Siguranța online

*Ne prezentăm, facem o introducere

Securitatea cibernetică este starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive şi reactive prin care se asigură confidenţialitatea, integritatea, disponibilitatea, autenticitatea şi non-repudierea informaţiilor în format electronic, a resurselor şi serviciilor publice sau private, din spaţiul cibernetic. Măsurile proactive şi reactive pot include politici, concepte, standarde şi ghiduri de securitate, managementul riscului, activităţi de instruire şi conştientizare, implementarea de soluţii tehnice de protejare a infrastructurilor cibernetice, managementul identităţii, managementul consecinţelor.

*10 reguli de siguranţă online

1) Primește pemisiunea părinţilor

2) Nu comunica cu necunoscuţi

3) Nu răspunde la asalturile online

4) Nu trimite fotografii personale

5) Nu instala fișiere din surse nesigure

6) Nu instala fișiere din surse nesigure

7) Nu instala fișiere din surse nesigure

8) Folosește parole complicate

9) Învaţă despre riscurile internetului

10) Învaţă despre riscurile internetului

*Hărţuirea pe internet

Hărţuirea, cunoscută drept cyberbullying atunci când are loc pe Internet, implică folosirea tehnologiilor informaţiei şi comunicaţiilor, cum ar fi mail-ul, telefoanele mobile, site-urile web defăimatoare, blog-urile etc., cu scopul de a ataca în mod deliberat, repetat şi ostil, un individ sau un grup de indivizi.

Agresorii cibernetici pot divulga date reale, cu caracter personal, despre victimile lor pe site-uri şi forumuri sau pot publica materiale în numele lor cu scopul de a le defăima şi/sau ridiculiza. De asemenea, unii agresori pot trimite şi e-mail-uri de ameninţare şi hărţuire, în timp ce alţii publică bârfe şi instigă alte persoane la comportamente răutacioase împotriva victimelor.

*Reputaţia online

Ti-ai cautat pana acum numele pe Google? Pentru ca, daca nu, e cazul sa o faci. Verifica atat rezultatele din Search cat si cele din Google Images. Chiar daca ai constiinta curata, este posibil ca problemele legate de reputatia ta sa provina dintr-o coincidenta de nume.

Este deja celebru cazul co-fondatorului BrandYourself.com, Pete Kistler. Prin 2008, acesta a descoperit adevaratul motiv pentru care companiile la care a aplicat nu il cheama nici macar la un interviu. Se pare ca pe Google mai existau o multime de alti Pete Kistler, printre care se numara si un individ suspectat de trafic de droguri. Si aici observam impactul reputatiei potentialilor angajati asupra angajatorilor.

Reputaţia online o creeăm singuri,deci putem să o modelăm după placul nostru

Pasul 1: Analizează-ţi reputaţia actuală

Pasul 2: Identifică punctele slabe

Pasul 3: Identifică punctele tari

Pasul 4: Construieşte-ţi strategia de comunicare online

Pasul 5: Construieşte-ţi reputatia online!

*Cum recunoaştem un calculator virusat

1. “Computerul vorbeste cu mine“ - Apar pe ecran tot felul de ferestre “pop-up” si mesaje publicitare, precizand ca PC-ul este infectat si ca are nevoie de protectie. Acesta este un exemplu tipic de infectare. Este vorba fie de un program spion (“spyware”) in computer sau de o infectare cu un antivirus fals (numit si “rogueware“).

2. “Computerul meu functioneaza extrem de incet“ - Acesta poate fi un simptom pentru multe cauze, inclusiv infectarea cu un virus. In cazul in care s-a produs infectarea cu un virus, vierme sau troian, acestea pot consuma resursele calculatorului, facandu-l sa functioneze mai greu decat de obicei.

3.Computerul are răspunsuri atipice la unele comenzi, refuză să deschidă unele aplicaţii, nu te poţi conecta la internet, se deschid pagini web nesolicitate şi aşa mai departe

4. “Antivirusul meu a disparut, firewall-ul este dezactivat” - O alta actiune tipica a amenintarilor de pe Internet este dezactivarea sistemelor de securitate (antivirus, firewall, etc) instalate pe calculator. Daca un singur program s-ar opri, poate ca ar fi vorba de o eroare de software, dar daca toate componentele de securitate s-ar dezactiva, aveti cu siguranta computerul infectat.

*Protecţia antivirus

Virusul informatic este în general un program care se instalează singur, fără voia utilizatorului, şi poate provoca pagube atât în sistemul de operare cât şi în elementele hardware (fizice) ale computerului.

Un cal troian (în engleză: trojan horse, cunoscut de asemenea doar ca troian) în cazul software-ul computerelor (având numele derivat din legenda calului troian) descrie un anumit tip de program spion (care este la rândul său un tip de software rău intenţionat), care apare că ar realiza ceva util, dar care în realitate realizează funcţii malefice care permit accesarea neautorizată a unui calculator, respectiv copierea fişierelor, şi chiar controlarea comenzilor calculatorui penetrat.

Un vierme este un program de calculator maliţios, autoreplicant, proiectat pentru a infecta calculatoare cu scopul de a livra o sarcină utilă distructivă. Un vierme normal se răspândeşte prin intermediul email-urilor, reţelelor de răspândire fişiere sau alte reţele deschise. Fiind răspândiţi pe o rază destul de mare, aceşti paraziţi de obicei se propagă exploatând anumite vulnerabilităţi din securitate în sistemul de la distanţă.

Software-ul antivirus este folosit în general pentru prevenirea şi eliminarea virușilor de computer, viermilor și cailor troieni.

*Securitatea informațiilor

Securitatea informației se ocupă cu protejarea informației și sistemelor informatice, de accesul neautorizat, folosirea, dezvăluirea, întreruperea, modificarea sau distrugerea lor. ISO/IEC27002/2013 tratează securitatea informațiilor prin cele trei componente principale: confidențialitatea, integritatea și disponibilitatea.[1] Confidențialitatea este asigurată prin criptarea informației. Integritatea se obține prin mecanisme și algoritmi de dispersie. Disponibilitatea se asigură prin întărirea securității rețelei sau rețelelor de sisteme informatice și asigurarea de copii de siguranță.

*Securitatea aplicațiilor software

Cerinţe

I confident¸ialitate I integritate I autentificare I autorizare I disponibilitate I non-repudiere

*Securitatea în rețele wi-fi

Folosirea encriptarii

Acesta este cel mai important lucru pe care il poti face. Toate retelele pot fi encriptate si astfel accesibile doar cu parola. Dispozitivele existente pe piata pot fi encriptate folosind doua strategii. Prima dintre ele este WEP. Aceasta este mai slaba si cu suficient acces la date, poate fi sparta in vreo cateva saptamani. Totusi, daca un hacker vede ca ai parola WEP, cel mai probabil va alege o alta sursa mai usoara si nu va pierde timpul cu a ta.

Pașii autentificării WEP:

1. Stația (STA) trimite o cerere de autentificare.
2. Punctul de acces (AP) generează un nonce și îl trimite stației.
3. Stația criptează nonce-ul cu cheia secretă comună și îl trimite înapoi punctului de acces.

4. Punctul de acces compară datele criptate primite cu cele aşteptate şi apoi trimite înapoi cadrul de autentificare cu rezultatul.

WPA, acronimul de la Wi-Fi® Protected Access, reprezintă o specificaţie pentru criptarea datelor pentru reţele LAN fără fir. Este o îmbunătăţire a funcţiei de securitate WEP folosind Extensible Authentication Protocol (EAP) pentru a securiza accesul la reţea şi o metodă de criptare pentru a securiza transmiterea datelor.

*Spam

Spamming (sau spam [spæm]) este procesul de expediere a mesajelor electronice nesolicitate, de cele mai multe ori cu caracter comercial, de publicitate pentru produse şi servicii dubioase, practicată în industria e-marketingului şi de proprietarii de situri pornografice. Spam-ul se distinge prin caracterul agresiv, repetat şi prin privarea de dreptul la opţiune.

*Cookies

Un cookie HTTP sau un modul cookie este un text special, deseori codificat, trimis de un server unui navigator web şi apoi trimis înapoi (nemodificat) de către navigator, de fiecare dată când accesează acel server. Cookie-urile sunt folosite pentru autentificare precum şi pentru urmărirea comportamentului utilizatorilor; aplicaţii tipice sunt reţinerea preferinţelor utilizatorilor şi implementarea sistemului de „coş de cumpărături”.

*Bannere

Bannerul web este un afisaj grafic, dreptunghiular, postat in partea de sus / jos, stanga sau drepta intr-o pagina web. In general bannerele sunt bazate pe imagini, mai mult decat pe text si au rolul de a promova un produs, un brand, un serviciu prin intermediul altui site gazda (blog, ziar online, forum, site). In majoritatea cazurilor bannerele sunt “livrate” prin intermediul unor servere de publicitate, dar pot fi si livrate personal prin intermediul unor coduri, preluari etc.

*Spywere

Programele spion[1] sau spyware (citit /'sp‿ai.wɛə/, din engleză spy/spionaj + ware/marfă) sunt o categorie de software rău intenţionat, ataşate de obicei la programe gratuite (jocuri, programe de schimbat fişiere, programe de chatpornografic, etc.), care captează pe ascuns date de marketing (prin analiza siturilor pe care le vizitează utilizatorul, de exemplu de modă, pantofi, cluburi de tenis, ş.a.m.d.) şi le folosesc apoi pentru a transmite utilizatorului reclame corespunzătoare dar nesolicitate.

*Keylogger

Un keylogger este un program care înregistrează fiecare bătaie de tastă pe o tastatură şi salvează aceste date într-un fişier. După ce colectează o anumită cantitate de date, le va transfera prin intermediul internetului unei gazde de la distanță, predeterminată. De asemenea, poate captura capturi de ecran şi utiliza alte tehnici pentru a urmări

activitatea utilizatorului. Un keylogger poate cauza pierderea parolelor, date de autentificare, şi alte informații similare.

*Comunicarea pe reţelele sociale

O reţea de socializare este, general vorbind, o reţea de persoane cu scopuri comune,

!Discuţie cu copii despre reţelele utilizate,după prezentarea sondajului

*Phishing

În domeniul securităţii calculatoarelor, înşelăciunea[1] (denumită în engleză phishing, pronunţat /'fi-şin/) reprezintă o formă de activitate infracţională care constă în obţinerea unor date confidenţiale, cum ar fi date de acces pentru aplicaţii de tip bancar, aplicaţii de comerţ electronic (ca eBay sau PayPal) sau informaţii referitoare la carduri de credit, folosind tehnici de manipulare a datelor identităţii unei persoane sau a unei instituţii.

!Prezentarea celor 2 virusuri cu tentă de phishing

!Întrebări de la public