

M Magazine 1.08



ATTUALITÀ

“L’agenda dei security officers per la sicurezza delle informazioni.
Asset, tecnologie e investimenti.”
di Dario Forte

Le priorità dei Chief Information Security officer

Una panoramica sulle tematiche più rilevanti per i CISO, dal punto di vista dei processi e, naturalmente, delle tecnologie.

Il 2008 viene visto, dal punto di vista della sicurezza, come un anno di consolidamento dei threat (minacce) e di crescita ulteriore di mercato. Si tratta di un anno molto importante, dove il valore della sicurezza per il business è sicuramente una priorità, che ha degli impatti legali sempre più importanti, non solo nei confronti dei business partner ma anche degli eventuali fruitori del servizio che, paradossalmente, potrebbero anche intraprendere azioni estreme (negli Usa si parla da tempo di Class Action) ad episodi/incidenti di grandi dimensioni. Ad ogni modo, è opinione comune che in questo momento storico esistano degli spunti di riflessione che bisognerebbe considerare, che vanno ben oltre la mera scelta di un partner di sicurezza basata su fattori economici. In questo articolo effettueremo una serie di considerazioni sugli argomenti di maggiore attualità.

Big trends in cyber crime in 2008

Quest'anno, secondo molti analisti, vi sono due grosse "famiglie" di problemi (threats), collegate tra di loro da vari fattori di tipo tecnico, organizzativo e legale. Entrambi costituiscono fattori cruciali per i CISO (Chief Infosecurity Officers) perché l'impatto potenzialmente rappresentato da ciascuno di essi potrebbe minare la stessa posizione di questa figura all'interno dell'azienda in cui opera.

Se guardiamo al 2008 da una prospettiva di tipo tecnico, le aziende si trovano a dover combattere con l'evoluzione di problematiche già viste, che rientrano nei cosiddetti "fraud related attacks", che, con l'andar del tempo, diventano sempre più sofisticati. Ci troviamo di fronte a termini come "advanced phishing" e "fraud Cross platform Web attacks". Entrambi non si possono più esclusivamente definire come unicamente correlati all'end user ma ormai si focalizzano anche sugli aspetti web, sfruttando le falle di sicurezza architetturali ed applicative, vecchie e nuove, delle aziende obiettivo.



SECURITY

What is "new"?

A dire il vero non si tratta di attacchi nuovi (inediti) veri e propri, ma le problematiche sul mondo Mac sono evidentemente in aumento. Sia i sistemi operativi Mac OsX sia la piattaforma iPhone sono ormai diventati un obiettivo interessante per gli attacker più o meno sofisticati. I survey vedono, primariamente negli Usa, un potenziale problema di sicurezza iPhone, soprattutto se adottato come smartphone aziendale cosa che, almeno per ora, non riguarda direttamente il nostro paese, vista la relativa disponibilità del device sul mercato.

Diverso, invece un altro spunto di attenzione che è quello dei sistemi virtualizzati.

Questo argomento è ancora sottovalutato dal punto di vista della sicurezza. I vendor in parte sono già al lavoro per prevenire i problemi, ma si sentono ancora in giro dei CIO (chief information officers) che non concordano con i CISO circa la reale contiguità tra le piattaforme virtualizzate e quelle "reali" che genera di fatto una potenziale transazione dei pericoli tra più ambienti, specie se le risorse dati sono condivise.

Un altro argomento di sicura importanza è il web 2.0 e i suoi derivati. È in aumento (e sempre più sofisticato) il fenomeno del cosiddetto "malicious spam" collegato ai blog, ai motori di ricerca, ai forum e, naturalmente, ai siti web. Non sempre le soluzioni a questo problema si sono dimostrate adeguate. In alcuni casi il problema del malicious spam è



Dario Forte, CFE, CISM, si occupa di sicurezza dal 1992 ed è Founder and CEO di DFLabs. Docente di Gestione degli Incidenti informatici all'Università di Milano, ha lavorato con NASA, Esercito Americano e Governo Italiano. Ha pubblicato nove libri e circa trecento articoli in Italia, Usa, Sudamerica e Asia. www.dflabs.com

stato affrontato con vecchie soluzioni ripositonate a livello di marketing, mentre il gap tra il problema e la “soluzione” è molto più ampio.

Dove il problema non è ancora sotto controllo

A modesto parere di chi scrive, lo Spam rimane ancora uno dei problemi più frequenti e solo relativamente risolti. In molti casi, infatti, sia i vendor sia i clienti gestiscono la prevenzione generando una potenziale limitazione del business. I falsi positivi sono gestiti in maniera potenzialmente dannosa, e continua ad essere potenzialmente limitato il traffico email legittimo. Non sempre ciò è dovuto alla tecnologia, bensì alle carenze in fase implementativa, sia lato cliente sia lato fornitore/partner. E' normale che stiamo parlando di problematiche ormai già note che, in alcuni casi i vendor fanno ancora fatica a gestire. Diversi, invece, i discorsi relativi alle nuove tecniche di attacco, che meritano una declinazione ed un'analisi a parte.

Quali tecnologie hanno superato le aspettative?

Aumenta il numero delle installazioni di strumenti di approfondimento e riscontro automatizzato degli allarmi. Rientrano nella categoria degli Automated Incident Response e Network Investigation tools. Senza voler menzionare alcun vendor, ci limiteremo a evidenziare la necessità di queste tecnologie, unitamente a quelle di analisi dei log, tutte finalizzate ad integrare le soluzioni di IDS/IPS e SIM/SEIM, le quali non consentono, al momento, di gestire l'approfondimento così come richiesto dal management.

Abbiamo parlato poc'anzi di log analysis. Si tratta di un mercato in continua crescita, con molti player che cercano di superare le barriere di ingresso con espedienti più o meno validi. Il consiglio in questo caso è quello comunque di affidarsi ad una consulenza per la scelta architetture, tecnologica e, soprattutto, progettuale. Ciò si rivela decisamente importante per valutare l'opportunità o meno di affidarsi ad un'architettura agent based, di per sé decisamente potente ma che richiede un attento studio di fattibilità.

Quali tecnologie hanno deluso le aspettative?

È opinione di chi scrive che, come detto poc'anzi, la gestione dello Spam sia ancora da migliorare, sia dal punto di vista dell'offerta sia da quello implementativo. Quest'ultimo fattore, forse, riveste un'importanza finanziaria superiore. Un vendor che propone una soluzione potenzialmente vincente corre il rischio di ottenere l'effetto contrario in caso di un'implementazione fatta da un partner non all'altezza. Questo i vendor lo sanno e, consequenzialmente, anche il Cliente inizia a chiedere maggiori garanzie in tal senso.

Un altro fuoco di paglia, almeno per la parte IT security, è dato dalla biometria.

Sicuramente utile per applicazioni di sicurezza nazionale, identificazione dei cittadini e mode “sexy” per l'accesso a token o personal computers e workstations, la biometria non ha raggiunto la diffusione desiderata nelle applicazioni di massa, che poi erano quelle annunciate ormai un quinquennio or sono come risolutive.

Ma allora cosa succederà?

Sicuramente aumenteranno gli incidenti o, perlomeno, aumenterà la presa di nozione di questi, ed aumenterà il bisogno di limitare le fuoriuscite di dati sensibili e riservati dal presidio aziendale. Questo potrà essere limitato da un'accorta scelta in DLP (Data Loss Prevention) ma anche in questo caso, pur in presenza di una scelta tecnologica efficace, sarà l'aspetto implementativo e progettuale a fare la differenza. Dal punto di vista strategico, quindi, si prevede una sempre maggior attenzione alle problematiche organizzative e alla loro mappatura sulle tecnologie disponibili. Più fonti, tuttavia, prevedono un pericoloso trend decisionale sulle tecnologie (da parte dei clienti finali) basato principalmente sul fattore economico. Questo è di base un errore molto grave, che, si spera, sia limitato ad interlocutori di tipo tattico, che forse sarebbe ora trattassero il problema in maniera differente ma che, allo stesso tempo, corrono il rischio di aumentare il livello di esposizione delle loro aziende, causato da valutazioni evidentemente errate. Una cosa è certa: vince chi fa della sicurezza un valore strategico.