PuntoSicuro

ARTICOLO DI PUNTOSICURO

Anno 20 - numero 4176 di Mercoledì 14 febbraio 2018

I rischi informatici e il profilo dell'attaccante

Qualunque responsabile della sicurezza informatica e della protezione dei dati personali sa benissimo che il primo passo, per mettere in sicurezza sistemi informativi e dati, è quello di condurre una accurata analisi di rischio.

L'analisi dei gli ultimi dati disponibili, in materia di violazione dei dati, mette in evidenza come soggetti interni all'organizzazione siano sempre più spesso responsabili, sia tramite attività criminali, come ad esempio furto di dati, sia come attività non deliberate, come un comportamento negligente da parte di dipendenti e collaboratori.

Anche se i titoli più roboanti dei mezzi di comunicazione di massa fanno riferimento alla violazione di sistemi impenetrabili, da parte di squadre di attaccanti dotate di conoscenze e tecnologie, la realtà è che il modo più frequente con cui gli hackers riescono introdursi nei sistemi informativi è legato all'attività dei dipendenti.

Un recente rapporto sulla sicurezza informatica da un quadro assai demoralizzante, circa la attuale gravità della situazione.

I ricercatori hanno trovato che i dipendenti, soprattutto operanti nei settori pubblici, ritengono che i loro colleghi siano le minacce maggiori alla sicurezza informatica. Il questionario, che è stato sottoposto, ha dato una risposta in questo senso pari al 100% delle risposte!

Fortunatamente, alcune aziende, che si stanno concentrando sugli aspetti di sicurezza, hanno cominciato ad analizzare più attentamente questa situazione e sembra che un maggior numero di aziende investirà, nel 2018, in tecnologie che permettano di identificare potenziali scenari di rischio provenienti dall'interno.

D'altro canto, questa situazione si confronta con quella legata ad un continuo aumento del carico di lavoro dei dipendenti, il 57% dei quali ha dichiarato, nella ricerca sopra illustrata, che essi non hanno tempo sufficiente per attuare misure di sicurezza più incisive, mentre il 54% ha fatto riferimento ad un budget insufficiente.

Un altro aspetto che il responsabile della sicurezza aziendale deve tenere presente è legato al fatto che il costo di messa sotto controllo di violazioni di sicurezza, provenienti dall'interno, è estremamente elevato.

Il 53% delle aziende interessati ha valutato in 100.000 $ e più il costo dell'intervento correttivo, mentre il 12% ha situato questo intervento a più di 1 milione di dollari.

Ecco quindi quali sono i passi che ogni azienda dovrebbe attuare per mettere sotto controllo i rischi provenienti dall'interno:

- effettuare controlli sul profilo personale dei dipendenti,
- tenere sotto controllo il comportamento dei dipendenti,
- adottare sempre il principio di minimizzazione delle autorizzazioni all'accesso ai dati,
- utilizzare procedure efficaci di controllo accesso
- monitoraggio delle nazioni dell'utente,
- educazione permanente di tutti i dipendenti.

Ancora una volta, il fatto che la violazione abbia origine criminale od origine accidentale spesso poco a che fare con il danno conseguente.

Ecco perché è molto meglio investire fin dall'inizio in appropriate misure di sicurezza, piuttosto che fronteggiare costi e sanzioni assai gravi, soprattutto se la violazione dei dati fa riferimento a dati personali.

Adalberto Biasiotti

www.puntosicuro.it