Robert Similea

Conștientizarea riscurilor și tipologia amenințărilor cibernetice

Masterclass

Tech Ac@demy

Investește în viitorul tău.
Digitalizarea nu mai este doar o opțiune!

UNIUNEA EUROPEANĂ

Instrumente Structurale 2014-2020

europroject
Centrul de Consultanță și Management al Proiectelor EUROPROJECT

Tehnologia deschide un întreg univers de noi oportunități. Noi produse și servicii devin tot mai populare și ajung să formeze o parte integrantă din viața noastră de zi cu zi. Cu fiecare nouă evoluție, crește însă și dependența noastră tehnologică, ceea ce înseamnă că securitatea cibernetică devine tot mai importantă.

Cu cât postăm mai multe date personale online și cu cât suntem mai conectați, cu atât suntem mai expuși riscului de a fi victime ale diferitor forme de criminalitate informatică sau de atac cibernetic.

Comoditatea râvnită a tranzacțiilor digitale care este adusa în viață noastră de dispozitive digitale, unele chiar extrem de mici pe care le porți la încheietura mâinii sau în buzunar, deschide o lume de posibilități: puteți să cumpărați un bilet de avion sau să chemați o mașină Uber, puteți să monitorizați casa sau afacerea, să solicitatați un împrumut, să vizualizați soldurile contului sau să plătiți facturile la fel de ușor cum puteți să participați la întâlniri de afaceri de acasă, trimiteți email, utilizați smartphone-ul pentru a plăti o cafea sau pentru a comanda produse alimentare, haine sau o mașină, fără a părăsi canapeaua.

Este greu să ne imaginăm un aspect al vieții noastre personale și profesionale care nu a fost redefinit prin comoditatea digitală.

Canalele digitale sunt un element indispensabil în toate industriile în timp ce clienții se adresează cu precadere întreprinderilor care pot oferi această viteză și comoditate.

Cu fiecare nouă evoluție, crește însă și dependența noastră tehnologică, ceea ce înseamnă că securitatea cibernetică devine tot mai importantă din cauză că relativul anonimat al canalelor digitale deschide noi uși pentru fraudă.

Cetățenii sunt adesea vectori ai atacurilor și vectori de răspândire a dezinformării, fiind probabil ca aceștia să fie expuși fără voia lor la vulnerabilități ale unor dispozitive și programe informatice ieftine și distribuite pe scară largă sau să devină victime ale tehnicilor de inginerie socială.

În ultimii ani, întrucât spațiul cibernetic a devenit din ce în ce mai militarizat și este transformat pe zi ce trece într-o armă, acesta a ajuns să fie considerat al cincilea câmp de luptă (celelalte 4 sunt terestru, maritim, aerian, cosmic).

Apărarea cibernetică protejează sistemele, rețelele și infrastructurile critice din spațiul cibernetic împotriva atacurilor militare și de alt tip.

Frauda cibernetică este o afacere înfloritoare din mai multe motive:

- Au avut loc mai multe deschideri de cont prin dispozitive digitale și internet care asigură accesul și anonimatul criminalilor cibernetici. Potrivit companiei de strategie și cercetare Javelin, aproximativ 80% dintre clienții adulți ai băncilor din SUA folosesc activități bancare online și mobile frecvent, un public țintă mare și unul vulnerabil totodata.
- Volume uriase de date de toate tipurile (inclusive date de identitate - caracter personal) sunt colectate, manipulate si stocate pe internet. Scurgerile de date personale s-au inmultit ceea ce produce un potop de informații, o mare parte dintre ele putandu-se obține cu relative ușurință de pe rețeaua întunecată (dark web).
- Piratii cibernetici fură, prelucreaza si tranzacționează date de identitate nu doar pentru a face bani dar și pentru a construi o imagine falsificata cat mai completă și convingătoare a identităților utilizatorului furat.

Frauda cibernetică este o afacere înfloritoare din mai multe motive:

- Oamenii difuzează în mod involuntar fragmente sau bucati ale identitatii lor pentru a completa diverse formulare, pentru a descarca aplicatii sau resurse gratuite, cupoane de reduceri etc. În septembrie 2018, Facebook a raportat o bresa de securitate care a afectat aproape 50 de milioane de conturi, ceea ce ar putea oferi atacatorilor acces pentru a vizualiza informațiile despre cont și pentru a utiliza conturile ca pe ale lor.
- Automatizarea scalează frauda la noi niveluri din cauza ca robotii (bot-ii) automati au accelerat viteza și volumul activității frauduloase. Atacurile automatizate pot compromite mai multe conturi și pot fura mai multe date în mai puțin timp, ceea ce duce la mai multă expunere pentru mai multe canale, servicii și companii.

Creșterea gradului de conștientizare este așadar esențială pentru construirea unei rezilience cibernetice eficace, însă nu este în niciun caz o sarcină simplă, deoarece este greu pentru nespecialiști să înțeleagă complexitatea securității cibernetice și riscurile asociate.

Cu toate acestea consumatorii nu se așteaptă ca fraudele și măsurile luate de companii pentru a combate criminalitatea cibernetică să interfereze cu experiența lor online, așa că presiunea cade astfel cu și mai multă putere asupra întreprinderilor pentru a se asigura că nu pun în pericol încrederea clienților în procesul de combatere a criminalității cibernetice si de prindere a infractorilor.

Clienții se simt frustrați când trebuie să străbată prin protocoale de verificare pentru a se autentifica sau pentru a finaliza o tranzacție și dovedesc o răbdare foarte scăzută pentru procesele de autentificare și verificare: nu doresc autentificări laborioase și cu mai multe niveluri, nu vor să răspundă la mai multe întrebări de autentificare sau chestionare pentru a demonstra că nu sunt roboți. Consumatorii doresc autentificare mai inteligentă dar nu mai multa autentificare.

Instituțiile financiare trebuie să poată verifica identitatea utilizatorului fara a compromite rapiditatea și ușurința tranzacției pentru clienții buni. Întotdeauna este nevoie să echilibreze securitatea ridicată - ceea ce poate însemna o durată mai mare, întârziere și o anumită latență - cu nevoia pentru a oferi o experiență pozitivă pentru clienți.

Triada CIA

Confidențialitatea

Integritatea

Disponibilitatea

CIA **este un model conceput pentru a ghida companiile și organizațiile să își formeze politicile de securitate. Tehnic, securitatea cibernetică înseamnă protejarea informațiilor împotriva accesului neautorizat, modificarea neautorizată și ștergerea neautorizată pentru a oferi confidențialitate, integritate și disponibilitate.**

- ***Confidențialitatea*** **se referă la prevenirea dezvăluirii datelor către părți neautorizate. Înseamnă, de asemenea, încercarea de a păstra identitatea părților autorizate implicate în distribuirea și păstrarea datelor private și anonime. Adesea, confidențialitatea este compromisă prin crăparea de date slab criptate, atacuri Man-in-the-middle (MITM), dezvăluind date sensibile.**

- **Măsurile standard pentru stabilirea confidențialității includ:**

  - **Criptarea datelor**
  - **Autentificare cu doi factori**
  - **Verificare biometrică**
  - **Jetoane de securitate**

Integritatea **se referă la protejarea informațiilor împotriva modificărilor de către părți neautorizate. Este o cerință ca informațiile și programele să fie schimbate numai într-o manieră specificată și autorizată. Printre provocările care ar putea pune în pericol integritatea se numără transformarea unei mașini într-un „computer zombie", integrarea malware în paginile web.**

Măsurile standard pentru a garanta integritatea includ:

- **Sume criptografice**
- **Utilizarea permisiunilor de fișiere**
- **Surse de alimentare neîntrerupte**
- **Copii de rezervă pentru date**

Disponibilitatea **se asigură că părțile autorizate pot accesa informațiile atunci când este nevoie. Datele au valoare numai dacă oamenii potriviți pot accesa la momentul potrivit.** ***Indisponibilitatea*** **informațiilor poate apărea din cauza incidentelor de securitate precum atacuri DDoS, eșecuri hardware, erori de programare, erori umane.**

Măsurile standard pentru a garanta disponibilitatea includ:

- **Backup de date pe unități externe**
- **Implementarea firewall-urilor**
- **Având surse de alimentare cu rezervă**
- **Redundanță de date**

Securitatea cibernetică și *securizarea navigării pe internet*

Securitatea cibernetică implică prevenirea sau detectarea incidentelor cibernetice, răspunsul la acestea și redresarea ulterioară.

Incidentele pot fi provocate intenționat sau nu și acoperă situații foarte diverse, de exemplu de la divulgări accidentale de informații până la atacuri asupra întreprinderilor șia infrastructurilor critice, furtul de date cu caracter personal și chiar ingerințe în procesele democratice. Toate aceste incidente pot avea efecte negative de amploare asupra persoanelor, a organizațiilor și a comunităților.

Ori de câte ori un dispozitiv nou se conectează online sau la alte dispozitive, crește și așa-numita „suprafață de atac" în materie de securitate cibernetică.

Conceptul de securitate cibernetică nu se limitează la securitatea rețelelor și a informațiilor, ci acoperă orice activitate ilegală care implică utilizarea tehnologiilor digitale în spațiul cibernetic. Prin urmare, acest concept poate include infracțiuni informatice precum lansarea de atacuri cu viruși informatici sau fraudele cu mijloace de plată fără numerar și poate viza atât sistemele, cât și conținutul.

<u>În încheiere, câteva sfaturi practice pentru securizarea navigării pe internet</u>

Evită sau refuză să instalezi softuri din inițiativa sau la propunerea unor terți (mai ales dacă sunt necunoscuți).

Urmează Principiul: dacă nu ai căutat un anume program, nu-l instala, dacă nu ai nevoie de anumite programe sau aplicații deja instalate, dezinstaleaza-le!

Ai grijă de datele tale personale!

Nu completa formulare primite via e-mail, prin care ţi se cer date cu caracter personal, parole, coduri secrete sau PIN-uri. Când vine vorba de date sensibile, instituţiile publice, băncile sau marile companii nu solicită să le fie transmise prin banalul e-mail sau, mai rau, prin mesaj SMS. Aşa că, cel mai probabil, acel mesaj prin care ţi se spune că banca ta doreşte să actualizeze datele clienţilor şi are nevoie şi de ale tale, inclusiv numărul cardului bancar, codul PIN şi parola de conectare la contul de Internet Banking... nu este de la bancă!

Indiferent de promisiune, ingineria socială îţi va cere ceva: să deschizi un fişier ataşat în e-mail sau transmis prin Instant Messaging, să urmezi un link, să instalezi un soft, să completezi cu datele tale un formular.

Ferește-te de ***schemele de inginerie socială*** cum ar fi de exemplu, un banner pe un site web unde scrie că este nevoie doar să dai click pe un link dacă vrei să afli cum s-a produs cel mai recent accident aviatic ori să vezi în ce ipostaze incendiare a fost surprinsă o celebritate.

Tot inginerie socială este şi atunci când eşti anunţat că tocmai ai câştigat o suma de bani, o excursie sau o cină romantică, în urma unei trageri la sorţi la care nu îţi aminteşti să te fi înscris, apoi eşti rugat să transmiţi datele personale ori să depui ceva bani într-un cont pentru a intra în posesia premiului. Priveşte cu suspiciune astfel de cereri şi nu te lăsa atras în schemă.

Dezvoltă un algoritm personal și unic pentru a combina aceste caractere astfel încât să poți genera parole puternice și unice, de fiecare dată când creezi un cont nou într-o aplicație.

Parola este un instrument de autentificare folosit pentru a dobândi acces la un echipament şi la datele sale. Pentru protecţia datelor tale, alege parole dificil de identificat de atacator cu ajutorul instrumentelor automatizate („brute force”) sau de ghicit de către acesta. Atacurile urmăresc identificarea parolei şi accesul la informaţia restricţionată prin acea parolă.

Masterclass

Tech Ac@demy

Investește în viitorul tău.
Digitalizarea nu mai este doar o opțiune!

UNIUNEA EUROPEANĂ

GUVERNUL ROMÂNIEI

Instrumente Structurale 2014-2020

europroject
Centrul de Consultanță și Management al Proiectelor EUROPROJECT