I NUOVI RISCHI PER LA SICUREZZA IN B

Le tecniche di abusi e attacchi informatici sono sempre più sofisticate. Raoul Chiesa, ex hacker e consulente It, avverte: non sempre gli istituti di credito sono ben protetti.

A cura di Editoria & Immagine
Hanno collaborato Pietro Ricciardi e Claudia Silivestro

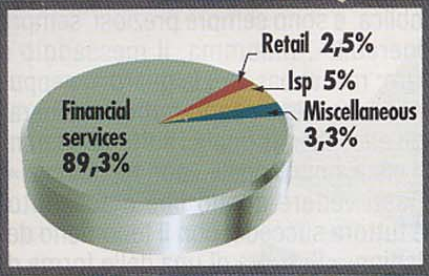
Le banche sono ancora vulnerabili di fronte agli attacchi informatici. **Raoul Chiesa**, membro del direttivo Clusit, esperto e consulente di sicurezza It, lancia una provocazione diretta: «Le normative relative al settore finanziario sono sempre più stringenti, soprattutto per la sicurezza delle informazioni, il rispetto degli standard nazionali e internazionali e le best practice. Il risultato dovrebbe essere una "banca inviolabile", ma non sempre è così».

Prima di lavorare come consulente, Chiesa è stato uno dei primi hacker italiani. Con il nickname Nobody è entrato nei sistemi di società di telecomunicazioni, istituzioni governative e finanziarie. Nel novembre 2005, nel corso dell'Idc banking forum a Milano, Chiesa ha citato i numeri di dieci anni di Penetration testing and security audit del Tstf, il network di Telecom Security Task Force, su 24 operatori finanziari di Europa, Asia, Nord e Sud America e Australia, dal 1995 al 2005. Il 100% dei sistemi si è rivelato passibile di intrusioni tramite le applicazioni web, e appena il 23% del campione mostrava un adeguato controllo sulla sicurezza perimetrale.

«Noi operatori osserviamo un elevato, quasi assoluto, rispetto delle normative, ma dal punto di vista teorico», spiega Chiesa. «Vengono effettuate ottime analisi dei rischi, le quali però non tengono conto degli aspetti pratici e tecnologici ai quali la tecnologia odierna, forzatamente, impone verifiche sul campo. Spesso l'analisi della difesa perimetrale indaga sulla presenza di un sistema firewall, mediante una serie di interviste al personale It della banca, ma quasi mai si va a verificare la configurazione del firewall, le regole di fiducia verso altri sistemi o terze parti, la modifica di alcune configurazioni o impostazioni di default».

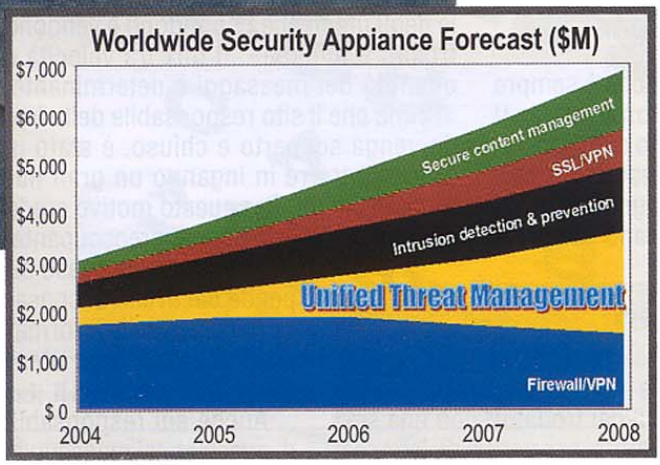
In questo modo, la banca gode di un falso senso di sicurezza, e al tempo stesso «l'infrastruttura It dell'azienda di credito inizia ad aprirsi con una piccola, insignificante esposizione», aggiunge Chiesa. Un anello debole della catena che

ANCA



COME DIFENDERSI

Come mostra il grafico in alto (fonte: Anti-phishing working report 2006). Il mondo finanziario è il primo bersaglio degli attacchi di phishing. Colpiti anche operatori di vendita al dettaglio e internet service provider. Come si proteggono gli istituti di credito? Prima di tutto, con le tecnologie per la gestione dei contenuti, che presentano una forte crescita (grafico in basso; fonte: Id 2006). Le altre contromisure prese dalle banche sono la crittografia nelle transazioni e nelle reti protette; l'analisi preventiva del traffico di rete in entrata; la gestione unificata delle minacce; i firewall.



La sicurezza delle applicazioni web

«La web application security è una delle problematiche più calde, se non la più calda, di questi ultimi tempi», dice **Raoul Chiesa**, membro del direttivo Clusit. «Per questo abbiamo deciso di pubblicare sul tema un quaderno per i professionisti del settore». Il documento, che dovrebbe essere pubblicato a maggio 2006, è stato scritto da sei autori, tra cui Chiesa, con il supporto dell'italian charter di *Open web application security project*, l'associazione di categoria internazionale che si occupa di definire e fornire gratuitamente metodologie, checklist e strumenti software per il controllo della sicurezza nelle applicazioni web based. Altri documenti utili per gli operatori sono già consultabili.

Le linee guida per lo sviluppo sicuro di applicazioni web:
http://www.owasp.org/documentation/guide.html
Le dieci vulnerabilità più critiche nelle applicazioni web
http://www.owasp.org/documentation/topten.html
(in Italiano al **http://www.clusit.it/whitepapers.htm**)
Per verificare la sicurezza degli applicativi:
http://www.owasp.org/documentation/testing.html
Infine, tra i software messi a disposizione da Owasp ci sono *WebScarab*, per «testare» la sicurezza degli applicativi web.
http://www.owasp.org/software/webscarab.html
WebGoat, un applicativo vulnerabile utilizzato per il training sulle applicazioni web:
http://www.owasp.org/software/webgoat.html
il progetto *Net Security*, che raccoglie una comunità di persone dedicata a sviluppare strumenti per la security in ambiente *MicroSoft.Net.*
http://owasp.net/default.aspx

può fare da punto di ingresso «a causa di insicurezze non rilevate, sezioni dell'It "dimenticate" dalle precedenti gestioni, canali di attacco non monitorizzati, zone della rete locale Lan non correttamente segmentate».

Quali sono i maggiori rischi per un istituto di credito? Un frodatore esperto può agire sui servizi di internet banking tramite azioni di phishing, anche associate allo sfruttamento di vulnerabilità non note, le cosiddette «zero day», «specialmente sui sistemi Microsoft Windows, smartphone Symbian e Pda Windows Ce», osserva Chiesa. Attacchi di alto livello sono possibili anche «tramite il social engineering, l'ingegneria sociale, diretti sia verso l'help desk e i call centre del servizio di internet banking, ma anche verso il cliente».

Tuttavia, è «l'evoluzione della tecnologia a presentare i maggior rischi: per la clientela oggi il correntista vuole comunicare in movimento, essere indipendente rispetto agli orari "canonici" e, quindi, operare in maniera autonoma», dice Chiesa. Questo significa che «il modello di business e interazione tra banca e cliente si sta spostando, in modo diametralmente opposto rispetto ai modelli precedenti». Gli istituti di credito possono trovarsi ad affrontare nuove sfide per le quali sono necessarie nuove soluzioni. «Sarebbe curioso», osserva Chiesa, «sentire se e quante banche che operano nel nostro Paese sono dotate di sistemi di database management cifrati, segregazione del codice sorgente delle applicazioni critiche, formazione contro attacchi "non convenzionali" come il social engineering».

La risposta migliore, secondo Chiesa, è quindi «ricerca, e tanta, unita a un'apertura e a una maggior comprensione verso il pirata informatico; più analisi pratiche, infine, da unire alle analisi teoriche del rischio, ottenendo così modelli di rischio reali e che rispecchino concretamente l'effettiva esposizione al rischio informatico». ●

POCA SICUREZZA

«Tutte le banche sono passibili di intrusioni tramite web», dice Raoul Chiesa, membro del direttivo Clusit. «E appena il 23% delle aziende di credito mondiali controlla adeguatamente la sicurezza perimetrale».