Pagamenti elettronici, qual è il livello di sicurezza attuale?

In questi giorni di fervide trattative per il varo della legge finanziaria, i pagamenti elettronici sono sotto i riflettori degli organi di informazione e all'attenzione della classe politica e dei cittadini come mai avvenuto in precedenza.

E' opportuno ricordare scenari di minacce informatiche che possono inficiare il valore assicurato dall'impiego del servizio di pagamento elettronico, come il caso relativo alle carte *contactless* (senza contatto) e *mobile wallet* (portafoglio mobile)

Nuove vulnerabilità offrono agli hacker la possibilità di aggirare i limiti di pagamento sulle carte contactless **Visa** indipendentemente dal terminale della carta, secondo una ricerca di **Positive Technologies** (Visa card vulnerability can bypass contactless limits.)

In un comunicato stampa del 29 luglio, Positive Technologies ha affermato che i ricercatori hanno testato più volte i difetti con cinque principali banche del Regno Unito e con carte e terminali al di fuori del Regno Unito. Hanno scoperto che i limiti potevano essere aggirati il □□100% delle volte e potevano consentire a un attaccante di rubare dai conti.

Scenario di attacco

L'attacco funziona manipolando due campi di dati che vengono scambiati tra la carta e il terminale durante un pagamento

contactless. Soprattutto nel Regno Unito, se il pagamento necessita di un'ulteriore verifica del titolare della carta (che è richiesta per pagamenti superiori a 30 sterline nel Regno Unito), le carte risponderanno "Non posso farlo", il che impedisce di effettuare pagamenti oltre questo limite. *In secondo luogo, il terminale utilizza impostazioni specifiche del paese, che richiedono che la carta o il portafoglio mobile forniscano un ulteriore verifica del titolare della carta, ad esempio inserendo il PIN della carta o l'autenticazione tramite impronta digitale sul telefono*", si legge nel comunicato stampa.

I controlli sono stati aggirati utilizzando un dispositivo che fungeva da proxy per intercettare la comunicazione tra il terminale di pagamento e la carta, un attacco noto come man in the middle (MITM). Questi attacchi MITM possono anche essere eseguiti utilizzando i portafogli mobili, consentendo a un truffatore di caricare fino a £ 30 senza sbloccare il telefono.

La sicurezza dei pagamenti elettronici

Secondo il comunicato "*Il dispositivo dice alla carta che la verifica non è necessaria, anche se l'importo è superiore a £ 30. Il dispositivo quindi comunica al terminale che la verifica è già stata effettuata con altri mezzi. Questo attacco è possibile perché Visa non richiede che gli emittenti e gli acquirenti dispongano di controlli che blocchino i pagamenti senza presentare la verifica minima*".

"L'industria dei pagamenti ritiene che i pagamenti contactless siano protetti dalle garanzie che hanno messo in atto, ma il fatto è che le frodi sono in aumento. Sebbene si tratti di un tipo di frode relativamente nuovo e al momento potrebbe non essere la priorità numero uno per le banche, se i limiti di verifica senza contatto possono essere facilmente aggirati,

ciò significa che potremmo vedere perdite più dannose per le banche e i loro clienti.”, secondo il comunicato.

Salvaguardia e raccomandazioni

I ricercatori Positive Technologies suggeriscono che gli utenti di carte contacless devono essere vigili nel monitorare i loro estratti conto bancari per rilevare tempestivamente le frodi e, se disponibili con la propria banca, implementare ulteriori misure di sicurezza come limiti di verifica dei pagamenti e notifiche via SMS.

https://www.key4biz.it/pagamenti-elettronici-qual-e-il-livello-di-sicurezza-attuale/276177/