Popa Cătălin TI-211 Atestare nr.1

**1. Prezentarea generală a securității informaționale**

**1.1 Definirea securității informaționale**

Securitatea informațională poate fi definită ca un sistem care asigură protejarea informațiilor digitale de acces neautorizat, utlizarea abuzivă, modificarea, distrugerea sau dezvăluirea neautorizată.

**1.2 Exemple relevante despre incidentele de securitate**

a. Un atac destul de des întâlnit este atacurile phishing, în care are loc trimiterea e-mailurilor false în încercarea de a obține informații personale și confidențiale, cum ar fi parole, carduri bancare sau lucurui personale.

b. De asemenea, există și atacuri asupra infrastructurii critice, cum ar fi atacurile cibernetice asupra centralelor nucleare sau asupra sistemelor de transport public, care ar putea avea consecințe grave pentru siguranța publică.

**2. Amenințări de securitate. Vulnerabilitatea sistemelor informaționale. Programe malițioase**

**2.1 Clasificarea vulnerabilităților**

a. În funcție de originea lor:

- vulnerabilități de software,

- vulnerabilități de hardware,

- vulnerabilități de rețea.

b. În funcție de impactul lor:

- vulnerabilități critice,

- vulnerabilități majore,

- vulnerabilități minore.

c. În funcție de modul de exploatare:

- vulnerabilități de tip zero-day,

- vulnerabilități de ingineria socială,

- vulnerabilități fizice.

**2.2 Tipuri de atacuri. Profilul Atacatorului**

a. Atacuri de tip phishing - acestea implică expedierea de e-mailuri sau mesaje text false, care încearcă să convingă victimele să dezvăluie informații personale sau să descarce fișiere malware. Atacatorii pot fi indivizi sau grupuri de infractori cibernetici, care au acces la tehnologii sofisticate de phishing și la baze de date de informații personale furate.

b. Atacuri de tip DDoS - acestea implică inundarea serverelor sau rețelelor cu trafic fals, pentru a le bloca și a le face inaccesibile utilizatorilor legitimi. Atacatorii pot fi indivizi sau grupuri de infractori cibernetici, care utilizează botnet-uri sau alte tehnologii de amplificare pentru a crește intensitatea atacului.

c. Atacuri de tip ransomware - acestea implică blocarea accesului la datele sau sistemul victimelor, până când acestea plătesc o răscumpărare pentru a obține accesul înapoi. Atacatorii pot fi indivizi sau grupuri de infractori cibernetici, care utilizează tehnologii sofisticate de criptare și tactici de inginerie socială pentru a obține accesul la sistemele victimelor.

d. Atacuri de tip malware - acestea implică infectarea dispozitivelor sau sistemelor cu software malicios, care poate fura date sau prelua controlul asupra sistemelor. Atacatorii pot fi indivizi sau grupuri de infractori cibernetici, care utilizează tehnologii sofisticate de programare și distribuție pentru a răspândi malware-ul.

**2.3 Programe malițioase, clasificare**

Programele malițioase sunt programe informatice dezvoltate cu scopul de a cauza daune sau a obține acces neautorizat la sistemele sau datele utilizatorilor. Acestea pot fi clasificate în diferite categorii, în funcție de modul în care infectează sau afectează sistemul, cum ar fi:

* virus,
* worm,
* trojan,
* ransomware,
* spyware.

**2.4 Programe antivirus**

Programele antivirus sunt o soluție importantă pentru protejarea dispozitivelor și rețelelor împotriva programelor malware, care pot cauza daune semnificative utilizatorilor și organizațiilor. Aceste programe utilizează diferite metode de detectare, inclusiv scanarea fișierelor și a memoriei pentru a identifica semne de activitate malware și pot folosi semnături de virus pentru a identifica programe malware cunoscute.

Exemple de antiviruși

* BitDefender,
* Kaspersky,
* Norton.

**2.5 Tehnici de inginerie socială**

Tehnicile de inginerie socială sunt metode folosite de atacatorii cibernetici pentru a manipula oamenii și a-i determina să dezvăluie informații personale sau să execute anumite acțiuni care ar putea duce la compromiterea securității cibernetice. Aceste tehnici includ:

* Phishing,
* Pharming.

**3. Atacuri asupra rețelelor de calculatoare**

**3.1 Atacuri de interceptare man-in-the-middle**

Un atac man-in-the-middle (MITM) reprezintă o tehnica de interceptare a comunicațiilor dintre două părți, astfel încât atacatorul poate asculta, modifica sau injecta informații în aceste comunicații fără ca vreuna dintre părți să observe acest lucru. Acest tip de atac poate fi utilizat pentru a obține informații confidențiale, cum ar fi parole, informații bancare sau informații de identificare personală.

**3.2 Atacuri de refuz al serviciului DoS**

Există mai multe atacuri asupra rețelelor de calculator, care pot afecta puternic. Dintre cele mai importante sunt DoS/DDos și malware.

Atacurile DoS sunt efectuate de la un singur dispozitiv, care trimite o cantitate mare de trafic către serverul țintă, blocând astfel accesul altor utilizatori la acel serviciu. În cazul atacurilor DDoS, atacatorii folosesc o rețea de dispozitive infectate cu malware pentru a trimite trafic către serverul țintă, ceea ce face ca atacul să fie mult mai puternic și mai greu de contracarat.

Pe lângă aceste, sunt și atacuri de tip malware, care de asemenea pot afecta rețele de calculator.

**3.3 Atacuri distribuite**

Aceste atacuri distribuite pot fi devastatoare, deoarece pot implica mii sau chiar milioane de computere infectate, ceea ce face ca atacul să fie mult mai puternic și mai greu de contracarat. Pentru a preveni astfel de atacuri, utilizatorii ar trebui să ia măsuri de securitate cibernetică pentru a proteja computerele lor de malware, cum ar fi instalarea unui program antivirus și a unui firewall.

**3.4 Metode de protecție**

Pentru a te proteja de astefel de atacuri, utilizatorul poate utiliza soluții de securitate cibernetică, cum ar fi firewall-uri și soluții anti-DDOS, anti DoS, care pot ajuta la detectarea și prevenirea atacurilor de acest tip. De asemenea, este important să se evite conexiunile nesigure, cum ar fi rețelele WiFi publice, care pot fi vulnerabile la atacuri MITM.

**4. Atacuri asupra aplicațiilor și serviciilor web**

**4.1 Atacuri asupra browser-ului**

Atacurile asupra browser-ului pot fi atacurile de tip clickjacking și phishing, sunt comune și pot fi periculoase pentru utilizatori.

**4.2 Clasificarea vulnerabilităților după OWASP**

a. Injection Flaws

b. Malicious File

**4.3 Atacuri asupra sit-uri web**

Asupra sit-uri de asemenea poate avea loc atacuri de tip phishing, în urma cărora poate avea loc pierderea de legătura cu siteul sau va lucra într-un mod foarte greu, iar utilizatorii nu vor avea acces la el.

**4.4 Metode și tehnologii de protecție**

Pentru a te proteja de astefel de atacuri, utilizatorul poate utiliza soluții de securitate cibernetică, cum ar fi firewall-uri și soluții anti-DDOS, anti DoS, care pot ajuta la prevenirea atacurilor respective.

**5. Cubul McCumber. Principiile fundamentale ale securității informației**

**5.1 Triada confidențialitate, disponibilitate, integritate (CIA)**

Triada confidențialitate, disponibilitate, integritate (CIA) este o paradigmă de securitate cibernetică care indică cele trei obiective principale ale securității informaționale: confidențialitatea, disponibilitatea și integritatea datelor.

**5.2 Cubul McCumber. Structura 3d a principiilor fundamentale ale securității**

Cubul McCumber este o structură 3D care reprezintă principiile fundamentale ale securității cibernetice. Cubul este alcătuit din trei axe principale: confidențialitatea, integritatea și disponibilitatea. Acestea sunt cele trei principii fundamentale ale securității cibernetice și sunt reprezentate pe cele trei axe ale cubului.

**5.3 Drepturi de acces în mediul Windows/Linux**

Pentru Windows: Administrator, Guest, utilizator standart

Pentru Linux: Guest, Administrator

**6. Principiul de confidențialitate. Criptarea simetrică. Algoritmi de criptare simetrică**

**6.1 Asigurarea confidențialității datelor în mediul online**

Pentru a asigura confidențialitatea datelor în mediul online, este necesar de a folosi mai întâi o rețea securizată și nu publică. De asemenea, este necesar de a folosi un ativirus web și folosirea VPN-ului, care de asemenea va ajuta mult în cazul confidențialității.

**6.2 Criptografia tradiționala. Algoritmul Caesar, Cifru bazate pe Substituție**

Criptografia tradițională se referă la metodele de criptare a datelor care au fost utilizate în trecut, înainte de dezvoltarea criptografiei moderne. Două dintre cele mai cunoscute metode de criptare tradiționale sunt Algoritmul Caesar și Cifrul bazat pe Substituție.

**6.3 Criptografia modernă. Algoritmul DES/AES**

Criptografia modernă se referă la metodele dee criptare a datelor care se folosec la moment. Ea se bazează pe algoritmi matematici avansați care sunt mult mai siguri decât criptografia tradițională.

Algoritmul DES și AES sunt două dintre cele mai utilizate algoritmi de criptare modernă.

**6.4 Cifru bazate pe transpoziție**

Cifrele bazate pe transpoziție sunt o altă categorie de cifre tradiționale care funcționează prin reordonarea literelor din textul clar. În loc să înlocuiască literele cu alte litere, cifrele bazate pe transpoziție își schimbă ordinea.

**7. Criptarea asimetrică. Algoritmi de criptare asimetrică**

**7.1 Distribuția Diffie-Hellman**

Distribuția Diffie-Hellman este o metodă criptografică utilizată pentru a permite două părți să stabilească o cheie comună de criptare fără a comunica această cheie direct. În schimb, cele două părți se angajează într-un schimb de mesaje criptate, folosind fiecare o cheie publică și o cheie privată.