Atestarea nr.1 la Tehnologii de securitate informaționale

Student Buza Cătălin TI-214

14/03/2023

1. Prezentare generală a securității informaționale:

* Definirea securității informaționale

Securitatea informațiilor se referă la protejarea datelor electronice și a sistemelor informatice împotriva accesului nerestricționat, modificări, dezvăluiri, întreruperi sau întreruperi. Acest lucru implică utilizarea tehnologiilor, procedurilor și tehnicilor pentru a proteja informațiile vitale și activele afacerii de amenințările de securitate cibernetică, cum ar fi ransomware, atacuri cibernetice, phishing și alte tactici criminale pe internet.

* Exemple relevante despre incidentele de Securitate

1. Atacul cibernetic asupra Sony Pictures Entertainment în 2014: în noiembrie 2014, Sony Pictures Entertainment a suferit un atac cibernetic semnificativ care a dus la expunerea informațiilor financiare și confidențiale ale angajaților, a e-mailurilor interne și a altor informații. Incidentul a fost atribuit Coreei de Nord și a avut legătură cu comedia „Interviul”, care l-a dezamăgit pe liderul nord-coreean Kim Jong-un.
2. Atacul cibernetic asupra Yahoo în 2013 și 2014: În 2016, Yahoo a anunțat că a suferit un atac cibernetic semnificativ în 2013 și 2014, care a dus la expunerea informațiilor confidențiale a cel puțin un milion de utilizatori. Datele au fost falsificate cu adrese de e-mail, numere de telefon, întrebări ascunse și răspunsuri. Crima a fost comisă de un grup de teroriști cibernetici ruși.
3. Atac cibernetic împotriva Equifax în 2017: În 2017, Equifax, una dintre cele mai mari agenții de raportare a creditelor din SUA, a suferit un atac cibernetic semnificativ care a dus la expunerea informațiilor personale despre aproximativ 147 de milioane de americani, inclusiv numele, adresa, numărul de securitate socială și alte informații confidențiale. Crima a fost comisă de un grup de teroriști cibernetici chinezi.

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

În funcție de impactul vulnerabilității, clasificați:

* Vulnerabilități criticate: au un impact semnificativ asupra sistemului informațional și pot fi exploatate rapid de atacatori.
* Vulnerabilități de nivel mediu: au o influență limitată asupra sistemului informațional și pot fi exploatate doar cu abilități tehnice specifice.
* Vulnerabilitati mici: au un efect mai mic asupra sistemului informatic și sunt mai puțin susceptibile de a fi exploatate.

Tipuri de atacuri. Profilul Atacatorului

Atacurile de tip phishing implică trimiterea de e-mailuri false, mesaje text sau alte forme de comunicare către utilizatori, în efortul de a-i determina să divulge informații personale sau să facă clic pe linkuri care instalează software rău intenționat. Atacatorii care folosesc această metodă sunt adesea criminali cibernetici cu experiență care caută informații sensibile, cum ar fi informații financiare sau de altă natură.

Atacurile ransomware implică instalarea unei aplicații rău intenționate care criptează datele sistemului computerului victimei și solicită plata pentru a restabili accesul.Grupurile de criminali cibernetici care doresc să facă profit sunt adesea atacatorii care folosesc această metodă.

Există mai multe tipuri de software rău intenționat, printre care:

Aceste programe software rău intenționate, cunoscute sub numele de viruși, fișiere țintă sau alte programe și se răspândesc prin utilizarea lor. Utilizarea virușilor poate fi folosită pentru a schimba datele sau pentru a deschide noi uși într-un sistem.

Troienii sunt programe software rău intenționate care se ascund în alte programe sau fișiere și sunt folosite pentru a spiona sistemele computerizate ale utilizatorilor sau pentru a obține acces nerestricționat la acestea.

Programele spion sunt programe software rău intenționate care sunt utilizate pentru a colecta informații despre utilizatorii de sisteme informatice, inclusiv cuvinte sensibile sau private sau alte date.

Ransomware-urile sunt programe de computer rău intenționate care criptează informațiile personale ale unui utilizator și solicită plata pentru a restabili accesul.

Adware-urile sunt programe software rău intenționate care blochează apariția ferestrelor pop-up sau a altor anunțuri neautorizate pe ecranul utilizatorului. sistem.

3.Atacuri asupra rețelelor de calculatoare

Atacurile asupra calculatoarelor pot avea repercusiuni grave asupra securității informațiilor, iar unele dintre cele mai frecvente includ:

* Atacurile „man-in-the-middle”: acestea implică interceptarea comunicațiilor între două părți și citirea sau modificarea datelor trimise. Această tehnică poate fi folosită de atacator pentru a obține informații private, cum ar fi un număr de card de credit sau o parolă.
* Atacuri pentru a refuza un serviciu DoS: Aceste atacuri implică inundarea unui server cu solicitări de la cât mai mulți utilizatori, împiedicându-l să proceseze cereri până când devine supraîncărcat. Acest lucru ar putea duce la indisponibilitatea serviciului sau chiar la blocarea serverului.
* Atacuri distribuite: Acestea sunt o formă mai sofisticată de atac DoS, care implică utilizarea unui grup de calculatoare infectate pentru a lansa un atac asupra unui server sau a unei rețele.

Mecanismele de protecție ale calculatoarelor pot fi utilizate pentru a se apăra împotriva acestor atacuri, cum ar fi:

* Criptarea datelor: utilizarea criptografiei pentru a proteja datele în timpul transmisiei poate ajuta la prevenirea atacurilor de interceptare. bărbatul din mijloc.
* Firewall-uri: instalarea unui firewall poate ajuta la protejarea rețelelor împotriva atacurilor DoS și a altor tipuri de atacuri.
* Sisteme pentru detectarea și oprirea intruziunilor: Aceste sisteme pot fi utile în identificarea și oprirea atacurilor asupra infrastructurii de comunicații.
* actualizarea atât a sistemelor de operare, cât și a software-ului: software-ul și actualizările sistemului de operare conforme cu reglementările pot fi utile în abordarea defectelor de securitate și prevenirea atacurilor.

Utilizarea tacticilor de inginerie socială implică încercarea unui atacator de a obține acces neîngrădit la informații private sau de a influența comportamentul țintei prin utilizarea relațiilor interpersonale și a psihologiei. Aceste tehnici sunt frecvent utilizate pentru a profita de slăbiciunea umană pentru a obține acces la sisteme sau informații care altfel ar fi protejate.

Un exemple de tehnici de inginerie sociala sociale sunt următoarele:

Phishingul este o tehnică folosită de atacatori pentru a trimite e-mailuri false sau mesaje text care constrâng utilizatorii să dezvăluie informații private, cum ar fi parole sau numere de card de credit, de obicei prin utilizarea unui site web fals care pare legitim.

4.Atacuri asupra aplicațiilor și serviciilor web

• Atacuri asupra browser-ului

Hackerii pot folosi o mare varietate de metode de atac fura date sau compromite buna funcționare a sistemelor. Acest lucru este valabil și pentru browser-ul în sine și alte aplicații care se conectează la rețea. Este important să știm ce tipuri de atacuri ne pot afecta atunci când navigăm și astfel să putem lua măsuri pentru a fi protejați.

• Clasificarea vulnerabilităților după OWASP

1. Injection
2. Broken aut
3. authentication and session management
4. Cross Site Scripting (XSS)
5. Insecure Direct Object References

• Atacuri asupra sit-uri web

1. Atac de otrăvire a cookie-urilor

Atacurile de otrăvire a cookie-urilor implică modificarea conținutului unui cookie(informații personale stocate pe computerul victimei) pentru a ocoli mecanismele de securitate.

1. Furt de cookie-uri

Furtul de cookie-uri este un tip de atac care se efectuează folosind astfel de scripturi din partea clientului a JavaScript.

1. Atacuri de tip phishing

Phishing este procesul în care un atacator încearcă să fure date sensibile, parole, acreditări

• Metode și tehnologii de protecție

1. Backup&Restore

Solutiile de back-up si restore permit organizatiilor sa-si imbunatateasca semnificativ activitatile de protectie a datelor si sa implementeze o gama variata de servicii chiar si cazul companiilor care genereaza volume foarte mari de date.

1. Sisteme de recuperare

În momentul în care ştergi un fişier de pe PC acesta nu este şters în mod fizic de pe hard-disk, ci doar îndepărtat din directorul în care se afla. Iniţial, el se regăseşte în Recycle Bin şi poate fi restaurat printr-un singur click. Dacă ai golit însă şi Recycle Bin, misiunea se complică, dar nu devine imposibilă. De aceea sunt programe gratuite de recuperare a datelor.

5.Cubul McCumber. Principiile fundamentale ale securității informației

Metoda Cubul McCumber este utilizată în securitatea informațiilor și își propune să prezinte o viziune convingătoare asupra principiilor de bază de securitate. Componentele de bază ale cubului sunt cele trei principii CIA de confidențialitate, integritate și disponibilitate.

Principiile fundamentale de securitate a informațiilor conform Cubul McCumber sunt următoarele:

* Confidențialitate: se referă la asigurarea că informațiile pot fi accesate numai de persoane autorizate și nu pot fi văzute de părți nerestricționate. Acest principiu necesită utilizarea tehnicilor de criptare și autentificare pentru a proteja informațiile confidențiale.
* Integritate: se referă la asigurarea că informațiile sunt exacte, cuprinzătoare și nu au fost modificate ilegal. Acest principiu necesită utilizarea codurilor hash digitale și a semnăturilor digitale ca metode de verificare a integrității datelor.
* Disponibilitate: se referă la asigurarea că informațiile sunt accesibile și disponibile atunci când este necesar. Acest principiu necesită utilizarea tehnicilor de backup și redundanță pentru a garanta că informațiile sunt accesibile chiar și în cazul unui accident de securitate.

Structura 3D a principiilor de securitate de bază, Cubul McCumber, oferă o vedere mai detaliată a acestor principii și demonstrează modul în care interacționează.

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

* Criptografia tradiționala. Algoritmul Caesar, Cifru bazate pe Substituție
* Criptografia tradițională este un corp de tehnici care se întind până la cele mai vechi epoci și implică conversia unui text necriptat într-un text criptat folosind reguli și proceduri matematice. Codul Cezar și codul substitut sunt două dintre cele mai cunoscute tehnici tradiționale de cifrare.
* Tehnica de cifrare Caesar presupune mutarea fiecărui caracter din textul clar într-una dintr-un număr predeterminat de poziții din alfabet. Pentru o schimbare de trei poziții, de exemplu, litrul A din textul clar va fi înlocuit cu litrul D în textul criptic. Este o idee bună să aveți un plan de rezervă în cazul în care ceva nu merge bine, dar nu este o idee rea să aveți unul pentru orice eventualitate.

Criptografia modernă. Algoritmul DES

* Criptografia modernă este o ramură a criptografiei care utilizează algoritmi criptografici sofisticați și puternici pentru a proteja informațiile sensibile. Cel mai utilizat algoritm modern de criptare se numește DES (Data Encryption Standard).
* IBM a creat DES în anii 1970 pentru a proteja datele din industria bancară, iar guvernul SUA l-a adoptat ca standard federal pentru criptare în 1976. O cheie de 56 de biți este folosită de algoritm pentru a cripta blocurile de 64 de biți de dată.
* Procesul de criptare DES utilizează mai multe runde de înlocuiri de bloc și permutări și utilizează o cheie pentru criptare pentru a controla ordinea în care sunt efectuate.

Cifru bazate pe transpoziție

* Ordinea literelor sau simbolurilor textului original este schimbată în clauzele de substituție bazate pe traducere, dar simbolurile reale în sine sunt lăsate nemodificate. Astfel rezultă cifrurile bazate pe traducerea mesajului prin rearanjarea simbolurilor din textul original, spre deosebire de cifrurile de substituție, în care cuvintele sau simbolurile din textul original sunt schimbate cu altele noi.

7. Criptarea asimetrică. Algoritmi de criptare asimetrică

Criptarea asimetrică este un tip de criptare care utilizează două chei diferite pentru codificarea și decodarea datelor. Criptografia cu cheie publică este folosită pentru a cripta datele, în timp ce criptografia cu cheie privată este folosită pentru a decripta datele. Este o metodă mai sigură decât criptarea simetrică, care folosește aceeași cheie pentru ambele operațiuni.

* Un algoritm de criptare asimetric numit Distribuția Diffie-Hellman este utilizat pentru a permite două părți să genereze o cheie partajată într-o manieră sigură și privată. Este frecvent utilizat pentru criptarea Internetului.
* RSA este un alt algoritm de criptare asimetrică. RSA utilizează un număr mare ca parte a cheii publice, făcându-l foarte dificil de spart prin metode de forțare brută. Acesta este utilizat într-o gamă largă de aplicații, inclusiv pentru criptarea tranzacțiilor online și a datelor stocate pe dispozitivele mobile.