APLICAREA MODELELOR NATO PENTRU CONSTITUIREA INFRASTRUCTURII INFORMAȚIONALE ÎN SITUAȚII DE CRIZĂ

Dr. Violeta VASILEVA
Future Innovation Labs, Sofia, Bulgaria
Conf. univ. dr. Veselina ALEKSANDROVA GAGAMOVA
Colegiul Național de Securitate și Apărare „G.S. Rakovski”, Sofia, Bulgaria
10.55535/GMR.2024.4.14

The effective functioning of the national security system during disasters, accidents and other crisis situations related to cyber security and cyber defence requires the realization of opportunities for inter-institutional interaction of all elements of the system. This paper presents certain opportunities as part of the methodology to apply NATO models to develop the system design of information infrastructure with capabilities to achieve the required levels of operational interoperability to respond to cyber threats to national security. For the architectural configuration, the NATO Technical Reference Model (NTRM) is applied and the NATO Common Operating Environment Component Model (NCOECM) is used for defining the information infrastructure components of the system design. By implementing the proposed methodology, a model of architectural configuration of an information infrastructure of a Security Operations Centre component has been developed – the Security Information Event Management (SIEM) Server. A specification of the technical and software configuration of the SIEM server is developed.

Keywords: NATO models; methodology; cybersecurity and cyber-defence; system design; interoperability and resilience;

Traducere și adaptare: **Diana-Cristiana LUPU**.

INTRODUCERE

Infrastructura informațională cuprinde unitatea componentelor sale, a relațiilor dintre acestea, principiile și regulile care guvernează proiectarea și dezvoltarea lor. Serverul SIEM *(Security Information Event Management/Managementul evenimentelor de securitate informațională)* ca și componentă a sistemelor informaționale de securitate cibernetică ar trebui configurat arhitectural prin implementarea modelelor NATO propuse. În acest scop, a fost dezvoltat un model al unei componente a infrastructurii informaționale (server SIEM) cu specificarea configurațiilor sale tehnice și *software*, utilizând cele două modele principale de referință NATO: 1. Modelul tehnic de referință NATO/*NATO Technical Reference Model (NTRM)* și 2. Modelul componentelor mediului de operare comun NATO/ *NATO Common Operating Environment Component Model (NCOEM)* [Allied Data Publication 34 (ADatP-34)].

Dezvoltarea arhitecturală necesită modelare, care ne ajută să înțelegem legătura dintre cerințe, pe de o parte, și conceptul arhitectural, pe de altă parte. Cerințele trebuie să fie prezentate într-un format de diagramă, conform *NATO C3 Technical Architecture Implementation Handbook* [ISSC NATO Open Systems Working Group, AC/322(Sc/5)N268, 2002]. NC3TA-IHB identifică, în Anexa A, șabloanele care trebuie completate de managerii de proiect și arhitecți, dar nu furnizează o metodologie pentru a face acest lucru. Este la latitudinea managerilor de proiect și a arhitecților să aleagă metodologiile adecvate, care se potrivesc nevoilor lor. Prin urmare, este nevoie de o metodologie pentru a completa șabloanele NC3TA din Anexa A. O propunere pentru o astfel de metodologie este prezentată de către autori. Ca exemplu de aplicare a unei astfel de metodologii, lucrarea prezintă dezvoltarea configurației arhitecturale a serverului SIEM.

MODELE PENTRU CONFIGURAREA ARHITECTURALĂ A COMPONENTELOR INFRASTRUCTURII INFORMAȚIONALE A SISTEMELOR ÎN MEDIUL DE MANAGEMENT AL CRIZELOR

Pentru a asigura reziliența sistemelor informaționale în mediul de conflict cibernetic, este necesar ca dezvoltarea sistemelor de securitate cibernetică pentru organizații să fie interoperabilă. Prin urmare, aplicarea modelelor NATO ar ajuta la dezvoltarea sistemelor de securitate cibernetică ale organizațiilor.

Unul dintre principalele modele de compatibilitate a sistemelor este *Modelul tehnic de referință NATO (NTRM)*. Acesta este un model pentru descrierea mediului informațional, definirea datelor aplicațiilor și a datelor componentelor infrastructurii informaționale. De asemenea, definește ariile de servicii (capacități care sunt grupate după funcții), precum și interfețele acestora. Structura Modelului tehnic de referință ia în considerare separarea datelor de aplicații, precum și a aplicațiilor de configurația *software*. Modelul este conceput pentru a separa aplicațiile și mediul extern de platformă, permițând compatibilitatea aplicației și independența față de dispozitivele externe (de exemplu, tastaturi, mouse, cameră web, unitate USB, hard disk extern, joystick, controler de joc etc.). În acest scop, modelul definește *Interfețele programului de aplicație/Application Program Interfaces (API)* și *Interfețele mediului extern/External Environment Interfaces (EEI).*

Modelul NTRM include cinci niveluri – trei categorii de obiecte (entități) și două interfețe, după cum urmează:

- *entitatea software a aplicației/Application Software Entity;*
- *interfața programului de aplicație/Application Program Interface (API);*
- *entitatea platformei aplicației/Application Platform Entity;*
- *interfața mediului extern/External Environment Interface (EEI);*
- *entitatea mediului extern/External Environment Entity.*

Aplicația *software* constă din aplicații *software* de utilizator și suport *(software)* sau, așa cum este, în general, popular, *software* de utilizator și aplicație.

Interfețele de programare a aplicațiilor/Application Programming Interfaces (API) sunt aplicații care implementează conexiunea dintre serviciu și platformă, respectiv, aplicații dintre *software*-ul aplicației și mediul aplicației.

Platforma mediului de aplicație conține un sistem de servicii care materializează fizic procesele informaționale, adică servicii de sistem și servicii de mediu fizic (schimb de date).

Interfețele mediului extern/External Environment Interfaces (EEI) oferă utilizatorului acces la date și aplicații. Mai mult, acestea oferă conexiuni între aplicație și mediul extern. Conceptul de interfețe interne completează descrierea API-urilor și a EEI-urilor.

Entitatea mediului extern/External Environment Entity include servicii externe care interacționează cu cele ale mediului fizic al aplicației *software*. Aceste servicii sunt clasificate în categoriile generale de servicii pentru utilizatori (mouse, display), servicii de schimb de informații și servicii de comunicații *(Local Area Network/LAN, Wide Area Network/WAN)*.

Conform NTRM, *entitatea platformei aplicațiilor/Application Platform Entity* include următoarele 12 arii de servicii ale platformei aplicațiilor (Allied Data Publication 34/ADatP-34):

- Servicii de interfață cu utilizatorul.
- Servicii de gestionare a datelor.
- Servicii de schimb de date. Aceste servicii oferă suport pentru schimbul de date între aplicații de pe aceeași platformă sau de pe platforme eterogene.
- Servicii de grafică. Aceste servicii oferă funcții necesare pentru crearea și manipularea graficelor.
- Servicii de comunicare. Aceste servicii oferă suport pentru aplicații distribuite, pentru accesul la date și interoperabilitatea aplicațiilor în medii de rețea eterogene sau omogene.
- Servicii ale sistemului de operare.
- Servicii de internaționalizare. În contextul NTRM, internaționalizarea oferă un set de caracteristici și servicii de reprezentare a datelor.
- Servicii de management al sistemului.
- Servicii de securitate.
- Servicii de calcul distribuite. Aceste servicii oferă suport specializat pentru aplicații care pot fi dispersate fizic sau logic între sistemele de computere dintr-o rețea.
- Servicii de inginerie software.

Servicii comune de aplicații de comandă și control (C2)/Common Command and Control (C2) Applications Services. Aceste servicii oferă posibilitatea de a vizualiza datele (adică, partajarea) într-un mod comun pentru întreaga rețea. Serviciile comune de aplicații C2 promovează interoperabilitatea între diverse domenii de misiune funcționale.

DEFINIREA ORGANIZĂRII COMPONENTELOR INFRASTRUCTURII INFORMAȚIONALE A SISTEMULUI DE SECURITATE CIBERNETICĂ

Pentru funcționarea eficientă a *Echipei de răspuns la incidente de securitate informatică/Computer Security Incident Response Team (CSIRT)*, este necesară furnizarea următoarelor componente ale infrastructurii informaționale a sistemului de securitate cibernetică în organizații:

- echipamente tehnologice cu senzori relevanți pentru monitorizarea infrastructurii de comunicații și informații;

- sisteme de detectare și prevenire a intruziunilor – IDS/IPS/IDPS; *Sistemele de detectare și prevenire a intruziunilor/Intrusion Detection and Prevention Systems (IDPS)* sunt utilizate pentru a integra tehnologiile IDS și IPS;
- sisteme de procesare și analiză a incidentelor informatice – *Sisteme de management al evenimentelor de securitate a informațiilor/Security Information Event Management (SIEM)* pentru a sprijini acțiunile echipei în citirea unui număr mare de evenimente înregistrate de la senzorii de apărare cibernetică;
- sisteme de supraveghere video, *Firewall*-uri din generația următoare;
- personal instruit și înalt calificat în domeniul apărării cibernetice;
- software pentru infracționalitatea cibernetică;
- un server web cu serviciu de informare privind conștientizarea cibernetică.

Serviciile furnizate de SOC[1] pot aparține următoarelor trei categorii principale:

- servicii de răspuns (servicii de reacție) furnizate ca răspuns la incidente – scopul principal al acestor servicii este limitarea pagubelor cauzate de incidente;
- servicii de răspuns preventiv la incidente (servicii proactive) – aceste servicii includ detectarea și reducerea posibilității apariției unui potențial incident sau eveniment legat de securitatea sistemului informatic sau a rețelei protejate;
- servicii de îmbunătățire a securității – aceste servicii ajută la îmbunătățirea calității securității interne. Acestea sunt asigurate de experți în domeniu, pentru ca, în cadrul organizației, să poată fi desfășurate activități comune eficiente pentru a preveni, indirect, apariția incidentelor.

Este extrem de important să se reacționeze rapid și eficient atunci când apar breșe de securitate. Unul dintre avantajele capacității de răspuns la incident este acela că menține un răspuns sistematic la incident (respectiv, gestionarea succesivă a incidentului), astfel încât să poată fi luate măsurile adecvate. Răspunsul la incident ajută personalul să minimizeze pierderea sau furtul de informații și întreruperea serviciilor, cauzate de accidente.

[1] Echipa de răspuns la incidente de securitate cibernetică/Computer Security Incident Response Team (CSIRT) sau Centrul pentru securitatea operațiilor/Security Operations Centre (SOC), CERT/CC (Computer Emergency Response Team/Coordination Center/Echipa de răspuns la urgențe cibernetice/Centrul de coordonare), IRT (Incident Response Team/Echipa de răspuns la incidente), CIRT (Computer Incident Response Team/Echipa de răspuns la incidente cibernetice), SERT (Security Emergency Response Team/Echipa de răspuns la urgențe de securitate), CIRC (Computer Incident Response Team/Echipa de răspuns la incidente cibernetice).

Sistem de management al evenimentelor de securitate a informațiilor

utilizarea SIEM pentru procesarea și analiza incidentelor informatice este propusă ca sistem de răspuns la incident. Soluțiile SIEM oferă o viziune cuprinzătoare, în timp real, asupra rețelei și ajută echipele să fie mai active în combaterea amenințărilor de securitate *(„What Is SIEM?”*, f.d.). Avantajul soluțiilor SIEM constă în faptul că acestea combină *managementul evenimentelor de securitate/security event management (SEM)*, care realizează analiza datelor pentru evenimente și fișiere jurnal în timp real pentru a asigura corelarea evenimentelor, monitorizarea amenințărilor de răspuns la incident, cu *managementul securității informaționale/ Security Information Management (SIM)*, care preia și analizează date de audit și generează un raport. *Software*-ul SIEM identifică datele și le sortează pe categorii, cum ar fi activitatea rău intenționată, autentificarea eșuată și de succes, precum și alte activități potențial rău intenționate.

Când *software*-ul identifică o activitate care poate reprezenta o amenințare pentru organizație, sunt generate alerte care indică o potențială problemă de securitate. Aceste alerte pot fi setate ca prioritate scăzută sau mare, folosind un ansamblu de reguli predefinite. De exemplu, dacă un cont de utilizator generează 20 de încercări eșuate de conectare în decurs de 20 de minute, aceasta poate fi marcată ca activitate suspectă, dar setată cu o prioritate mai mică, deoarece este mai probabil ca utilizatorul să-și fi uitat informațiile de conectare. Cu toate acestea, în cazul în care contul are 120 de încercări de conectare nereușite în decurs de 5 minute, este mai probabil să fie un atac, marcat ca incident de mare severitate *(„What is SIEM? SIEM Defined, Explained, and Explored”*, Forcepoint.com, 2023).

Soluțiile SIEM oferă o metodă eficientă pentru detectarea amenințărilor, raportarea în timp real și analiza pe termen lung a înregistrărilor de audit și a evenimentelor de securitate.

Deoarece soluțiile SIEM pot colecta înregistrări de audit ale evenimentelor de pe mai multe aplicații și dispozitive, acestea permit experților în securitatea IT să identifice, să revizuiască și să răspundă mai rapid la potențialele încălcări de securitate. Identificarea amenințării în stadiile incipiente asigură un efect de atenuare.

Sisteme de răspuns la accidente – detectarea și prevenirea intruziunilor/IDS/IPS/IDPS

Detectarea intruziunilor este procesul de monitorizare a evenimentelor care au loc într-un sistem sau o rețea de computere și de analiză a semnalelor de posibile incidente, care sunt încălcări sau amenințări iminente privitoare la încălcarea

politicilor de securitate a computerului, politicilor de utilizare acceptabilă sau practicilor standard de securitate. *Sistemul de detectare a intruziunilor/Intrusion Detection System (IDS)* este un *software* care automatizează procesul de detectare a tentativelor de intruziune în rețea. *Sistemul de prevenire a intruziunilor/Intrusion Prevention System (IPS)* este un *software* care are toate capacitățile unui sistem de detectare a intruziunilor și poate încerca, de asemenea, să oprească eventualele incidente. Termenul *Sisteme de detectare și prevenire a intruziunilor/Intrusion Detection and Prevention Systems (IDPS)* este folosit pentru a integra tehnologiile IDS și IPS.

Multe IDPS pot identifica informații, ceea ce poate însemna că un atac este iminent sau că un anumit sistem sau o caracteristică a sistemului prezintă un interes deosebit pentru atacatori. O altă aplicație a IDPS este aceea de a obține o mai bună înțelegere a amenințărilor care sunt detectate, folosind tehnologii de inteligență artificială și analizând atât frecvența, cât și caracteristicile atacurilor. Scopul este de a putea defini măsurile de securitate adecvate. Unele IDPS își pot schimba profilul de securitate atunci când este detectată o nouă amenințare.

Tehnologia IPS diferă de tehnologia IDS prin faptul că tehnologia IPS poate răspunde unei amenințări deschise, încercând să împiedice succesul acesteia. Sistemele IPS au senzori care funcționează în modul antrenament sau simulare (Petters, f.d.).

Alături de aceste sisteme, componentele infrastructurii informaționale a sistemului de securitate cibernetică din organizații includ sisteme de supraveghere video, *firewall*-uri de ultimă generație și altele.

Firewall-ul tradițional oferă controlul accesului, adică verifică starea traficului de rețea. *Firewall*-ul de generație următoare/*Next-generation firewall* (NGFW) poate bloca amenințările moderne, cum ar fi *malware*-urile și atacurile la nivel de aplicație.

Este necesar să concluzionăm că încălcările și atacurile din prezent impun necesitatea dezvoltării capacității de a detecta, investiga și atenua consecințele accidentelor informatice. Acesta este un motiv pentru a defini o opțiune pentru organizarea componentelor infrastructurii informaționale a sistemului de securitate cibernetică în organizațiile aflate în mediu de conflict cibernetic. Sunt luate în considerare două domenii: furnizarea de servicii și monitorizarea evenimentelor de securitate pentru prevenirea accidentelor.

Infrastructura informațională a sistemului de securitate cibernetică din organizații include următoarele componente – servere și stații de lucru ca opțiune: *SIEM*, pentru gestionarea și analiza incidentelor, *Security Server; WAP (Web*

Application Proxy); DNS (Domain Name Server); Database Server, pentru baze de date; *Active Directory (AD) – Domain Controller (DC) cu Active Directory*; server de e-mail – *Exchange Server; Logs Server*, pentru înregistrarea evenimentelor; *IDS/IPS (IDPS); Server NVR (Network Video Recorder)*, pentru supraveghere video; *PBX (Private Branch Exchange* – sistem telefonic), server web cu instalare *WordPress* etc., precum și stații de lucru ale administratorilor de securitate, utilizatori la distanță. Acestea sunt prezentate în *figura 1*.

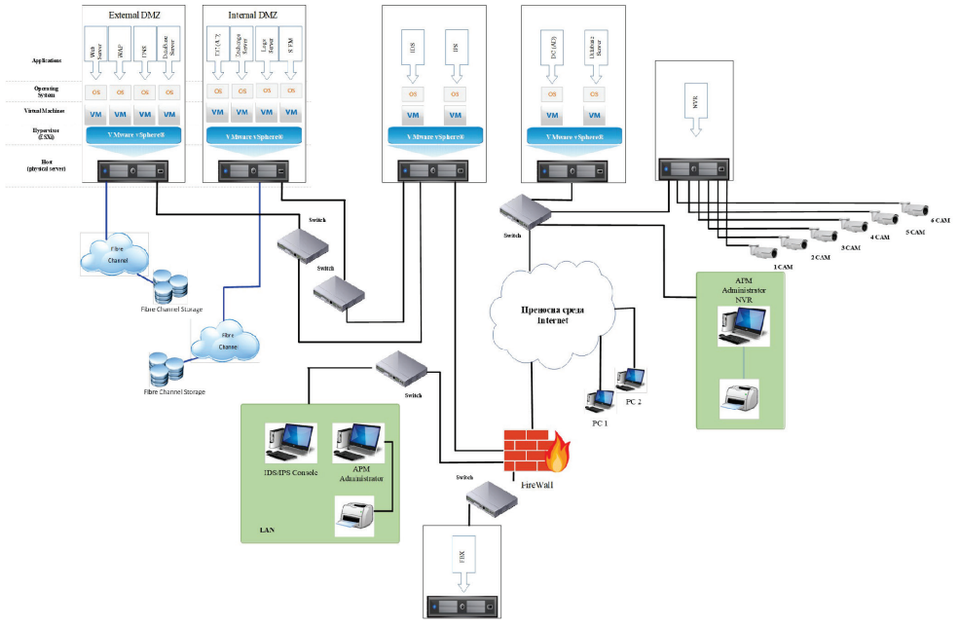

Figura 1: Componentele infrastructurii informaționale a sistemului CIRT (compilația autorilor)

În configurația arhitecturală a componentelor infrastructurii informaționale a sistemului de securitate cibernetică din organizații, pentru termenul de *„componentă”* sunt utilizați și termenii de *configurație funcțională, platformă* și *configurare*.

Diferitele componente (platforme) ale infrastructurii informaționale a sistemului de securitate cibernetică sunt considerate configurații funcționale. Fiecare dintre acestea are o distribuție a elementelor sale pe cinci niveluri: servicii rețea; servicii nucleu; servicii infrastructură; servicii comune aplicații suport și servicii aplicații.

În această secvență, sunt definite configurațiile funcționale ale platformelor (componentelor), așa cum se arată în *figura 1*, precum și proiectarea sistemului acestora. Conform conceptului de configurare arhitecturală a componentelor

infrastructurii informaționale, pentru fiecare dintre componente sunt elaborate următoarele descrieri sau configurații, care reprezintă un aspect diferit – configurație funcțională, tehnică și *software*. Pentru fiecare dintre cele trei configurații, este dezvoltat un design grafic și tabelar *(„Șablon de configurare funcțională/Functional Configuration (FC) Template" – NSV-12, „Șablon de configurare tehnică/Technical Configuration (TC) Template" – NTV-3, „Șablon de configurare software/Software Configuration (SC) Template" – NTV-4)*, conform șabloanelor[2] [(ISSC NATO Open Systems Working Group, AC/322(Sc/5)N268, 2002, pp. 49-67, Annex A] Concepției NTRM.

CONFIGURAȚIA ARHITECTURALĂ A UNUI SERVER PENTRU PRELUCRAREA ȘI ANALIZA INCIDENTELOR CIBERNETICE – SERVER PENTRU MANAGEMENTUL EVENIMENTELOR DE SECURITATE (SIEM)

Configurația funcțională a serverului pentru procesarea și analiza incidentelor informatice – *Security Information Event Management (SIEM)* este prezentată sub formă grafică, *figura 2*, și în formă tabelară, *tabelul 1*, care reprezintă *„Șablonul de configurare funcțională" NSV-12*, conform conceptului de configurație arhitecturală. Configurația funcțională este constituită prin cele cinci niveluri de servicii enumerate anterior: servicii aplicații; servicii comune aplicații suport; servicii infrastructură; servicii nucleu; servicii rețea.

Elementele următoarelor componente funcționale sunt situate pe fiecare dintre aceste niveluri: componente de management; componente de rețea; componente de aplicație; componente de bază; componente de securitate.

La nivel de configurație funcțională, a fost dezvoltată arhitectura SIEM. Aceasta este prezentată mai detaliat în cadrul configurației tehnice și *software*.

O configurație tehnică este o tranziție de la o viziune tehnică la configurații *software* care definesc segmente specifice, precum și componentele lor și produsele *software*. Profilurile de interoperabilitate interne și externe (IIP-uri și EIP-uri) sunt indicate și aici.

Configurația *software* prezintă *software*-ul pentru executarea configurației tehnice. Componentele și standardele utilizate în configurația tehnică sunt transformate în produse și segmente.

[2] Anexa A – *Șabloanele de conformitate NC3TA/NC3TA Compliance Templates* include Configurațiile funcționale Șablonul 12 de vizualizare a sistemului NATO/*NATO System View Template 12* (NSV-12), Configurațiile tehnice Șablonul 3 de vizualizare tehnică NATO/*NATO Technical View Template 3* (NTV-3), Configurațiile software NATO Șablon de vizualizare tehnică 4/*NATO Technical View Template 4* (NTV-4) *Software Configuration*.

Configurația funcțională a SIEM

Șablonul NSV-12, *„Șablonul de configurare funcțională"*, este utilizat într-o formă tabelară, care prezintă serviciile funcționale și interfețele *(Tabel 1)*.

Tabel 1: Șablonul NSV-12, „Șablonul de configurare funcțională" al serverului SIEM (compilația autorilor).

NSV-12	ȘABLON DE CONFIGURARE FUNCȚIONALĂ/FUNCTIONAL CONFIGURATION (FC)				
Titlul proiectului	SISTEM INFORMAȚIONAL CIRT				
POC proiect	Nume		Adresă		Tel/Fax/Email
Titlul FC	Componente funcționale ale sistemului de management și evenimente de securitate informațională/SIEM				
Tipul FC *Notă:* *Alegeți tipul existent, în caz contrar, creați un nou FC, sub una dintre categoriile principale sau creați o nouă categorie*	SERVER SIEM Analiză, profilare, automatizare și rezumare a potențialelor amenințări. Investigarea incidentelor, informații despre amenințări.				
Servicii FC la:	Servicii bază			Servicii rețea	
Notă: *Descrieți serviciile aplicației în termeni funcționali*	*Nivelul servicii rețea*	*Nivelul servicii nucleu*	*Nivelul servicii infrastructură*	*Nivelul aplicație suport*	*Nivelul aplicație misiune specifică*
	Echilibrare trafic Stivă rețea	Control configurație/ Instalație la distanță; Sisteme operare; Software Windowing; Aplicații; Instrumente. Baze de date	Scanare vulnerabilități Informații utilizator Informații resurse Informații amenințare	Culegere date Corelație Normalizare Agregare date	Aplicații analiză Aplicații raportare Aplicații monitorizare în timp real Aplicații server

Interfață funcțională *Notă:* *Descrieți interfața funcțională cu alte FC-uri în ceea ce privește serviciile de interoperabilitate necesare (ex: e-mail, autentificare) și atributele necesare de calitate și cantitate (ex: nr. de mesaje, acreditări de securitate) folosind șabloanele NSV1 (a-d), NSV3 și NTVI*	Interfață SSH[3] port 22 Interfață SMTP[4] port 25 Interfață RDATE[5] port 37 Interfață Port Mapper port 111 Interfață HTTPS[6] port 443 Interfață Syslog port 514

Configurația tehnică a SIEM

Scopul principal al configurației tehnice este de a determina standardele tehnologice și tehnice care trebuie aplicate în proiectarea și construcția sistemului. Configurația tehnică este o transformare tehnică a configurației funcționale. Aceasta înseamnă că serviciile aplicației care sunt descrise în configurația funcțională sunt transformate în componente, cu standardele lor de bază. Aici sunt indicate și profilurile de interoperabilitate internă și externă, care sunt dezvoltate atât grafic *(figura 2, figura 3)*, cât și tabelar *(tabelul 2)* în NTV-3 *„Șablon de configurare tehnică (TC)”*.

[3] Secure Shell (SSH) este un protocol criptografic, https://www.ssh.com/, accesat la 5 ianuarie 2024.
[4] Simple Mail Transfer Protocol (SMTP) este un protocol TCP/IP utilizat în transmiterea unui e-mail înșelător, https://www.smtp.com/, accesat la 5 ianuarie 2024.
[5] RDATE este un Get și este posibil să seteze date și timpul de la o gazdă la distanță pentru Unix OS e-mail, http://manpages.ubuntu.com/manpages/bionic/man8/rdate.8.html, accesat la 5 ianuarie 2024.
[6] Hypertext Transfer Protocol Secure (HTTPS), https://www.ssl.com/faqs/what-is-https/, accesat la 5 ianuarie 2024.

În configurațiile tehnice, profilurile interne de interoperabilitate sunt definite în cadrul protocoalelor și standardelor relevante. Pentru a permite flexibilitate în vederea înlocuirii produselor învechite cu altele noi, este recomandabil să alegeți standarde deschise și produse care utilizează astfel de standarde. Configurația tehnică este prezentată în *tabelul 2*.

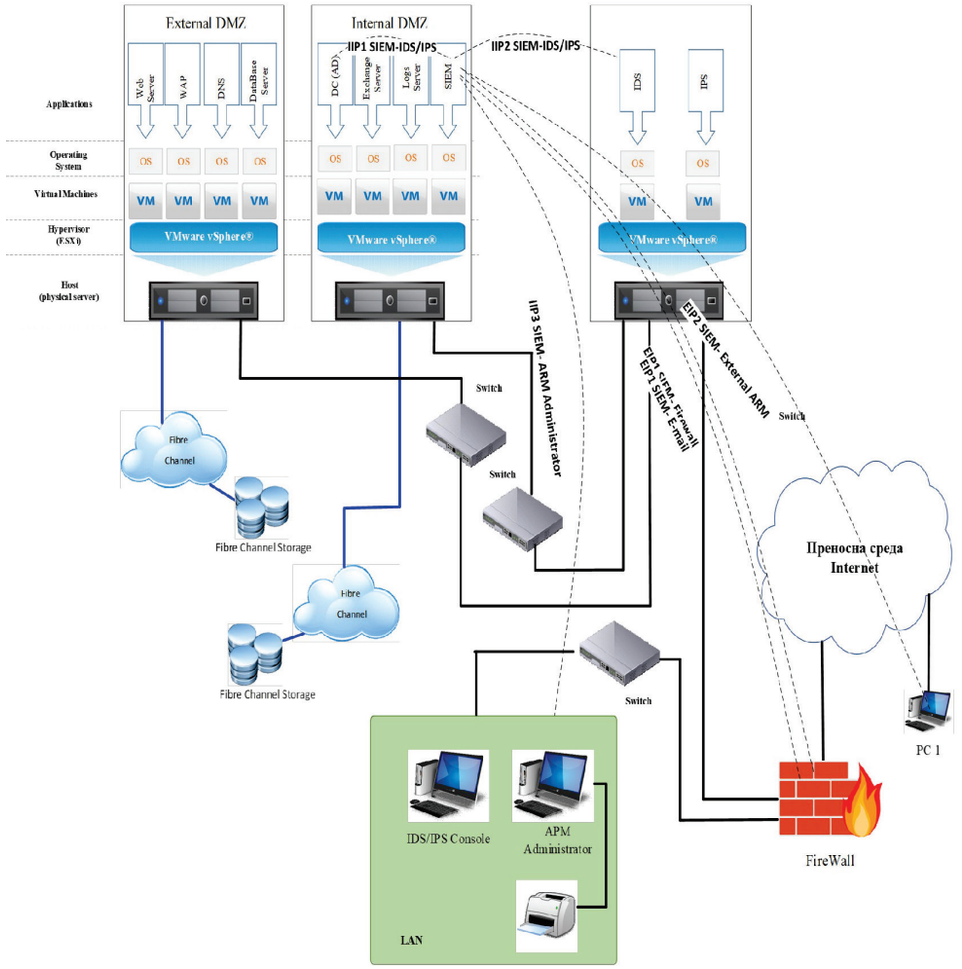

Figura 2: Configurație tehnică cu profiluri de interoperabilitate între componentele mediului informațional (compilația autorilor)

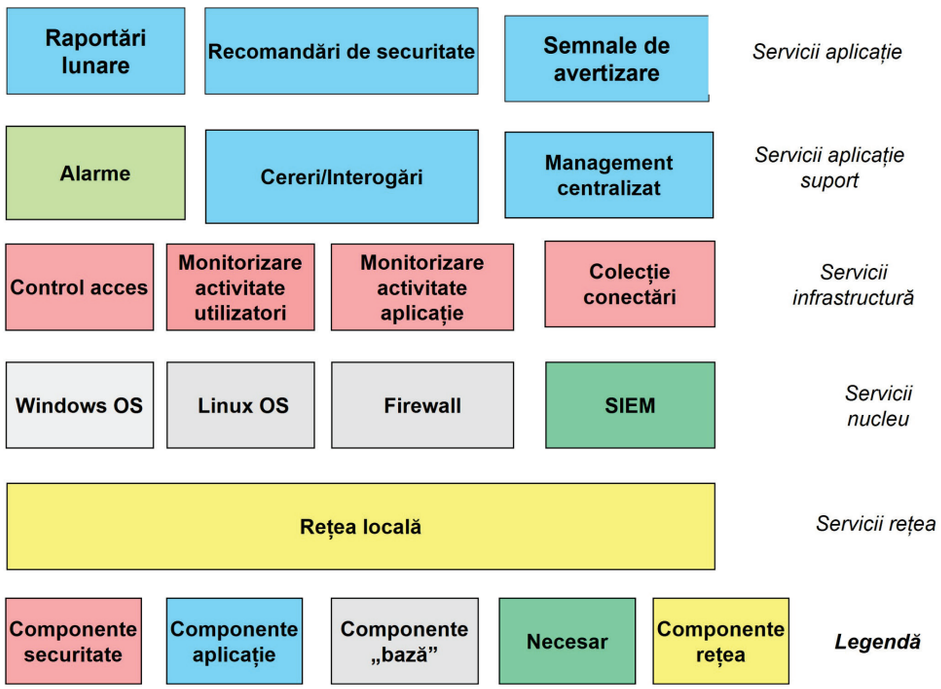

Figura 3: Reprezentare grafică a configurației tehnice a serverului SIEM conform NCOECM (compilația autorilor)

Tabel 2: Configurația tehnică NTV-3 a serverului SIEM (compilația autorilor)

NTV-3	ȘABLON DE CONFIGURARE TEHNICĂ/TECHNICAL CONFIGURATION (TC) (a se completa în faza de achiziții pentru arhitectura-țintă)				
Componente și standarde TC la: Note: Atașati o descriere detaliată pentru fiecare componentă	*Nivelul servicii rețea*	*Nivelul servicii nucleu*	*Nivelul servicii infrastructură*	*Nivelul aplicație suport comună*	*Nivelul aplicație specific misiunii*
	Rețea locală	Windows OS Linux OS Firewall SIEM	Control acces Management identitate Monitorizare activitate utilizatori Analiză comportament Monitorizare activitate aplicație Colecție conectări	Alarme Cereri / interogări Management centralizat	Rapoarte lunare Recomandări de securitate Semnale de alarmă

Profile interoperabilitate internă/Internal Interoperability Profiles (IIP) între TC și: *Notă: Atașați o descriere detaliată pentru fiecare IIP*	IIP1 – Server Director activ/Active Directory – Controler domeniu/ Domain Controller IIP2 – Server *“IDS/IPS”* IIP3 – Stație de lucru pentru monitorizare și administrare sistem de operare (OS) Windows
Profil interoperabilitate între TC și: *Notă: Atașați o descriere detaliată pentru fiecare E1P* EIP-Număr și funcționalitate de bază: *Notă: Utilizați numerotare, după cum urmează EIP<TCnr>-<TCnr>*	EIP1 – Firewall EIP2 – Stație de lucru – O stație de lucru la distanță pentru administrarea sistemului de operare (OS) Linux EIP3 – Server Email

Profilele interoperabilitate internă (IIP) sunt următoarele:

- Profil IIP1 – Schimb date cu serverul director activ (Kerberos, LDAP[7], File Replication, Global Catalog, DNS)
- Profil IIP2 – Schimb date cu un server IDS/IPS
- Profil IIP3 – Schimb date cu o stație de lucru Windows OS

Configurația software a SIEM

După cum a fost menționat, configurația *software* este o implementare *software* a configurației tehnice. Configurația *software* constă din produsele reale care sunt utilizate, ce descriu soluția *software* a configurației tehnice. Configurația *software* reprezintă *software*-ul pentru executarea configurației tehnice, ceea ce înseamnă

[7] Lightweight Directory Access Protocol (LDAP) pentru interacțiunea cu serverele directoare și utilizat pentru autentificare și stocarea informațiilor despre utilizatori, grupuri și aplicații, https://ldap.com/, accesat la 7 ianuarie 2024.

că acele componente și standarde utilizate în configurația tehnică se transformă în produse și segmente. Configurația *software* a SIEM este prezentată grafic în *figura 4* și, sub formă tabelară, în *tabelul 3*.

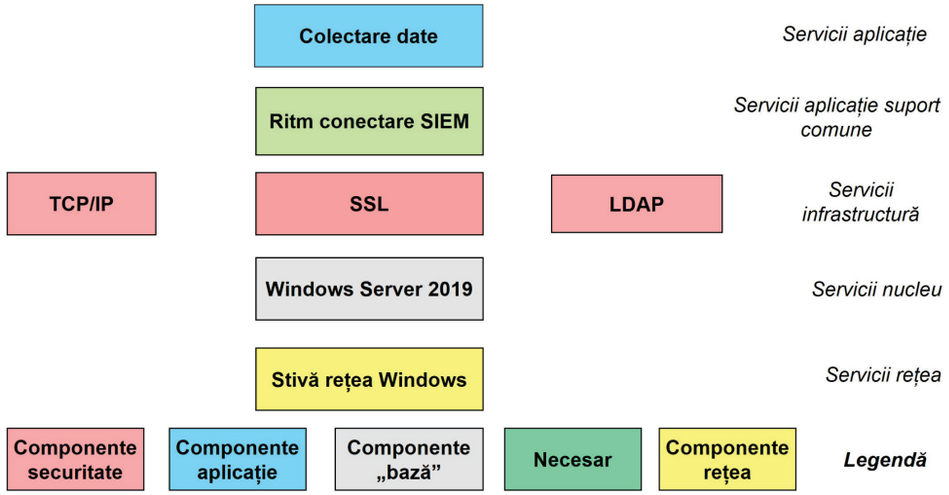

Figura 4: Reprezentare grafică a configurației software SIEM conform NCOECM (compilația autorilor)

În cadrul mediului informațional, pachetele *software*, care sunt situate orizontal în reprezentarea grafică a configurației *software*, sunt prezentate în unități separate, cunoscute și sub denumirea de segmente. Segmentele sunt similare ca funcționalitate cu modulele și pot fi adăugate cu ușurință pe orice platformă *hardware*. Segmentarea oferă utilizatorului posibilitatea de a alege dintre componentele *software* împachetate și testate care sunt considerate necesare într-o anumită situație. Configurația *software*-ului SIEM este prezentată în *tabelul 3.*

Tabel 3: Șablon configurație software NTV-4 SIEM (compilația autorilor)

NTV-4	ȘABLON CONFIGURAȚIE SOFTWARE/SOFTWARE CONFIGURATION (SC) (a se completa în faza de achiziții pentru arhitectura-țintă)				
Produse SC în: *Notă: Indicați numărul versiunii software și standardul/le care trebuie acoperite de pachetul de software*	*Nivel servicii rețea*	*Nivel servicii nucleu*	*Nivel servicii infrastructură*	*Nivel aplicație suport comun*	*Nivel aplicație misiune specifică*
	Stivă rețea Windows	Windows Server 2019	TCP/IP[8], SSL[9], LDAP	Ritm conectări SIEM[10]	Colectare date
Segmente:	*Segment 1*	*Segment 2*	*Segment 3*	*Segment 4*	*Segment 5*
Notă: Descrieți produsele constitutive ale diferitelor segmente	Stivă rețea Windows	Windows Server 2019	TCP/IP, SSL, LDAP Ritm conectări	Colectare date	
Interfețe	Interne	Interne	Externe	Externe	Externe
Interfețe *Notă: Descrieți interfețele în termeni de APIs încorporate în produse sau ca produse separate; Menționați standardele dorite și posibilele setări de parametri*	IIP1– UDP[11] port 88 pentru autentificare Kerberos[12] IIP1 – TCP port 3268 și 3269 pentru Global Catalog IIP1 – TCP și UDP port 53 pentru DNS[13] IIP1 – TCP 139 și UDP port 138 pentru replicarea fișierelor IIP1 – UDP port 88 pentru autentificare Kerberos IIP1 – TCP port 3268 și 3269 pentru Global Catalog IIP1 – TCP și UDP port 53 pentru schimburi DNS IIP1 – TCP 139 și UDP port 138 pentru replicarea fișierelor IIP1 – TCP port 514 pentru colectarea conectărilor EIP1 – Interfață pentru schimb informații cu Firewall EIP2 – TCP port 514 pentru colectarea conectărilor EIP3 – TCP port 80 pentru aplicații web EIP3 – TCP port 443 pentru aplicații web EIP3 – TCP port 22 pentru schimb mesaje				

[8] TCP/IP -Transmission Control Protocol/Internet Protocol.
[9] SSL – Secure Sockets Layer.
[10] Log Rhythm: SIEM Platform&Security Operations Center.
[11] UDP – User Datagram Protocol.
[12] Kerberos – protocol de autentificare dezvoltat de Massachusetts Institute of Technology. Introduction to Kerberos, https://www.ibm.com/docs/en/streams/4.2.1?topic=authentication-introduction-kerberos, accesat la 7 ianuarie 2024.
[13] DNS – Domain Name Server.

CONCLUZII

Pentru dezvoltarea arhitecturii centrului de răspuns la incidente informatice al unei organizații, se oferă o propunere de utilizare a modelelor NATO pentru a configura arhitectural componentele infrastructurii informaționale a sistemelor de securitate cibernetică.

Se poate concluziona că autorii au prezentat o metodologie de aplicare a modelelor NATO pentru constituirea infrastructurii informaționale în condiții de criză, care include configurarea arhitecturii și proiectarea de sistem a componentelor sale într-un mod specific – prin utilizarea modelelor NATO. Au fost folosite diverse instrumente, precum figuri, tabele și explicații textuale. Această prezentare a infrastructurii informaționale nu este foarte populară în rândul echipelor de dezvoltatori, în special în domeniul proiectării sistemelor informaționale reziliente. Sperăm că subiectul este interesant, deoarece definirea infrastructurii informaționale și configurația s*oftware*-ului acesteia ar putea fi folosite cu succes pentru a îmbunătăți proiectarea unor astfel de sisteme, cu scopul de a face față provocărilor mediului de criză.

PRECIZĂRI

Această lucrare a fost finanțată de Ministerul Educației și Științei în implementarea Programului Științific Național – Securitate și Apărare, care este finanțat de Ministerul Educației și Științei al Republicii Bulgaria în implementarea Strategiei Naționale de Dezvoltare a Cercetării Științifice 2017-2030, adoptată prin Hotărârea Consiliului de Miniștri nr. 731 din 21 octombrie 2021.

BIBLIOGRAFIE:

1. Allied Data Publication 34 (ADatP-34) (f.d.). *NATO C3 Technical Architecture, Volume 2 Architectural Descriptions and Models* (Versiunea 6.0). ISSC NATO Open Systems Working Group. Accesat de la NC3TA-Vol 2- v6.xml.
2. Demirov P., S. E. (2019). Informatsiya tai information natasreda, kato obekt za zashtita v cyber prostranstvoto. *Sborniktrudove NK, ISSN 1314-1937.* NVU "V. Levski".
3. ISSC NATO Open Systems Working Group, AC/322(Sc/5)N268. (2002). *NATO C3 Technical Architecture Implementation Handbook (NC3TA-IHB* (Vol. Versiunea 1).
4. Introduction to Kerberos, https://www.ibm.com/docs/en/streams/4.2.1?topic=authentication-introduction-kerberos, accesat la 7 ianuarie 2024.
5. Lightweight Directory Access Protocol (LDAP), https://ldap.com/, accesat la 7 ianuarie 2024.
6. Petters, J. (f.d.). Varonis.com, https://www.varonis.com/blog/ids-vs-ips, accesat la 9 august 2024.
7. Secure Shell (SSH), https://www.ssh.com/, accesat la 5 ianuarie 2024.

8. Simple Mail Transfer Protocol (SMTP), https://www.smtp.com/, accesat la 7 ianuarie 2024.
9. *"What is SIEM? SIEM Defined, Explained, and Explored".* (https://www.forcepoint.com/cyber-edu/siem, accesat la 19 august 2024.
10. *"What Is SIEM?"*. (f.d.). Splunk.com, https://www.splunk.com/en_us/data-insider/what-is-siem.html#overview, accesat la 7 ianuarie 2024.
11. Vasileva, V. (2020). Information Sharing Processes in Public Sector Cybersecurity Structures. *9th International Conference on Application of Information and Communication Technology and Statistics in Economy and Education,* pp. 136-147. Sofia: Publishing Complex – UNWE, http://icaictsee.unwe.bg/past-conferences/ICAICTSEE-2019.pdf, accesat la 5 august 2024.