

Social Engineering: (un nuovo metodo d'attacco orientato contro le imprese)

23.01.2017

A colpo d'occhio

Negli ultimi giorni la centrale d'annuncio e d'analisi per la sicurezza dell'informazione MELANI ha ricevuto numerose segnalazioni di casi di truffe telefoniche ai danni di imprese svizzere. I criminali si spacciano per la banca della ditta, sostenendo di dover effettuare un update del sistema e-banking il giorno successivo. Fissano così un appuntamento per il quale richiedono la presenza di tutti i collaboratori del settore finanza. Ciò allo scopo di risolvere il problema del principale elemento di sicurezza, la firma collettiva e, in ultima analisi, di effettuare il pagamento fraudolento.

In questi ultimi giorni si è osservato un aumento di telefonate verso imprese, potenziali vitti-me, durante le quali un truffatore si fa passare per il collaboratore di una banca. In molti casi le informazioni inerenti la banca presso cui è cliente la ditta presa di mira, sono reperibili sul-la pagina web di quest'ultima, sotto forma di coordinate bancarie. In alternativa queste informazioni possono venir appurate precedentemente tramite chiamate telefoniche o richieste via e-mail.

Per proteggersi da attacchi del genere, MELANI consiglia le misure seguenti:

- In quest'ambito è raccomandabile un'adeguata sensibilizzazione dei collaboratori, in particolare di quelli che occupano posizioni chiave.
- Tutti i processi riguardanti il traffico dei pagamenti devono essere chiaramente disciplinati all'interno dell'azienda e in ogni caso devono essere sempre rispettati dai collaboratori. Gli istituti finanziari non vi richiederanno né telefonicamente né per iscritto di comunicare i vostri dati d'accesso e-Banking.
- Nessuna banca seria vi chiederà di partecipare a test per un qualsivoglia update di sicurezza. Le banche, rispettivamente i gestori di servizio a cui esse si affidano, dispongono di speciali sistemi di controllo, per analizzare gli update di sicurezza prima che questi diventino visibili ai clienti.
- Non installate mai dei software se vi viene imposto telefonicamente o per iscritto.
- Non permettete a nessun estraneo l'accesso al vostro computer.
- Riducete le informazioni inerenti la vostra ditta pubblicate in Internet a ciò che è strettamente necessario. Se possibile evitate di rivelare i nomi dei vostri collaboratori così come indicazioni sulle coordinate bancarie.
- In caso di presa di contatto sospetta o insolita non rivelate alcuna informazione interna.
- In caso di contatto o richiesta insolita è consigliabile consultarsi all'interno dell'azienda per verificare la veridicità del mandato.
- Se siete vittima di una truffa, annunciate il caso a l'ufficio federale di polizia fedpol tramite l'apposito formulario effettuate una denuncia alla Polizia Cantonale.

Per la sicurezza IT delle PMI, MELANI ha pubblicato un [documento](#) di istruzione.