Sicurezza nel 2011: le aree di focalizzazione secondo IBM

In attesa dei risultati del report annuale IBM X-Force 2010, relativo ai principali trend e rischi per la sicurezza, IBM anticipa quali saranno le aree di maggiore attenzione di cui le aziende dovranno tener conto nel 2011.
In un contesto in cui quotidianamente si assiste alla comparsa e all'adozione di nuove tecnologie e nuovi modelli di business, l'ambito di riferimento per la sicurezza aziendale dovrà necessariamente allargarsi: la sicurezza degli end-point verrà ridefinita, andando oltre i personal computer e i portatili per coprire aree emergenti quali il mobile computing, le infrastrutture critiche, il cloud computing, i social network.

Inoltre affinchè le organizzazioni possano gestire in modo efficace e completo i rischi della sicurezza, la security dovrà spostarsi sempre di più dalla semplice protezione degli asset alla protezione dei servizi critici: dovrà cioè essere incorporata nel tessuto dell'infrastruttura di un'organizzazione, ovvero concepita 'by design', e guardare con maggiore attenzione verso i temi della conformità, della sicurezza "interna", della privacy e della gestione delle identità.

Qui di seguito una sintesi delle principali tendenze:

- **La sicurezza di dispositivi mobili e di altri smartphone diventerà una priorità**, dato che un numero sempre maggiore di dipendenti cerca di accedere alle reti aziendali con i propri dispositivi mobili. Considerando i dati sensibili memorizzati su questi dispositivi e la facilità con la quale tali dispositivi possono essere persi o rubati, le aziende si troveranno a dover adottare misure per fronteggiare i rischi di sicurezza associati a questi eventi.

- **Gli attacchi alle infrastrutture critiche**, come le reti elettriche e i sistemi idrici, **saranno i bersagli principali per i cybercriminali** alla ricerca di un forte impatto con il minimo sforzo. Dato che il panorama delle minacce diventa sempre più sofisticato, i cybercriminali non cercano solo di attaccare i dati o di rubarli, ma puntano sempre più alle infrastrutture critiche. Le infrastrutture critiche gestite dalle amministrazioni pubbliche, dai settori energia, sanità, banche, trasporti e altri si stanno rapidamente trasformando in sistemi più intelligenti ed interconnessi, ma anche più vulnerabili rispetto al crimine informatico. Per questo prevediamo un aumento degli investimenti da parte dei settori pubblico e privato per combattere tali minacce e salvaguardare i cittadini.

- **La sicurezza** non sarà più un inibitore, ma **diventerà un elemento di abilitazione all'adozione di tecnologie innovative quali il cloud computing, i social network e la virtualizzazione**. Molte organizzazioni preferiranno adottare soluzioni personalizzate per la sicurezza del cloud, che vadano a proteggere in particolare i carichi di lavoro gestiti sul cloud, così come i meccanismi ed i controlli che si intendono utilizzare.

- **Le amministrazioni pubbliche daranno sempre maggiore enfasi alla compliance**, creando nuove complessità per le aziende. Dato che le pubbliche amministrazioni di tutto il mondo adottano legislazioni sempre più rigorose per garantire la sicurezza e la protezione delle infrastrutture critiche, trovarsi al vertice dei cambiamenti nel panorama della conformità sarà la priorità principale per le organizzazioni che vogliano fare business in altri paesi. Se, ad esempio, una banca globale vuole operare in uno specifico paese o mercato, dovrà attenersi agli obblighi relativi alla conformità di quella regione. In caso contrario, rischia di perdere la possibilità di fare affari in quel mercato.

- Per quanto riguarda le minacce alla sicurezza, **le aziende porranno una rinnovata attenzione all'interno dell'organizzazione**. Infatti le minacce interne – anche se spesso involontarie – continueranno ad aumentare: tra l'aumento dei dispositivi mobili e degli smart phone che accedono alle reti e quello dei dipendenti che inavvertitamente cadono prede dei cyber-criminali mentre si trovano collegati alla rete aziendale, le organizzazioni dovranno cercare nuovi modi per garantire che le proprie risorse non vengano compromesse da minacce interne.

- **Il 2011 sarà l'anno in cui le organizzazioni agiranno in modo proattivo per disegnare e sviluppare applicazioni**, servizi e sistemi con la sicurezza prevista 'by design' e non aggiunta successivamente. Fissare la sicurezza a posteriori porterà solo rischi e costi più elevati che le aziende non possono più permettersi. Non si tratta di una nuova idea o di un nuovo concetto. Tuttavia, dato che il mondo è sempre più interconnesso, tecnologico e intelligente, i clienti adotteranno misure sempre più proattive per garantire la sicurezza della loro infrastruttura fin dalle primissime fasi di realizzazione. Constatiamo inoltre che i professionisti della sicurezza informatica sono sempre più allineati con i responsabili delle linee di business, contribuendo all'integrazione della sicurezza nell'intero ciclo di vita dei prodotti e dei servizi IT e garantendo una progettazione di software sicuro fin dall'inizio.

Il team IBM X-Force è la principale organizzazione di ricerca sulla sicurezza di IBM che ha catalogato, analizzato e cercato più di 50.000 vulnerabilità dal 1997. Il report IBM X-Force Trend and Risk riunisce dati provenienti da numerose fonti di informazioni, tra cui il proprio database comprendente più di 50.000 vulnerabilità sulla sicurezza informatica, milioni di eventi di intrusione monitorati su decine di migliaia di sensori di rete gestiti ed installati sulle reti dei clienti IBM di tutto il mondo, il suo "crawler" web globale e i suoi "spam collector" internazionali. **Il rapporto semestrale di X-Force rappresenta l'analisi più completa del settore sulle vulnerabilità** e viene utilizzato per aiutare i clienti ad essere costantemente aggiornati sulle minacce.

IBM Security Solutions comprende un vasto portafoglio di soluzioni hardware e software, offerte di servizi professionali e gestiti che coprono tutta la gamma dei rischi informatici e di sicurezza aziendale, tra i quali quelli relativi alle persone, alle identità, ai dati e alle informazioni, alle applicazioni e ai processi, alle reti, ai server ed endpoint e alle infrastrutture fisiche.

Per ulteriori informazioni visitate i siti
www.ibm.com/services/it/security
e www.ibm.com/software/it/tivoli/solutions/threat-mitigation