UNIVERSITATEA POLITEHNICA DIN BUCUREŞTI

Şcoala Doctorală de Electronică, Telecomunicații și Tehnologia Informației

Decizie nr. 708 din 16.07.2021

TEZĂ DE DOCTORAT

- rezumat -

Ing. Eugen NEACȘU

PROTECȚIA INTEGRATĂ A SISTEMELOR INFORMATICE CRITICE

INTEGRATED PROTECTION OF CRITICAL INFORMATION SYSTEMS

COMISIA DE DOCTORAT

Prof. Dr. Ing. Gheorghe BREZEANU Universitatea Politehnica din Bucureşti	Preşedinte
Prof. Dr. Ing. Paul ȘCHIOPU Universitatea Politehnica din Bucureşti	Conducător de doctorat
Prof. Dr. Ing. Adrian TULBURE Universitatea 1 Dec. 1918 Alba Iulia	Referent
Prof. Dr. Ing. Ioan BACIVAROV Universitatea Politehnica din Bucureşti	Referent
CSI. Dr. Ing. Victor VLĂDĂREANU Institutul de Mecanica Solidelor al Academiei Române	Referent

BUCUREŞTI 2021

Cuprins

Capitolul 1

Introducere

Crearea unui sistem robust de securitate integrată presupune aderarea riguroasă la procesele de protecție digitală solidă. Numai atunci când securitatea digitală, fizică și cibernetică funcționează împreună, un sistem informatic poate fi considerat cu adevărat sigur. În acest context, primul capitol prezintă o introducere în domeniul tezei de doctorat, evidențiind oportunitatea sectorului ales privind protecția sistemelor informatice critice. Capitolul continuă cu detalierea obiectivelor lucrării, fiind sintetizat cu prezentarea structurii aferente.

1.1 Prezentarea domeniului tezei de doctorat

Cerința de rentabilitate și de arhitecturi moderne de sistem i-a făcut pe proprietarii de sistem să se îndrepte spre tehnologii interconectate. Aceste tehnologii oferă proprietarilor de active acces la arhitecturi deschise și tehnologii de comunicații îmbunătățite care nu erau disponibile anterior. Avantajele au fost imediate și semnificative, cu eficiență, funcționare și analiză îmbunătățită, disponibile pentru a ajuta beneficiarul să se asigure că infrastructura sa a funcționat în conformitate cu cerințele de securitate. Desigur, odată cu aceste oportunități de conexiune a venit o expunere crescută la risc, la scenarii de atac și la exploatări din surse externe.

1.2 Scopul tezei de doctorat

Prezenta lucrare relevă o incursiune a metodelor de securizare a sistemelor informatice critice, prezentând tehnici de protecție a fluxurilor informaționale, metode de administrare a securității sistemelor cât și o soluție integrată pentru protecția sistemelor informatice.

1.3 Conținutul tezei de doctorat

Teza de doctorat este compusă din 6 capitole, 8 anexe, lista tabelelor, lista figurilor și lista abrevierile folosite. Lucrarea se închide cu expunerea referințelor bibliografice apelate în corpul tezei.

Capitolul 1 reprezintă partea introductivă a tezei de doctorat, în care este expus conceptul de sistem informatic critic, dinamica tehnologiilor actuale cât și obiectivele majore necesar a fi implementate pentru a se asigura o securitate sporită a sistemelor. Capitolul continuă cu prezentarea obiectivelor principale ale tezei și cu expunerea conținutului acesteia.

Capitolul 2 detaliază conceptul de sistem informatic, prezentând principalele fundamente de securitate ce stau la baza acestuia. Totodată, în acest capitol sunt prezentate cele mai importante amenințări la adresa sistemelor informatice critice, tipuri de atacuri cibernetice, atât la nivel de hardware, cât și software, punând accent pe noile tendințe tehnologice, dar și măsuri de prevenție ce pot diminua posibilele pagube la nivelul sistemelor gestionate. Ca și contribuție originală, am efectuat o analiză de securitate cu privire la atacurile de tip phishing, arătând principalele defecte tehnice ale protocoalelor utilizate, metode de îmbunătățire a utilității serviciului dar și soluții de reducere a dificultății de implementare a protocoalelor anti-spoofing. Sunt necesare eforturi extinse pentru îmbunătățirea interfețelor de user pentru sistemele de e-mail, în scopul permiterii utilizatorilor să verifice proactiv rezultatele autentificării.

Capitolul 3 analizează principalele metode de securizare a comunicațiilor, axându-se pe acele protocoale necesare criptării traficului de date. Totodată, au fost punctate soluții eficiente de îmbunătățire a utilității și de reducere a dificultății de implementare a protocoalelor de securitate SIP, RTP și IPsec. O altă contribuție originală, prezentată în sfârșitul capitolului, este realizarea, implementarea și dezvoltarea unei rețele VoIP utilizând infrastructura PKI, fapt ce a dus la noi măsuri practice de configurare a rețelei pentru eliminarea potențialelor atacuri asupra sistemului.

Capitolul 4 integrează principalele metode de management informațional al sistemelor informatice. Capitolul prezintă atât aspecte teoretice, cât și practice, privind abordarea într-un mod coordonat a securității. Contribuția originală este dată de crearea unui model centralizat de securitate pentru infrastructurile critice, prin dezvoltarea unui plan de securitate aferent unui Centru de Date, cu rol de infrastructură critică, în care sunt concentrate instrumente vitale ce asigură integritatea serviciilor oferite.

Capitolul 5 prezintă o soluție optimă de administrare a securității la nivelul unui sistem informatic critic, prin dezvoltarea unui model standard de securizare a accesului la o bază de date, a traficului dintre aplicațiile utilizate și baza de date, cât și a integrității stocării informațiilor private – **Sistem de Securitate Integrat** (SSI). Prin constituirea acestui sistem am reușit implementarea unui model de analiză și detecție centralizată a principalelor evenimente informatice din cadrul unei infrastructuri critice. De asemenea, au fost create politici personalizate de securitate pentru sistemul de operare, necesare protejării datelor în fața vulnerabilităților extinse. O analiză și evaluare a fluxului de date a concis formarea unui pattern stabil de securitate ce contribuie în mod original la limitarea evenimentelor informatice, cât și la diminuarea posibilelor daune.

Capitolul 6 este dedicat principalelor contribuții privind protecția integrată a sistemelor informatice critice, axându-se consistent pe modelul de securitate creat și anume, Sistemul de Securitate Integrat. Acest concept informatic semnifică un progres în dezvoltarea protecției infrastructurilor critice, putând fi modificat facil pentru a permite un mod rapid de interogare a multiplelor sisteme gestionate. Totodată, capitolul prezintă principalele idei care au stat la baza acestei cercetări științifice complexe, evidențiază contribuțiile originale și se încheie prin exprimarea direcțiilor de dezvoltare ulterioară ale autorului.

Capitolul 2

Repere teoretice privind sistemele informatice

Al doilea capitol se axează pe noțiunile elementare privind sistemele informatice critice, evidențiind fundamentele de securitate ce stau la baza dezvoltării infrastructurii tehnologice. De asemenea, sunt prezentate principalele tipuri de atacuri informatice asupra sistemelor, lucru ce se concretizează printr-un studiu de caz propriu cu privire la noile tendințe de utilizare a instrumentelor de extragere a datelor de autentificare prin atacuri de tip phishing.

2.1 Rolul sistemelor informatice

Infrastructurile critice, ce conțin sisteme informatice interconectate, sunt infrastructuri cu scop decizional în protecția funcționării sistemelor, dar și în derularea proceselor informaționale. De regulă, aceste infrastructuri de care depind siguranța și stabilitatea proceselor, pot fi incluse în categoria IC speciale. Nu este neapărat necesar ca orice infrastructură ce este sau poate deveni, într-un anume moment, critică, să facă parte din aceeași categorie [4].

2.2 Fundamente de securitate

Politicile de securitate sunt rezultatul necesității integrării unui sistem informatic critic în noile contexte tehnice, economice și socio-umane. Prin abordarea unei politici de securitate, factorii decizionali transpun în practică conceptele și noțiunile articulate în mod unitar. Totodată, prin conceperea politicilor integrate se asigură protecția corespunzătoare a informațiilor vehiculate în cadrul organizației în scopul nealterării datelor transmise ori accesarea ilegală a tehnologiilor dezvoltate. Acest concept cuprinde securizarea personalului, a rețelelor informatice și de comunicații, a mediilor de stocare și a tuturor spațiilor în care își desfășoară activitatea organizația [6].

2.3 Atacuri cibernetice

Frecvența și întinderea atacurilor cibernetice continuă să crească și, cu toate acestea, în ciuda gravității problemei, rămâne extrem de dificil de diferențiat sursele unui atac. Atacurile cibernetice efectuate de o serie de entități reprezintă o amenințare crescândă pentru securitatea statelor și a cetățenilor acestora.

2.3.1 Categorii de amenințări

Există trei surse principale de amenințări: activiști, criminali cibernetici și entități statale iar - pe baza dovezilor - uneori este greu să le diferențiem. Într-adevăr, uneori pot lucra împreună atunci când interesele lor sunt aliniate. Frecvența și severitatea crescândă a atacurilor face mai importantă ca oricând înțelegerea sursei. Știind cine a planificat un atac ar putea facilita capturarea vinovaților sau încadrarea unui răspuns adecvat. În plus, există riscul ca un atac cibernetic să fie atribuit greșit sau confundat cu un atac guvernamental și să declanșeze un război cibernetic sau fizic mai larg. Alternativ, un hack sponsorizat de guverne poate fi deghizat ca un caz de cyberactivism sau criminalitate cibernetică pentru a evita un răspuns tip - guvern la guvern [11].

2.3.2 Tipuri de atacuri cibernetice

Riscurile de securitate sunt precum virusurile, iar securitatea cibernetică este medicamentul. Amândouă vin sub diferite forme. Pentru a elimina riscurile de securitate, trebuie să implementăm tehnologia adecvată. Cu alte cuvinte, trebuie să cunoaștem diferitele tipuri de atacuri cibernetice pentru a veni cu cel mai bun mod de a le gestiona.

Următoarele amenințări privind securitatea cibernetică sunt cele mai răspândite tipuri de atacuri la nivelul sistemelor informatice [13]:

a) atac de tip phishing – phishing-ul este un tip înșelăciune în care site-urile web false, e-mailurile false și mesaje text sunt trimise prin intruziunea unei surse legale, cum ar fi o bancă. Astfel de e-mailuri sunt adesea trimise pentru a obține parola utilizatorului și detaliile cardului de credit. În această formă de activitate, utilizatorul este deseori rugat să își actualizeze sau să-și aprobe conturile pentru a obține informațiile sale personale. Facebook a devenit rampă de lansare pentru atacuri de tip phishing. Conturile infectate au trimis linkuri malware către alte persoane prin intermediul aplicației Messenger. Putem evita phishing-ul astfel: nu deschidem atașamentele nedorite, nu accesăm link-urile necunoscute primite pe e-mail. Se recomandă deschiderea manuală a link-ului în browser. De asemenea, verificăm antetele înainte de a deschide un e-mail de la un cunoscut;
b) atac de tip ransomware – ransomware este o formă de malware, care, după restricționarea accesului la fișiere și computere, îi obligă pe utilizatori să efectueze plata pentru a elimina restricțiile. E-mailurile de phishing sunt exemple frecvente de injecții cu ransomware. Acesta este practic de două tipuri: ransomware cu criptare și ransomware cu ecran de blocare. Ransomware-ul cu criptare împiedică utilizatorul să acceseze un fișier de pe hard disk-ul computerului criptându-le, în timp ce ransomware-ul cu ecran de blocare oprește accesul la computer prin metode de tip imagine. Pentru a obține acces la computer, ransomware-ul va afișa o notificare sau un avertisment pe computer că a fost blocat și solicită plata pentru a-l debloca. Putem preveni

astfel de atacuri efectuând back-up des. Este recomandat a nu se plăti niciodată răscumpărarea și este necesară anunțarea instituțiilor abilitate;

c) atac de tip brute force - în această metodă hacker-ul folosește toate combinațiile de taste posibile pentru a decripta textul cifrat și a-l converti în text simplu pentru descifrarea mesajului care este transmis. Această metodă devine din ce în ce mai dificil de utilizat cu sistemele criptografice moderne, deoarece cantitatea de timp, bani, resurse și energie care ar fi necesare pentru a sparge codul nu ar justifica în mod normal eforturile depuse în acest sens. Uneori atacatorul preia mai multe bucăți diferite de text cifrat care au fost generate de același sistem criptografic pentru a le analiza pentru un model comun care ar putea duce la un indiciu pentru ruperea lor. Chiar și această tehnică este foarte dificilă cu sistemele informatice moderne care sunt concepute în așa fel încât să evite orice încercări de analiză statistică. O tehnică similară este utilizată în combinație cu brute force și este cunoscută drept atac meet-in-the-middle;
d) atac de tip Man in the Middle - când presupunem că trimitem date către un singur site, dar, în realitate, acestea sunt redirecționate și către alte surse, această condiție este cunoscută sub numele de atacurile omului din mijloc (Man in the Middle). De obicei, apare din cauza programelor malware inactive care sunt prezente pe sistem de ceva timp. Va părea că introducem datele într-o rețea potrivită, dar în realitate nu este așa. Ne putem apăra prin rularea programelor antivirus actualizate pe toate dispozitivele, inclusiv pe telefoane;
e) atac de tip fragmentare - este folosit ca metodă de a obține pachete în jurul unui firewall de filtrare a pachetelor. Într-un atac de fragmentare de bază, pachetele sunt împărțite în fragmente, primul pachet conținând datele complete ale antetului. Pachetele rămase nu conțin informații despre antet. Deoarece unele routere filtrează pachetele pe baza acestor informații de antet, pachetele rămase fără date de antet nu sunt filtrate și trec prin firewall.

Studiu de caz: Analiză de securitate a atacurilor de tip phishing.

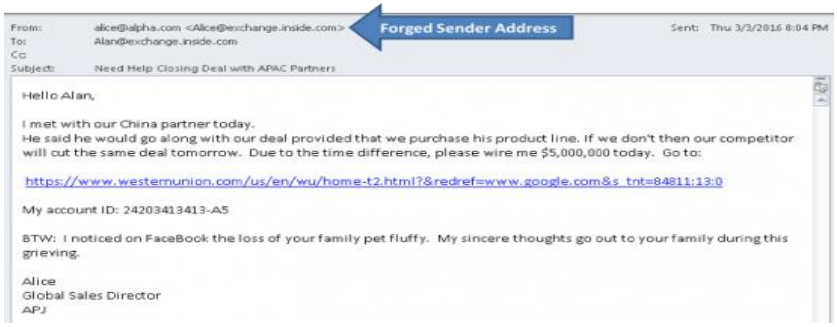

Figura 2.8 *Spoofing e-mail [15]*

Pentru a efectua un atac tip phishing, atacatorii pot manipula două câmpuri cheie pentru a trimite e-mailuri. Mai întâi, după stabilirea unei conexiuni SMTP la serverul de mail țintă, atacatorul poate folosi comanda MAIL FROM și poate seta adresa expeditorului oricui dorește să-l identifice. După aceea, adresa MAIL FROM este inserată în antet ca *Return-Path*. În plus, atacatorii pot modifica un alt câmp numit *From*

în antetul e-mailului. Acest câmp *From* specifică adresa care va fi afișată pe interfața de e-mail. Când un utilizator primește e-mailul, utilizatorul va vedea adresa *From* (de exemplu: alice@alpha.com în Figura 2.8). Dacă utilizatorul răspunde la e-mail, mesajul de răspuns va merge la *Return-Path* setat de MAIL FROM. De reținut faptul că cele două adrese nu sunt neapărat aceleași. Spoofingul prin e-mail este un pas critic al atacurilor de phishing pentru a câștiga încrederea victimei. Între timp, falsificarea este, de asemenea, un semnal puternic al atacurilor. Rezultatele detectării falsurilor sunt adesea folosite de sistemele de detectare a phishing-ului [16].

Pentru a detecta și preveni falsificarea e-mailurilor, sunt propuse protocoale SMTP de extensie: SPF, DKIM și DMARC. Toate cele trei protocoale au fost publicate sau standardizate de Internet Engineering Task Force (IETF).

Defecte tehnice ale protocoalelor: în primul rând, SPF și DKIM întâmpină ambele problema *identifier alignment*. Înseamnă că adresa de e-mail a expeditorului pe care o vede un utilizator poate fi diferită de adresa utilizată efectiv pentru efectuarea autentificării. Pentru SPF, autentificarea se concentrează pe *Return-Path* și examinează dacă adresa IP a expeditorului este listată în înregistrarea SPF a domeniului *Return-Path*. Un atacator poate seta domeniul *Return-Path* la propriul domeniu și poate seta înregistrarea SPF pentru a trece autentificarea. Cu toate acestea, ceea ce vede utilizatorul receptor pe interfața de e-mail este setat de câmpul *From*. DKIM are o problemă similară, dat fiind faptul că domeniul de semnare a e-mailului cu cheia DKIM poate fi diferit de domeniul de pe *Return Path*. DMARC ajută la rezolvarea problemei prin aplicarea alinierii identificatorilor. În al doilea rând, redirecționarea e-mailurilor este o problemă pentru SPF. Redirecționarea prin e-mail înseamnă că un serviciu de e-mail redirecționează automat e-mailurile către alt serviciu. Un scenariu obișnuit este acela că utilizatorii își configurează adesea serviciul de e-mail pentru a redirecționa toate e-mailurile către Outlook sau Gmail. În timpul redirecționării prin e-mail, metadatele de e-mail (de exemplu: *Return-Path*) rămân neschimbate. SPF va eșua după redirecționarea e-mailului, deoarece adresa IP a expeditorului nu se va potrivi cu înregistrarea SPF a expeditorului original. În al treilea rând, listele de corespondență reprezintă o problemă majoră atât pentru SPF, cât și pentru DKIM. Când un mesaj este trimis către o listă de corespondență, aceasta va difuza mesajul către toți abonații. Acesta este un proces similar cu redirecționarea e-mailurilor. În timpul acestui proces, adresa IP a listei de corespondență va deveni adresa IP a expeditorului, care este diferită de adresa IP a expeditorului original. Acest lucru va duce la eșecul SPF. Listele de corespondență vor cauza probleme DKIM, deoarece majoritatea listelor de corespondență modifică conținutul e-mailului înainte de a-l transmite abonaților. Modificarea obișnuită constă în adăugarea unui *footer* cu numele listei de corespondență și un link pentru dezabonare. Temperarea conținutului e-mailului va provoca eșecul DKIM. DMARC ajută la rezolvarea unora dintre probleme, dar nu și la problema listei de corespondență. Pentru listele de corespondență, DMARC+SPF va eșua sigur - dacă *Return-Path* este modificat, DMARC va eșua din cauza nealinierii identificatorilor; dacă *Return-Path* este nemodificat, SPF va eșua din cauza nepotrivirii IP. Pentru DMARC+DKIM, va eșua dacă lista de corespondență trebuie să modifice conținutul e-mailului.

2.3.3 Măsuri de prevenție

Având în vedere gama de elemente de securitate, ne putem rezuma la 5 obiective pe care trebuie să le implementăm pentru a furniza un nivel de securitate ridicat la nivelul sistemelor informatice critice:

1. evaluarea securității - este vital să evaluăm standardele de securitate. Hardware-ul și software-ul ar trebui să fie actualizate în mod constant pentru a rezista la cele mai recente atacuri cibernetice. În afară de aceasta, este esențială prioritizarea securității serverelor;
2. control centralizat - în orice sistem informatic, există o varietate de dispozitive, software și configurații de rețea implicate. Ca atare, este crucial să beneficiem de o configurație care să permită controlul tuturor bazelor de date interconectate și gestionarea centralizată în orice platformă de securitate cibernetică;
3. menținerea standardelor de securitate – realizarea unui program de analiză pentru detectarea activităților neobișnuite. Acesta reprezintă un mod eficient de a rezolva problemele de securitate. De fiecare dată când sistemul este utilizat, acest program trebuie să devină activ. Dacă sistemul este utilizat dintr-un loc necunoscut, programul poate bloca accesul și poate salva informațiile relevante. În plus, acest program este capabil să detecteze orice fel de instalare de program rău intenționat;
4. instruirea personalului - hackerii obțin adesea acces prin aplicații mobile, e-mailuri, link-uri corupte etc. Majoritatea angajaților nu sunt conștienți de aceste pericole, oferind hacker-ilor acces la informații sensibile. Este important ca personalul să fie instruit împotriva acestor tipuri de vulnerabilități, prin cursuri specializate în domeniul INFOSEC, cât și proceduri proprii de utilizare a sistemelor;
5. respectarea legislației în domeniu - pentru a conștientiza necesitatea securității și pentru a ne asigura că luăm măsuri de securitate adecvate, trebuie aplicate anumite legi de reglementare. De exemplu, Uniunea Europeană are GDPR (Regulamentul general privind protecția datelor) pentru a impune companiilor să respecte procedurile de securitate. Nerespectarea acestor politici duce la amenzi masive, asigurându-se astfel faptul că organizațiile rămân în siguranță în fața potențialelor amenințări.

2.4 Contribuții

Securitatea rețelei se învârte în jurul celor trei principii cheie ale confidențialității, integrității și disponibilității. În funcție de aplicație și context, unul dintre aceste principii ar putea fi mai important decât celelalte.

Analiza conceptului de sistem informatic, secțiunea 2.1, a presupus detalierea elementelor componente, a indicatorilor care reflectă starea de securitate a organizației, elementele de identificare și criteriile care stau la baza performanței sistemelor informatice critice.

În secțiunea 2.2 am reliefat procesul de implementare a politicilor de securitate necesare securizării infrastructurilor gestionate, axându-mă pe cele două abordări prezentate: abordarea funcțională și cea structurală a sistemului informatic. În continuare, am definit și exemplificat elementele componente ale SI: baza informațională, baza tehnică, sistemul de programare, baza științifică și metodologică, resursa umană, cadrul organizatoric. Deși literatura de specialitate nu oferă suficiente detalii referitoare la interdependențele SI, am prezentat trei problematici principale ale acestora, reușind să identific majoritatea abordărilor ce vizează un întreg sistem de infrastructuri critice interdependente care interacționează între ele.

În secțiunea 2.3, după ampla prezentare a principalelor atacuri cibernetice la adresa sistemelor informatice, am adus o contribuție originală prin efectuarea unui studiu de caz privind analiza de securitate a atacurilor de tip phishing, rezultând următoarele aspecte:

- ✓ în primul rând, se evidențiază o nouă perspectivă asupra valorilor și preocupărilor percepute ale protocoalelor anti-spoofing din perspectiva furnizorilor de e-mail. Aceste rezultate arată motivele care stau la baza adoptării lente a SPF, DKIM și DMARC, subliniind principalele direcții de optimizare;
- ✓ în al doilea rând, se prezintă implicația cheie a rezultatelor pentru proiectanții de protocol, furnizorii de e-mail și utilizatorii. Discutăm despre soluțiile posibile user-end, pentru a compensa posibila autentificarea defectă a serverului.

În partea finală a capitolului se prezintă principalele contramăsuri pe care trebuie să le implementăm pentru a furniza un nivel de securitate ridicat la nivelul sistemelor informatice critice.

Capitolul 3

Protecția sistemelor informatice critice

Al treilea capitol prezintă o incursiune în securizarea sistemelor informatice, prezentând principalele protocoale de securizare a comunicațiilor, metode de implementare și necesitățile actuale ale sistemelor de comunicații de mare întindere. În finalul capitolului este simulată operabilitatea unui sistem informatic critic, prin realizarea practică a unei rețele VoIP, oferind o optimizare a implementării unor politici de securitate la nivelul rețelelor de comunicații în scopul protecției datelor cu caracter confidențial.

3.1 Considerații generale

În prezent, cele mai eficiente metode de păstrare a integrității și confidențialității informației sunt date de tehnicile criptografice. Lucrarea de faţă realizează o incursiune în aceste tehnici de securizare a informaţiei și propune soluții, atât comunităţii criptografice cât şi specialiștilor în administrarea și securizarea sistemelor informatice.

Infrastructura cu chei publice (PKI) este un termen general pentru tot ceea ce este folosit pentru a stabili și gestiona criptarea cheii publice, una dintre cele mai comune forme de criptare pe Internet. Este inclus în fiecare browser web utilizat astăzi pentru a asigura traficul public, dar organizațiile îl pot implementa și pentru a-și asigura comunicațiile interne și accesul la dispozitivele conectate. Cel mai crucial concept implicat în PKI este, după cum sugerează și numele său, cheile criptografice publice care se află în nucleu său. Aceste chei, nu numai că fac parte din procesul de criptare, dar ajută la autentificarea identității părților sau dispozitivelor care comunică.

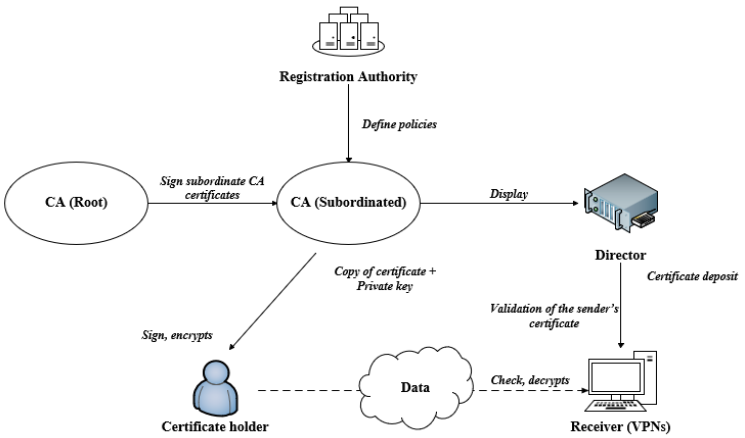

Figura 3.6 *Structura PKI [6]*

Certificatele PKI sunt documente care acționează ca pașapoarte digitale, atribuite oricărei entități care dorește să participe la o conversație securizată PKI. Pot include destul de multe date. Una dintre cele mai importante informații pe care le include un certificat este cheia publică a entității. Certificatul este mecanismul prin care este distribuită cheia respectivă. Dar există și piesa de autentificare. Un certificat include o atestare de la o sursă de încredere că entitatea este cea care pretinde că este. Această sursă de încredere este în general cunoscută sub numele de autoritate de certificare (CA). PKI este excelent pentru securizarea mesageriei din același motiv pentru care este excelent pentru securizarea traficului web: datele care circulă pe Internetul public pot fi interceptate și citite cu ușurință dacă nu sunt criptate și poate fi dificil să ai încredere că expeditorul este cine pretinde a fi dacă nu există o modalitate de a-și autentifica identitatea.

3.2 Tehnici de securizare a comunicațiilor

3.2.1 Securizarea SIP

Protocolul SIP (Session Initiation Protocol) reprezintă un protocol dezvoltat în scopul stabilirii, modificării şi încheierii unei sesiuni multimedia peste Internet, deținând funcţionalităţi de livrare a mesajelor. Din punctul de vedere al utilizatorului, principalul avantaj al protocolului SIP reprezintă furnizarea unui mod de adresare al cărui format nu impune memorarea de adrese IP, capacitatea de înregistrare într-un server şi de a efectua apeluri utilizând acelaşi ID de la PC-uri diferite sau posibilitatea de a trimite apeluri către alţii. Protocolul de semnalizare funcționează ca un standard central pentru un model de comunicaţii şi denumește o arhitectură VoIP ce cuprinde diferite tipuri de entităţi comunicante şi comportamentul acestora [38].

3.2.2 Securizarea RTP

RTP este protocolul ce furnizează servicii de livrare pentru date ce se bazează pe caracteristica de timp real (mesaje audio şi video interactive). RTP utilizează protocolul UDP. Deşi nu asigură calitatea serviciilor în reţelele IP, furnizează mijlocul de detectare a unor evenimente importante în contextul transmisiilor multimedia cum ar fi: pierderile de pachete, sosirile de pachete şi întârzierile variabile în livrarea pachetelor. Protocolul nu corectează aceste probleme, lăsându-le pe seama protocoalelor de nivel mai înalt precum codecul sau aplicaţia VoIP [48].

3.2.3 Securizarea IPsec

Securizarea IPsec are la bază algoritmi de criptare/autentificare și funcții matematice, în scopul asigurării integrității, confidențialității și non-repudierii informațiilor conținute în fiecare pachet IP ce este trimis prin rețea. Funcționalitatea IPsec se bazează

pe proprietățile criptografice ale unor algoritmi celebrii (cum ar fi: Diffie-Hellman, RSA, DES, AES). În momentul de față, IPsec este printe cele mai folosite tehnologii utilizate în criptarea transmisiei pe Internet. Față de SSL (Secure Sockets Layer) și TLS (Transport Layer Security), IPsec se găsește la nivelul III al stivelor TCP/IP și ISO-OSI, făcând posibilă securizarea aplicațiilor ce folosesc această stivă [66].

3.3 Implementarea unei rețele VoIP

Pentru ilustrarea rețelei de comunicații de mare întindere VoIP, am ales platforma Cisco Packet Tracer (varianta 7.1.1). Implementarea acestei soluții necesită resurse scăzute datorită arhitecturii practice a platformei utilizate. Pentru început vom adăuga pe platformă următoarele componente: 1 router 2811, 2 unități PC, 2 IP Phone și 1 switch 2960 [74].

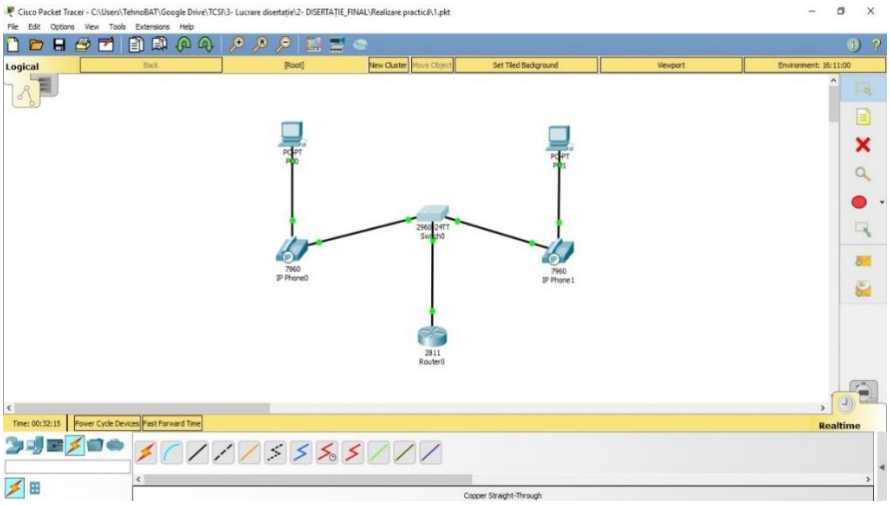

Figura 3.32 *Interconectare rețea*

Pentru a demonstra funcționalitatea rețelei vom apela de pe IP Phone 1 (93001) numărul aferent IP Phone 2 (93002).

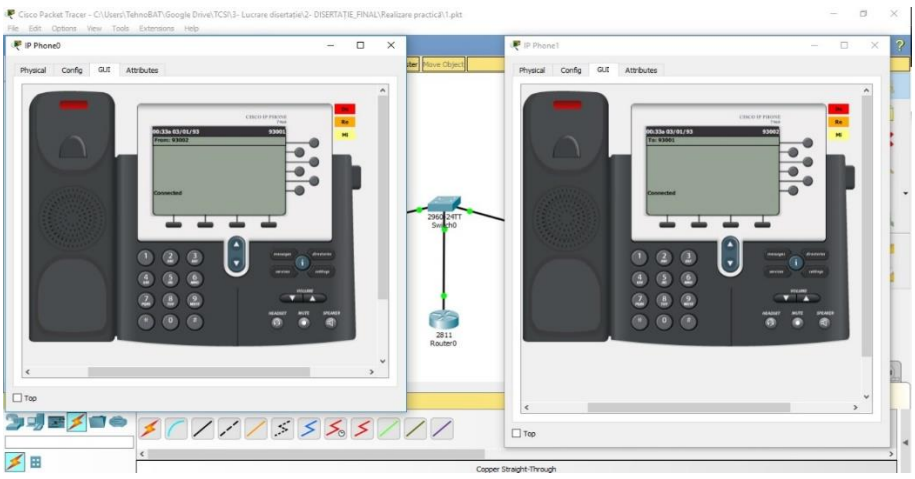

Figura 3.34 *Conectare VoIP*

Din figura 3.34 se poate observa faptul că rețeaua VoIP creată este funcțională, iar conexiunea dintre cele două IP Phone-uri este reușită.

În cazul în care traficul VoIP nu deține nicio metodă de securizare, este foarte ușor pentru un atacator să intercepteze traficul din rețea, acesta putând chiar reconstitui întreaga convorbire. Din acest considerent este utilă o cât mai bună protecție a rețelei și o atenție constată asupra vulnerabilităților ce există la nivelul sistemelor de comunicații.

Studiu de caz: Analiză de securitate a rețelei VoIP.
Atacul asupra traficului VoIP nu diferă față de cel asupra unei rețele obişnuite, în schimb conectarea la o reţea VoIP diferă faţă de cea la o reţea obişnuită. În timp ce serverele de mail, DHCP, DNS sunt accesibile prin anumite VLAN-uri, reţelele VoIP sunt în VLAN-uri separate. Atacatorii care nu sunt conectaţi în segmentul corect de reţea nu vor putea să iniţializeze atacul. Separarea serviciilor în VLAN-uri constituie o măsură importantă de prevenire a atacurilor. Un VLAN poate fi folosit în multe scopuri, inclusiv pentru securitate, QoS, segmentare, niveluri de prioritate. Pachetele VoIP trebuie să aibă o prioritate mai mare față de pachetele de date întrucât, persoanele care folosesc telefoanele VoIP nu trebuie deranjate în privința calității audio de procesul de transfer de date inițializat de către altcineva.

3.4 Contribuții

Capitolul 3 prezintă o analiză detaliată a principalelor metode de protecție a sistemelor informatice, pornind de la elementul cheie (informația) până la criptarea comunicațiilor de mare întindere, abordând problematicile de securitate aferente.

Secțiunea 3.1 prezintă considerații esențiale din domeniul comunicațiilor, fiind o complementare pentru protecția sistemelor informatice, abordând atribute tehnologice esențiale ale infrastructurii cu chei publice (PKI). Aceasta oferă posibilitatea de a îndeplini cerințele minime de securitate prin generarea certificatelor, verificarea construcției generate de cheile publice, validarea semnăturilor electronice, stocarea și accesibilitatea CRL-urilor, dar și definirea politicilor de grup în concordanță cu principiile de utilizare a criptografiei. Totodată, infrastructura PKI este esențială pentru implementarea criptografiei în cadrul aplicațiilor ce presupun sesiuni de comunicații securizate. Principalele beneficii se regăsesc prin: posibilitatea de protecție a aplicațiilor INTRANET/EXTRANET (riscul fiind diminuat de utilizarea protocoalelor de securitate), asigurarea integrității datelor transmise în rețea utilizând algoritmi criptografici puternici (AES, RSA etc.), autentificare la nivelul sistemului de operare, dar și stocarea securizată a cheilor asociate. O contribuție originală în acest subcapitol este reprezentată de analiza comparativă a algoritmilor cu cheie publică/cheie privată, evidențiind avantajele și caracteristicile specifice fiecăruia.

În secțiunea 3.2 sunt abordate principalele tehnici de securizare a comunicațiilor, utilizând protocoalele SIP, RTP și IPsec. Protocolul SIP prezintă avantajul procurării unui mod de adresare ce nu impune menținerea de adrese IP, fiind utilizat același ID

pentru înregistrarea pe server și pentru realizarea de apeluri. RTP furnizează o modalitate de detecție a principalelor evenimente în cadrul transmisiilor de date multimedia (pierderi/sosiri/întârzieri de pachete de date), utilizând servicii de livrare pentru informații ce sunt fundamentate pe caracteristica de timp real (audio, video). IPsec reprezintă o metodă de securizare răspândită în mediile LAN (client-server), având la bază algoritmi de criptare și funcții matematice, utilizarea sa asigurând principalele mecanisme de securitate (ESP, AH, IKE). O altă contribuție originală constă în analiza pachetelor de date aferente fiecărui protocol în parte, oferind informații vitale despre vulnerabilitățile de securitate în utilizarea lor.

Contribuția principală în cadrul acestui capitol a fost implementarea și criptarea conexiunilor VoIP și videoconferință utilizând infrastructura PKI, efectuând și o analiză de securitate a principalelor vulnerabilități, rezultând următoarele (secțiunea 3.3):

- ✓ flexibilitate în implementare. În acest fel, se evită întreţinerea unei infrastructuri complexe de tunele VPN în condiţiile în care există o infrastructură PKI ce pune la dispoziţie certificatele şi cheile;
- ✓ se evită problemele puse de protocolul IPsec în cazul unei infrastructuri NAT;
- ✓ încărcarea suplimentară a pachetelor de date datorită antetelor adăugate în cazul în care se foloseşte SRTP este considerent mai mică față de IPsec, oferind un avantaj în cazul conexiunilor cu bandă mică;
- ✓ transmiterea fluxului media (voce şi video) în cazul SRTP se face prin protocolul UDP care este un protocol fără confirmare. Este mai puţin susceptibil la întârzieri față de protocolul TCP din cazul IPsec. Refacerea convorbirii în cazul unor pachete pierdute cade în seama codec-urilor folosite;
- ✓ adoptarea infrastructurii PKI în vederea implementării protocolului TLS este absolut necesară pentru protejarea conexiunii, ceea ce oferă avantajul că informaţiile critice ce pot afecta securitatea comunicaţiilor transmise prin SRTP sunt inaccesibile în faţa unor potenţiale interceptări.

Capitolul 4

Managementul securității informaționale

Managementul securității informaționale este o măsură proactivă care permite companiilor să identifice cu precizie și să consolideze imediat apărarea, fiind astfel cu un pas înaintea criminalilor cibernetici. Capitolul prezintă atât aspecte teoretice, cât și practice, privind managementul securității la nivelul unei infrastructuri critice, fiind realizat un plan de securitate al unui Centru de Date ce evidențiază o abordare coordonată a securității sistemelor informatice ce integrează toate resursele disponibile pentru asigurarea protecției infrastructurii critice.

4.1 Administrarea centralizată a securității

Un model centralizat ar părea alegerea corectă. Prin direcționarea și gestionarea securității în cadrul unui organism central, se oferă o supraveghere mai bună a posibilelor breșe de securitate. Administrarea centralizată este, în general, cea mai eficientă, deoarece resursele pot fi gestionate într-un mod rentabil în întreaga infrastructură, limitând astfel duplicarea eforturilor și utilizând mai bine resursa umană și instrumentele informatice. Se realizează, de asemenea, o oarecare sustenabilitate, deoarece în cazul apariției unui incident, acesta poate fi tratat într-un mod uniform, în cel mai scurt timp.

4.2 Plan de securitate

Prin planul de securitate sunt identificate soluțiile de securitate existente sau care sunt puse în aplicare pentru protecția elementelor de infrastructură critică. Toate datele din acest plan sunt fictive, fără a conține informații sensibile. Se va alege o infrastructură critică (Centrul de Date) denumită DATANET SYSTEMS [79].

4.2.1 Descriere organizațională

Centrul de Date DATANET SYSTEM dispune de un număr de 50 de angajați (personal de securitate: 25, personal administrativ: 5, personal de pază: 15, personal conducere: 5).

4.2.2 Analiza mediilor de securitate

Analiza riscurilor la adresa securității se bazează pe scenariile de amenințări, identificarea punctelor vulnerabile ale fiecărui element al CD și impactul asupra acestuia în cazul producerii unui eveniment nedorit (în cazul exploatării unei vulnerabilități de către o amenințare).

4.2.3 Managementul PSO

Serviciile din cadrul Compartimentului INFOSEC cu atribuții în domeniul securității infrastructurii critice sunt în subordinea directă a directorului.

4.2.4 Managementul riscului

Măsurile de prevenire, control și diminuare a riscului derivă din evaluarea de risc efectuată. Identificarea, selectarea și stabilirea priorităților în ceea ce privește contramăsurile și procedurile, realizându-se distincție între măsurile permanente - măsurile permanente de securitate (de natură tehnică), care identifică investițiile de securitate indispensabile și măsurile nepermanente de securitate (de natură organizatorică), care pot fi activate gradual în funcție de diferitele niveluri ale riscurilor și amenințărilor identificate [79].

4.2.5 Niveluri de alertă

Nivelurile de alertă sunt stabilite pentru punerea în aplicare a măsurilor de securitate în momentul producerii unui eveniment cu impact asupra CD. Măsurile preventive sunt întreprinse pentru a menține la un nivel acceptabil securitatea CD, precum și pentru a permite furnizarea continuă a serviciilor specifice. Diseminarea informației privind nivelul de alertă se face ierarhic, conform organigramei Centrului, prin mijloacele de comunicare normale [79].

4.3 Contribuții

Complexitatea amenințărilor la adresa sistemelor informatice critice – parte a infrastructurilor naționale, din ce în ce mai interconectate, fac necesară stabilirea și funcționalitatea condițiilor de securitate a sistemelor gestionate. Protecția integrată a infrastructurilor critice pe teritoriul național pleacă de la principiul confidențialității, ceea ce presupune reducerea vulnerabilităților de securitate prin flexibilitatea adaptării la interesele naționale; de asemenea, este esențială pentru protejarea cetățenilor, securitatea serviciilor furnizate, dar și pentru integritatea teritorială a României.

În acest context, capitolul începe cu secțiunea 4.1 ce prezintă un rol esențial în buna guvernare a unei infrastructuri critice și anume, administrarea securității. Este absolut necesar ca această administrare să se facă centralizat deoarece, prin furnizarea tuturor evenimentelor la nivel de NOC, poți obține un timp de răspuns mult mai mic pentru reacția la evenimentele/incidentele de securitate. Totodată, rezultatele evenimentelor din interiorul organizației trebuie bine cunoscute în cadrul departamentului INFOSEC ce administrează tot ce ține de sisteme, fiind benefică elaborarea unei proceduri de reacție rapidă pentru fiecare tip de atac cunoscut. Cele mai dificile situații de eliminare a posibilelor surse de risc este resursa umană, deoarece aceasta poate fi ademenită în scopul penetrării din interior a camerelor de comunicații ce au sisteme informatice de tip stand-alone și conțin principalele credențiale necesare administrării întregii infrastructuri critice. Personalul trebuie instruit, specializat și verificat periodic.

Secțiunile următoare (4.2.1 ÷ 4.2.5) aduc contribuții originale prin crearea unui mod de securizare complet (protecție fizică, personal, procedurală, INFOSEC), plecând de la constituirea unei organizări funcționale a unei infrastructuri critice, până la realizarea managementului de securitate. Amenințările potențiale se pot materializa într-un spectru foarte larg, cum ar fi proliferarea, terorismul internațional, răspândirea criminalității organizate sau pandemiile (COVID-19). În plus, globalizarea pune și mai multă presiune pe amenințările existente cu, consecințe directe pe care le agravează cererea de energie, schimbările climatice, urbanizarea, criza economică actuală, precum și creșterea demografică și consecințele sale socioeconomice. Toate aceste amenințări potențiale prezintă un risc de securitate pentru infrastructurile noastre critice, care sunt vulnerabile la efectele unui atac. De asemenea, reziliența cibernetică ilustrează importanța interfețelor și a conexiunilor bazelor de date. Importanța interacțiunii și dependențelor este evidentă: sunt elemente esențiale pentru evaluarea sensibilității sistemului în ansamblu. Nu numai că diferitele sectoare sau subsectoare sunt critice, dar dependența lor reciprocă este crucială pentru scenariile în care vor prevala efectele în cascadă. În acest domeniu se desfășoară cercetări pentru toate scenariile de atac posibile.

Schimbul rapid de informații cu privire la potențialele amenințări și vulnerabilități joacă un rol crucial. Ca atare, a devenit necesară o rețea specifică: CIWIN (Critical Infrastructure Warning Information Network). Această rețea îndeplinește două funcții: este primul și cel mai important forum electronic pentru schimbul de informații legate de CIP (Critical Infrastructure Protection); mai mult, servește ca o funcționalitate rapidă de alertă între statele membre pentru a informa autoritățile responsabile cu privire la riscurile și amenințările comune. Toate statele membre au semnat un memorandum de înțelegere pentru a contribui la participarea operațională în rețea. Modul în care trebuie asigurate aceste informații este încă în curs de dezvoltare. Dacă vorbim de infrastructurile critice europene, acestea sunt desemnate în funcție de cea mai mare importanță pentru comunitate și care, dacă sunt perturbate sau distruse, ar produce disfuncționalități în cadrul mai multor state membre. Aceasta include efectele transfrontaliere rezultate din interdependențele dintre infrastructurile interconectate din diferite sectoare.

Contribuția principală a acestui capitol este realizarea unui plan de securitate complet al unui operator de Centru de Date (analiza mediilor de securitate, managementul centralizat al securității, analiza riscurilor la adresa sistemelor informatice critice, managementul riscului). Practic, acest instrument reprezintă integrarea tuturor politicilor de securitate prezentate la nivelul unei infrastructuri critice ce are în componență un Centru de Date cu sisteme informatice critice în gestiune, date privind riscurile, amenințările și punctele vulnerabile ale infrastructurii, măsuri de prevenire a producerii incidentelor de securitate dar și un sistem de alertare pe niveluri prioritare. Planul de securitate a fost realizat prin îndrumarea metodologică a organizațiilor deținătoare de infrastructuri critice.

Capitolul 5

Contribuții privind implementarea unui Sistem de Securitate Integrat

În acest capitol este conceput un Sistem de Securitate Integrat (**SSI**) în scopul securizării bazelor de date. Informațiile sunt o entitate valoroasă care trebuie să fie tratate și gestionate ferm, ca în cazul oricărei resurse economice. Deci, o parte sau toate datele pot avea importanță tactică pentru organizația respectivă și, prin urmare, trebuie să fie păstrate în mod protejat și confidențial. Documentația realizată este rezultatul întregului studiu privind protecția sistemelor informatice critice.

5.1 Definirea obiectivelor și a cerințelor de securitate

Auditul bazei de date este activitatea de monitorizare și înregistrare a acțiunilor de configurare de la *useri database* și *useri nondatabase*, pentru a asigura securitatea bazelor de date. Există cinci obiective principale pentru a dezvolta o pistă de audit:

1) auditul standard al aplicațiilor;
2) pista de audit la nivel de aplicație;
3) auditarea evenimentelor bazei de date;
4) auditul declanșatorului bazei de date;
5) audit extern.

5.2 Sistem de Securitate Integrat (SSI)

Pentru a asigura protecția informațiilor stocate în mod eficient administrarea securității necesită controale adecvate, care sunt distincte într-o misiune, cât și un scop specific pentru sistem. **SSI** îmbină sistemele de securitate multi-nivel și le integrează într-o singură soluție. Cerința de a obține o protecție adecvată, deși a fost adesea neglijată sau trecută cu vederea, este acum din ce în ce mai pregnantă.

5.2.1 Etapa de implementare

SSI conține mai multe mecanisme disponibile care trebuie să existe atunci când asigurăm securitatea bazele de date:

- ✓ redactarea din timp a datelor sensibile în rezultatele interogării SQL, înainte de afișarea aplicației, astfel încât utilizatorii neautorizați să nu poată vizualiza datele sensibile. Permite redactarea consecventă a coloanelor bazei de date între modulele aplicației care accesează aceleași informații despre baza de date. Redactarea datelor minimizează modificările aplicațiilor, deoarece nu modifică datele reale din stocarea bazelor de date interne și păstrează tipul de date și formatarea originale atunci când datele transformate sunt returnate aplicației. Redactarea informațiilor nu are impact asupra activităților operaționale ale bazei de date, cum ar fi copierea de rezervă și restaurarea, actualizarea și corecția, precum și asupra clusterelor cu disponibilitate ridicată;
- ✓ mascarea datelor ofensează datele sensibile înlocuindu-le cu alte date – de obicei caractere care vor îndeplini cerințele unui sistem conceput pentru a testa sau a lucra în continuare cu rezultatele mascate. Mascarea asigură faptul că părțile vitale ale informațiilor de identificare personală (PII) – cum ar fi primele șase cifre ale unui cod numeric personal – sunt ascunse sau dezidentificate în alt mod;
- ✓ criptarea datelor se realizează prin conversia și transformarea datelor în text cifrat codat, utilizând calcule matematice și algoritmi ilizibili. Restaurarea mesajului necesită un algoritm de decriptare corespunzător și cheia de criptare originală.

SSI reprezintă un model standard de hardening (securizare) a accesului la o bază de date, a traficului dintre aplicație și baza de date, cât și a stocării informațiilor într-o bază de date. Totodată, prin integrarea acestui sistem se implementează un model de analiză și detecție centralizată a acestui setup ce poate fi considerat un standard într-un Centru de Date. Detecția centralizată se va putea realiza utilizând tehnologia APEX de dezvoltare PL/SQL care permite un mod rapid și facil de interogare a multiplelor baze de date gestionate simultan. Setup-ul standard include și o zonă în cadrul bazei de date de stocare criptată a datelor, fapt ce se va demonstra foarte ușor prin analiza fișierelor care găzduiesc datele. Această facilitate este utilă pentru acele organizații care au în componență multiple sisteme informatice critice.

Criptarea traficului bazei de date. Oracle acceptă criptarea la nivel de rețea atât prin Secure Sockets Layer (SSL), utilizând certificate semnate X.509v3, cât și criptare nativă fără certificate. Soluția cu criptarea la nivel de rețea nu este doar faptul că datele sensibile în tranzit sunt protejate atunci când este utilizată criptarea, ci și faptul că SID-ul este protejat. Fără criptare, SID poate fi ușor enumerat prin atacuri Man-in-the-middle.

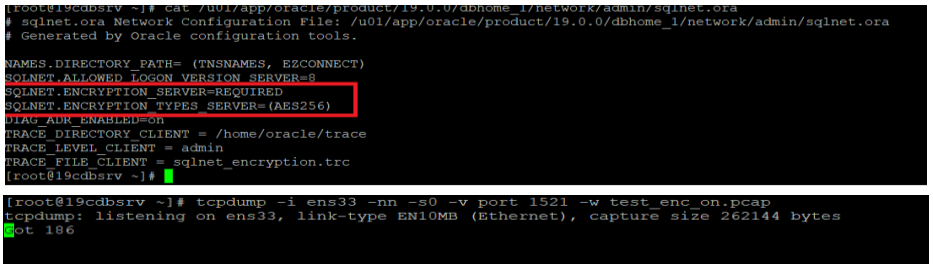

Figura 5.15 *Colecția pachetelor pe placa de rețea*

Integritatea datelor.

Funcționalitatea avansată de integritate a datelor de securitate este separată de criptarea rețelei. Configurarea este similară cu cea a criptării rețelei, utilizând următorii parametri din fișierele *sqlnet.ora* ale serverului și/sau ale clientului:

Verificăm cheile de criptare:

```
SQL> col KEY_ID format a55
col ACTIVATING_PDBNAME format a15
select KEY_ID,ACTIVATING_PDBNAME,ACTIVATION_TIME from v$encryption_keys;
```

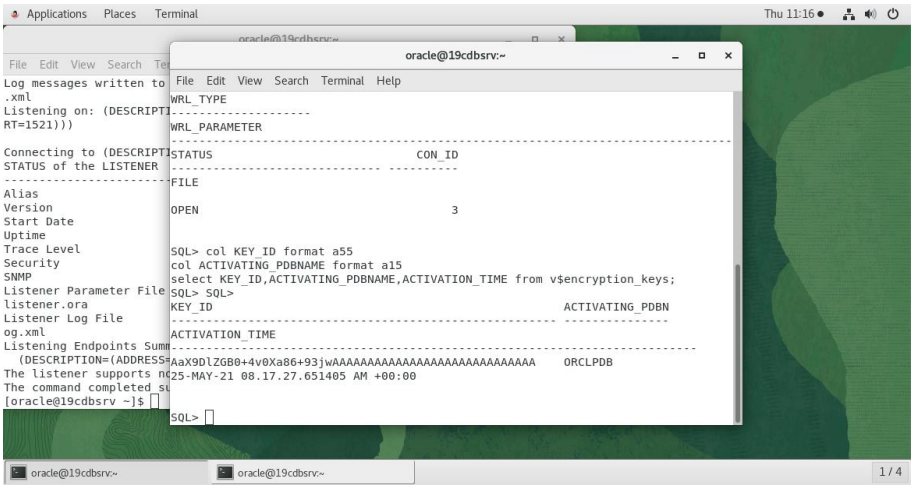

Figura 5.20 *Verificare chei criptare*

Citim fișierele de date și vom vedea că în fișierul necriptat datele pot fi citite, dar în cel criptat e imposibil a fi citite:

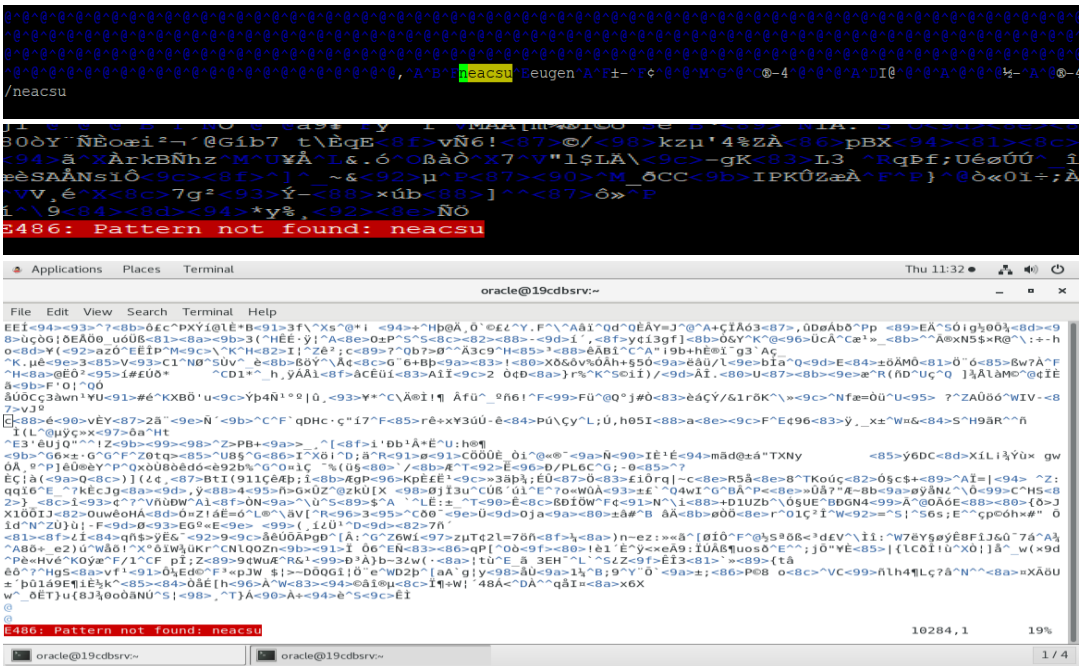

Figura 5.21 *Verificare integritate date*

Principiul minimului privilegiu este faptul că utilizatorilor li se vor acorda doar acele privilegii care sunt de fapt necesare pentru a-și îndeplini în mod eficient sarcinile. Pentru a implementa concret acest principiu, **Sistemul de Securitate Integrat** restricționează următoarele:

- ➔ numărul de privilegii *SYSTEM* și *OBJECT* acordate utilizatorilor bazei de date;
- ➔ numărul de persoane cărora li se permite să facă conexiuni privilegiate *SYS* la baza de date;
- ➔ numărul de utilizatori cărora li se acordă orice privilegii, cum ar fi privilegiul *DROP ANY TABLE*. În general, nu este nevoie să acordăm privilegii *CREATE ANY TABLE* unui utilizator fără privilegii DBA;
- ➔ numărul de utilizatori cărora li se permite să efectueze acțiuni care creează, modifică sau elimină obiecte din baza de date, cum ar fi instrucțiunile *TRUNCATE TABLE, DELETE TABLE, DROP TABLE*;
- ➔ privilegiile *CREATE ANY JOB, BECOME USER, EXP_FULL_ DATABASE* și *IMP_FULL_DATABASE*;
- ➔ privilegiile legate de bibliotecă numai pentru utilizatorii de încredere;
- ➔ acces non-administrativ al utilizatorilor la obiecte deținute de *SYS*;
- ➔ permisiuni pentru facilitățile de rulare;
- ➔ se blochează conturile de utilizator implicite (predefinite);
- ➔ se monitorizează acordarea privilegiilor *ALTER SYSTEM, AUDIT SYSTEM* și *CREATE EXTERNAL JOB* numai utilizatorilor și rolurilor ce dețin necesitatea de a cunoaște;
- ➔ se limitează privilegiile contului proxy (pentru autorizare) numai la *CREATE SESSION*;
- ➔ se utilizează roluri de aplicații sigure pentru a proteja rolurile care sunt activate de codul aplicației.

5.2.2 Dezvoltarea politicilor de securitate

Deși cel mai frecvent tip de încălcare a politicilor sunt încercările de acces neintenționat ale utilizatorilor, cum ar fi navigarea către directoare restricționate, astfel de încălcări sunt de obicei cele mai puțin semnificative, deoarece limitările de acces și politicile de drepturi bine concepute abordează această problemă. Încălcările politicii administrative reprezintă cel mai semnificativ tip de eveniment, indiferent dacă este deliberat sau accidental, din cauza naturii drepturilor administrative. Privilegiile contului de administrator acordă un grad semnificativ de acces la sisteme persoanelor care solicită să își îndeplinească sarcinile specifice. Totuși, acest lucru nu implică autorizarea utilizării acelor drepturi de sistem în afara domeniului sau a procesului autorizat. Capacitatea conturilor de administrator de a permite crearea contului de utilizator, modificarea conturilor, vizualizarea datelor restricționate și modificarea drepturilor de acces la date necesită o analiză atentă a modalităților de atenuare a riscurilor asociate unor capacități atât de puternice.

5.2.3 Etapa de analiză

Pentru a implementa un sistem de monitorizare a securității și detectare a atacurilor bazat pe înregistrarea evenimentelor de securitate, trebuie abordate următoarele probleme [95]:

- ➔ gestionarea volumelor mari de evenimente de securitate;
- ➔ stocarea și gestionarea informațiilor despre evenimente într-un nod central;
- ➔ identificarea și reacția la atacuri;
- ➔ restricționarea personalului să ocolească controalele auditului de securitate.

5.2.4 Evaluarea de securitate a sistemului

Scopul principal al unui sistem de monitorizare a securității și de detectare a atacurilor este de a ajuta la identificarea evenimentelor suspecte dintr-o rețea care pot indica activități dăunătoare sau erori de procedură [98]. **Sistemul de Securitate Integrat** (SSI) contribuie la soluționarea necesității securității în cadrul sistemele informatice critice. Oferă o soluție de monitorizare a securității, un proces continuu de planificare, implementare, gestionare și testare, deoarece aceasta este însăși natura monitorizării securității. Deoarece amenințările la adresa rețelelor informatice se schimbă întotdeauna, trebuie să se schimbe și sistemul care monitorizează securitatea. Aplicarea acestui proces la administrarea securității a presupus:

- identificarea modalităților de a reduce riscul la niveluri acceptabile;
- atenuarea riscurilor de securitate;
- identificarea principalelor obiective ce trebuie securizate;
- evaluarea cerințelor de eficacitate și securitate.

5.3 Rezultate. Concluzii

Datele sunt o resursă foarte decisivă pentru orice organizație datorită protecției. Auditul regulat al bazei de date gestionate nu ar trebui lăsat niciodată la voia întâmplării sau a soluțiilor de tip patchwork. În perioada de audit, părțile interesate trebuie să identifice faptul că un sistem este configurat conform standardului care asigură atenuarea riscului.

Numărul cazurilor de amenințări și incidente care au dominat raportarea mass-media de ani de zile a servit la creșterea gradului de conștientizare și a stimulat majoritatea organizațiilor să investească timp și resurse în apărarea împotriva acestei probleme de securitate predominante. Totuși, cea mai mare amenințare la adresa infrastructurilor informatice poate să nu fie sub forma unui atac din exterior, cum ar fi de la un virus, ci poate rezida în interiorul rețelei interne.

Sistemul de Securitate Integrat (SSI) reprezintă o soluție de protecție completă, care poate realiza cu ușurință următoarele:

- ✓ audit de acces și autentificare;
- ✓ audit utilizatori;

- ✓ audit administratori;
- ✓ auditarea activității suspecte;
- ✓ auditarea vulnerabilităților și a amenințărilor;
- ✓ implementarea politicilor pe sistemele gestionate;
- ✓ criptarea fluxului informațional.

Fără o soluție de audit cuprinzătoare, organizațiile pun în pericol informațiile prețioase. Datele corupte, inexacte sau compromise reprezintă venituri pierdute, timp pierdut și relații compromise. Auditul este un proces continuu, indiferent de ce sistem sau furnizor este utilizat. Chiar și elementele de bază ar trebui revizuite periodic pentru a evita un fals sentiment de securitate. Baza de date este o componentă sensibilă în infrastructurile critice astfel, este important ca aceasta să fie configurată corect pentru a asigura o securizare integrată a informațiilor.

Corelarea informațiilor despre evenimentele de securitate implică colectarea de evenimente de securitate de la mai multe sisteme și plasarea acestor date într-o locație centrală sigură. Când informațiile de securitate au fost corelate, inginerul de securitate poate analiza acest nod central pentru a identifica încălcări sau atacuri externe. Acest nod nu este important doar pentru analiza cyberint, ci și ca instrument pentru detectarea atacurilor și abordarea vulnerabilităților. Planificarea utilizării analizei cyber diferă de abordările altor soluții, deoarece implică investigarea incidentelor după ce acestea au avut loc, în loc de o analiză în timp real a incidentelor. Prin urmare, o istorie detaliată a evenimentelor din mai multe sisteme trebuie menținută pentru o perioadă mai lungă de timp (de preferat 6 luni). Din cauza acestei nevoi suplimentare, un sistem eficient de securitate ar trebui să fie centralizat și să aibă o cantitate semnificativă de capacitate de stocare pentru a stoca un număr mare de înregistrări într-o structură de bază de date adecvată.

Trebuie luată în considerare și securitatea datelor analizei cyberint, deoarece accesul la aceste informații ar trebui să fie rar necesar. Dacă totuși este necesar accesul, acesta ar trebui să fie furnizat doar câtorva persoane de încredere din palierul de securitate al infrastructurii gestionate. Accesul administratorului la aceste informații ar trebui să fie strict reglementat în cadrul unui proces stabilit de control al modificărilor – care are o supraveghere suplimentară. Nimeni altcineva nu ar trebui să aibă capacitatea de a accesa aceste informații, de a întrerupe colectarea acestora sau de a le modifica.

Capitolul 6

Concluzii

Lucrarea intitulată *PROTECȚIA INTEGRATĂ A SISTEMELOR INFORMATICE CRITICE* abordează o temă indispensabilă pentru această perioadă, în care informația reprezintă putere în contextul geopolitic actual. Protecția datelor este o preocupare permanentă a tuturor entităților care se ocupă de gestionarea sistemelor critice, indiferent de situația economică a organizațiilor componente. Securitatea sistemelor informatice critice necesită asistență specializată și un angajament față de standardele celor mai bune competențe. În această lucrare, au fost prezentate cele mai bune practici bazate pe procese și tehnologii dovedite care vă vor ajuta să vă protejați infrastructura și organizația. Ați învățat principalele metode de protecție a sistemelor informatice critice de la dezvoltarea rețelei, până la operațiuni de criptare și optimizare a fluxului informațional. Trebuie să însușiți o abordare proactivă a securității, o abordare care începe cu o evaluare pentru a vă identifica și clasifica riscurile la nivelul rețelei de comunicații. În plus, trebuie să înțelegeți detaliile tehnice de securitate legate de politica de securitate și procedurile de răspuns la incidente. Această lucrare a acoperit numeroase bune practici care vă vor ajuta să orchestrați o strategie pe termen lung pentru infrastructura pe care o administrați.

6.1 Rezultate obţinute

În capitolul 2 sunt detaliate elementele de bază ale sistemelor informatice, axându-mă pe conceptul de *protecție integrată*. A fost prezentată terminologia folosită în acest domeniu, dar și fundamentele matematice necesare înțelegerii conceptelor moderne de securitate: confidențialitate, integritate, autentificare și non-repudiere.

În procesul de definire a SIC, au fost identificate și propuse următoarele rezultate:

- ✓ criteriile de bază ale SI necesare indenficării performanței sistemului;
- ✓ modalități de interconectare a SIC;
- ✓ tehnici de analiză structurală, cât și funcțională, a unui sistem informatic;
- ✓ interdependențele între infrastructuri ca urmare a complexității serviciilor furnizate;
- ✓ metode de evaluare a vulnerabilităților SI;
- ✓ identificarea și analiza principalelor surse de amenințări în cadru unei infrastructuri critice;

- ✓ furnizarea principalelor procedee de îmbunătățire a utilității sistemelor;
- ✓ analiza problematicii privind dificultatea de implementare a securității (din punct de vedere al unui administrator de sistem);
- ✓ elaborarea unor măsuri proprii de prevenție în fața intruziunilor din exterior (având în componență 5 obiective: evaluarea securității, control centralizat, menținerea standardelor de securitate, instruirea personalului, respectarea legii).

Capitolul 3 prezintă cele mai bune tehnici criptografice utilizate la ora actuală în cadrul sistemelor informatice și de comunicații, necesare protecției datelor gestionate. Am plecat de la principalele metode de protejare a informațiilor, specifice tehnologiei contemporane și am ajuns la aceste rezultate:

- ✓ identificarea celor mai uzuale tehnici de ascundere a informațiilor: determinarea anumitor forme în mesajele criptate, a punctelor slabe și măsuri de prevenție a interceptării mesajelor;
- ✓ prezentarea tehnicilor criptografice actuale și a noțiunilor de management al cheilor criptografice;
- ✓ explicarea metodelor necesare implementării unei protecții integrate la nivel de nod de comunicații;
- ✓ analiza de securitate a principalilor algoritmi criptografici utilizați pentru secretizarea informației;
- ✓ integrarea și documentarea unei infrastructuri cu chei publice, făcând parte din procesul de criptare;
- ✓ idenficarea și analiza de securitate a celor mai importante tehnici de securizare a comunicațiilor de mare întindere (SIP, RTP, IPsec);
- ✓ justificarea pachetelor de date din structura mesajelor transmise în rețea;
- ✓ asigurarea flexibilității în implementare a protocoalelor este realizată evitând întreținerea unei infrastructuri complexe de tunele VPN în condițiile în care avem o infrastructură PKI ce pune la dispoziție certificatele și cheile de criptate;
- ✓ înțelegerea considerațiilor tehnologice privind adoptarea PKI în vederea implementării protocolului TLS pentru protejarea conexiunilor, informațiile critice ce pot afecta securitatea comunicațiilor transmise prin SRTP sunt inaccesibile în fața unor potențiale interceptări.

Principalul beneficiu al securizării informației este posibilitatea de asigurare a integrității datelor sensibile, putând furniza la nivelul rețelei un grad ridicat de protecție.

Capitolul 4 este dedicat administrării centralizate a securității infrastructurilor critice gestionate la nivel organizațional, furnizând instrumentele necesare identificării cu precizie a riscurilor de securitate, dar și consolidarea protecției instituționale. Sunt prezentate aspecte practice ce relevă o abordare coordonată a administrării sistemelor ce integrează totalitatea resurselor disponibile pentru asigurarea necesarului de securitate. Concluziile expuse în acest capitol impun o retehnologizare completă a echipamentelor de telecomunicații din cadrul infrastructurilor critice, investiții masive în resursele informatice, cooptarea și perfecționarea inginerilor de securitate ce administrează aceste sisteme, dar și dezvoltarea unor programe software de reacție în timp util la intruziunile prezentate.

Amenințările potențiale se pot materializa într-un orizont foarte larg, cum ar fi: terorismul internațional, proliferarea, criminalitatea organizată sau pandemiile (COVID-19). Globalizarea pune presiune pe amenințările existente, cu consecințe directe asupra oamenilor. Este absolut necesară dezvoltarea la nivel național a conceptului de *reziliență cibernetică* ce ilustrează clar importanța interfețelor și a conexiunilor bazelor de date.

Capitolul 5 prezintă principalele etape parcurse în proiectarea, implementarea și configurarea unui **Sistem de Securitate Integrat** (SSI) în scopul securizării bazelor de date ce constituie o entitate valoroasă ce pot avea importanță tactică pentru entitățile interesate. Un prim pas a fost definirea obiectivelor și a cerințelor de securitate (auditul standard, pista de audit la nivel de aplicație, auditarea evenimentelor BD, auditarea declanșatorului bazei de date, audit extern). Auditul bazelor de date este necesar pentru a urmări anumite evenimente ce pot penetra măsurile de securitate configurate. În continuare, am parcurs etapa de implementare care a constat în: crearea scheletului **SSI**, modificarea structurii bazei de date, configurarea declanșatorilor BD, modificarea scripturilor la nivelul sistemului de operare, configurarea pachetelor la nivelul BD, realizarea setărilor de profil la nivel de aplicație și implementarea funcționalității de integritate a informațiilor stocate prin criptarea traficului bazei de date. Pasul următor a constat în dezvoltarea unor politici de securitate locale pentru sistemul de operare, necesare securizării datelor în fața vulnerabilităților extinse. Integrarea acestor măsuri stabile, monitorizate și revizuite asigură obiectivele de securitate ale studiului efectuat. **SSI** reprezintă practic un model de securizare a accesului la traficul de date dintre aplicațiile utilizate și baza de date din nodul central. Prin conceperea acestui sistem am realizat un model de analiză și detecție centralizată ce poate fi considerat un standard în cadrul unei infrastructuri critice (de exemplu, într-un Centru de Date). Acest sistem are în componență o analiză de risc privind vulnerabilitățile posibile în sistem și o evaluare de securitate completă, pentru a ajuta la îmbunătățirea și dezvoltarea practicilor de monitorizare a securității sistemelor informatice.

6.2 Contribuţii originale

În elaborarea acestei lucrări, au fost aduse următoarele contribuții originale la securitatea sistemelor informatice critice:

1. analiza succintă a elementelor componente, indicatorilor și a criteriilor care reflectă starea de securitate a SI (secțiunea 2.1);
2. au fost definite și exemplificate următoarele: baza informațională, baza tehnică, sistemul de operare, baza științifică, cât și cadrul organizatoric – prezentând problematicile principale ale interdependențelor SI în scopul identificării abordărilor ce vizează un întreg sistem de infrastructuri critice care interacționează între ele (secțiunea 2.2);
3. analiza de securitate a principalelor atacuri cibernetice la adresa SI (secțiunea 2.3.1);

4. realizarea unui studiu de caz privind analiza atacurilor de tip phishing, furnizând importante aspecte de securitate (secțiunea 2.3.2);
5. elaborarea unor contramăsuri necesar a fi implementate pentru combaterea agresiunilor informatice, fapt ce a dus la furnizarea unui nivel de securitate ridicat al SI (secțiunea 2.3.3);
6. analiza comparativă a algoritmilor cu cheie publică/cheie privată (secțiunea 3.1);
7. analiza comparativă a pachetelor de date transmise într-o rețea de mare întindere (secțiunea 3.2);
8. implementarea și criptarea conexiunilor unei rețele VoIP utilizând infrastructura PKI (secțiunea 3.3);
9. realizarea unui studiu de caz privind analiza de securitate a unei rețele VoIP, identificând principalele vulnerabilități ale rețelei și crearea măsurilor de prevenție (secțiunea 3.3);
10. elaborarea unor măsuri practice de configurare a rețelei pentru eliminarea potențialelor atacuri în infrastructură;
11. constituirea procesului de administrare centralizată a securității (secțiunea 4.1);
12. realizarea unui model de gestionare a riscurilor informaționale (gravitate – impact);
13. realizarea unui plan de securitate integrat al unui Centru de Date (analiza mediilor de securitate, management centralizat al securității, analiza riscurilor la adresa SIC, managementul riscului), instrument ce furnizează imaginea clară a amenințărilor și a punctelor vulnerabile ale infrastructurii critice, măsuri de prevenire a producerii incidentelor de securitate, dar și un sistem de alertare pe niveluri de prioritate (secțiunea 4.2);
14. elaborarea a două scenarii pentru analiza riscurilor de securitate: atac terorist și cutremur (încadrarea în scale de gravitate a impactului, consolidarea capacității de reacție);
15. conceperea, implementarea și dezvoltarea unui Sistem de Securitate Integrat (capitolul 5);
16. realizarea unui ghid privind protecția datelor în mediul virtual, în scopul consolidării protecției eficiente a datelor personale (anexa 7);
17. realizarea unui test în domeniul INFOSEC, destinat evaluării cunoștințelor necesare inginerilor de securitate ce administrează sisteme informatice critice (anexa 8).

6.3 Lista lucrărilor originale

A. Articole științifice în publicații indexate ISI Web of Science

[A1] E. NEACȘU, P. ȘCHIOPU, *An Analysis of Security Threats in VoIP Communication Systems*, International Conference on Electronics, Computers and Artificial Intelligence ECAI, ISBN: 978-1-7281-6843-2 IEEE Xplore, doi:

10.1109/ECAI50035.2020.9223162, ISSN 2378-7147, WOS: 000627393500042, 2020.

[A2] E. NEACȘU, P. ȘCHIOPU, *Proposed Pattern for Data Confidentiality in Wireless Communications*, Proc. SPIE 11718, Advanced Topics in Optoelectronics, Microelectronics and Nanotechnologies X, 1171836, ISBN: 978-1-5106-4272-0, doi: 10.1117/12.2573269, ISSN 0277-786X, WOS: 000641147900113, 2020.

[A3] E. NEACȘU, P. ȘCHIOPU, *A Security Analysis of Public Key Cryptographic Systems Used for Electronic Signature*, University Politehnica of Bucharest, Scientific Bulletin, Series C Electrical Engineering and Computer Science, ISSN 2286-3540, WOS: 000628640200011, 2021.

B. Articole științifice în publicații indexate BDI

[B1] E. NEACȘU, *Data Protection System Based on Digital Signature*, Bulletin of the University of Pitesti, Series: Electronics and Computers Science, ISSN 2344-2158, 2020.

[B2] E. NEACȘU, *The Effectiveness of the Statistical Testing of Randomness in a Complete Cryptographic System*, Bulletin of the Polytechnic Institute of Iași, Section of Electrical Engineering, Power Engineering and Electronics, ISSN 1223-8139, 2020.

C. Articole științifice în publicații cu punctaj de recunoaștere

[C1] E. NEACȘU, *Metode de Securizare a Comunicațiilor VoIP și Videoconferință. Securizarea IPsec*, Sesiunea de Comunicări Științifice Studențești SCSS 2, Departamentul de Metode și Modele Matematice, Secțiunea 13 - 3, Universitatea Politehnica din București, 2017.

[C2] E. NEACȘU, *Criptarea Sesiunii RTP (Real-time Transport Protocol)*, Sesiunea de Comunicări Științifice Studențești SCSS 2, Departamentul de Metode și Modele Matematice, Secțiunea 13 - 2, Universitatea Politehnica din București, 2018.

[C3] E. NEACȘU, *Providing Secure End-to-End Networks*, Workshop on Innovative Techniques, Diversity & Connectivity WITDC-19, Center for Research and Training in Innovative Techniques of Applied Mathematics in Engineering Traian Lalescu (CiTi), București, 2019.

D. Proiect de cercetare

[D1] E. NEACȘU, *Plan de Securitate al Operatorului*, Sector Tehnologia Informației și Comunicații, Subsector Infrastructuri de Securitate Informatică, Universitatea Națională de Apărare Carol I, Facultatea de Comandă și Stat Major, Protecția Infrastructurilor Critice PIC, București, 2020.

E. Rapoarte de activitate științifică în cadrul programului de doctorat

[E1] Raportul științific nr. 1/2019, *Dinamica Mediului de Securitate și Rolul Sistemelor Informatice*.

[E2] Raportul științific nr. 2/2019, *Identificarea și Contracararea Atacurilor Cibernetice*.

[E3] Raportul științific nr. 3/2020, *Securizarea Comunicațiilor de Mare Întindere (VoIP)*.

[E4] Raportul științific nr. 4/2020, *Vulnerabilități, Riscuri și Măsuri de Protecție Împotriva Atacurilor asupra Sistemelor de Comunicații (VoIP)*.

6.4 Perspective de dezvoltare ulterioară

Lucrarea elaborată propune un nou sistem pentru securizarea datelor sensibile în cadrul infrastructurilor critice. Demonstrarea performanțelor și a securității recomandă acest Sistem de Securitate Integrat (SSI) drept o nouă soluție de protecție a datelor sensibile în sistemele informatice.

Ca și perspectivă de dezvoltare ulterioară, îmi doresc elaborarea unei aplicații pentru detecția centralizată la nivel de nod de comunicații, utilizând tehnologia APEX de dezvoltare PL/SQL, ce îmi va permite conturarea unui mod mai facil de configurare și interogare a multiplelor baze de date gestionate simultan. Personal, consider că securitatea cibernetică este un factor decisiv în dezvoltarea tehnologică a oricărui Stat, iar practicile care asigură securitatea sistemelor informatice trebuie adaptate noilor provocări ce amenință integritatea infrastructurilor de comunicații.

Bibliografie

[4] C. Răcuciu, D. Grecu, *Criptografie și securitatea informației*, Editura Renaissance, Bucureşti, ISBN 978-606-8321-89-9, 2010.

[6] **E. NEACȘU**, P. ȘCHIOPU, *Proposed Pattern for Data Confidentiality in Wireless Communications*, Proc. SPIE 11718, Advanced Topics in Optoelectronics, Microelectronics and Nanotechnologies X, 1171836, ISBN: 978-1-5106-4272-0, doi: 10.1117/12.2573269, ISSN 0277-786X, WOS: 000641147900113, 2020.

[11] Ghid pentru securitate cibernetică, https://www.sri.ro/assets/files/publicatii/ghid_de_securitate_cibernetica.pdf

[13] **E. NEACȘU**, P. ȘCHIOPU, *A Security Analysis of Public Key Cryptographic Systems Used for Electronic Signature*, University Politehnica of Bucharest, Scientific Bulletin, Series C Electrical Engineering and Computer Science, ISSN 2286-3540, WOS: 000628640200011, 2021.

[15] Email Spoofing, https://blogs.cisco.com/security/what-is-email-spoofing-and-how-to-detect-it

[16] B. Robisson, P. Manet, *Differential Behavioral Analysis*. Cryptographic Hardware and Embedded Systems - CHES 2007, Lecture Notes in Computer Science, vol. 4727, pp. 413-426. Springer Berlin/Heidelberg, 2007.

[38] P. C. Pfleeger, *Security in Computing*. Prentice Hall, Inc., 1989.

[48] **E. NEACȘU**, *Criptarea Sesiunii RTP (Real-time Transport Protocol)*, Sesiunea de Comunicări Științifice Studențești SCSS 2, Departamentul de Metode și Modele Matematice, Secțiunea 13 - 2, Universitatea Politehnica din București, 2018.

[66] **E. NEACȘU**, *Metode de Securizare a Comunicațiilor VoIP și Videoconferință. Securizarea IPsec*, Sesiunea de Comunicări Științifice Studențești SCSS 2, Departamentul de Metode și Modele Matematice, Secțiunea 13 - 3, Universitatea Politehnica din București, 2017.

[74] **E. NEACȘU**, P. ȘCHIOPU, *An Analysis of Security Threats in VoIP Communication Systems*, International Conference on Electronics, Computers and Artificial Intelligence ECAI, ISBN: 978-1-7281-6843-2 IEEE Xplore, doi: 10.1109/ECAI50035.2020.9223162, ISSN 2378-7147, WOS: 000627393500042, 2020.

[79] **E. NEACȘU**, *Plan de Securitate al Operatorului – Sector Tehnologia Informației și Comunicații*, Subsector Infrastructuri de Securitate Informatică, Universitatea Națională de Apărare Carol I, Facultatea de Comandă și Stat Major, Protecția Infrastructurilor Critice PIC, București, 2020.

[95] Cilluffo, J. Frank. *A Global Perspective on Cyber Threats*. Center for Cyber and Homeland Security. June 16, 2015.

[98] Feakin, Tobias. *Developing a Proportionate Response to a Cyber Incident*. Council on Foreign Relations Press. August 2015.