UNIVERSITATEA DE STAT DIN MOLDOVA
FACULTATEA DE RELAȚII INTERNAȚIONALE, ȘTIINȚE POLITICE ȘI ADMINISTRATIVE

REFERAT

LA DISCIPLINA SECURITATEA INFORMAȚIONALĂ

TEMA: PRINCIPALELE COMCEPTE ȘI NOȚIUNI DE SECURITATE INFORMAȚIONALĂ

REALIZAT DE: *COBZAC NATALIA*

SSN / ANUL 2 / GRUPA 01

VERIFICAT DE: *BUSUNCIAN TATIANA*

CHIȘINĂU 2023

REZUMAT: *Acest referat explorează conceptele și noțiunile cheie din domeniul securității informaționale, evidențiind importanța acestora în era digitală. Securitatea informațională se concentrează pe protejarea confidențialității, integrității și disponibilității datelor, oferind un cadru esențial pentru combaterea amenințărilor cibernetice. În cadrul referatului, am analizat conceptele de confidențialitate, integritate și disponibilitate a datelor și am evidențiat motivele pentru protejarea acestora. Confidențialitatea se referă la protejarea datelor sensibile și a informațiilor personale împotriva accesului neautorizat, în timp ce integritatea asigură autenticitatea și acuratețea datelor, evitând modificările neautorizate. Disponibilitatea datelor este crucială pentru a asigura că informațiile rămân accesibile și funcționale în orice moment.*

CUPRINS

INTRODUCERE

Tehnologiile bazate pe web au adus multe avantaje organizațiilor și clienților acestora, dar încălcările securității informațiilor sunt încă o preocupare controversată. Sistemele antivirus, anti-malware, anti-spam, anti-phishing, anti-spyware, firewall, autentificare și detecție a intruziunilor sunt toate aspecte tehnologice care abordează securitatea informațiilor, dar nu pot garanta un mediu sigur pentru informații. Hackerii vizează oameni, mai degrabă decât computere, pentru a crea o breșă; exemplele de greșeli ale utilizatorului includ comportamentul inadecvat de securitate a informațiilor, cum ar fi luarea unui număr de securitate socială ca nume de utilizator și parolă, scrierea parolelor pe hârtie lipicioasă, partajarea numelui de utilizator și a parolei cu colegii, deschiderea e-mailurilor necunoscute și descărcarea atașamentelor acestora, precum și descărcarea

de software. de pe internet. Comportamentul acceptabil de securitate a informațiilor ar trebui să fie combinat în mod ideal cu aspectele tehnologice. Astfel, în mediul de securitate a informațiilor, aplicarea mai multor abordări de securitate este necesară pentru a atenua riscul de încălcare a securității informațiilor.

Ce este securitatea informațiilor? Este, așa cum ar trebui să se concluzioneze dintr-un studiu amplu al materialelor publicate, este totul despre confidențialitate, integritate și disponibilitate (CID). Pentru a măsura InfoSec[1], trebuie măsurate elementele CID; măsurători care sunt evazive. Concluzia este că nu avem măsurători general acceptate de confidențialitate, integritate și disponibilitate, în afară de numărul brut al incidentelor dăunătoare, împreună cu estimări slabe ale daunelor. Când numărul de incidente dăunătoare scade din cauza unui program InfoSec eficient, problema de măsurare crește. Fără incidente înseamnă că nu există imagini „înainte" și „după" și nicio întoarcere măsurabilă de la evitarea incidentelor.

Tom Peltier, un alt autor și profesor în InfoSec, afirmă că, securitatea informațiilor cuprinde utilizarea controalelor fizice și logice de acces la date pentru a asigura utilizarea corectă a datelor și pentru a interzice modificarea, distrugerea, dezvăluirea, pierderea sau accesul neautorizat sau accidental la date. înregistrări și fișiere automate sau manuale, precum și pierderea, deteriorarea sau utilizarea greșită a activelor informaționale.

Din nou, nu obținem o definiție. Mai degrabă, aici este o descriere a ceea ce face securitatea computerului. Un alt text autorizat oferă o altă definiție apropiată: „Securitatea computerelor încearcă să asigure confidențialitatea, integritatea și disponibilitatea componentelor sistemelor de calcul". Aici, încercarea este cea care contează. Nu există un concept intrinsec de completitudine sau precizie în asta. Desigur, există multe activități desfășurate în cadrul departamentelor IT tradiționale, cum ar fi protocoalele de testare care contribuie semnificativ la integritate, care sunt acoperite de această definiție, dar nu ar fi incluse de majoritatea observatorilor în grupul de funcții cunoscut sub numele de „securitate informațională".

[1] Securitatea informațiilor, denumită adesea InfoSec, se referă la procesele și instrumentele concepute și implementate pentru a proteja informațiile sensibile de afaceri împotriva modificărilor, întreruperii, distrugerii și inspecției.

Securitatea informațională este de o importanță crucială în societatea modernă din mai multe motive:

- Protecția datelor personale: Cu creșterea volumului de date personale stocate electronic, asigurarea confidențialității acestor informații devine esențială pentru prevenirea furtului de identitate și a utilizării frauduloase a acestor date.

- Protecția afacerilor și a proprietății intelectuale: Pentru organizații, securitatea informațională este vitală pentru protejarea informațiilor de afaceri și a proprietății intelectuale împotriva concurenței neloiale sau a spionajului industrial.

- Continuitatea afacerii: Asigurarea disponibilității datelor și a infrastructurii informatice este esențială pentru menținerea funcționării normale a afacerilor în fața amenințărilor precum atacurile cibernetice sau dezastrele naturale.

- Conformitatea legală: Multe jurisdicții au legi și reglementări stricte privind protecția datelor și securitatea informațională. Organizațiile trebuie să respecte aceste norme pentru a evita consecințe legale.

- Încrederea clienților: O securitate informațională adecvată contribuie la încrederea clienților și partenerilor, ceea ce poate influența succesul și reputația unei organizații.

În acest context, înțelegerea profundă a conceptelor și noțiunilor legate de securitatea informațională este esențială pentru protejarea datelor și resurselor și pentru menținerea integrității și disponibilității acestora. Acest referat va explora în detaliu aceste concepte și va evidenția importanța lor în lumea modernă a tehnologiei informatice.

CONFIDENȚIALITATEA ÎN SECURITATEA INFORMAȚIONALĂ

Unul dintre pilonii fundamentali ai securității informaționale este confidențialitatea, care se referă la protejarea datelor personale sau an informațiilor sensibile de accesul neautorizat sau de divulgarea acestora către persoane sau entități care nu au dreptul sau nevoia de a le cunoaște. Principiul de confidențialitate se bazează pe ideea că informațiile pot fi accesate și utilizate doar de către persoanele sau entitățile autorizate, iar accesul trebuie să fie bine limitat.

Confidențialitatea include următoarele elemente importante:

- Protejarea informațiilor personale: Un acces neautorizat la informații personale precum numele, adresa, datele de identificare sau istoricul medical trebuie protejat. Acest lucru este esențial pentru a proteja intimitatea persoanelor.

- Protecția datelor legate de afaceri: Companiile și organizațiile trebuie să păstreze secrete și să protejeze datele de afaceri sensibile pentru a preveni spionajul industrial sau concurența neloială.

- Secretele de stat: Guvernele ar trebui să protejeze informațiile clasificate și sensibile, cum ar fi documentele de securitate națională, pentru a preveni orice amenințări la securitatea națională.

Din mai multe motive, protejarea confidențialității informațiilor este esențială:

- Pentru a preveni furtul de identități: Furtul de identitate poate folosi date personale precum numele, adresa, numărul de securitate socială sau informațiile financiare, ceea ce poate avea repercusiuni financiare și personale grave.

- Protejarea intimității: Un element esențial al libertății individuale este dreptul la viața privată. Protejarea confidențialității garantează că informațiile personale și comportamentul unei persoane nu sunt expuse sau utilizate în mod necorespunzător.

- Prevenirea pierderilor de bani: Scurgerea sau divulgarea neautorizată a datelor sau informațiilor confidențiale face ca organizațiile să piardă sume mari de bani. Protejarea acestor informații ajută la păstrarea profitabilității și reputației organizației.

- Conformitate cu legea: În conformitate cu legile privind protecția datelor și confidențialitatea, organizațiile sunt obligate să păstreze confidențialitatea datelor personale; încălcarea acestor legi poate duce la sancțiuni legale.

- Conservarea încrederii partenerilor și clienților: O organizație care păstrează confidențialitatea informațiilor câștigă încrederea clienților și partenerilor, ceea ce poate duce la relații de afaceri solide și loialitatea clienților.

În cele din urmă, conceptul de confidențialitate este esențial în securitatea informațională și are un impact semnificativ asupra vieții fiecărui individ, an organizațiilor și a societății în general. Pentru an evita efectele negative și pentru a proteja datele și viața privată, este esențial să protejați confidențialitatea informațiilor.

INTEGRITATEA DATELOR

Literatura de specialitate recunoaște o distincție între integritatea datelor și integritatea sistemului. Integritatea datelor se referă la datele în sine, adică biții și octeții stocați în sistem. Integritatea sistemului este un termen mai general, care se referă, în plus, la integritatea elementelor de procesare, cum ar fi hardware-ul, sistemul și software-ul de aplicație. Cea mai generală definiție, pe care o numim definiția calității datelor, se datorează lui Courtney și Ware. Se bazează pe conceptul de așteptare a calității datelor: datele au integritate în măsura în care calitatea lor îndeplinește, sau depășește, cerințele de calitate pe care utilizatorii le așteaptă de la ele. Definiția Courtney-Ware este singura care încorporează cerințe de viață. De exemplu, actualitatea datelor se poate deteriora dacă datele nu sunt actualizate în mod regulat. Astfel, integritatea datelor devine unul dintre elementele esențiale ale securității informaționale, care se referă la asigurarea că datele rămân nealterate, autentice și complete pe parcursul ciclului lor de viață. Imaginați-vă datele ca un document important pentru a înțelege ideea. Când confidențialitatea acestui document este compromisă, fie prin erori sau modificări neautorizate, încrederea în informații este subminată.

Aspecte importante ale integrității datelor includ:

- Protejarea împotriva modificărilor neautorizate: Integritatea datelor se referă la asigurarea faptului că datele nu pot fi modificate sau deteriorate de persoane neautorizate sau de erori accidentale.

- Autenticitatea: Datele trebuie să fie autentice, adică nu falsificate sau manipulate.

- Completare: Integritatea garantează că datele sunt complete și că nu au fost șterse sau pierdute în mod neautorizat.

Există o serie de metode și abordări care sunt utilizate pentru a garanta că datele sunt sigure. O lucrare de Khidzir (2018) prezintă o metodă de criptare difuzată folosind text cifrat dinamic, care oferă garanție de securitate pentru decriptarea textului și atacuri. Replicarea datelor este unul dintre procesele de de-duplicare a datelor care este utilizat pentru a reduce spațiul de stocare și utilizarea lățimii de bandă. Cealaltă modalitate este crearea căutării de cuvinte cheie pentru păstrarea confidențialității. Acesta permite să rezolve decriptarea și să returneze numai fișierele care conțin cuvintele cheie specificate.

DISPONIBILITATEA DATELOR

Termenul „disponibilitate” se referă la permiterea accesului utilizatorilor autorizați la activele și informațiile aferente atunci când utilizatorii au nevoie. Integritatea datelor de la distanță poate fi obținută folosind o metodă de păstrare a confidențialității bazată pe identitate. Această abordare demonstrează că informațiile de date sunt sigure și pot fi utilizate într-un sistem în timp real. De asemenea, poate verifica integritatea datelor în mod eficient, fără a descărca datele reale. În plus, *homomorphic token* [2] este, de asemenea, o metodă pentru date distribuite codificate cu ștergere și stocare distribuită scalabilă. Acest lucru face posibilă efectuarea de operațiuni securizate și complexe asupra datelor externalizate, cum ar fi coluziunea serverului și atacurile de modificare a blocurilor. Deoarece informațiile de date sunt stocate în *cloud computing*[3] și integritatea lor a fost verificată de către un verificator terță parte, este imposibil să accesați datele clientului.

Pentru a asigura disponibilitatea datelor, se folosesc diverse tehnici și tehnologii:

- Rezerve care sunt redundante: utilizarea backup-urilor și an infrastructurii redundante pentru an asigura că datele și serviciile rămân disponibile în caz de eșec al infrastructurii sau echipamentului.

- Recuperarea după un dezastru: Organizațiile dezvoltă planuri de recuperare după dezastre pentru a minimiza timpul de inactivitate și pentru a restabili rapid serviciile în caz de evenimente majore, cum ar fi cutremure, inundații sau atacuri cibernetice majore.

- Controlul traficului: Pentru a distribui traficul și an asigura că resursele nu sunt supraîncărcate, se utilizează load balancing[4] și alte tehnici de gestionare a traficului.

- Actualizare și întreținere: Actualizarea și întreținerea continuă a sistemelor și an infrastructurii pentru a preveni eșecurile cauzate de software sau hardware depășit.

- Monitorizarea rezultatelor: O monitorizare continuă a funcționării infrastructurii și a resurselor este efectuată pentru an identifica orice probleme care pot afecta disponibilitatea.

[2] Homomorphic token este o tehnică criptografică care permite efectuarea de calcule pe date criptate – fără a necesita decriptare.

[3] Cloud computing este furnizarea de servicii de calcul – inclusiv servere, stocare, baze de date, rețele, software, analiză și informații – prin internet („the cloud”) pentru a oferi inovație mai rapidă, resurse flexibile și economii de scară.

[4] Se referă la distribuirea eficientă a traficului de rețea de intrare pe un grup de servere backend, cunoscute și ca fermă de servere.

ATACURI CIBERNETICE

Sistemele cyber-fizice sunt combinația dintre lumea cibernetică și componentele lumii fizice pentru a crește performanța fizică. Utilizările sistemelor cyber-fizice sunt crescute, din cauza cu cât mai multe dispozitive cibernetice și fizice sunt conectate pentru a oferi tehnologii de ultimă generație, iar ulterior amenințările și atacurile cibernetice au loc și raportate exponențial. Problemele și provocările de securitate ale sistemelor cyber-fizice au devenit o problemă globală și este necesar urgent un mecanism adecvat pentru sistemele cyber-fizice. În această lucrare, este discutată o investigație despre relația dintre sistemele cyber-fizice și dispozitivele de internet, definițiile acesteia și unele dintre domeniile sale. Provocările și problemele de securitate sunt studiate și discutate în contextul sistemelor cyber-fizice. În această lucrare sunt prezentate diverse vulnerabilități ale sistemelor cyber-fizice, amenințări cibernetice și atacuri cibernetice asupra sistemului cyber-fizic. În cele din urmă, au sugerat măsuri de securitate, metode și protocoale de securitate pentru minimizarea amenințării cibernetice sau a atacurilor asupra sistemului cyber-fizic.

Din cauza atacurilor cibernetice care cresc pe tot globul în zilele noastre, securitatea și confidențialitatea au devenit preocupări majore pentru utilizatori și companii. Când datele circulă de la sursă la destinație în rețeaua deschisă, protecția datelor sensibile este o altă problemă. Un atac cibernetic poate afecta această rețea deschisă sau dispozitivele de sistem pentru a încălca informații sau pentru a dezactiva dispozitivele pentru utilizare greșită personală. Hackerii au intrat în bunuri conectate, cum ar fi mașini, centre comerciale, case inteligente și bănci inteligente, pentru a colecta bani, a pirata sistemul și a încălcat informații personale. Diversele organizații au pus accent pe securitatea cibernetică pentru a proteja confidențialitatea, datele și dispozitivele.

În continuare, vom explora mai multe exemple de atacuri cibernetice și modul în care acestea au afectat organizațiile și utilizatorii:

- Atacurile de rețea. Datele ar putea fi expuse unui atac din cauza lipsei de securitate și controale. Atacurile la rețele sunt clasificate în două tipuri, cum ar fi atacul activ înseamnă că datele sunt modificate și atacul pasiv înseamnă că datele sunt monitorizate sau nu se modifică. Rețelele și datele sunt vulnerabile la oricare dintre următoarele tipuri de atacuri dacă nu aveți un plan de securitate în organizație. Aceste atacuri apar de obicei pe rețele și dispozitive. Atacurile comune ale rețelei sunt interceptarea rețelei, modificarea datelor, falsificarea identității (falsificarea adresei

IP), atacurile bazate pe parole, refuzul serviciului, atacul cu cheie compromisă, snifferul, atacul la nivelul aplicației, atacurile de acces. , atacuri de recunoaștere, atacuri la confidențialitate și atacuri distructive.

- Atacurile criptografice. Un atac criptografic este o procedură de evitare a securității unui sistem prin descoperirea unei slăbiciuni într-un cifr, algoritm de securitate, protocol criptografic sau model de gestionare a cheilor și sisteme de operare. Această practică este numită și „criptanaliza". Criptanaliza poate fi împărțită într-un număr de clase de atacuri. Aceste atacuri sunt atacuri de forță brută, alese text clar; Adaptive a ales atacuri cu text clar, text clar cunoscut, text cifrat cunoscut, text cifrat ales, cheie aleasă, cripto analiza de cauciuc și încuietoare cripto.

- Amenințări cibernetice. O amenințare cibernetică se numește atac rău intenționat. Aceste atacuri sunt identificarea deficiențelor de securitate într-un sistem cyber-fizic pentru întreruperea integrității unei organizații sau a sistemelor personale. Scopul amenințării cibernetice este de a deteriora sau dezactiva funcționarea sistemului. Există multe tipuri de amenințări cibernetice disponibile și pot proveni din surse primare: natură (cutremur, uragane, inundații și incendii) și oameni, atacuri fizice, defecțiuni ale echipamentelor, defecțiuni ale liniilor (defecțiuni ale liniilor electrice ale nodului), scurgeri electromagnetice și interferență electromagnetică.

- Software rău intenționat. Software-ul rău intenționat (Malware) este utilizat pentru a compromite funcționarea sistemului cyber-fizic, a fura informații și a ocoli controalele de acces ale sistemului cyber-fizic. Obiectivul principal al software-ului rău intenționat este provocarea daunelor computerului gazdă. Software-ul rău intenționat este un termen larg care se referă la o varietate de coduri rău intenționate. Cele mai comune programe malware sunt adware, roboți, ransomware, bug-uri, rootkit-uri, spyware, spyware, hackeri, wabbits, dialer, blue sniffing, phishing, bluejacking, mouse captare, pharming, browser hijacker, cai troieni, viruși și viermi.

Aceste exemple demonstrează amploarea și complexitatea atacurilor cibernetice și subliniază importanța protejării adecvate a datelor și a sistemelor împotriva acestor amenințări. Combaterea acestor atacuri implică o combinație de măsuri tehnice, politici de securitate și conștientizare a utilizatorilor.

RISCURI, AMENINȚĂRI ȘI VULNERABILITĂȚI

Înainte de a aborda amenințările de securitate, activele sistemului (componentele sistemului) care alcătuiesc dispozitivele de internet trebuie mai întâi identificate. Este important să înțelegeți inventarul de active, inclusiv toate componentele, dispozitivele și serviciile de Internet. Un activ este o resursă economică, ceva valoros și sensibil deținut de o entitate. Principalele active ale oricărui sistem de dispozitive de internet sunt hardware-ul sistemului (inclusiv clădiri, utilaje etc.), software-ul, serviciile și datele oferite de servicii.

Vulnerabilitățile sunt punctele slabe ale unui sistem sau ale designului acestuia care permit unui intrus să execute comenzi, să acceseze date neautorizate și/sau să efectueze atacuri de refuzare a serviciului. Vulnerabilitățile pot fi găsite într-o varietate de zone ale sistemelor dispozitivelor de internet. În special, acestea pot fi slăbiciuni în hardware-ul sau software-ul sistemului, slăbiciuni în politicile și procedurile utilizate în sistemele și slăbiciunile utilizatorilor de sistem înșiși.

Sistemele de dispozitive de internet se bazează pe două componente principale; hardware de sistem și software de sistem și ambele au defecte de design destul de des. Vulnerabilitățile hardware sunt foarte greu de identificat și, de asemenea, dificil de remediat, chiar dacă vulnerabilitatea a fost identificată din cauza compatibilității și interoperabilității hardware și, de asemenea, a efortului necesar pentru a fi remediată. Vulnerabilitățile software pot fi găsite în sistemele de operare, software-ul de aplicație și software-ul de control, cum ar fi protocoalele de comunicație și unitățile dispozitivelor. Există o serie de factori care duc la defecte de proiectare a software-ului, inclusiv factorii umani și complexitatea software-ului. Vulnerabilitățile tehnice apar de obicei din cauza slăbiciunilor umane. Rezultatele neînțelegerii cerințelor includ începerea proiectului fără un plan, comunicarea slabă între dezvoltatori și utilizatori, lipsa resurselor, abilităților și cunoștințelor și eșecul de a gestiona și controla sistemul.

Expunerea este o problemă sau o greșeală în configurația sistemului care permite unui atacator să desfășoare activități de culegere de informații. Una dintre cele mai provocatoare probleme este reziliența împotriva expunerii la atacuri fizice. În majoritatea aplicațiilor online, dispozitivele pot fi lăsate nesupravegheate și probabil să fie plasate într-o locație ușor accesibilă atacatorilor. O astfel de expunere ridică posibilitatea ca un atacator să captureze dispozitivul, să extragă secrete criptografice, să le modifice programarea sau să le înlocuiască cu dispozitive rău intenționate aflate sub controlul atacatorului.

O amenințare este o acțiune care profită de slăbiciunile de securitate dintr-un sistem și are un impact negativ asupra acestuia. Amenințările pot proveni din două surse primare: oameni și natură. Amenințările naturale, cum ar fi cutremurele, uraganele, inundațiile și incendiile pot provoca daune grave sistemelor informatice. Puține măsuri de protecție pot fi implementate împotriva dezastrelor naturale și nimeni nu le poate împiedica să se întâmple. Planurile de recuperare în caz de dezastru, cum ar fi planurile de rezervă și de urgență, sunt cele mai bune abordări pentru a securiza sistemele împotriva amenințărilor naturale. Amenințările umane sunt cele cauzate de oameni, cum ar fi amenințările rău intenționate constând în amenințări interne (cineva are acces autorizat) sau externe (persoane sau organizații care lucrează în afara rețelei) care caută să dăuneze și să perturbe un sistem.

Atacurile sunt acțiuni întreprinse pentru a dăuna unui sistem sau a perturba operațiunile normale prin exploatarea vulnerabilităților folosind diverse tehnici și instrumente. Atacatorii lansează atacuri pentru a atinge obiective fie pentru satisfacție personală, fie pentru răsplată. Măsurarea efortului depus de un atacator, exprimată în termeni de expertiză, resurse și motivație, se numește costul atacului. Actorii de atac sunt oameni care reprezintă o amenințare pentru lumea digitală. Ar putea fi hackeri, criminali sau chiar guverne. Un atac în sine poate avea mai multe forme, inclusiv atacuri active de rețea pentru a monitoriza traficul necriptat în căutarea de informații sensibile; atacuri pasive, cum ar fi monitorizarea comunicațiilor de rețea neprotejate pentru a decripta traficul slab criptat și obținerea de informații de autentificare; atacuri de aproape; exploatare de către persoane din interior și așa mai departe.

Echilibrul dintre cele trei puncte – confidențialitate, integritate și disponibilitate – este unul greu de realizat. O concentrare prea mare pe disponibilitate va compromite probabil integritatea și confidențialitatea, în timp ce concentrarea pe confidențialitate și integritate va afecta inevitabil disponibilitatea. Un punct de luat în considerare dacă aleg să adopte această metodă este că infractorii cibernetici sunt, de asemenea, conștienți de aceste principii și pot exploata adesea aceste cunoștințe pentru a obține acces la infrastructura IT.

MĂSURI DE SECURITATE INFORMAȚIONALĂ

Pentru a reuși cu implementarea securității cibernetice eficiente, trebuie să fim conștienți de obiectivele principale de securitate, după cum urmează:

Confidențialitatea este o caracteristică de securitate importantă, dar poate să nu fie obligatorie în unele scenarii în care datele sunt prezentate public. Cu toate acestea, în majoritatea situațiilor și scenariilor, datele sensibile nu trebuie dezvăluite sau citite de entități neautorizate. De exemplu, datele pacienților, datele de afaceri private și/sau datele militare, precum și acreditările de securitate și cheile secrete, trebuie să fie ascunse de entitățile neautorizate.

Pentru a oferi servicii de încredere utilizatorilor, integritatea este o proprietate de securitate obligatorie în majoritatea cazurilor. Diferite sisteme au diferite cerințe de integritate. De exemplu, un sistem de monitorizare la distanță a pacientului va avea o verificare a integrității ridicate împotriva erorilor aleatorii din cauza sensibilității informațiilor. Pierderea sau manipularea datelor poate apărea din cauza comunicării, ceea ce poate cauza pierderi de vieți umane.

Conectivitatea omniprezentă agravează problema autentificării din cauza naturii mediilor online, acolo unde posibila comunicare ar avea loc între dispozitiv la dispozitiv, om la dispozitiv și/sau om la om. Cerințe diferite de autentificare necesită soluții diferite în sisteme diferite. Unele soluții trebuie să fie puternice, de exemplu autentificarea cardurilor bancare sau a sistemelor bancare. Pe de altă parte, majoritatea vor trebui să fie internaționale, de exemplu, pașaportul electronic, în timp ce altele trebuie să fie locale. Proprietatea de autorizare permite doar entităților autorizate (orice entitate autentificată) să efectueze anumite operațiuni în rețea.

Un utilizator al unui dispozitiv (sau dispozitivul însuși) trebuie să fie capabil să acceseze serviciile oricând, oricând este necesar. Diferitele componente hardware și software din dispozitivele de internet trebuie să fie robuste, astfel încât să ofere servicii chiar și în prezența entităților rău intenționate sau a situațiilor adverse. Diferite sisteme au cerințe de disponibilitate diferite. De exemplu, sistemele de monitorizare a incendiilor sau de monitorizare a asistenței medicale ar avea probabil cerințe de disponibilitate mai mari decât senzorii de poluare de pe marginea drumurilor.

Atunci când se dezvoltă tehnici de securitate pentru a fi utilizate într-o rețea securizată, responsabilitatea adaugă redundanță și responsabilitate pentru anumite acțiuni, îndatoriri și planificare a implementării politicilor de securitate a rețelei. Responsabilitatea în sine nu poate opri atacurile, dar este utilă pentru a ne asigura că celelalte tehnici de securitate funcționează corect. Problemele de bază de securitate, cum ar fi integritatea și confidențialitatea, pot fi inutile dacă nu sunt supuse răspunderii. De asemenea, în cazul unui incident de repudiere, o entitate ar fi

urmărită pentru acțiunile sale printr-un proces de responsabilitate care ar putea fi util pentru a verifica povestea din interior a ceea ce s-a întâmplat și cine a fost de fapt responsabil pentru incident.

Un audit de securitate este o evaluare sistematică a securității unui dispozitiv sau serviciu prin măsurarea gradului de conformitate cu un set de criterii stabilite. Datorită multor erori și vulnerabilități în majoritatea sistemelor, auditul de securitate joacă un rol important în determinarea oricăror deficiențe exploatabile care pun datele în pericol. În Internet, necesitatea unui sistem de auditare depinde de aplicație și de valoarea acesteia.

Confidențialitatea este dreptul unei entități de a determina gradul în care va interacționa cu mediul său și în ce măsură entitatea este dispusă să împărtășească informații despre ea însăși cu alții.

CONCLUZIE

În concluzie, în lumea digitală în continuă schimbare, înțelegerea și aplicarea conceptelor de securitate informațională sunt cruciale pentru protejarea datelor și a resurselor noastre și pentru menținerea integrității și disponibilității acestora. Securitatea informațională nu este doar un obiectiv tehnic, ci o responsabilitate colectivă a fiecărui individ, organizație și societate în ansamblu. Securitatea informațională este un domeniu important, datele și sistemele noastre informatice pot fi vulnerabile la numeroase amenințări și atacuri cibernetice. Acest referat discută conceptele și noțiunile esențiale despre securitatea informațională și subliniază importanța acestora. Confidențialitatea, integritatea și disponibilitatea datelor reprezintă pilonii de bază ai securității informaționale. Protejarea confidențialității asigură că informațiile sensibile rămân în siguranță, evitând astfel consecințe precum furtul de identitate sau pierderea datelor personale. Integritatea datelor se concentrează pe menținerea autenticității și a acurateții datelor, prevenind modificările neautorizate sau coruperea informațiilor. Disponibilitatea datelor asigură că acestea rămân accesibile și funcționale atunci când sunt necesare, evitând astfel întreruperile și downtime-ul. Pentru a contracara amenințările cibernetice, este esențial să implementăm măsuri de securitate adecvate, cum ar fi criptarea datelor, gestionarea vulnerabilităților, monitorizarea activităților și educația utilizatorilor. În plus, colaborarea între organizații și guverne este esențială pentru a combate amenințările la nivel global

Creșterea exponențială a dispozitivelor de internet a dus la riscuri mai mari de securitate și confidențialitate. Multe astfel de riscuri sunt atribuite vulnerabilităților dispozitivelor care decurg din criminalitatea cibernetică de către hackeri și utilizării necorespunzătoare a resurselor sistemului. Dispozitivele de internet trebuie construite astfel încât să asigure un control ușor și sigur al utilizării. Consumatorii au nevoie de încredere pentru a îmbrățișa pe deplin dispozitivele de internet pentru a se bucura de beneficiile acestuia și pentru a evita riscurile de securitate și confidențialitate. Majoritatea dispozitivelor și serviciilor de internet sunt expuse unui număr de amenințări comune, așa cum am discutat mai devreme, cum ar fi virușii și atacurile de refuzare a serviciului. Luarea unor pași simpli pentru a evita astfel de amenințări și gestionarea vulnerabilităților sistemului nu este suficientă; astfel, este necesară asigurarea unui proces de implementare a politicilor fără probleme, susținut de proceduri puternice.

BIBLIOGRAFIE

1. Abomhara M, M. Køien G. Cyber Security and the Internet of Things: Vulnerabilities, Threats, Intruders and Attacks. JCSANDM [Internet]. 2015 May 22 [cited 2023 Nov. 7]; 4(1): 65–88.
2. Aminzade, M. (2018). *Confidentiality, integrity and availability – finding a balanced IT framework. Network Security, 2018(5), 9–11.* doi:10.1016/s1353-4858(18)30043-6
3. Anderson, J. M. (2003). *Why we need a new definition of information security. Computers & Security, 22(4), 308–313.* doi:10.1016/s0167-4048(03)00407-3
4. Chai, K. Y., & Zolkipli, M. F.(2021). Review on confidentiality, integrity and availability in information security. Journal of ICT in Education, 8(2), 34-42. https://doi.org/10.37134/jictie.vol8.2.4.2021
5. Singh, Ajeet and Jain, Anurag, Study of Cyber Attacks on Cyber-Physical System (April 28, 2018). Proceedings of 3rd International Conference on Internet of Things and Connected Technologies (ICIoTCT), 2018 held at Malaviya National Institute of Technology, Jaipur (India) on March 26-27, 2018, Available at http://dx.doi.org/10.2139/ssrn.3170288
6. Sohrabi Safa, N., Von Solms, R., & Furnell, S. (2016). *Information security policy compliance model in organizations. Computers & Security, 56, 70–82.* doi:10.1016/j.cose.2015.10.006
7. Ravi S. Sandhu. 1993. On Five Definitions of Data Integrity. In Proceedings of the IFIP WG11.3 Working Conference on Database Security VII. North-Holland Publishing Co., NLD, 257–267.