Cinque suggerimenti per assicurare la sicurezza dei dati

Gli attacchi alla sicurezza aziendale si fanno sempre più frequenti: nel solo 2014, oltre 500 milioni di identità in tutto il mondo sono cadute nelle mani della criminalità informatica, mentre le infezioni di malware sono troppo frequenti per poterle contare.
Nel tentativo di affrontare questi problemi, qual è l'approccio migliore? I cinque suggerimenti che seguono possono rappresentare una buona indicazione.

1 FARE DELLA SICUREZZA UNO STRUMENTO DI INNOVAZIONE

Una solida strategia di sicurezza può fare molto più che proteggere un'azienda dagli attacchi, può anche accelerare l'adozione di nuove tecnologie migliorando l'efficienza e la produttività. Quando si adottano nuove soluzioni o tecnologie, la valutazione del rischio connesso dovrebbe essere eseguita sistematicamente come parte del processo per assicurarne la protezione. Integrare la sicurezza offre alle aziende maggiore protezione, consentendo di innovare ulteriormente.

2 ESSERE PREPARATI

Un errore che le aziende fanno spesso è di dare per scontato che implementare misure di sicurezza sia una procedura da effettuare una tantum, mentre in realtà si tratta di un processo in costante evoluzione che prevede controlli regolari sulla vulnerabilità della rete. Per quanto ci si possa tutelare, gli incidenti legati alla sicurezza avvengono, ed è il modo in cui sono gestiti a fare la differenza. Se è presente un piano di azione contingente, è possibile recuperare l'operatività in tempi brevi. Identificare in anticipo le minacce ridurrà sensibilmente i tempi di recupero e i costi associati a un'eventuale violazione della sicurezza.

3 ANDARE OLTRE LA NORMA DI LEGGE

Molte aziende sono convinte che per essere protette dagli attacchi cibernetici sia sufficiente ottemperare alle leggi che regolamentano la privacy, la contabilità e la tutela dei consumatori.
Tuttavia questo atteggiamento limita la portata e l'efficacia di una buona policy di sicurezza, poiché la compliance si riferisce normalmente a minacce specifiche. Alla luce di questo, un'efficace policy di sicurezza deve basarsi su altri presupposti, spaziando dalla salvaguardia delle informazioni alla riduzione delle minacce.

4 RESPONSABILIZZARE GLI INDIVIDUI

Le organizzazioni dovrebbero individuare i singoli responsabili del rispetto delle policy di sicurezza. Le responsabilità specifiche dovrebbero essere mappate, assieme a una visione chiara dei confini di ciascuna. Questo dovrebbe essere documentato e condiviso in tutta l'azienda e dovrebbe includere momenti di formazione del personale, in modo da informare ognuno delle proprie responsabilità in termini di sicurezza dei dati.

5 LA SICUREZZA COME ASPETTO STRATEGICO

Considerato che i dati e le informazioni sono alla base del patrimonio aziendale, non ci si può permettere di ignorare la sicurezza.
Senza una policy precisa, sia l'azienda sia i clienti sono a rischio. Comprendere le potenziali minacce e vulnerabilità, creare un piano che tenga conto degli obiettivi strategici dell'azienda, e assicurarsi che la protezione sia integrata nell'infrastruttura informatica consentono alle aziende di trasformare la sicurezza da voce di costo a elemento strategico nella gestione dell'azienda.
www.checkpoint.com ■

MARCO COPPOLINO

Responsabile tecnico – Consys.it