Proiect la informatica

Tema: ,,Securitatea platilor pe internet’’

Realizat de Margarint Nicoleta si Chitaica Loredana

Clasa Xll-a ,,C’’

1. Amenintarile ce pot apare in timpul unei plati

Malware (prescurtarea de la "malicious software" în limba engleză) este un termen generic şi se referă la orice software rău-intenţionat (maliţios) care a fost creat cu scopul de a rula în mod neautorizat şi ascuns faţă de utilizatorul computerului.

Înregistratoarele de taste, **keyloggers** în limba engleză, sunt programe destinate înregistrării tastelor apăsate decătre utilizator şi folosite pentru a obţine informaţii sensibile ca parole, coduri PIN, numere de carduri. Aceste programe rulează în background şi sunt invizibile.

2. Tipuri de atacuri

Un atac de tip **“drive-by-download”** se referă la descărcarea ne-intentionata (fără ştiinţa utilizatorului) şi fără ca acesta să observe, pe un computer sau terminalul mobil, a unor programe maliţioase.

Un atac de tip **“man-in-the-middle”** (omul de la mijloc), este un atac sofisticat în care atacatorul se interpune ca “stație de transit” în comunicația dintre două sisteme. Atacatorul controlează toată conversatia, fiind capabil să intercepteze si modifice mesajele schimbate de cele două parti. Folosind un astfel de atac atacatorul ar putea modifica date ale unor tranzactii financiare.

Un atac de tip **“man-in-the-browser”** este un tip de atac “man-in-the-middle” prin care un troian (program malitios prezentat ca un program legitm) infectează un browser web folosindu-se de vulnerabilitătile de securitate ale browser-ului. Atacatorul modifică pagini web, elemente ale unei tranzactii sau chiar întreaga tranzactie, toate aceste actiuni având loc “în background”, fără ca utilizatorul să observe.

3. Procese prin care se realizeaza activitati criminale in sistmele informatice

În domeniul informatic, **phishing** (eng) reprezintă o formă de activitate criminală care constă în obtinerea datelor confidentiale, cum ar fi credentialele de acces (username,

parola, PIN, OTP) pentru aplicatii financiare sau informatii referitoare la cardul de credit, folosind tehnici de manipulare a identitãtii unei persoane sau a unei institutii.

Un atac de tip phishing constã în trimiterea de cãtre atacator a unui mesaj electronic, folosind programe de mesagerie instantã (e-mail) – **PHISHING**, sau telefon (SMS) - **SMSishing**, în care utilizatorul este sfãtuit sã introducã credentialele de access (nume utilizator, parola), numere de card, coduri PIN.

Un exemplu de phishing: primiţi un email în care aţi fost informat că aţi câşitgat o excursie în străinătate iar tot ce trebuie să faceţi pentru a primi voucherul de călătorie este să introduceţi (pe un site asemenator cu cel al băncii) următoarele informaţii pentru a confirma identitata: numele, adresa şi datele cardului dvs.

Exemplu de smsihing: primiţi un mesaj SMS de la un număr necunoscut care pretinde a fi banca dvs. şi care va invită să descărcaţi o nouă versiune a aplicaţiei de mobile banking.

Vishing este un termen care provine din termenii voice și phishing și reprezintă o formă de inșălatorie prin care utilizatorul este păcălit să furnizeze informaţii sensibile, credenţialele de acces, numere de card, sau coduri de acces.

4. Pentru efectuarea unei tranzactii online sau unei plati, va recomanda sa:

- nu efectuaţi tranzacţii decât pe platformele cunoscute de intermedieri online;
- verificaţi cu atenţie reputaţia cumpărătorului şi ce tranzacţii a efectuat în trecut (atunci când este posibil);
- comunicaţi cu partenerul de afaceri şi pe alte canale nu doar pe email (ex. telefon, video-call);
- verificaţi cu atenţie termenii şi condiţiile platformei care intermediază vânzarea;
- vă informaţi cu privire la riscurile care pot apărea în urma unei astfel de tranzacţii;

De asemenea, vă încurajăm ca în situația în care considerați că ați fost victima unei astfel de tentative de înșelătorie să înștiințați cât mai rapid organele de poliție locale.

5. Dispozitivile folosite de dvs. pentru efectuarea tranzactiilor electronice reprezintã elemente importante ce trebuie securizate. Adesea prin compromiterea lor, atacatorii reusesc sã desfãsoare tranzactii frauduloase si sã obtinã câstiguri materiale (în defavoarea dumneavoastrã). Va recomandam urmatoarele masuri:

Calculator	Tableta/ smartphone
Instalaţi pe calculatorul dumneavoastră numai aplicaţii cu licenţă validă şi care provin din surse sigure;	Protejaţi accesul la smartphone-ul sau tableta dumneavoastră folosind una din opţiunile de securitate disponibile (PIN, parola, sau “semn grafic”);
Instalati o solutie de securitate ce oferã cel putin protectie anti-virus;	Actualizaţi sistemul de operare de pe smartphone-ul sau tableta dumneavoastră (Android, iOS, Windows);
Nu conectati dispozitive necunoscute la calculatorul dumneavoastrã (de ex. stick-uri USB gãsite în locuri publice);	Instalaţi aplicaţii (Apps) doar din magazinele de aplicaţii oficiale (Google Play, Apple App Store, Microsoft Store);
Dezactivaţi conexiunile de reţea pe care nu le utilizaţi, opţiunile wireless – WiFi, Bluetooth;	Efectuati copii de sigurantã pentru datele dvs. (backups) în mod periodic;
Nu uitati sã efectuati copii de sigurantã pentru datele dvs. pe un suport extern (backups) în mod periodic;	Dezactivati optiunile de conectivitate (Wi-Fi, Bluetooth, NFC, etc) pe care nu le utilizati în mod curent
Nu folosiţi alte computere care nu vă aparţin (la Internet Café, hotel, aeroport sau la “prieteni”) atunci când faceţi tranzacţii bancare.	

6. Amenintari privind utilizarea serviciilor de plata pe internet

- Nu este recomandat sã accesati site-ul de Internet Banking al bãncii dintr-un link primit pe email sau SMS. Linkurile primite pe email vă pot redirecţiona către un site fals controlat de atacator. Acesta vă poate păcăli să introduceţi credenţialele de acces pe acest site fals controlat de atacatori.

- Verificati cu atentie dacã atunci când desfãsurati operatiuni financiare conexiunea utilizatã este una securizatã (https://).
- Dezactivati salvarea parolelor (în special salvarea automatã a acestora) în browser;
- Credenţialele de acces (utilizator, parola, cod acces, etc) sunt informaţii personale şi nu trebuie comunicate altor persoane. NU notaţi pe foi hârtie sau în fişiere text nesecurizate aceste informaţii .
- este recomandat că parola să fie schimbată periodic. De asemenea este foarte important să nu folositi aceeasi parola pentru mai multe servicii (ex. cont email, cont internet banking, cont reţea socializare, etc).

Banciile NU apelează (telefonic, email sau SMS) la clienţii săi pentru a cere informaţii precum: CNP, număr card, PIN, ID logare, parola sau orice alte informaţii personale.