# Vulnerabilitati si contramasuri

Lumea in care traim este intr-un continu proces de dezvoltare privind domeniul tehnologiei informatiei si al calculatoarelor. Pe zi ce trece apar tot mai multe aplicatii si servicii menite sa ne usureze modul de a trai si de a face sa ne simtim cat mai confortabil folosindu-le. Un exemplu bun poate fi plata facturilor online deoarece timpul necesar indepliniri acestei actiuni este unul foarte mic precum si a faptului ca nu este nevoie sa ne deplasam mai mult de cativa metri pentru a face asta. Totusi, confortul si rapiditatea indepliniri a unor astfel de sarcini vine cu multe riscuri deoarece putem cadea usor in plasa atacurilor cibernetice. Plecand de la premiza ca sistemele software sunt scrise de oameni , unii dintre ei bine pregatiti iar altii mai putin pregatiti, ajungem la concluzia ca nimic nu este sigur in aceasta lume a internetului si ca orice aplicatie sau platforma web are vulnerabilitati care pot fi exploatate de indivizi a caror intentie este sa castige bani sau sa-si arate capacitatile intelectuale.

Noua, utilizatorililor unor astfel de aplicatii, ne sunt deseori oferite multe optiuni de a ne proteja mai bine conturile de utilizator, precum si datele personale sau informatii care tin de intimitatea noastra impotriva atacurilor hackerilor. Totusi, rareori utilizatori detin informatii despre faptul ca-si pot proteja mai bine datele personale si de aici rezulta de ce atat de multi oamneni cad in plasa furtului de date, bani, etc.

In continuarea acestui eseu va voi povesti cat de usor de spart era contul de facebook pe care il detin de catre cineva care nu poseda cunostiinte avansate in domeniul securitatii.

Eu si un bun prieten de-al meu stam impreuna si butonam telefoanele. Faptul ca eu stam pe Facebook i-a starnit prietenului meu curiozitatea de a incerca sa-mi acceseze contul. Eu eram sigur ca asa ceva este imposibil deoarece singurul mod de a face asta era sa-mi reseteze parola si asta nu se putea intampla pentru ca ar fi trebuit sa imi stie parola la adresa de email ori sa aiba acces la telefonul mobil pentru a face schimbarea parolei prin trimitere de SMS ori sa stie raspunsul la intrebarile personale care imi fusesera puse cand imi creasem contul, intrebari menite sa ma ajute sa resetez parola in cazul in care o uitasem, putand introduce o noua parola in cazul in care raspunsurile la intrebari coincideau cu cele originale.

Deoarece la logarea pe orice platforma din zilele noastre apare si un link cu “Forget your password?” acesta a fost primul pas facut de prietenul meu. Dupa asta, utilizatorul este redirectionat catre o pagina unde poate alege mai multe optiuni de resetare a parolei. Optiunea folosita de prietenul meu se referera la resetarea parolei dand raspunsuri corecte la intrebarile personale la care raspunsesem cand facusem “Sign Up”. Avand in vedere ca era un prieten apropiat, a stiut raspunsurile la intrebari si a reusit “sa puna stapanire” pe contul meu. Eram socat cu cata usurinta facuse acest lucru si cat de putine masuri luasem pentru a-mi proteja informatiile personale.

Dupa acel incident m-am informat cum sa previn alte incidente de acel gen si am gasit cateva informatii foarte utile. Una din informatii a fost autentificarea in mai multi pasi. Presupunad ca cel care ar dori sa intre pe contul meu stie parola, acesta nu se poate loga cu success pana nu introduce un al doilea cod care este generat la fiecare minut si se care se poate gasi doar in cazul in care sunt deja logat pe reteaua de socialiare. O a doua masura a fost activarea notificarilor telefonice prin SMS ori de cate ori cineva incearca sa se conecteze la contul meu de pe un dispozitiv strain. In cazul acesta as sti daca cineva s-a logat si as lua rapid contramasurile necesare inlaturari posibilei amenintari.