Attenzione SU...

IL WEB È DIVENTATO UN LUOGO PERICOLOSO? POSSIAMO DIFENDERCI!

Siamo completamenti immersi nel Web, che coinvolge ogni momento della nostra vita sia personale che professionale. Internet è diventata il motore della "quarta rivoluzione industriale" (nota anche come "Industry 4.0"), generando opportunità di crescita e sviluppo impensabili fino a pochi decenni fa. Inevitabilmente il business creato dalla rete non poteva non avere - come in tutte le attività umane - qualche "effetto collaterale" negativo. Stiamo parlando evidentemente del Cybercrime che in questi ultimi anni ha assunto dimensioni impressionanti.

Pochi ma significativi dati possono illustrare questa affermazione:
• nel solo 2015 sono andati persi nel mondo 445 miliardi di dollari per salvaguardare la proprietà intellettuale, per i lavori bruciati e per il tempo speso a rimediare i danni del crimine informatico. Il 97% delle 500 imprese più ricche del mondo secondo Fortune hanno subito almeno un attacco informatico (cit. Peter Warren Singer);
• il peso del Cybercrime nell'economia mondiale è stimato in 650 miliardi di dollari nel 2016. Gli analisti prevedono che tale valore arriverà a 1.000 miliardi di dollari nel 2020.

I molti rischi per le Imprese che svolgono attività commerciali con l'estero

Sarebbe impossibile in questa sede elencare le numerose minacce portate dal Cybercrime alle imprese, anche perché ogni giorno viene inventata una nuova modalità di attacco, da parte di hackers sempre più organizzati. I grandi guadagni sommati al bassissimo rischio di essere scoperti hanno fatto crescere in modo esponenziale l'esercito dei cybercriminali.
Vogliamo qui porre l'attenzione su una truffa informatica che sta colpendo sempre più pesantemente le imprese che praticano import/export.
È la truffa definita "The Man in the Mail", nota anche come BEC (Business Email Compromise). È basata sul "phishing" (attacco portato con l'uso delle email). Il metodo è tanto semplice quanto efficace: i delinquenti intercettano la posta elettronica di un'azienda, ne spiano le comunicazioni, la carta intestata, le firme dei responsabili, lo stile della corrispondenza. Dopo questa fase di "studio", i cybercriminali sono in grado di inserirsi nello scambio di email in corso tra cliente e fornitore, inviando fatture ed email false con le quali riescono a dirottare i pagamenti del cliente su un conto diverso da quello del fornitore: il conto appositamente predisposto da loro!
La Polizia Postale segnala che nella Regione Emilia Romagna questa truffa è quella che negli ultimi mesi sta procurando i danni maggiori a molte imprese: si parla di perdite in denaro, per bonifici inviati sul conto "sbagliato", di decine ed anche centinaia di migliaia di euro per azienda. Proprio in Romagna si è registrato qualche mese fa il caso più eclatante: quasi un milione di euro, che la malcapitata azienda ben difficilmente riuscirà a recuperare, sebbene siano in corso indagini e collaborazioni con la banca - ovviamente estera - coinvolta (incolpevolmente) nella truffa.
Come difendersi? In questo caso ben poco possono fare i tradizionali strumenti software di sicurezza informatica: la truffa utilizza il meccanismo sempre convincente del "social engineering" (sfruttare cioè le debolezze delle persone per carpire la loro buona fede). L'unica vera, efficace difesa è la CONSAPEVOLEZZA dei rischi, l'attenzione ai dettagli (sempre in queste email di phishing c'è qualche indizio che dovrebbe farci nascere sospetti). Purtroppo la scarsa conoscenza informatica dei dipendenti rende fin troppo facile il lavoro dei cybercriminali. Per questo diventa sempre più importante curare la formazione all'interno delle imprese, un investimento fortemente sottovalutato ma che potrebbe rendere più sicura la nostra vita nel Web.

Giorgio Sbaraglia