PERICOLUL DE LÂNGĂ NOI, LIPSA SECURITĂȚII IT (III)

Riscurile de securitate se mută cât mai aproape de noi. Dacă înainte vorbeam de atacurile de phishing, în care eram îndemnați să ne introducem datele confidențiale pe un server plasat în lumea largă, în prezent atacatorii sunt pe calculatorul nostru.

Călin M. RANGU,
vicepreşedinte CEO,
IIRUC Service

Omul rău, sub forma sa virtuală, se regăseşte în atacurile de *Man-in-the-middle* şi *Man-in-the-browser*.

Să luăm exemplul aplicațiilor de internet banking ale băncilor. Pentru autentificare şi autorizare se foloseau tokenuri care îți generau o secvență unică pe care o introduceai. Aceste tokenuri foloseau tehnologia Challenge-Response şi One-Time-Password (OTP). Păreau sigure şi dădeau încredere că nimic rău nu se mai poate întâmpla. Şi aşa a fost pentru multă vreme (dacă 2 ani pot însemna prea mult). În prezent, atacatorul este infiltrat în browser, se află între client şi bancă. Vechile tokenuri foloseau pentru autentificare acea secvență unică, care putea fi folosită şi pentru autorizarea tranzacției. Prin introducerea secvenței şi captarea ei de către atacator, în prezent se poate opera imediat şi o tranzacție nedorită de client. Majoritatea tokenurilor au un timp de aşteptare de până la 30 de secunde, suficient pentru o operațiune.

Din fericire, au apărut şi tehnologiile de contracarare. Tokenurile moderne fac saltul în domeniul semnăturilor dinamice şi al separării domeniilor. Astfel, autentificarea este o operațiune separată de cea de autorizare a unei tranzacții. Iar pentru valorile mai mari, secvența de autentificare este calculată direct în funcție de suma tranzacționată şi chiar numărul contului sau alte elemente suplimentare de autentificare. Separarea de domeniu este foarte importantă, deoarece protejează crescător clientul în funcție de tipul şi 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 şi un factor generator de business. Deci investiția nu mai trebuie privită doar ca salvarea banilor dintr-o pierdere potențială, un cost de oportunitate, ci ca generatoare de profit prin implementarea unor soluții inovative, bazate pe aceste tehnologii. Acelaşi token poate avea, în cadrul unui domeniu separat, o secvență de autorizare diferită şi 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 încă inexpugnabil prin sistemele de securitate ale cardurilor cu chip, în special standardele CAP, EMV, 3DES. Practic, informația personală, credențialele principale, sunt securizate în cadrul cipului de pe carduri. Normal, mai avem separat şi PIN-ul personal în cadrul autentificării cu mai multe elemente. Noile tokenuri prezintă o fantă specială de inserare a cardului bancar cu cip, prin care, practic, tokenul nu mai este personalizat deloc, totul depinzând de ceea ce e înmagazinat pe cipul cardului. Dacă se fură cardul şi se găseşte un token în care să utilizezi cardul, tot mai trebuie cunoscute PIN-ul şi username-ul de acces în sistem. În noul context, phishingul devine un atac învechit, fără rost. Atacatorului îi trebuie nu numai datele de autentificare, ci şi cardul şi terminalul fizic.

Probabil phishingul va continua pentru a obține datele de pe cardul bancar şi PIN-ul acestuia, pentru a face operațiuni pe internet, dar nu va mai afecta deloc soluții de internet banking.

Din această cauză chiar şi phisingul se modifică. Nu ştiu dacă ați auzit de Vhishing în loc de Phishing. Ce este Vhsihingul? Un phishing pentru Voice-over-IP (VoIP), despre care vom vorbi în edițiile viitoare. Acesta se manifestă, mai nou, la atacurile peste Skype, în care utilizatorul este convins că sună la un număr cunoscut (de exemplu, call-centerul băncii), dar la celălalt capăt nu răspunde persoana aşteptată, ci call-centerul atacatorului, căruia, cu nonşalanță, victima îi poate da datele proprii de autentificare pentru o operațiune telefonică. Evident, operațiunea se va efectua, dar în contul atacatorului.