

Internet Bankingul — cel mai expus canal de distribuție (I)

Internetul este în criză, securitatea lui nu și-o mai poate asuma nimeni. O luptă de gherilă se instaurează încet încet. Riscurile de securitate se mută cât mai aproape de noi. Dacă înaintea vorbeam de atacurile de phishing, în care eram îndemnați să ne introducem datele confidențiale pe un server plasat undeva în lumea largă, în prezent **atacatorii sunt pe calculatorul nostru.**

Omul rău, sub forma sa virtuală, se regăsește în atacurile de Man-in-the-middle și Man-in-the-browser.

Să luăm **exemplul aplicațiilor de Internet Banking ale băncilor.** Pentru autentificare și autorizare se foloseau token-uri care îți generau o secvență unică, pe care o introduceai. Aceste tokenuri foloseau tehnologia Challenge-Response și One-time-password (OTP). Păreau sigure și dădeau încredere că nimic rău nu se mai poate întâmpla. Și așa a și fost pentru multă vreme (doar 2 ani!). În prezent, atacatorul este infiltrat în browser, se află între client și bancă. Vechile tokenuri foloseau pentru autentificare acea secvență unică, folosibilă și pentru autorizarea tranzacției. Prin introducerea secvenței și captarea ei de către atacator, în prezent se poate opera succesiv și o altă tranzacție nedorită de client. Majoritatea token-urilor au un timp de așteptare de până la 30 secunde, perfect suficient pentru o operațiune fraudată.

Din fericire, au apărut și **tehnologiile**

de contracarare. Tokenurile moderne fac saltul în domeniul semnăturilor dinamice și al separării domeniilor. Astfel, autentificarea este o operațiune separată de aceea de autorizare a tranzacției. Iar, pentru valori mai mari, secvența de autentificare este calculată direct în funcție de suma tranzacționată și chiar de numărul contului sau alte elemente suplimentare de autentificare. Separarea de domeniu este foarte importantă, deoarece protejează crescător clientul, în funcție de tipul și valoarea operațiunii.

Noile soluții permit utilizarea lor inclusiv **pentru operațiunile comerciale pe Internet**, pentru achizițiile de pe Internet. Astfel, **o soluție de securitate poate deveni pentru prima dată și un factor generator de business.** Deci, investiția nu mai trebuie privită doar ca salvare a banilor dintr-o pierdere potențială, un cost de oportunitate, ci ca fiind generatoare de profit, prin implementarea unor soluții inovative, bazate pe aceste tehnologii. Același token poate avea, în cadrul unui domeniu separat, o secvență de autorizare diferită, și opțiunea de comerț electronic. Multe magazine virtuale sunt conectate la gateway-urile băncilor pentru conectarea la operatorii de carduri (gen VISA sau Mastercard). Clienții băncii pot avea opțiunea de a efectua operațiuni sigure la aceste magazine virtuale.

În plus, aceste noi tehnologii au un **sistem de autentificare inexpugnabil** (încă...) prin sistemele de securitate ale cardurilor cu chip, în special standardele CAP, EMV, 3DES. Practic, informația personală, cre-

dențialele principale sunt securizate în cadrul chipului de pe carduri. Normal, mai avem separat și PIN-ul personal în cadrul autentificării cu mai multe elemente. Noile tokenuri prezintă o fantă specială de inserare a cardului bancar cu chip, prin care practic tokenul nu mai este personalizat de loc, totul depinzând de ce e înmagazinat pe chip-ul cardului. Dacă se fură cardul și se găsește un token în care să utilizezi cardul, tot mai trebuie cunoscute PIN-ul și user-name-ul de acces la sistem. Practic, în noul context, phishingul devine un atac învechit, fără nici un rost. Atacatorului îi trebuie nu numai datele de autentificare ci și cardul și terminalul fizic.

Probabil phishing-erul va continua, pentru a obține datele de pe cardul bancar și PIN-ul acestuia, pentru a face operațiuni pe Internet, dar nu va mai afecta de loc soluții de Internet Banking.

Din această cauză, **chiar și phishingul se modifică, evoluează.** Nu știu dacă ați auzit de **Vhishing în loc de Phishing.**

Ce este Vhishingul? Un phishing pentru Voice-over-IP (VoIP). Se manifestă mai nou la atacurile peste Skype, în care tu crezi că suni la un număr al cuiva cunoscut, de exemplu call-center-ul de la bancă, dar la celălalt capăt nu răspunde exact persoana așteptată, nu răspunde operatorul de la call-center-ul băncii ci al atacatorului, căruia, cu nonșalanță, îi dai datele proprii de autentificare pentru o operațiune telefonică. Nici o problemă, operațiunea se va efectua, dar în contul atacatorului...

■ DR. CĂLIN RANGU
CEO IIRUC SERVICE