CyberSecurity Awareness

Adriana NĂSTASE

Universitatea Româno-Americană, București, România

Abstract

Securitatea cibernetică este un fenomen global care reprezintă o provocare socio-tehnică complexă pentru guverne, dar care necesită implicarea indivizilor. Deși securitatea cibernetică este una dintre cele mai importante provocări cu care se confruntă guvernele astăzi, vizibilitatea și conștientizarea publicului rămân limitate. Aproape toată lumea a auzit de securitate cibernetică,

cu toate acestea, urgența și comportamentul persoanelor nu reflectă un nivel ridicat de conștientizare. Internetul este considerat prea des ca un mediu sigur pentru schimbul de informații, tranzacții și controlul lumii fizice.

Cu toate acestea, războaiele cibernetice sunt deja în desfășurare și este nevoie urgentă de a fi mai bine pregătiți. Incapacitatea de a încadra securitatea cibernetică a dus la eșecul dezvoltării politicilor adecvate. În această lucrare, discutăm provocările în elaborarea politicii privind securitatea cibernetică și oferim strategii pentru o mai bună comunicare a securității cibernetice.

Comunicarea securității cibernetice se confruntă cu paradoxuri, ceea ce a dus la faptul că societatea nu ia măsurile adecvate pentru a face față amenințărilor.

Vizibilitatea limitată, complexitatea socio-tehnologică, impactul ambiguu și natura contestată a combaterii securității cibernetice complică elaborarea politicilor. Încadrarea folosind puncte de vedere utopice sau distopice poate fi contraproductivă și poate duce la neglijarea dovezilor.

Cuvinte cheie: *cybersecurity awareness, safety, security*

Introducere

Securitate cibernetică, un cuvânt care a atras o atenție considerabilă și este considerat drept cel mai utilizat termen în toate domeniile care folosesc internetul. Progresele tehnologice recente au impus necesitatea de a explora diferite aspecte ale securității cibernetice. Cibernetizarea rapidă odată cu introducerea dispozitivelor inteligente a forțat atât organizațiile guvernamentale, cât și cele private să creeze o conștientizare cu privire la amenințările cibernetice și la securitatea cibernetică. Țările dezvoltate, cum ar fi Noua Zeelandă, au fost pioniere în introducerea de noi tehnologii și, în unele cazuri, au fost mandatate legal să implementeze proceduri de securitate cibernetică în diferite sectoare, inclusiv în instituțiile de învățământ.

Deși, necesitatea unor astfel de implementări nu este niciodată pusă la îndoială, totuși, a existat o dezbatere continuă cu privire la cadrul de implementare, în special pentru programele școlare, burse și licență. Importanța conștientizării securității cibernetice este stabilită prin prezentarea diverselor statistici, urmate de implementările actuale pentru conștientizarea securității cibernetice în termeni de cursuri, seminarii etc. Acest articol va contribui la înțelegerea stării de conștientizare a securității cibernetice a utilizatorilor de internet, prin descoperirea metodelor de protejare împotriva atacurilor cibernetice și câte tipuri de atacuri există.

DE CE ESTE IMPORTANTĂ CONȘTIENTIZAREA CIBERNETICĂ?

Securitate: trebuie să ne protejăm computerele și datele în același mod în care asigurăm ușile casei noastre.

SECURITATE CIBERNETICĂ = SIGURANȚĂ

Siguranță: trebuie să ne comportăm în moduri care să ne protejeze împotriva riscurilor și amenințărilor care vin odată cu tehnologia.

CUM AFECTEAZĂ CRIMINALITATEA CIBERNETICĂ ROMÂNIA?

În ultimul deceniu, problema criminalității informatice a apărut din ce în ce mai des în atenția publicului larg astfel că, guvernele din întreaga lume au luat decizia de a înființa organisme specializate pentru a se ocupa în mod special de toate problemele legate de criminalitatea cibernetică. Chiar dacă s-au luat aceste măsuri, gradul de conștientizare a populației în

privința riscurilor cibernetice nu au cunoscut o îmbunătățire semnificativă. De exemplu, pandemia COVID-19 a dus la o deteriorare a condițiilor de muncă, perturbări ale piețelor financiare, accentuând nevoia de lichidare în companii. Escrocherii cibernetice, fraude, dezinformări și alte infracțiuni cu

activități cibernetice reprezintă o zonă în creștere, pe măsură ce persoanele aflate în izolare își petrec mai mult timp în mediul online.

România ocupă locul al doilea în acest top, întrucât 84% dintre români nu au nici o idee despre cum să raporteze o infracțiune cibernetică sau un comportament online ilegal. România fiind în topul celor mai nesigure state din lume în fața atacurilor cibernetice, în condițiile în care pandemia de COVID-19 a determinat o creștere de 1,5 ori a numărului de infracțiuni comparativ cu anii trecuți. Perioadele de criză cum este cea generată de contextul pandemiei COVID-19, creează provocări pentru infractori pentru a găsi noi canale de angajare în infracțiuni. De exemplu, pandemia COVID-19 a dus la o deteriorare a condițiilor de muncă, perturbări ale piețelor financiare, accentuând nevoia de lichidare în companii. Escrocherii cibernetice, fraude, dezinformări și alte infracțiuni cu activități cibernetice reprezintă o zonă în creștere, pe măsură ce persoanele aflate în izolare își petrec mai mult timp în mediul online.

EXPERIMENT

Prin intermediul campaniei, au fost postate mai multe bannere de test cu mesaje de tip phishing pe diferite site-uri pentru a testa ușurința cu care oamenii dau click pe un banner în momentul în care li se propune un câștig sigur. Astfel, în doar 6 zile de campanie, peste 7000 de persoane au dat click pe un banner care le promitea un câștig sigur (55%), câștigarea unor aparate de folosință

îndelungată (38%), investiții sigure (5%) sau o vacanță de vis (2%). Majoritatea celor care au dat click sunt bărbați (60%) cu vârsta între 35-54 ani.

Pentru a ajuta la creșterea gradului de conștientizare a riscului de fraudă online, după accesarea banner-ului de test, cetățenii au fost redirecționați către sigurantaonline.ro unde au fost invitați să completeze un quiz prin care să aprofundeze mai multe sfaturi despre cum să se protejeze online.

Pentru a veni în întâmpinarea nevoii de informare a românilor, Poliția Română, Directoratul Național de Securitate Cibernetică și Asociația Română a Băncilor au lansat campania

#SiguranțaOnline. Concluzie: Peste 7000 de români au căzut pradă “phishing-ului” pus la cale de campania #SiguranțaOnline.

VIRUȘI

Virușii informatici sunt programe software concepute în mod deliberat de atacatorii online pentru a vă invada computerul, pentru a interfera cu funcționarea acestuia și pentru a ne copia, corupe sau șterge datele. Aceste programe software rău intenționate sunt numite viruși, deoarece sunt concepute nu numai pentru a infecta și a deteriora un computer, ci și pentru a se răspândi pe alte computere pe internet.

Virușii informatici sunt adesea ascunși în ceea ce par a fi programe utile sau distractive sau atașamente de e-mail, cum ar fi jocuri pe calculator, clipuri video sau fotografii. Mulți astfel de viruși sunt răspândiți din neatenție de către utilizatorii de computere, care, fără să vrea, îi transmit prin e-mail prietenilor și colegilor.

Caracteristici:

• Un virus se atașează la un program, fișier sau disc;

• Când programul este executat, virusul se activează și se replic;

• Virusul poate fi benign sau malign, dar își execută sarcina utilă la un moment dat (adesea la contact);

• Virușii pot provoca blocări ale computerului și pierderi de date;

• Pentru a recupera sau a preveni atacurile de virus:

- Evitați site-urile web/e-mail-urile potențial nesigure;
- Restaurarea sistemului;
- Reinstalați sistemul de operare;
- Utilizați și întrețineți software antivirus

VIERMI

Viermii sunt viruși mai sofisticați care se pot replica automat și se pot trimite către alte computere, preluând mai întâi controlul asupra anumitor programe software de pe computer, cum ar fi e-mailul.

Caracteristici:

• Program independent care se reproduce și trimite copii de la computer la computer prin conexiuni de rețea;

• La sosire, viermele poate fi activat pentru a se replica

BOMBA LOGICĂ ȘI CALUL TROIAN

Bombă logică este un program malware care distrug datele atunci când sunt îndeplinite anumite condiții. De exemplu, poate formata un hard disk sau poate modifica fișierele de date (eventual prin inserarea de biți aleatori de date) la o anumită dată sau oră sau dacă o anumită înregistrare a angajatului lipsește din baza de date a angajaților. De exemplu: un angajat plasează o bombă logică în interiorul unui sistem pentru a distruge datele atunci când înregistrarea sa este eliminată la încetare.

Un cal troian este un program care pare să facă un lucru, dar de fapt face altul. Un cal troian poate fi folosit pentru a configura ușa din spate într-un sistem informatic, astfel încât intrusul să poată avea acces mai târziu. Numele se referă la calul din războiul troian, cu o funcție similară de a înșela apărătorii pentru a aduce un intrus înăuntru.

INGINERIE SOCIALĂ

Ingineria socială manipulează oamenii să efectueze acțiuni sau să divulge informații confidențiale. Similar unui truc de încredere sau unei simple fraude, termenul se aplică la utilizarea înșelăciunii pentru a obține informații, a comite fraude sau a accesa sisteme informatice.

PHISHING

Phishing-ul este un tip de inginerie socială. Utilizarea de e-mailuri care par să provină dintr-o sursă de încredere pentru a păcăli un utilizator să introducă acreditări valide pe un site web contrafăcut. De obicei, e-mailul și site-ul web par să facă parte dintr-o organizație de încredere cu care utilizatorul este familiarizat. O entitate aparent de încredere solicită informații sensibile, cum ar fi SSN, numere de card de credit, ID-uri de conectare sau parole prin e-mail.

PHARMING

Pharming-ul este un alt tip de inginerie socială. Sesiunea unui utilizator este redirecționată către un site web mascat. Pe site-ul fals, tranzacțiile pot fi imitate și pot fi adunate informații precum acreditările de conectare. Cu aceasta, atacatorul poate accesa site-ul real și poate efectua tranzacții folosind acreditările unui utilizator valid pe acel site. Link-ul furnizat în e-mail duce la o pagină web contrafăcută care colectează informații importante și le transmite proprietarului.

BOTNET

Când computerul este infectat, este probabil să devină un bot. Deoarece atacurile sunt internaționale, ele sunt greu de localizat și de eradicat. O rețea bot este un număr de computere compromise utilizate pentru a crea și trimite spam sau viruși sau pentru a inunda o rețea cu mesaje ca un atac de tip denial of service. Zombie este un computer compromis care poate găzdui muzică ilegală și/sau filme. Botnet este o „armată de zombi" sau o colecție de computere compromise, zombi, folosite pentru a trimite spam, viruși sau atacuri distribuite de denial of service.

MAN IN THE MIDDLE ATTACK

Atacatorii „Man in the middle" pot implementa puncte de acces fără fir captivante lângă cele legitime, dar pretind că sunt legitime. Punctul de acces momeală seamănă cu cel legitim, păcălind utilizatorii involuntari să renunțe la acreditările lor. Un atacator se pretinde a fi destinația ta finală în rețea. Când o persoană încearcă să se conecteze la o anumită destinație, un atacator îl poate induce în eroare către un alt serviciu și poate pretinde că este acel punct de acces la rețea sau server.

ROOTKIT

RootKit-ul este o colecție de programe pe care un hacker le folosește pentru a masca intruziunile și pentru a obține acces la nivel de administrator la un computer sau o rețea de computere.

Caracteristici:

• La pătrunderea într-un computer, un hacker poate instala o colecție de programe, numită rootkit;

• Elimină dovezile de spargere;

• Modifică sistemul de operare

SPARGEREA PAROLEI – DICTIONARY ATTACK ȘI BRUTE FORCE

Pattern	Calculation	Result	Time to Guess ($2.6x10^{18}$ tries/month)
Personal Info: interests, relatives		20	Manual 5 minutes
Social Engineering		1	Manual 2 minutes
American Dictionary		80,000	< 1 second
4 chars: lower case alpha	26^4	$5x10^5$	
8 chars: lower case alpha	26^8	$2x10^{11}$	
8 chars: alpha	52^8	$5x10^{13}$	
8 chars: alphanumeric	62^8	$2x10^{14}$	3.4 min.
8 chars alphanumeric +10	72^8	$7x10^{14}$	12 min.
8 chars: all keyboard	95^8	$7x10^{15}$	2 hours
12 chars: alphanumeric	62^{12}	$3x10^{21}$	96 years
12 chars: alphanumeric + 10	72^{12}	$2x10^{22}$	500 years
12 chars: all keyboard	95^{12}	$5x10^{23}$	

Acest tabel arată diferitele combinații de parole și lungimi de parole și cât timp ar dura un atac de dicționar sau un atac de forță brută pentru a ghici parola. Discuțiile despre crearea corectă a parolelor și tehnicile de schimbare vor avea loc mai târziu în secțiunea Practici utilizator a prezentării. Brute Force Attack este o tehnică de criptoanaliză sau alt tip de metodă de atac care implică o procedură exhaustivă care încearcă toate posibilitățile, una câte una.

Atacul dicționarului este un atac care încearcă toate expresiile sau cuvintele dintr-un dicționar, încercând să spargă o parolă sau o cheie. Un atac de dicționar folosește o listă predefinită de cuvinte în comparație cu un atac cu forță brută care încearcă toate combinațiile posibile.

IDENTIFICAREA COMPROMISURILOR DE SECURITATE

Simptome:

• Software-ul antivirus detectează o problemă;

• Spațiul pe disc dispare în mod neașteptat;

• Apar brusc ferestre pop-up, uneori vânzând software de securitate;

• Apar fișiere sau tranzacții care nu ar trebui să fie acolo;

• Computerul încetinește până la un crawl;

• Mesaje, sunete sau afișări neobișnuite pe monitor;

• Coruperea unui dispozitiv: 1 dispozitiv este corupt la fiecare 53 de secunde; 97% nu și-au revenit niciodată;

• Indicatorul mouse-ului se mișcă singur;

• Computerul se oprește sau repornește spontan;

• Adesea probleme nerecunoscute sau ignorate

DETECTAREA PROGRAMELOR MALWARE

Simptome de spyware:

• Modificări la pagina de pornire a browser-ului;

• Ajungeți pe un site ciudat atunci când efectuați o căutare;

• Firewall-ul bazat pe sistem este dezactivat automat;

• O mulțime de activitate în rețea, deși nu este deosebit de activă;

• Ferestre pop-up excesive;

• Pictograme noi, programe, favorite pe care nu le-ați adăugat;

• Alerte de firewall frecvente despre programe necunoscute atunci când încercați să accesați internetul;

• Performanță slabă a sistemului

Concluzii

Pentru a ne proteja de atacurile cibernetice trebuie să recurgem la următoarele metode:

• Instalarea unui antivirus;

• Utilizarea unor firewall-uri bazate pe gazdă;

• Protejarea sistemului de operare actualizându-l periodic;

• Folosirea de parole puternice;

• Evitarea trucurilor prostești ale hackerilor;

• Copie de rezervă a informațiilor importante

Bibliografie

https://www.slideshare.net

https://www.staysafeonline.org

https://www.tamworth.gov.uk

https://www.mga.edu

https://www.cisa.gov

https://www.wikipedia.com