

Come causare la perdita di dati sensibili in azienda...

Da tempo si ritiene che i danni peggiori in azienda possano essere arrecati da 'insider attack', ma reali policy efficaci a 360 gradi per contrastare il fenomeno non sono ancora state adottate.

Un'azienda può acquistare i migliori software di sicurezza conosciuti, ma questo non serve a nulla se gli utenti finali non vengono formati correttamente sul loro ruolo. La consapevolezza degli utenti risulta fondamentale per mantenere i dati sensibili al sicuro.

La Data Loss Prevention (Dlp) è innanzitutto un processo, la tecnologia è solo un fattore abilitante per l'automazione. Il processo deve includere la formazione e lo sviluppo della consapevolezza, coprendo aree come le risorse umane, la gestione dei dati e la conformità dei dati. L'obiettivo è quindi quello di istruire con continuità i data owners e chi li custodisce in merito alle policy utili a ridurre i casi di non conformità.

Di seguito sono elencati i modi in cui i dipendenti, maliziosamente o inconsapevolmente, possono perdere dati sensibili, e come un sistema Dlp possa fare la differenza.

Utilizzo non appropriato dell'e-mail. Gli amministratori It hanno in questi anni avuto successo nel rilevare e bloccare le e-mails malevoli in ingresso, ma gli utenti possono sempre inviare dati sensibili fuori dai confini aziendali, nonostante ci siano filtri 'umani' o quarantene. Se ad esempio i dati sono presenti in documenti che vengono sì verificati, ma non nella loro totalità, e se contengono informazioni su clienti o dettagli sulla proprietà intellettuale? Per i messaggi in arrivo, i vari filtri non sono in grado di fermare ogni tentativo di phishing. Alcuni link verso siti maligni possono ancora transitare, e basta un click dato da un utente poco accorto per infettare, con un malware, tutta una rete aziendale.

Warning dell'instant messaging. Alcuni programmi di instant messaging sono diventate applicazioni di routine per addetti sempre più mobili. Il personale in mobilità fa spesso ricorso a questi sw per comunicare da remoto con i responsabili o con i colleghi. Gli hackers hanno trovato il modo di inviare link e allegati dannosi per gli utenti, attraverso la creazione di account fraudolenti che assomigliano a messaggi legittimi da parte di colleghi. Quello che è peggio è che certi sw di Im possono essere scaricati gratuitamente e, una volta installati, sfuggire al controllo dei dipartimenti It aziendali. Come per le e-mail, le policy aziendali dovranno essere chiare in merito alle informazioni che non possono o possono essere inviate via i sistemi di Im.

Social Networking. Mentre si lotta contro la vulnerabilità di e-mail o Im, gli hackers stanno estendendo il loro campo d'azione ai siti di social networking come Facebook, MySpace, Twitter, ecc. Recentemente si è scoperto che questi siti possono essere utilizzati per attacchi analoghi a quelli via e-mail o Im. In Facebook è noto come le caselle possono essere piene di ogni cosa, da inviti all'aperitivo del giovedì sera ad appelli per aderire a cause civili, ecc. Per gli utenti del social network, cliccare sui link è come respirare. I malintenzionati lo sanno bene, e per questo inviano inviti analoghi a quelli di amici. Aprendo il link si consente al sw malevolo di infettare il proprio Pc.

Password. Altro annoso problema, che i malintenzionati continuano a ben utilizzare. L'utilizzo crescente di pwd per ogni genere di sistema, come ad esempio e-mails, banking online, ecc., dal momento che non tutti hanno una memo-

ria da elefante, porta molti utenti ad utilizzare per molti, se non tutti gli applicativi, la stessa password. Questo è come fidarsi che l'anello debole di una catena sopporti ugualmente un peso. Ogni sito ha le sue vulnerabilità ed è bene aspettarsi che prima o poi vengano utilizzate da menti malevole. Una policy che gestisca gli utenti dovrebbe spiegare e definire molto bene cosa fare, ad es. utilizzare password diverse a dipendenza degli accessi, ecc.

Access rights estesi. Altro problema ricorrente. Spesso al personale viene consentito l'accesso a più applicazioni aziendali, maggiori rispetto a quelle di cui si ha effettivamente bisogno nel lavoro quotidiano. Se un impiegato scontento dell'azienda, con eccessivi diritti di accesso, entra in possesso di dati sensibili dell'azienda la fritata è fatta, con la possibilità di mettere l'azienda in grave difficoltà, anche se solo di immagine. Una corretta policy nel dare cosa a chi serve veramente potrebbe mitigare qualche futuro problema.

Conclusione. Questi sono solo piccoli esempi che però danno un'immagine di come la sicurezza, ventilata o sventolata, a livello aziendale, a volte possa essere messa in pericolo. Da tempo si ritiene che l'insicurezza o comunque i danni peggiori possano essere arrecati da 'insider attack', ma reali policy efficaci a 360 gradi non sono state ancora adottate, o meglio ogni azienda spera che quanto fa possa essere sufficiente... Come diceva un vecchio refrain, "meditate gente (responsabili sicurezza It), meditate".

Renato Giovanelli
Ated-Ict Ticino
www.ated.ch