La protezione dei dati a prova di cybercrime

Data: 3 luglio 2013 | Autore: Rosangela Muscetta

ROMA, 07 MARZO 2013 - Soprattutto a livello aziendale, vi sono pericoli relativi alla gestione dei flussi informativi, caratterizzati spesso da una loro cattiva gestione, che minacciano quotidianamente la competitività aziendale, richiedendo policy opportune per arginarne i rischi e gli eventuali danni ad essi connessi.
Quello del cybercrime, invece, inteso come insieme di organizzazioni e attività finalizzate a realizzare profitti attraverso attacchi informatici, è un mondo variegato che può colpire tutti: dagli utenti privati alle imprese e tra le stesse imprese, non solo banche e infrastrutture critiche del Paese (come telecomunicazioni, sanità, trasporti, etc.), ma anche quelle aziende che possono rappresentare un hub per una grandissima quantità di informazioni atta a essere monetizzata nonché le piccole realtà imprenditoriali magari all'avanguardia in qualche nicchia di mercato.[MORE]

Ma per essere ben costruiti, gli attacchi informatici spesso richiedono uno studio preliminare del bersaglio. In tal senso, i social network rappresentano l'ultima frontiera per recuperare una serie di dati e attuare attacchi di successo. Accedendo a "Linkedin" o "Twitter", per esempio, si riesce a selezionare uno specifico individuo, che ricopre un ruolo in una qualche organizzazione d'interesse, ricostruire le sue relazioni professionali o private, intuire facilmente il suo indirizzo di posta elettronica aziendale e inviargli una mail di phishing fortemente mirata, magari col nome di un amico e facendo riferimento a una conversazione avvenuta sui social.
Difficile sospettare e sottrarsi a questo tipo di attacco estremamente contestualizzato e, una volta

infettata la postazione, l'attaccante ha sotto il suo controllo una parte all'interno del perimetro aziendale.
L'obiettivo non solo è quello di trovare una via di accesso ai conti bancari dell'azienda che tradizionalmente sono più consistenti dei conti privati, ma anche trafugare informazioni di business o segreti industriali da rivendere, causare malfunzionamenti o disservizi o ricattare l'azienda, minacciando malfunzionamenti o disservizi.

Le aziende, ovviamente, si preoccupano di proteggersi, dando per scontato che l'interno sia invulnerabile. Invece è fondamentale segmentare le reti proprio all'interno, profilandone i diversi livelli di accesso, in modo da proteggere al meglio il patrimonio di dati aziendali; ed è comunque necessario predisporre a guardia della rete delle sonde che, in caso di attacchi rilevati, siano in grado di disconnettere il sistema o, qualora si voglia perseguire un approccio più morbido per non interrompere il business, siano in grado di dare l'allarme.
Infine, perché questi accorgimenti tecnologici siano efficaci, è essenziale un monitoraggio costante degli eventi che permetta di rilevare eventuali anomalie, come traffici sospetti e inusuali da postazioni utenti verso i server, abuso di determinati protocolli, tentativi ripetuti di autenticazione ai sistemi provenienti da postazioni utente, tentativi a tappeto di scansioni verso i servizi esposti su determinati sistemi.
Da non sottovalutare il tema della consapevolizzazione degli utenti, che non vuol dire vietare ai propri dipendenti o collaboratori di fare determinate cose, come a esempio, accedere alla propria posta personale dal Pc dell'ufficio, bensì indirizzare le persone verso una serie di comportamenti esemplari e prudenti che aiutino a preservare o, quanto meno, a non compromettere la sicurezza aziendale.

Rosangela Muscetta [http://www.economia-conoscenza-itc-km.blogspot.it]