



La scarsa **SICUREZZA** delle **AZIENDE** italiane

Negli ultimi anni abbiamo parlato spesso delle crescenti esigenze di sicurezza IT delle aziende e organizzazioni, sottoposte a tipologie di rischi e attacchi sempre più vari e pericolosi. Ma a quanto pare un conto sono le necessità teoriche, un conto è la dura realtà. Questo almeno è quanto si deduce da un'indagine su 200 responsabili IT aziendali italiani realizzata dal fornitore specializzato Horus Informatica, secondo la quale il livello di sicurezza IT delle aziende non sembra adeguato alle effettive necessità.

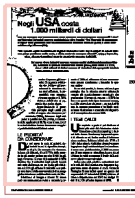
UNA SITUAZIONE PREOCCUPANTE

Nell'indagine, il 70% delle aziende dichiara che è il budget limitato a non permettere di implementare una protezione IT idonea, e il 48% sostiene che sia la limitata cultura IT a non permettere di effettuare le scelte migliori. Seguono poi mancanza di personale IT specializzato (25%) e di un'infrastruttura IT idonea (15%), il che fa pensare a una necessità diffusa di affidare a operatori specializzati la gestione di questi aspetti.

Il livello di cultura IT in azienda è ritenuto scarso o sufficiente nel 73% dei casi andando a impedire uno sfruttamento ottimale

Una ricerca traccia un quadro preoccupante per le poche risorse e la bassa cultura IT, soprattutto riguardo ai rischi legati alle tecnologie innovative come mobile, cloud, virtualizzazione e Web 2.0





Negli **USA** costa **1.000 miliardi** di dollari

Se i top manager non sono coinvolti nelle decisioni sulle strategie di sicurezza IT i risultati finanziari aziendali corrono seri rischi. Lo dice l'analisi 'The Financial Management of Cyber Risk' promossa dall'American National Standard Institute (ANSI) e dalla Internet Security Alliance (ISA).

"Con questo report mandiamo un segnale di allerta a tutti i top manager: la scarsa sicurezza è un problema molto serio, e vi sta costando un sacco di soldi", spiega Karen Hughes, director homeland security standards program dell'ANSI.

Nel report viene infatti citata una recente analisi dell'Amministrazione Obama, secondo la quale le aziende USA hanno perso, tra il 2008 e il 2009, circa 1.000 miliardi di dollari a causa di violazioni della proprietà intellettuale dovuti a cyberattacchi.

anche di quanto già investito. Il rapporto evidenzia che laddove gli investimenti in sicurezza siano stati effettuati, le potenzialità non vengono sfruttate appieno: il 50% dichiara infatti che si potrebbe fare molto di più.

Approfondendo la gerarchia percepita degli ambiti più critici si scopre che sicurezza perimetrale (45%), sicurezza degli endpoint e perdita dei dati (44%), e controllo delle applicazioni (41%) sono le aree in cui le aziende italiane hanno riscontrato maggiori problematiche nell'ultimo anno.

LE PRIORITA' DA CONSIDERARE

Da qui nasce la scala di priorità degli ambiti in cui si dovrebbe investire di più. Un esempio è la sicurezza in base alle identità, di cui il 77% delle aziende ha già sentito parlare ma solo il 40% ha già implementato. In tema di funzionalità il 38% dichiara che il controllo degli accessi basato sul ruolo dell'utente sia tra quelle più richieste, e il 32% gli affianca il controllo con policy user-based delle conversazioni di messaggistica istantanea e del trasferimento dei file.

Mancanza di budget e cultura IT fanno però scontrare ancora realtà e necessità por-

tando il 76% ad affermare di non essere ancora pronto attualmente a investire in questo ambito.

In termini pratici, la ricerca evidenzia per esempio che le aziende stanno adottando sempre più massicciamente tecnologie che permettono il lavoro da remoto - il 55% ha fino a un quarto della forza lavoro sul campo, e il 22% arriva fino alla metà -, ma poi il 60% non ha nessuna protezione o un livello molto basso di sicurezza e controllo dei dispositivi di memorizzazione removibili.

I TEMI CALDI

Un capitolo a parte è poi dedicato ai temi più caldi del momento: virtualizzazione e cloud computing. I risultati della ricerca forniscono importanti spunti di riflessione sul livello medio di informazione e cultura. Sebbene infatti solo il 7% e il 16% delle aziende indichino rispettivamente la gestione degli ambienti cloud e virtualizzati come aree problematiche, il 34% ammette poi di non sapere se virtualizzazione e cloud abbiano in realtà aumentato il livello delle minacce alla sicurezza aziendale.

Infine una nota positiva: nonostante tutto la crisi del 2009 sembra aver impattato leggermente meno di quanto si creda. Secondo l'indagine Horus infatti quasi un quarto dei responsabili IT intervistati (22%) dichiara di avere a disposizione nel 2010 un budget IT dal 10 al 30% più alto rispetto al 2009. ■

© clabert - Fotolia.com

biz

29