grandi o medio-grandi, spesso multisede.

Abbiamo chiesto a Cicognini quali sono i servizi più richiesti: «*Le statistiche ci dicono che i MSS più richiesti sono senz'altro quelli legati alla **sicurezza perimetrale** (ovvero essenzialmente la gestione dei firewall), seguiti da quelli legati alla **content security** (antivirus, antispam, URL filtering ecc). Purtroppo oggi riuscire a definire in modo ragionevole un perimetro è sicuramente un problema, perché da tempo esistono varie forme di telelavoro (la più frequente è quella del personale di vendita) ed è pure prassi consolidata quella di connettersi nei modi più disparati a fornitori, clienti, partners ecc*».

Per il futuro I.NET punta su **servizi** più **consulenziali**, «*dei quali I.NET si è dotata negli ultimi due anni. Abbiamo oggi svariati collaboratori esperti di analisi dei rischi, di auditing procedurale e tecnologico, di pianificazione della business continuity, e così via.*

*Tramite loro I.NET può davvero aiutare i propri clienti a valutare correttamente i rischi cui sono esposti, e a scegliere dei rimedi che raggiungano lo scopo inteso con un costo proporzionato al valore del bene da proteggere*».

Negli ultimi anni I.NET ha investito pesantemente nelle proprie risorse umane

e nelle proprie infrastrutture continuando sulla strada di costruire fisicamente dei luoghi dove davvero le informazioni possano essere molto più al sicuro che altrove. Da novembre 2004 inoltre i **data center** di I.NET sono **certificati BS 7799**.

## Init Srl

Dal 1997, Init offre servizi di consulenza, progettazione e gestione di **sistemi di sicurezza** e di internetworking in Italia e nel mondo. Init punta sulla qualità dei servizi erogati e sull'eccellenza tecnologica delle competenze messe in campo. La clientela di Init spazia dalle grandi multinazionali alle PMI. L'obiettivo di Init è di usare la stessa attenzione e la stessa qualità indipendentemente dalla dimensione dell'azienda assistita.

I servizi più richiesti a Init sono la **gestione flat della sicurezza** con una particolare attenzione alla qualità. Questo si concretizza in un canone annuale fisso particolarmente economico accompagnato a sla di erogazione di elevata qualità. «*La sensibilità per la sicurezza informatica è generalmente più sentita dalle aziende che utilizzano Internet e la sicurezza per il proprio business*», sottolinea l'ing. Sergio Leoni, che prosegue indicando quali sono i servizi su cui investe Init per il futuro: «*Servizi di outsourcing, progetti e delivery di progetti brand independent e servizi focalizzati su problematiche verticali in contesti: sicurezza, backup, networking*».

Init vuole distinguersi sul mercato per la qualità e la trasparenza dei servizi verso l'utenza. «*Ci poniamo verso il mercato come riferimento tecnologico per il cliente, adottando soluzioni d'avanguardia e fornendo know-how trasversale*» precisa Leoni. «*Penso che le problematiche di sicurezza informatica e tutti gli argomenti affini trovino a volte poco terreno fertile su cui attecchire, per una mancanza di cultura e per una falsa percezione della sua estensione. È una cultura in movimento quindi immagino che la sensibilità sia in aumento come del resto anche il mercato; sarà un problema delle aziende essere duttili per seguire le fluttuazioni di domanda*». Similmente nell'affrontare la 196/03 si vede che molte aziende la considerano solo una incombenza in più anche se stanno crescendo i casi in cui l'approccio è costruttivo e colto come una occasione di miglioramento.

## Innovia Security Srl

Innovia Security è la sezione di Innovia dedicata alla information security e alla tutela degli asset aziendali. I campi di intervento spaziano dalla consulenza specialistica e dalla advisory strategica al change management e alla progettazione e implementazione di tecnologie di sicurezza. Proprio grazie all'approccio consulenziale Innovia Security può operare in modo trasversale su tutti i settori produttivi: tlc, finanza, servizi e pubblica amministrazione con netta prevalenza di aziende medio-grandi.

Abbiamo chiesto a Stefano Di Capua come le aziende affrontano la problematica della sicurezza: «*La cultura della sicurezza è radicata nelle grandi aziende ma è poco presente a livello di PMI. L'adeguamento alle prescrizioni del decreto 196/03 ha fatto alzare il livello di attenzione di manager e imprenditori su tematiche spesso trascurate o sottostimate. Le prescrizioni della precedente 675/96 erano percepite come inadeguate e poco aderenti alla realtà, mentre i contenuti della 196 risultano più ragionevoli e applicabili. Nel complesso, però, la sensazione più diffusa è quella della pura imposizione normativa*».

A Inovia Security vengono più spesso richiesti «i classici servizi di implementazione tecnologica, in particolare soluzioni antivirus/antispam e security gateway multifunzione. Una grossa fetta dell'attività è costituita dalla consulenza per l'adeguamento alla 196/03 e dai security assessment». Per il futuro Innovia Security punta sui servizi di sicurezza gestiti e sui **programmi di sensibilizzazione** per il personale tecnico e l'utenza finale. «La prevenzione passa sempre per la conoscenza» sottolinea Di Capua. «*E soprattutto l'approccio a 360°: tecnologico, organizzativo, legale, psicologico. Ne è la dimostrazione lo Psychological Risk Assessment elaborato dall'associazione internazionale ICAA, una valutazione oggettiva del rischio legato al fattore umano nelle organizzazioni*».

Per la scelta del partner con cui gestire la sicurezza in oustsourcing Di Capua consiglia un'azienda in cui il personale non sia solo tecnologicamente competente ma anche intelligente e amante del proprio lavoro» fa la differenza nei momenti critici. Una grande curiosità per il mercato porta inoltre ad avere le idee chiare sui prodotti e sulle soluzioni al di là delle mode».

Innovia infine è convinta che assisteremo a una progressiva convergenza tra sicurezza fisica e logica e si sta preparando sin da adesso investendo nella ricerca.

## IT Security

IT Security è stata fondata nel 2004 da Giuseppe Ferrito a Messina dove ha la propria sede. Grazie a una serie di partner estende la propria area operativa anche in realtà nazionali e internazionali. I principali clienti di IT Security sono aziende del settore pubblico, pmi e istituti di formazione. Abbiamo chiesto a Giuseppe Ferrito come vivono in genere le aziende i problemi riguardanti la sicurezza: «*È un settore in continua espansione in cui spesso per mancanza di competenze i clienti si vedono costretti a ricorrere all'outsourcing*». *La politica di IT Security è di operare in modo che* «*a fronte di costi che si ammortizzano in pochi mesi, si possono offrire tecnologie affidabili per anni, garantite dalla qualità controllata e da un'ampia gamma di prodotti, dalla riconosciuta reputazione dei marchi distribuiti, dall'introduzione di congegni innovativi, nonché da un alto livello di servizio e una comprovata velocità di consegna*».

Attualmente i servizi più richiesti a IT Security sono antivirus, firewalling, sicurezza perimetrale, privacy e backup dati. Per il futuro Ferrito scommette sulle sicurezza per reti geografiche, favorite dall'aumentare della connettività e sulle attività di computer forensic, vale a dire la produzione di documentazione relativa a verifica e controllo di attività svolte con mezzi informatici (computer, reti pubbliche e private), in modo che sia utilizzabile in sede processuale.

IT Security sceglie di «*affiancare i propri clienti fin dalla progettazione dell'infrastruttura di sicurezza e di seguirne la realizzazione, la messa in servizio e l'utilizzo in condizioni di assoluta affidabilità. Il modo migliore per fare sicurezza, prosegue Ferrito, è l'outsourcing: se si è una piccola o media azienda è sempre meglio affidarsi a chi fa della sicurezza informatica il proprio lavoro e non tentare di risolvere il problema internamente. Per le grandi aziende può essere comodo implementare la sicurezza in outsourcing in aree ben prefissate o rivolgersi a esperti del settore per testare il grado di sicurezza delle strutture o degli apparati*».

## Lis Liscom

Liscom, azienda del gruppo LIS, offre servizi di sicurezza non solo informatica per medie e grandi aziende. Il suo SOC (Security Operations Center) operativo 24 ore al giorno, 365 giorni l'anno, gestisce da remoto i sistemi di sicurezza informatica installati presso i clienti ed è in grado di intervenire tempestivamente in caso di problemi.

La sicurezza informatica riguarda qualsiasi azienda faccia uso di strumenti informatici e Liscom può vantare molteplici tipologie di clienti, da produttori di hardware informatico a gruppi internazionali di industrie metal-meccaniche e importanti aeroporti italiani. Ma come si pongono di fronte ai problemi della sicurezza? «Purtroppo, nella maggioranza dei casi» lamenta Massimo Pellistri, «*la sicurezza è ancora giudicata come un costo e non come supporto a una maggiore efficienza del business. I vertici aziendali spesso affrontano il problema da un punto di vista prettamente tecnologico, cioè risolvibile con un software o con un hardware. Il problema in realtà è più esteso e coinvolge non solo le competenze per utilizzare tali strumenti ma anche le procedure e i processi interni che vi sottendono. Il problema della sicurezza informatica è più culturale e organizzativo che tecnico. Come dice Bruce Schneier, guru della sicurezza informatica,* ***La sicurezza è un processo, non un prodotto***».

I servizi offerti da Liscom sono quanto mai vari e dipendono dalla sensibilità del cliente al problema. «*Alcuni nostri clienti hanno subito danni a causa di un attacco informatico o di un virus. In questi casi i servizi più richiesti sono il vulnerability assessment e il penetration test e sottoscrivono contratti di sicurezza gestita in outsourcing al fine di tutelarsi da altri attacchi. Altri clienti sono invece sensibili al loro patrimonio informativo e cercano soluzioni che proteggano i dati, in particolare da dipendenti infedeli*».

Secondo Pellistri, inoltre, «*Le previsioni del mercato indicano un* ***costante ed elevato incremento*** *della sensibilità sui problemi relativi alla sicurezza nei prossimi anni. Di proposito ho parlato di sicurezza e non di sicurezza informatica poiché l'integrazione fra la sicurezza fisica e quella logica è alle porte. I sistemi di sicurezza tradizionali utilizzano*

*sempre più i sistemi informatici: telecamere con Web server integrati, sistemi software avanzati per l'antiterrorismo ecc. Il gruppo a cui appartiene Liscom, oltre che teorizzare un futuro dove la* ***sicurezza fisica e la sicurezza logica saranno integrate****, è anche in grado di offrire servizi integrati avendo alle spalle quasi venti anni di esperienza sulla sicurezza a 360 gradi*».

Il punto di forza di Liscom «*è dato dalla composizione del nostro team di tecnici esperti, qualificati e di madre lingua italiana. Inoltre il gruppo possiede la licenza di vigilanza e il nostro personale è sottoposto a controlli periodici condotti dalla questura, procedura necessaria per il nostro staff che è inquadrato come Guardie Giurate*». Concludendo, Pellistri aggiunge: «*I problemi non aspettano che tu sia pronto, per cui è meglio farsi trovare pronti*».

## NetHouse SpA

Nethouse, nata a Torino nel 1998, opera nel settore del terziario avanzato e-business services oriented. I servizi integrati di consulenza, sviluppo e gestione di soluzioni avanzate per l'e-business le permettono di rivolgersi principalmente a medie-grandi aziende, pubblica amministrazione, associazioni di categoria ed enti istituzionali.
Abbiamo chiesto al dottor Montrucchio come vede i problemi riguardanti la sicurezza: «*Dal punto di vista legislativo, il decreto 196/03 rappresenta un'ottima base di partenza, seppure presenti in parecchi punti lacune e incertezze. La sicurezza informatica non viene percepita come fattore di competitività e tutela del proprio know how bensì come un* ***semplice adempimento****. Manca una cultura idonea a comprendere gli effettivi benefici legati a questo tema, cultura che non significa solo acquisto di costose apparecchiature informatiche… Tematiche come il* ***social engineering*** *per esempio trovano scarsa penetrazione nell'ambiente della formazione del personale*». Con social engineering ci si riferisce a quelle tecniche, utilizzate solitamente dagli hacker, per ottenere dati a cui non potrebbero comunemente avere accesso. Tali dati sono carpiti fingendo di essere qualcun altro. I noti casi di fishing degli ultimi tempi in cui malintenzionati si fanno passare per il servizio tecnico di una banca e chiedono a un utente di collegarsi a un sito e inserire la propria user id e password per accedere al conto online ne sono un buon esempio.
NetHouse punta inoltre per l'immediato futuro allo sviluppo di **sistemi integrati di sicurezza** in cui si abbia la convergenza di implementazioni a basso costo di sistemi di disaster prevention e recovery e di sistemi di posta elettronica certificati e sicuri. Di fondamentale importanza infine la formazione e divulgazione dell'etica hacking e del social engineering per poterle combattere attivamente dall'interno.
Trai i punti di forza di NetHouse oltre all'attenzione per la qualità dei servizi erogati è «*la componente di* ***ricerca e sviluppo*** *su sistemi Unix/BSD/Linux*» sottolinea Montrucchio.
A chiunque debba scegliere un fornitore di sicurezza in outsourcing il presidente di NetHouse offre cinque semplici suggerimenti:

- *rapporto di fiducia tra fornitore e management aziendale*
- *partnership tecnologiche innovative e di alto livello*
- *congruo rapporto tra prestazione/prezzo*
- *portfolio aziendale, perché ne racchiude il knowhow*
- *scelta oculata solo tra i professionisti del settore.*

## Netpeople Srl

«*Netpeople è la business unit di Softpeople focalizzata sull'offerta di servizi e soluzioni in ambito* ***privacy*** *&* ***security governance****, caratterizzati da una metodologia referenziata, basata su normative e standard internazionali, e da un approccio integrato e interdisciplinare*» *ci dice l'ing. Simone Marini, amministratore delegato di Netpeople.* «*I nostri clienti, aziende italiane e multinazionali, appartengono principalmente ai settori manifacturing, automotive e utilities. Le aziende, purtroppo, spesso percepiscono i problemi riguardanti la sicurezza come un costo quando sono spinte dalla normativa (legge privacy, BS 7799 per partecipazione a bandi ecc.) e solo poche riescono a trasformare gli obblighi di legge in* ***opportunità****, creando valore aggiunto*».
Attualmente Netpeople lavora prevalentemente in ambito privacy (audit, DPS e misure minime, manuale della sicurezza, formazione), identity & access management, business impact analisys/business continuity (security monitoring, sicurezza perimetrale, vulnerability assessment). In un immediato futuro Netpeople conta di incrementare la diffusione di servizi più maturi quali la privacy & security governance e la gestione dei processi di sicurezza e privacy attraverso una consolle centralizzata di monitoraggio dei processi. In questo contesto Netpeople si distingue grazie alla «*metodologia e alle competenze verticali, all'****integrazione delle aree di intervento*** *(tecnologie, organizzazione, normativa), alla gestione di progetti complessi e al trasferimento di know how al cliente*».
Come scegliere dunque un partner per gestire la sicurezza in outsourcing? «*Occorre verificarne le competenze distintive anche tramite le referenze, la capacità di affrontare progetti complessi in flessibilità ed economicità e di gestire problemi non solo tecnologici, ma anche organizzativi, e di trasferire know how all'azienda*» risponde Marini. «*Troppo spesso [gli obblighi imposti dalla 196/2003] sono considerati un semplice costo. La nostra metodologia prevede l'integrazione delle diverse aree di intervento per trasformare un obbligo in un'opportunità per verificare i livelli di sicurezza e agire di conseguenza*».

## Pres srl

Pres si occupa di networking, di system integration con i relativi servizi correlati e di sicurezza informatica. Partner dei più importanti vendor presenti in Italia, PRES è **certificata UNI EN ISO9001: 2000** per il suo sistema qualità ed è membro del **Clusit**, l'Associazione italiana per la sicurezza informatica.
I clienti di Pres vanno dalle grandi aziende quali Osram, Lavazza o TNT, ad aziende ospedaliere, banche e assicurazioni, fino a molte piccole e medie aziende alle quali offre una serie di servizi ad hoc, anche in outsourcing. In genere le aziende tendono a sottovalutare il problema della sicurezza, «*C'è comunque un diffuso atteggiamento di diffidenza e di "perché dovrebbe capitare proprio a me?", salvo poi… chiudere la stalla quando i buoi sono scappati*» commenta Giovanni De Giovanni, amministratore delegato di Pres. L'interesse maggiore delle aziende è nel campo dei servizi di sicurezza gestita: «*Le esigenze si sposano bene con la nostra offerta modulare David, che consiste in un servizio in outsourcing attivo sulle 24 ore, e che offre lo stato dell'arte in termine di protezione perimetrale*». Per il futuro Pres punta oltre che sulla sicurezza sulla consulenza a elevato valore aggiunto e più in generale tutti i servizi IT e VoIP.
Tra i suoi punti di forza Pres può contare «*su un team molto preparato, sulla* ***velocità di intervento*** *e sulla* ***flessibilità***» dice con orgoglio De Giovanni. Per tutti coloro che devono scegliere un fornitore di sicurezza il suo consiglio è: «*Mantenere all'interno dell'azienda la definizione e l'evoluzione delle politiche di sicurezza e, lasciando da parte la (comprensibile) diffidenza, affidare la gestione dell'infrastruttura a un partner specializzato le cui capacità gli permetteranno di dedicarsi al business aziendale, tralasciando gli eventuali problemi di cui si farà carico l'outsourcer*».

## Secure Group Srl

Secure Group, azienda certificata BS 7799, si occupa della sicurezza delle informazioni a 360° e da anni progetta e gestisce la protezione dei dati in più di 80 realtà aziendali. «*Fare sicurezza significa: individuare e valutare il rischio, predisporre interventi organizzativi mirati, adottare tecnologie specifiche utili per il controllo costante e continuo delle reti, dei dati e applicazioni. Attività che richiedono conoscenze specifiche, investimenti adeguati in ricerca/sviluppo e una forte verticalizzazione del management e della struttura per* ***garantire adeguati livelli qualitativi***» commenta Roberto Farinetti, managing partner.
I principali clienti di Secur Group sono grandi realtà bancarie e industriali, aziende di telecomunicazioni, manifatturiere e pubblica amministrazione pur non tralasciando le piccole e medie aziende alle quali offre, con la medesima serietà, le proprie soluzioni.
«*Le aziende sono sempre più consapevoli dell'esistenza di rischi reali legati alla mancanza di una adeguata sicurezza delle informazioni (rischi operativi, rischi finanziari, rischi legali ecc.)*» conferma Farinetti «*Spesso però manca una conoscenza manageriale delle metodologie e delle strategie utili a misurare e gestire il rischio. Gli interventi sono prevalentemente di carattere tecnologico e finalizzati a cogliere un singolo aspetto del problema. Raramente esiste un quadro strategico e operativo generale e una capacità e volontà di creare una efficace cultura di tutela del patrimonio informativo aziendale*».
I servizi più richiesti a Secur Group sono la progettazione del sistema perimetrale di difesa, la messa in sicurezza (hardening) dei sistemi e delle reti, l'accesso sicuro alla rete aziendale mediante VPN SSL, la protezione antivirus, la revisione dell'intera rete in ottica di sicurezza, i servizi gestiti delle infrastrutture di sicurezza e l'audit. Nel prossimo futuro Secur Group crede molto nei servizi di ***intrusion prevention***, ***strong autenthication***, ***event correlation***, servizi integrati di gestione, business continuità, security awareness & education».
Abbiamo infine chiesto a Farinetti quali, secondo la sua esperienza, sono le domande da porsi per scegliere un fornitore di sicurezza in oustsourcing:

- «*Possiede referenze documentabili in servizi analoghi?*
- *Possiede un proprio livello di sicurezza adeguato e dimostrabile?*
- *Il livello di servizio è misurabile, contrattualmente definito e adeguato alle esigenze del cliente?*
- *Esistono momenti formali e metodologie di verifica della qualità del servizio ricevuto?*
- *Il servizio è erogato 24x7 con personale in presidio operativo?*
- *Possiede un team di risorse specializzate che possono intervenire on site presso il cliente in caso di incidente?*
- *Dimostra una adeguata esperienza nella realizzazione delle infrastrutture da gestire?*»

## Teligo Srl

Teligo, branch italiana della multinazionale Via-Networks e presente nel nostro paese dal 1990, è un ISP specializzato in soluzioni rivolte alle PMI che richiedono in outsourcing la gestione dei servizi per l'infrastruttura, l'accesso, la sicurezza e la gestione delle soluzioni basate su Web. I clienti principali di Teligo sono aziende che hanno bisogno di collegare in sicurezza le loro sedi in Italia e in Europa, PMI europee che estendono alle sedi italiane la loro VPN. Abbiamo chiesto a Ivan Botta di fare una fotografia della situazione della sicurezza nelle aziende italiane: «*C'è' molta confusione. Alcuni operatori terrorizzano le aziende con l'obbiettivo di vendere un firewall, altri un software per fare il DPS, ma è il* ***servizio che conta***». In questo quadro i servizi più richiesti a Teligo sono quelli in outsourcing: «*Network VPN, sicurezza perimetrale e monitoraggio. Ci viene spesso richiesto di ospitare nel nostro data center le applicazioni del cliente, le monitoriamo, gestiamo la sicurezza e garantiamo la* ***continuità del servizio***». Per quanto riguarda il futuro quali saranno i servizi su cui puntare? «*Con full wan facciamo l'outsourcing del centro stella, al cliente consegniamo una* ***rete privata sui CPE*** *(Customer Premise Equipment – apparecchiatura che connette un cliente a una rete), tutto con connettività controllata a Layer 2 e non su IP; hosting dedicato; connettività bilanciata con più circuiti in back-up tra loro. Stiamo iniziando inoltre con il* ***VoIP*** *che per noi è un servizio da appoggiare sull'infrastruttura fornita al cliente*». Teligo per differenziarsi dai competitor punta sulla qualità del servizio e su sla su misura per il singolo cliente. «*Il nostro servizio di pre-sales e di assistenza è consulenza vera e propria, inizia in fase di proposizione del servizio e continua nel supporto giornaliero*».
Si fa un gran parlare della 196/03: come vengono in generale percepite queste nuove norme dalle aziende? «*In molti casi è stata l'occasione per affrontare il tema della sicurezza, per fare un'analisi, per capire il problema e realizzare che la sicurezza è un aspetto importante. In altri un'occasione persa se l'azienda si è limitata all'adempimento formale*».

## Telvox Srl/Scai SpA

Telvox srl è una controllata SCAI che nasce come SCAI Sicurezza nel 1996, attiva da sempre nella sicurezza dei sistemi. Con l'acquisizione di Telvox Teleinformatica di Bologna, diventa nel 2002 la nuova Telvox, con esperienza in campo applicativo, specialmente nella firma/cifratura dati. Massimo Cipolletta ci parla dei loro clienti tipici: «*Sono principalmente large account tra cui ricordiamo Banca d'Italia, Consip, Sogei, San Paolo IMI. Telvox fornisce soluzioni per l'archiviazione di grandi quantità di dati con MDS (AUI) e per la dematerializzazione dei documenti e di validazione dei flussi*».
Telvox si occupa principalmente di **valutazione del rischio** e consulenza sulla **redazione del DPS**. «*Non è raro poi, che in seguito a questi primi approcci, le aziende inizino a interessarsi alle nostre soluzioni e alla possibilità di integrarle ai loro sistemi, per esempio per la messa in sicurezza di flussi* ***documentali***, *grazie al nostro* ***motore crittografico multipiattaforma MBM***» aggiunge Cipolletta.
Oltre alla sicurezza sistemistica, Telvox fornisce soluzioni di sicurezza applicativa con API multipiattaforma di firma e cifratura, PKI (Public Key Infrastructure – infrastruttura per la gestione di certificati a chiave pubblica) e progetti di integrazione della sicurezza. Telvox è proprietaria di tutti i codici sorgente delle proprie applicazioni e quindi può facilmente **personalizzare** e **aggiornare** in piena autonomia le soluzioni che propone.
Abbiamo chiesto a Cipolletta come scegliere un fornitore per la sicurezza in outsourcing: «*I parametri chiave sono: la solidità e l'esperienza da un lato e la flessibilità che permette tempi di reazione rapidi; questa è l'impostazione strategica che ha voluto negli anni darsi Telvox*». Per concludere: «*Il continuo aggiornamento è la chiave del successo di ogni azienda solida e affidabile. Naturalmente ciò è possibile laddove vi è solidità finanziaria con conseguente capacità di gestione di progetti di rilevante impegno. L'esperienza Telvox deriva anche dalla sicurezza dell'appartenenza al gruppo SCAI*».