Carige sotto controllo

di Giancarlo Magnaghi

Il Gruppo Banca Carige ha affidato a Telecom Italia la gestione di alcune funzioni del proprio sistema di sicurezza perimetrale. Ce ne parla Cesare Maggiolo, responsabile ICT - Gestione e Supporto.

Il Gruppo Banca Carige è un gruppo bancario e assicurativo di medie dimensioni, nato dal raggruppamento, attorno alla Cassa di Risparmio di Genova e Imperia, di alcune banche e società d'assicurazione liguri e toscane, che opera su tutto il territorio nazionale con una rete integrata di punti vendita, fornendo prodotti e servizi bancari, finanziari, assicurativi e previdenziali a oltre 1.700.000 clienti. Essendo un gruppo nato dalla fusione di elementi eterogenei, che dispone di un'offerta ampia e variegata, la funzione dei sistemi informativi è fondamentale per assicurare il funzionamento corretto e uniforme dei processi aziendali, e il presidio della sicurezza di una rete così complessa sicuramente non rappresenta un facile compito.
Per avere maggiori informazioni sulle strategie di questo gruppo, che di recente ha affidato a Telecom Italia la gestione di alcune funzione del proprio sistema di sicurezza perimetrale, abbiamo intervistato Cesare Maggiolo, responsabile ICT - Gestione e Supporto.

? ! Come è strutturato il gruppo Carige?

Il gruppo bancario Carige, presente in 51 province appartenenti a 12 regioni e forte di un organico di oltre 5.000 dipendenti, è composto da più banche: la capogruppo Banca Carige, Cassa di Risparmio di Savona, Cassa di Risparmio di Carrara, Banca del Monte di Lucca e Banca Cesare Ponti. Appartengono al gruppo anche la SGR (Società di Gestione del Risparmio) Carige Asset Management SGR e le due compagnie di assicurazione Carige Vita Nuova (ramo vita) e Carige Assicurazioni (ramo danni). La rete bancaria del gruppo è costituita da circa 500 sportelli e 600 terminali Bancomat, mentre le assicurazioni dispongono di oltre 400 agenzie. Grazie ad accordi di gruppo, l'attività delle banche e delle assicurazioni è fortemente sinergica, tanto che le banche vendono anche prodotti assicurativi e le assicurazioni vendono anche prodotti bancari.

? ! Come è composta le rete informatica?

La Direzione ICT dispone complessivamente di circa 180 addetti a Genova, per analisi, sviluppo e gestione, e di alcuni consulenti esterni.
Il centro di calcolo è di tipo tradizionale ed è costituito da due poli (uno principale e uno alternativo) ambedue a Genova. Nel polo principale vi sono un sistema IBM, che supporta le applicazioni tradizionali, e una server farm; nel polo alternativo abbiamo un sistema IBM, che dispone di capacità d'elaborazione in grado di aumentare in caso d'emergenza.
Le applicazioni di front-end, buona parte delle applicazioni Intranet e l'Internet Banking (con circa 60.000 clienti) operano in ambiente z/Linux con WebSphere e sono operative in entrambi i poli sui sistemi IBM. La gestione del servizio di trasporto delle informazioni è affidata a Telecom Italia.

? Quali elementi avete considerato quando avete deciso di affidare in outsourcing alcune funzioni relative alla sicurezza della vostra rete?

! Dopo una ricerca di mercato e l'emissione di una dettagliata "Richiesta di proposta", abbiamo affidato in outsourcing a Telecom Italia l'esame e la gestione dei log degli eventi anomali segnalati dai firewall. La gestione dei firewall è stata mantenuta all'interno ed è effettuata da personale Carige.
Telecom garantisce un presidio 24x7 ed esegue l'analisi degli allarmi e le loro correlazioni; nel caso si determini il rischio di un potenziale attacco, ne viene fornita tempestivamente comunicazione a Carige. Abbiamo effettuato questa scelta per evitare di costituire una struttura specializzata, attiva 24x7, e per passare da un'attività passiva di controllo dei firewall a un'attività proattiva.

? In cosa consiste il servizio fornito da Telecom Italia?

! Oltre alla gestione degli allarmi cui abbiamo già accennato, Telecom effettua anche altre attività: il Vulnerability Assesment e il Penetration Test.
Il vulnerability assesment consiste nella verifica dei prodotti software, dei livelli delle release e di patch installate sui server, che sono confrontati con un data base di vulnerabilità. Il Penetration Test è il tentativo di penetrare nel sistema, utilizzando strumenti e metodi normalmente utilizzati dagli hacker, per scoprire se ci sono punti deboli nel sistema di difesa. Un'altra prova da effettuare è il penetration test della fonia, cioè la scansione di tutti i numeri interni della rete telefonica alla ricerca d'eventuali modem che potrebbero creare punti di debolezza nel sistema di difesa.
Questi test sono stati affidati, anche nel passato, ad altre società e sono ora effettuati da Telecom Italia. Anche questo servizio è stato esternalizzato, poiché riteniamo che mantenere all'interno la cultura necessaria e aggiornarla continuamente per effettuare questi controlli comporti costi superiori rispetto all'utilizzo di una società specializzata in questo tipo d'attività. Nel contratto di outsourcing è compresa anche la realizzazione di un sistema d'accesso a Internet, controllato da una black list di siti Internet, catalogati dinamicamente in base agli URL e alla classificazione dei contenuti, che permetterà a un migliaio di utenti di accedere liberamente, secondo il proprio profilo, a tutto il Web, esclusi solo i siti contenuti nella black list, mentre tutti gli altri potranno accedere solamente ai siti elencati in una white list.

« La rete bancaria del gruppo è costituita da circa 500 sportelli e 600 terminali Bancomat, mentre le assicurazioni dispongono di oltre 400 agenzie

? Quali sono i criteri che utilizzate per controllare come funziona il servizio?

! Il servizio è garantito 24x7; qualora fossero rilevati degli attacchi, Telecom è tenuta a informare immediatamente i responsabili della sicurezza dei sistemi Carige per intraprendere le azioni più opportune.

? Da quanto tempo è partito questo servizio e quali risultati ha portato?

! Il servizio è partito dal dicembre 2004; in questo periodo sono emersi alcuni allarmi relativi a tentativi di accesso da sistemi interni al Gruppo, per errori d'impostazione dei sistemi stessi, e, quindi, queste indicazioni sono state utili per tarare meglio i nostri server.

? Quali ritenete che siano i principali benefici /inconvenienti di questo rapporto di outsourcing?

! Il vantaggio è di disporre, con il giusto rapporto costi/prestazioni, di un servizio per il quale avremmo dovuto effettuare notevoli investimenti interni sia in tecnologia sia in risorse umane. Al momento non abbiamo individuato alcuno svantaggio.

? Come affrontate i problemi di sicurezza "non tecnici", come social engineering e phishing?

! Per quanto riguarda in particolare il phishing, la nostra Direzione Marketing ha pubblicato sui siti Internet delle Banche del Gruppo una nota per informare i Clienti dell'esistenza di questo fenomeno.
Il problema della cultura della sicurezza e della privacy del nostro personale è gestito con molta attenzione. Abbiamo prodotto una normativa interna sulla "prevenzione di frodi perpetrate attraverso Internet", che costituisce una guida operativa per il nostro personale.

? Nei vostri sistemi di home banking, utilizzate la posta elettronica per inviare informazioni ai clienti o preferite evitare questo mezzo per motivi di sicurezza?

! Per ragioni di sicurezza preferiamo non inviare email al Cliente, che può comunque verificare in tempo reale l'esito delle operazioni collegandosi al sito di Internet banking in modo sicuro.