Ministerul Educaţiei, Culturii și Cercetării al Republicii Moldova

Universitatea Tehnică a Moldovei

Departamentul Ingineria Software și Automatică

**ATESTARE**

Disciplina: Tehnologia Securității Informaționale

A efectuat: st.gr.TI-216,

Rosca Dorin

A verificat :

lect.univ.  
Răducanu Octavian

Chișinău 2023

1. Prezentare generală a securității informaționale:

· Definirea securității informaționale:

Securitatea informațională reprezintă un set complex de practici, tehnologii și proceduri concepute pentru a proteja informațiile împotriva accesului neautorizat, utilizării neautorizate și distrugerii. Aceste practici pot fi aplicate într-o varietate de domenii, inclusiv în mediul online, în rețelele de calculatoare, în sistemele informatice și în comunicarea electronică, cu scopul de a asigura confidențialitatea, integritatea și disponibilitatea datelor

· Exemple relevante despre incidentele de Securitate:

Atacul Sony Pictures din 2014 - a fost unul dintre cele mai grave breach-uri de securitate cibernetică suferite de o companie americană care a dus la dezvăluirea informațiilor financiare și personale ale angajaților, precum și la scurgeri de informații despre filmele care urmau să fie lansate de companie.

Atacul SolarWinds din 2020 - Acesta a fost unul dintre cele mai mari atacuri cibernetice din istorie, afectând mai multe organizații din întreaga lume. Atacatorii au exploatat o vulnerabilitate din software-ul SolarWinds pentru a obține acces neautorizat la sistemele informatice ale companiilor și agențiilor guvernamentale din SUA și din alte țări.

Atacul Orange din 2021 - operatorul de telecomunicații a fost ținta unui atac cibernetic. Atacul a vizat datele personale ale clienților companiei din Franța, inclusiv numele, adresele, numerele de telefon și adresele de e-mail. Orange a luat măsuri imediate pentru a remedia problema și a implementat soluții suplimentare de securitate cibernetică pentru a preveni incidente similare în viitor.

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

· Clasificarea vulnerabilităților:

Clasificarea vulnerabilităților se poate face în funcție de natura și originea lor. Astfel, vulnerabilitățile pot fi clasificate în funcție de sursa lor (interne sau externe), de gradul de expunere la riscuri (critice sau minore), de tipul de atac pe care îl permit (atacuri de tip denial-of-service, phishing, cross-site scripting etc.) sau de nivelul de dificultate de exploatare (ușor, mediu sau avansat).

· Tipuri de atacuri. Profilul Atacatorului:

Există o varietate de tipuri de atacuri cibernetice, cum ar fi atacurile de tip phishing, malware, denial-of-service (DoS), ransomware sau atacuri de tip zero-day. Aceste atacuri sunt de obicei efectuate de către atacatori cu diferite profiluri, care pot fi grupuri de hackeri organizate, atacatori individuali sau chiar state naționale. Atacatorii pot avea motive diferite pentru a efectua un atac cibernetic, cum ar fi dobândirea de informații confidentiale sau financiare, distrugerea sau blocarea unui sistem, furarea de date personale sau compromiterea securității naționale.

· Programe malițioase, clasificare:

Programele malware pot fi clasificate în mai multe categorii, cum ar fi viruși, worm-uri, troieni, ransomware, spyware, adware, keyloggeri sau rootkit-uri. Fiecare categorie se caracterizează prin modul de propagare, scopul și modul de acțiune al programului malware.

· Programe antivirus:

Programele antivirus sunt programe software care detectează, previn și elimină programele malware de pe dispozitivele utilizatorilor. Iată câteva exemple de programe antivirus: Norton Antivirus ,McAfee ,Avast Antivirus, Bitdefender Antivirus, Kaspersky Antivirus)

· Tehnici de inginerie social:

Ingineria socială este o metodă prin care atacatorii manipulează oamenii pentru a obține acces neautorizat la informații sau sisteme. Iată câteva tehnici comune de inginerie socială:

Phishing - este o tehnică prin care atacatorii trimit e-mailuri sau mesaje text false, care par să fie de la o sursă de încredere, pentru a obține informații personale sau financiare.

Pretexting - este o tehnică prin care atacatorii creează o poveste falsă sau un pretext pentru a obține informații de la o victimă.

Vishing - este o variantă a tehnicilor de phishing care implică folosirea apelurilor telefonice în loc de e-mailuri sau mesaje text.

Baiting - este o tehnică prin care atacatorii oferă o „momeală“ (un document fals, un fișier infectat sau alte lucruri tentante) pentru a convinge victimele să ofere informații sau să acceseze un sistem infectat.

Scareware - este o tehnică prin care atacatorii creează alerte false de securitate pentru a convinge utilizatorii să instaleze programe malware sau să ofere informații personale.

3. Atacuri asupra rețelelor de calculatoare

· Atacuri de interceptare man-in-the-middle:

Atacurile de interceptare man-in-the-middle (MITM) sunt o formă de atac în care un atacator interceptează și manipulează comunicațiile dintre două sau mai multe dispozitive. În acest tip de atac, atacatorul se poziționează între dispozitivele care comunică (de exemplu, între un computer și serverul web), astfel încât poate monitoriza și chiar modifica datele care sunt transmise între acestea.

· Atacuri de refuz al serviciului DoS:

Atacul de tip DoS (Denial-of-Service) este o tactică prin care un atacator încearcă să blocheze accesul la un anumit serviciu sau resursă prin suprasolicitarea acestora cu un volum mare de cereri sau pachete de date. Diferența față de DDoS este că în acest caz, atacatorul operează de pe un singur dispozitiv sau de pe un număr mic de dispozitive, spre deosebire de o rețea întreagă de dispozitive infectate.

Atacurile de tip DoS pot avea consecințe negative pentru utilizatori sau pentru organizațiile care furnizează serviciul, deoarece acestea nu mai pot accesa resursa sau serviciul dorit.

· Atacuri distribuite:

Atacurile distribuite (DDoS) sunt o tactică prin care un atacator utilizează o rețea de dispozitive infectate (botnet) pentru a suprasolicita un server sau o rețea, astfel încât acestea să nu mai poată procesa cererile legitime.

· Metode de protecție:

Există o serie de metode și tehnologii pe care organizațiile le pot utiliza pentru a proteja rețelele și sistemele lor împotriva atacurilor cibernetice. Acestea includ, printre altele:

Utilizarea unor soluții de securitate, cum ar fi firewall-uri, soluții de protecție antivirus sau anti-malware, sisteme de detecție a intruziunilor și soluții de criptare a datelor.

Implementarea unor politici de securitate clare și bine definite, precum și a unor proceduri de securitate, care să asigure că angajații respectă normele și standardele de securitate.

Monitorizarea constantă a rețelelor și a traficului de date, pentru a detecta eventualele activități suspecte sau neobișnuite.

Actualizarea constantă a sistemelor și a software-ului folosit, pentru a se asigura că acestea beneficiază de cele mai recente patch-uri și actualizări de securitate.

Formarea angajaților în ceea ce privește bunele practici de securitate cibernetică și educația lor în ceea ce privește amenințările actuale și cum să le gestioneze.

4. Atacuri asupra aplicațiilor și serviciilor web

· Atacuri asupra browser-ului:

Atacurile asupra browser-ului sunt o tactică prin care atacatorii exploatează vulnerabilități în software-ul browser-ului pentru a prelua controlul asupra acestuia sau a infecta sistemul gazdă cu programe malware. Aceste atacuri pot fi efectuate prin intermediul unor site-uri web infectate sau prin intermediul phishing-ului.

· Clasificarea vulnerabilităților după OWASP:

OWASP (Open Web Application Security Project) este o organizație care se ocupă cu identificarea și clasificarea vulnerabilităților în aplicațiile web. Clasificarea vulnerabilităților după OWASP include diverse categorii, cum ar fi injecțiile, expunerea datelor sensibile, probleme de autentificare și autorizare, vulnerabilități în gestionarea sesiunilor.

· Atacuri asupra sit-uri web:

Atacurile asupra site-urilor web sunt o tactică prin care atacatorii încearcă să compromită site-uri web prin exploatarea vulnerabilităților lor. Aceste atacuri pot include injecții SQL, Cross-Site Scripting (XSS), Cross-Site Request Forgery (CSRF), atacuri de tipul man-in-the-middle (MITM) și multe altele. Scopul acestor atacuri poate fi furarea datelor personale sau de afaceri, distrugerea site-ului sau preluarea controlului asupra acestuia.

· Metode și tehnologii de protecție:

Pentru a proteja aplicațiile și serviciile web de atacuri cibernetice, se pot utiliza următoarele tehnici și metode de protecție:

Validarea și verificarea datelor de intrare pentru a preveni injecțiile SQL și alte tipuri de atacuri.

Utilizarea unor framework-uri și librării de securitate care să ofere protecție împotriva vulnerabilităților cunoscute.

Implementarea de măsuri de securitate precum autentificarea cu factori multipli, criptarea datelor și utilizarea de token-uri de securitate pentru a preveni CSRF.

Limitarea accesului la resursele serverului și la datele stocate, inclusiv prin utilizarea de sandbox-uri.

Monitorizarea activităților suspecte prin analiza jurnalelor și a evenimentelor de securitate.

Testarea regulată a aplicațiilor și serviciilor web, inclusiv prin efectuarea de teste de penetrare și de securitate.

5. Cubul McCumber. Principiile fundamentale ale securității informației

· Triada confidențialitate, disponibilitate, integritate (CIA):

Triada confidențialitate, disponibilitate și integritate (CIA) reprezintă principiile fundamentale ale securității informației. Aceste principii sunt interconectate și se referă la protejarea informațiilor de accesul neautorizat (confidențialitate), asigurarea disponibilității informațiilor pentru utilizatori autorizați și evitarea pierderii sau corupției datelor (disponibilitate), precum și prevenirea modificării sau alterării informațiilor fără permisiune (integritate

· Cubul McCumber. Structura 3D a principiilor fundamentale ale securității:

Cubul McCumber reprezintă o metodă de reprezentare a principiilor fundamentale ale securității informației prin intermediul unei structuri tridimensionale. Aceasta include cele trei principii de bază ale securității informației: confidențialitatea, integritatea și disponibilitatea, precum și alte aspecte relevante, cum ar fi autenticitatea, non-repudierea și securitatea fizică. Cubul McCumber este util pentru a înțelege interconectarea acestor principii și pentru a oferi o perspectivă comprehensivă asupra securității informațiilor în diferite medii și contexte.

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

· Asigurarea confidențialității datelor în mediul online:

Pentru a asigura confidențialitatea datelor în mediul online, este important să se utilizeze protocoale de securitate, cum ar fi SSL/TLS, care asigură criptarea comunicațiilor între client și server. De asemenea, este esențial să se gestioneze cu grijă parolele și să se evite trimiterea de informații personale prin canale nesigure, cum ar fi rețelele Wi-Fi publice. Alte măsuri, cum ar fi autentificarea în doi pași și criptarea fișierelor stocate în cloud, pot contribui, de asemenea, la creșterea securității datelor online.

· Criptografia tradiționala. Algoritmul Caesar, Cifru bazate pe Substituție:

Algoritmul Caesar este o metodă simplă de criptare, care implică înlocuirea fiecărei litere a unui mesaj cu o literă situată un număr fix de poziții mai înainte în alfabet. Cifrul bazat pe substituție este o altă metodă de criptare tradițională, care implică înlocuirea fiecărei litere dintr-un mesaj cu o altă literă, conform unei scheme predefinite.

· Criptografia modernă. Algoritmul DES/AES:

Algoritmul DES (Data Encryption Standard) este unul dintre primele algoritme de criptare simetrică, dezvoltat în anii '70, iar AES (Advanced Encryption Standard) este o versiune mai nouă, dezvoltată în anii 2000, care utilizează blocuri de 128 de biți și chei de 128, 192 sau 256 de biți pentru a cripta datele. Ambele algoritme sunt considerate robuste și sunt utilizate pe scară largă în securitatea informației, dar AES este considerat mai sigur decât DES, deoarece are o dimensiune mai mare a cheii și poate fi mai rapid în anumite aplicații.

· Cifru bazate pe transpoziție:

Cifrul bazat pe transpoziție este un tip de cifru în care ordinea literelor din textul clar este schimbată, fără a le înlocui cu alte caractere. Acesta se bazează pe permutarea literelor într-un anumit mod pentru a genera textul criptat, făcând dificilă citirea acestuia fără cunoașterea algoritmului de decriptare.

7. Criptarea asimetrică. Algoritmi de criptare asimetrică

· Distribuția Diffie-Hellman:

Distribuția Diffie-Hellman este o metodă de schimb de chei criptografice ce permite două entități să comunice în mod sigur prin intermediul unei rețele nesigure. Ea se bazează pe un set de operații matematice pentru a genera chei unice și securizate de comunicare între cele două părți, fără a fi necesară transmiterea cheilor prin intermediul rețelei.

· Algoritlul RSA:

Algoritmul RSA este un algoritm de criptare asimetrică care se bazează pe utilizarea unui set de chei publice și private. El este utilizat pentru a cripta și decripta date, semna digital documente și autentifica identitatea unui utilizator într-un sistem informatics.