Scritto da Administrator
Martedì 13 Settembre 2016 16:35

Dai dettagli delle carte di credito dei clienti alle informazioni sui dipendenti, le aziende di oggi si basano su dati sensibili, che rappresentano la linfa vitale delle moderne organizzazioni di qualsiasi dimensione, sia pubbliche che private. La perdita di dati e le violazioni sono all'ordine del giorno, ma ci sono ancora molte idee sbagliate su come e perché succedono. Se è vero che nell'immaginario comune il pericolo di perdita dei dati è legato ad ambientazioni hollywoodiane in cui gli attacchi informatici vengono sferrati da minacciosi hacker che operano da stanze da letto buie e tenebrose, la realtà è che la perdita di dati spesso è il risultato di uno sfortunato incidente o di una falla strutturale all'interno dell'azienda. Può dipendere da qualsiasi cosa, da un errore umano a da una "errata interpretazione" delle regole impostate nella rete aziendale.

{loadposition user7}

Perdita di dati e violazione dei dati – qual è la differenza?

Viste le enormi differenze in questo tipo di incidenti, possiamo dividerli in due gruppi separati: violazioni dei dati e perdite dei dati.

In una violazione dei dati, i criminali hanno di solito bisogno di accedere a un server attraverso una vulnerabilità, o attraverso un tipo di attacco che potrebbe essere prevenuto adottando le giuste misure di sicurezza sul posto.In una perdita di dati è possibile che non ci siano falledi sicurezza evidenti ma che i dati si trovinonelle mani sbagliate per alcune azioni irresponsabili avvenute internamente all'azienda, o per esempio, a causa delle azioni dannose di un dipendente scontento .

La differenza tra “perdita” e “violazione” dei dati non è universale. La maggior parte degli esperti potrebbe classificare tutti questi tipi di perdita di dati come violazioni; in fin dei conti, entrambe le opzioni possono danneggiare la vostra azienda. Ma separandole è più facile analizzarne i problemi e capire al meglio come si verificano questi incidenti.

Così quando parliamo di perdita di dati, quali sono i punti deboli che dobbiamo prendere in considerazione?

1. Errore umano

Nonostante gli investimenti fatti in una soluzione di sicurezza, l'errore umano è una di quelle cose che non potrete mai spiegare – almeno non del tutto. Secondo il 2015 Information Security Breaches Survey di PCW, il 50% delle peggiori violazioni dello scorso anno è stato causato da un errore umano involontario.

Solo pochi mesi fa, per esempio, il Federal Deposit Insurance Corp. ha subito le conseguenze di un episodio in cui un dipendente si è allontanato dagli ufficicon un disco USB che conteneva i dati personali di 44,000 clienti. Successivamente si è stabilito che i dati erano stati scaricati “inavvertitamente e senza intenti malevoli”.

Il famoso detto dice, “errare è umano,” ma questo non significa che non sia possibile prevenire queste perdite di dati. Secondo il sondaggio 2015 di PWC il 33% delle grandi aziende afferma che la responsabilità sulla protezione dei dati non è chiara mentre il 72% delle aziende, dove i criteri di sicurezza non sono stati compresi correttamente, ha subito perdite di dati riconducibili al personale.

Assicurarsi che tutti i dipendenti abbiano una “consapevolezza informatica” e che la responsabilità della protezione delle reti non è solo appannaggio di pochi specialisti, ridurrà sensibilmente costosi errori.

2. Furto

Sfortunatamente a volte i furti avvengono anche dall'interno; ne è un esempio quanto è accaduto nel Regno Unito, doveOFCOM, l'autorità competente e regolatrice indipendente per le società di comunicazione, è venuto a conoscenza di un ex dipendente che ha raccolto dati di terze parti a scopo di lucro per un periodo di oltre sei anni.Il fatto è venuto a galla soltantoquando l'ex dipendente ha tentato di passare questi dati ai nuovi datori di lavoro, che hanno avvisato OFCOM di queste criminose attività.

A nessuna azienda piace trattare i propri dipendenti con sospetto, ma questo tipo di perdite di dati può essere prevenuto evitando inutili rischi. Quando sono coinvolti dei documenti sensibili, per esempio, assicuratevidi garantirne l'accesso soltanto a chi ne ha veramente necessità. Registrare tutti i dati dell'azienda in un unico gigantesco e comune server non è mai una buona idea.

3. Uso non corretto

Anche quando le intenzioni dei dipendenti non sono malevole, le loro azioni minori possono ledere la sicurezza IT della rete e portare a perdite di dati.

Secondo un rapporto di Cisco del 2014 , approssimativamente un quarto dei dipendenti intervistati ha ammesso di condividere informazioni riservate con amici, parenti o persino sconosciuti, e circa la metà dei dipendenti intervistati ha condiviso i dispositivi di lavoro con persone al di fuori dell'azienda senza supervisione.

Questi comportamenti potrebbero sembrare piuttosto “innocenti”, ma portano i dati sensibili dell'azienda fuori dal suo controllo. Le impostazioni e le procedure di sicurezza possono essere introdotte per limitare questo tipo di attività, ma persino questo tipi di misure possono essere superate.

Ora che abbiamo identificato i tre principali punti deboli per la perdita di dati, probabilmente vi state chiedendo come rinforzarli? Consultate questo recente post, Digital patch kit: come

proteggersi dalle perdite di dati
, per avere delle indicazioni pratiche su tutte le necessità della vostra azienda.

Fonte: ESET

{jcomments on}

{loadposition user6}