Infrastructură de tip poligon cibernetic. Aspecte privind arhitectura funcțională

Electra MITAN

Institutul Național de Cercetare-Dezvoltare în Informatică – ICI București

electra.mitan@ici.ro

Rezumat: Scopul acestei lucrări a fost studiul conceptului de poligon cibernetic (PC). S-a urmărit realizarea unei prezentări teoretice sistematizate a literaturii care acoperă acest subiect. A fost prezentată o taxonomie pentru sistemele de PC și arhitectura funcțională, incluzând conținut tehnic, tipuri, clasificări, caracteristici, utilitate. Rezultatele acestui studiu pot fi utilizate ca bază pentru inițiative viitoare în dezvoltarea și evaluarea instrumentelor necesare în conformitate cu cele mai bune practici existente.

Cuvinte cheie: Securitate cibernetică, exercițiu de securitate, poligon cibernetic, arhitectură.

Cyber range type infrastructure. Aspects regarding the functional architecture

Abstract: The purpose of this paper was to study the concept of cyber range (CR). A systematized theoretical presentation of the literature covering this topic was considered. A taxonomy for CRs systems and functional architecture was presented, including technical content, types, classifications, features, utility. The results of this study can be used as a basis for future initiatives in the development and evaluation of these tools in line with existing best practices.

Keywords: Cyber security, Security exercise, Cyber range, Architecture.

1. Introducere

În contextul internațional actual, cu evoluții rapide în plan strategic și tehnologic, demersul de asigurare a securității cibernetice constituie o paradigmă în continuă evoluție. Spațiul cibernetic este caracterizat de dinamism, complexitate și imprevizibilitate. Din perspectiva securității, acest domeniu se transformă ca urmare a intensificării amenințărilor asociate.

Incidentele de securitate la nivel mondial au arătat că există o creștere a complexității și severității amenințărilor la adresa securității cibernetice. Atacatorii devin mai organizați, iar vectorii de atac folosesc tehnici și instrumente avansate și automatizate. Prima linie de apărare împotriva acestor atacuri este creșterea gradului de conștientizare a securității cibernetice în rândul publicului și a abilităților de securitate în rândul profesioniștilor din acest domeniu, pentru a fi la curent cu cele mai noi tehnici și instrumente de amenințare (Barbu, 2016).

În acest sens s-au dezvoltat programe de instruire care includ organizarea de laboratoare și exerciții de securitate cibernetică. În termeni generali, un exercițiu de securitate cibernetică este un exercițiu de antrenament care presupune scenarii de atac și/sau apărare în mediul virtual și/sau fizic, cu ajutorul cărora se pot îmbunătăți înțelegerea și abilitățile participanților. Rezolvarea incidentelor implică pregătirea (procesul de stabilire a politicilor, procedurilor și acordurilor privind gestionarea și răspunsul la incidentele de securitate), detectarea, alertarea (procesul de conștientizare a unui potențial incident de securitate și de raportare a acestuia), sortarea (procesul de examinare a informațiilor disponibile referitoare la un eveniment, pentru a determina dacă a avut sau nu loc un incident de securitate), răspunsul (procesul de încercare a limitării proporțiilor unui incident de securitate), recuperarea și continuarea activităților după incident. Scopul abordării sistematice a gestionării incidentelor de securitate este acela de a asigura posibilitatea reluării activităților/ operațiunilor cât mai repede. Este posibilă păstrarea informațiilor despre incidente pentru analiză și îmbunătățirea securității generale a bazelor de date. Ciclul de viață al unui exercițiu de securitate este format din cinci etape: pregătire (stabilirea obiectivelor; construirea scenariului; construirea metodei de notare; mediul), antrenare, execuție (testarea mediului dezvoltat, conform obiectivelor

https://doi.org/10.33436/v30i4y202010

exercițiului; desfășurarea exercițiului, în care fiecare participant atacant și/sau apărător face demersurile necesare în încercarea de a-și atinge obiectivele stabilite), evaluare (evaluarea participanților pe baza unei metode de notare, cu luarea în considerare a tuturor obiectivelor de învățare) și repetare (curățarea mediului și repetarea întregului proces pentru un nou exercițiu).

În practică, exercițiile de securitate sunt efectuate și evaluate într-o perioadă de câteva ore până la câteva zile, în timp ce pregătirea și cursul teoretic durează de cele mai multe ori câteva luni până la finalizare. Exercițiile de securitate sunt foarte costisitoare și consumatoare de timp. Pentru a întreține și gestiona exercițiile de securitate și mediul lor, a fost propus conceptul de poligon cibernetic – PC (*cyber range*), un mediu virtual utilizat pentru instruirea profesioniștilor în domeniul securității și dezvoltarea tehnologiei specifice în vederea detectării și prevenirii atacurilor cibernetice din lumea reală.

Potrivit Institutului Național de Standarde și Tehnologie (*National Institute of Standards and Technology* – NIST), poligoanele cibernetice sunt definite ca reprezentări interactive simulate aparținând unei organizații și includ: rețea locală, sistem, instrumente și aplicații (vezi Figura 1) și pun la dispoziție un mediu legal și sigur cu ajutorul căruia utilizatorii câștigă experiență practică, își dezvoltă abilitățile cibernetice și se antrenează pentru crearea unui mediu securizat de aplicații (National Initiative for Cybersecurity Education, Cyber Ranges, 2017).

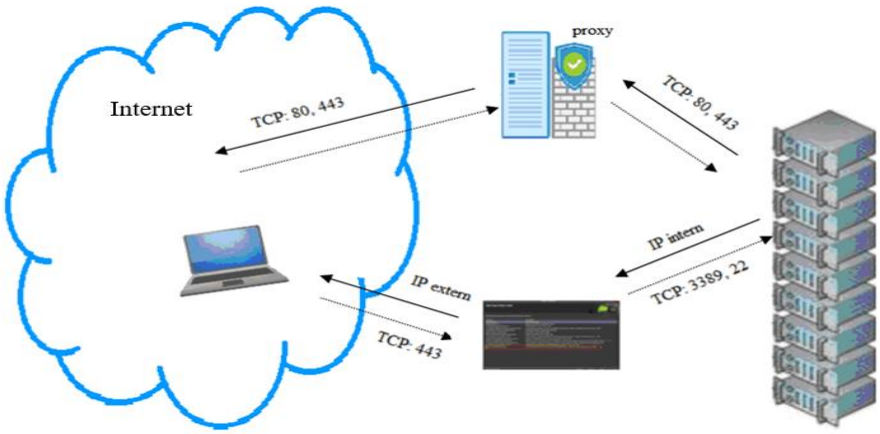

Figura 1. Comunicații PC (cercetare proprie)

Utilizarea PC poate conduce la:

- îmbunătățirea cunoștințelor și a capacităților individuale și ale echipei;
- aplicarea cunoștințelor într-un mediu de rețea simulat, dezvoltarea abilităților cibernetice, lucrul în echipă pentru rezolvarea problemelor cibernetice, pregătirea pentru examene sau evaluări de acreditare cibernetică;
- evaluarea capacităților cibernetice, testarea de noi proceduri și instruirea echipelor cu privire la noile medii și protocoale organizaționale și tehnice.

Modelele tradiționale de educație și formare sunt insuficiente pentru a umple golul de competențe în materie de securitate cibernetică. Poligoanele oferă tehnologie care permite operaționalizarea, previziunea și monitorizarea instruirii și performanței profesioniștilor în domeniul securității cibernetice. PC conferă încredere solicitanților de forță de muncă în domeniul securității cibernetice și angajatorilor forței de muncă în acest domeniu prin aceea că instruirea va aduce și succesul în muncă.

Problematica propusă în cadrul acestui articol, cu caracter teoretic, face obiectul unei componente din proiectul de cercetare PN 19370102/2019 – „*Poligon cibernetic pentru sisteme de control industrial - ROCYRAN*”. După Introducere sunt prezentate, în paragraful 2, componentele tehnice ale unui PC și taxonomia lui, apoi, în paragraful 3, este dată arhitectura funcțională, urmată de clasificarea PC, în paragraful 4. În paragraful 5 sunt descrișii parametrii de caracterizare ai PC, apoi în paragraful 6, utilitatea PC și în final sunt incluse concluzii.

2. Componentele tehnice ale unui PC. Taxonomie

Caracteristicile de bază ale poligoanelor cibernetice, considerate drept catalizatori în reducerea decalajului de competențe ale forței de muncă în domeniul securității cibernetice, sunt: componente tehnice, realism și fidelitate, accesibilitate și utilizare, scalabilitate și elasticitate, curriculum și rezultate ale învățării.

Componentele tehnice ale unui PC sunt prezentate în cele ce urmează:

- *Range / Learning Management System* (RLMS) – conține caracteristicile standard ale unui LMS și caracteristicile unice ale unui PC;
- *Orchestration Layer* (OL) – luând date de la RLMS, acest strat reunește toată tehnologia sau componentele unui PC; facilitează conectarea rețelei infrastructurii fundamentale cu stratul de virtualizare/izolare și infrastructura țintă, permite extensibilitatea dinamică a PC care acceptă *cloud* public, *cloud* privat și infrastructură HW dedicată (Alive, Open Stack, CloudShell);
- *Underlying Infrastructure* (UI) – PC se găsește pe o infrastructură de rețea, servere și stocare, și poate fi construit direct deasupra infrastructurii fizice (*switch*-uri, *router*-e, *firewall*-uri, puncte finale etc.) într-un *rack*, deși acest lucru este de obicei costisitor și nu este scalabil. Din motive de scalabilitate, cost și extensibilitate, mulți furnizori de PC au în vedere o infrastructură virtuală ceea ce conferă realism sau fidelitate PC (HW dedicat, *cloud* public/privat);
- *Virtualization Layer* (VL) – acționează ca un *firewall* între infrastructura țintă (cu vectori de atac asociați) și infrastructura de bază (*cloud*: dedicat, public, privat) (ESX, hyper-V, Ravello, Xen);
- *Target Infrastructure* (TI) – este mediul simulat în care au loc antrenamentele. În funcție de utilizare, poate coincide cu infrastructura IT și de securitate din lumea reală. Un PC avansat conține servere, stocare, puncte finale, aplicații și *firewall*-uri. RLMS generează scripturi pentru a instrui OL să creeze TI. Aceste scripturi includ informații de configurare specifice, intervale de adrese IP, informații de routare, stive de server etc. (operațiuni de securitate – ID/IPS, SEM, FW; aplicații – servere, rețea, stocare);
- ordonanțare; dezvoltare TTP; dezvoltare scenarii de atac; management echipă; raportare.

Taxonomia PC (vezi Figura 2) include următoarele elemente (Priyadarshini, 2018):

- **Scenariu** – **scop** (obiective), **subiect** (dezvoltarea acțiunii), **tip** (static sau dinamic; învățare, testare securitate, experimentare), **domeniu** (cloud, IoT), **instrumente** folosite pentru crearea mediului sau a subiectului, **managementul ciclului de viață** (creare, editare, dezvoltare, generare, rulare);
- **Mediu** – **generare** (utilizatori, trafic, atac), **tip** (simulare, hibrid, emulare, hardware);
- **Învățare** – **instruire**, **analiză**, **evaluare** (tip, metodă);
- **Management** – **interfață** (jurnal de bord, portal), **poligon** (acces la distanță, raportare), **comandă și control**, **resurse** (stocare date), **rol**;
- **Echipe** – roșie, albastră, albă, verde, galbenă, portocalie, gri, violet, autonomă;
- **Monitorizare** – **metode** (automate, manuale), **instrumente** (software și hardware, soluții de gestionare a evenimentelor), **jurnal de bord**, **straturi** (TCP/IP, abstract);

Scenariul este definit de **mediul** de execuție, de subiectul/povestea care indică pașii de execuție ai unui test/exercițiu de antrenament și reprezintă mediul operațional și cerințele de **învățare** care trebuie să asigure îndeplinirea tuturor obiectivelor propuse. Scenariul furnizează documentație, rezumate, ordine de acțiune și asigură contextul operațional reprezentativ pentru obiectivele de testare și formare. Managementul asigură crearea, generarea, editarea, dezvoltarea și rularea scena-

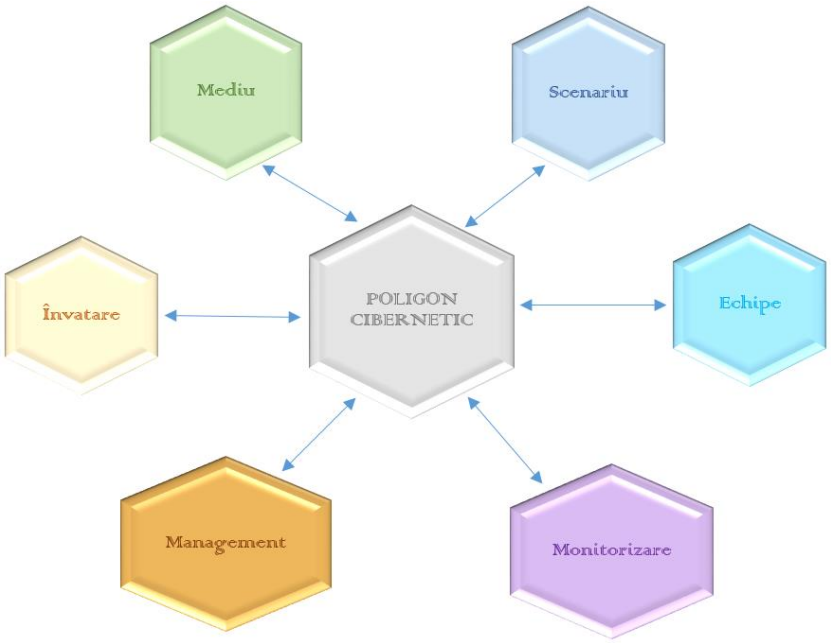

Figura 2. Taxonomia PC. Funcționalități (cercetare proprie)

riului cu ajutorul unor componente specializate sau generate. Scenariile pot fi statice sau dinamice; pot urmări scopuri diferite: testare, educare și experimentare; pot acoperi diferite domenii ca: aplicații de rețea hibridă, rețelistică, sisteme SCADA (SCADA, 2020), inginerie socială, sisteme IoT, infrastructură critică, sisteme bazate pe *cloud*, sisteme autonome. **Managementul** include tablourile de bord care prezintă starea curentă, modulele de raportare cu funcții de start, înregistrarea dispozitivelor și simulare. Evaluarea pune în evidență performanțe tehnice, de un anumit nivel, observate în timpul procesului de **monitorizare** a exercițiilor și testelor de securitate cibernetică. Mecanismul de notare este utilizat pentru a măsura performanțele echipelor și a evalua progresul realizat în timpul unui exercițiu sau al unui test. Evaluarea funcționalității poate apela la metode cantitative și calitative. Într-un exercițiu de securitate cibernetică, pregătirea în echipă include de la o persoană la un grup de indivizi care proiectează, dezvoltă, gestionează și participă la un exercițiu de securitate cibernetică sau la un test. În cadrul unui exercițiu de securitate cibernetică, pe baza rolului pe care îl deține, fiecărei echipe i se atribuie o culoare diferită pentru a-și identifica atribuțiile. Au fost identificate mai multe **echipe**. **Echipa roșie** gestionează atacarea computerelor utilizatorilor folosind anumiți vectori de infecție. **Echipa albastră** gestionează apărarea mediului și prevenirea atacurilor, gestionează caracteristicile infrastructurii de rețea și a infrastructurii aplicațiilor. **Echipa Albă** creează mediul de instruire, proiectează scenarii pentru exerciții și experimente. **Echipa Verde** este responsabilă pentru dezvoltarea, monitorizarea și întreținerea infrastructurii de exerciții proiectate de echipa albă dar și de remedierea erorilor și a blocajelor din infrastructură apărute în timpul desfășurării unui exercițiu. **Echipa Galbenă** raportează conștientizarea situației curente și, în unele cazuri, simularea utilizatorilor care navighează pe *link*-uri de *phishing* sau instalează aplicații *malware*, ceea ce conduce la compromiterea securității rețelei. **Echipa Violet** realizează comunicarea între diferite echipe, prin intermediul schimbului de informații, pentru a spori eficacitatea exercițiului. **Echipa Portocalie** gestionează atribuirea de sarcini tehnice diferite membrilor echipei albastre în timpul exercițiului. **Echipa Gri** gestionează solicitările normale de trafic și serviciile care trebuie întreținute. Anumite roluri ale unei anumite echipe pot fi automatizate cu ajutorul unor instrumente și tehnici diferite; astfel se constituie componenta – **echipa autonomă** a respectivei echipe.

3. Arhitectura funcțională a unui PC

Pe baza taxonomiei se evidențiază o arhitectură funcțională unificată (vezi Figura 3) ce include componente principale și, în cadrul fiecărei componente, se identifică o serie de sub-componente: **Portal** (Utilizatori, Administrare, Clienți); **Management** (PC, Scenarii,

Exerciții/Teste); **Modul de antrenare și instruire** (Notare, Instruire, Analiză); **Modul de testare** (Definire cazuri testare, Analiză și verificare); **Scenarii** (Creare/Editare, Dezvoltare, Generare, Executare, Control, Ștergere); **Monitorizare** (Colectare, Analiză, Logare); **Mediu de rulare** (Emulare, Simulare, Generare trafic, Generare atac, HW, Generare comportament utilizatori); **Stocare date** (Parametri de simulare, Definire scenarii, Reguli, Index informații, Date replicate, Instrumente) [Mudassar, 2020].

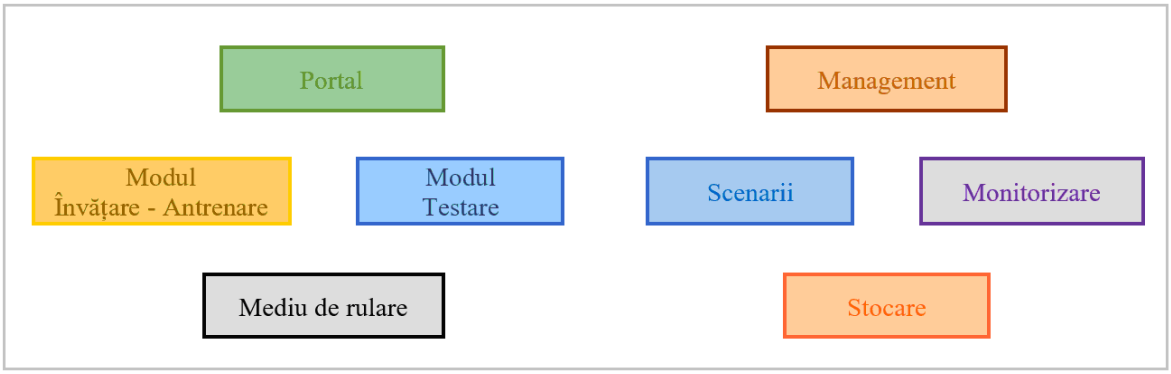

Figura 3. Arhitectura funcțională a PC (cercetare proprie)

Portalul constituie interfața pentru comunicarea între un PC sau un banc de teste de securitate și mai mulți utilizatori: administratori de PC, utilizatori ai echipei albe care creează și editează scenarii de securitate cibernetică și alți clienți care folosesc PC pentru teste și experimente. Se pot desfășura activități de gestionare a PC sau a bancului de teste, ceea ce presupune gestionarea resurselor și gestionarea accesului altor utilizatori (instructor, tester, stagiar, creator de scenarii – membru al echipei albe). Aceste scenarii pot fi implementate pentru exerciții și experimente de securitate cibernetică. Clienții pot utiliza resursele pentru testare și experimentare, în funcție de cerințe.

Managementul asigură gestionarea resurselor (capacitate memorie, procesare și stocare) și a rolurilor (atribuirea de sarcini pentru exerciții și experimente de securitate cibernetică). Managementul PC și al testelor de securitate este legat de administrarea generală. Se pot atribui roluri managerilor de exerciții și experimente, precum și resurselor de calcul necesare pentru desfășurarea fiecărui exercițiu și derularea experimentului. Managementul unui exercițiu asigură segregarea rolurilor și a resurselor exercițiului sau a unui participant la experiment. Se pot realiza mai multe scenarii, în cadrul cărora se pot gestiona mai multe exerciții sau experimente într-un mediu definit. Colectarea extinsă a informațiilor și a analizelor jurnalului se realizează pe infrastructura PC și a bancului de teste într-o manieră optimă.

Învățare – antrenare pune la dispoziție un tutorial de instruire care constă în concepte de securitate cibernetică și exerciții practice cu caracter educațional. Rezultatul antrenamentului este evaluat folosind un mecanism de notare. Se pot utiliza mai multe mecanisme de notare, cum ar fi: punctarea bazată pe *flag*-uri, punctarea bazată pe *task*-uri, punctarea cu ajutorul informațiilor cuprinse în jurnalul de evenimente. După analiza acțiunii folosind *feedback*-ul participanților la instruire și a informațiilor legate de evenimente, prin eliminarea elementelor ineficiente din desfășurarea exercițiilor de securitate crește nivelul calitativ al acestora.

Testarea și evaluarea securității sunt elemente cheie. Există două tipuri principale de teste care pot fi efectuate: testarea securității unui sistem / produs, respectiv testarea unei noi metode sau tehnici de apărare sau atac. Un modul de testare are ca scop definirea cazurilor de testare, care vor fi transformate în scenarii ce se implementează și execută în mediul de rulare. După executarea scenariului, prin modulul scenariului și mediul de rulare, rezultatul se trimite înapoi la modulul de testare pentru efectuarea analizei finale și evaluarea sistemului / produsului supus testării.

Scenariul în care membrii echipei albe pot accesa interfața pentru crearea de scenarii și pot crea, edita, implementa, genera, executa, controla, salva și șterge scenarii de securitate. Există o listă de scenarii predefinite care pot fi modificate conform cerințelor impuse de un anumit scenariu proiectat. Toate activitățile se desfășoară într-un mediu emulat, simulat sau hibrid. Generatorul de

scenarii este utilizat pentru generarea de noi scenarii de securitate utilizând configurații de scenarii minime. Se execută scenariul și se efectuează diferite acțiuni pe parcursul defășurării lui, cum ar fi: forțarea traficului în rețea, inițierea comportamentului unui utilizator, în diferite etape, pentru a face scenariul mai realist. De menționat faptul că este permisă modificarea scenariului în timpul execuției sale.

Monitorizarea permite supervizarea exercițiului de securitate și realizarea experimentelor. Se pot colecta jurnalele de acces și realiza analize pe aceste jurnale. Sursele de jurnal conțin diferite interfețe de rețea și sisteme de operare. Jurnalele au diferite formate și, cu ajutorul tehnicilor de pre-procesare, sunt aduse la același format. Apoi, analiza este efectuată în vederea identificării diferitelor activități efectuate în exerciții de către participanții la experiment, în diferite etape ale unui exercițiu și a unui scenariu de experiment.

Mediul de rulare include infrastructura pe care este implementat scenariul, reprezentată de platforme fizice, virtuale, hibride și *cloud*. Echipa roșie atacă infrastructura, iar echipa albastră apără infrastructura. Activitățile ambelor echipe creează evenimente care sunt monitorizate și notate. Exercițiul de securitate cibernetică și mediul de experimentare sunt mai realiste prin generarea comportamentului utilizatorului și un trafic de rețea aleator.

4. Clasificarea PC

Tipurile de PC dezvoltate până în prezent au o varietate de caracteristici și capabilități. Există patru tipuri principale de PC: simulare, suprapunere, emulare și hibrid.

Prin **simulare** se recreează un mediu de rețea sintetic bazat pe comportamentul componentelor reale ale rețelei, rulează în instanțe virtuale și nu necesită echipament fizic de rețea. Într-un mediu de simulare tipic, mașinile virtuale (*virtual machines* – VM) replică un server specific, rețea și stocare a unei anumite infrastructuri IT (mici, medii, mari etc.). Aceste șabloane VM sunt standardizate și oarecum limitate în privința simulării infrastructurii IT reale. Apropierea de infrastructura țintă asigură fidelitatea exercițiului. Avantajul unui mediu de simulare este viteza de reconfigurare și capacitatea de a utiliza echipamente de stocare și server generice. Dezavantajele principale ale unei rețele simulate sunt o latență imprevizibilă și nerealistă, precum și fluctuația performanței rețelei.

În cazul **suprapunerii** avem PC care rulează pe rețele reale, servere și mediu de stocare. Acestea au un avantaj semnificativ în ceea ce privește fidelitatea față de cazul simulare, dar au un cost considerabil al hardware-ului și al infrastructurii de rețea. De obicei, aceste rețele sunt configurate ca bancuri de testare globale.

Prin **emulare** rulează PC pe o infrastructură de rețea dedicată, mapând o rețea/server/ infrastructură de stocare construită pe infrastructură fizică: o infrastructură fizică care devine PC. Se pot furniza experiențe cu medii multiple interconectate. Se pot include generări de trafic care emulează numeroase protocoale, tipare sursă, fluxuri de trafic, atacuri și conectivitate la Internet. Realizată corect, emularea creează experiențe adevărate, mai degrabă decât acțiuni și răspunsuri pre-programate.

Configurațiile **hibrid** apar din combinații personalizate a oricăruia dintre tipurile descrise anterior.

Clasificarea PC se poate face pe baza următoarelor criterii (Priyadarshini, 2018):

- după infrastructura asociată: public / privat / federativă;

Pe infrastructură federativă sunt PC: NCR (NCR Cyber Range, 2020), CRATE (CRATE Cyber Range, 2020), NATO (NATO Cyber Range, 2020), Raytheon (Raytheon Cyber Range, 2020) și DoD (DoD Cyber Range, 2020), iar IBM (IBM Cyber Range, 2020) este pe infrastructură privată. CISCO (CISCO Cyber Range, 2020), Baltimore (Baltimore Cyber Range, 2020) și Virginia (Virginia Cyber Range, 2020) sunt exemple de PC care aparțin atât grupurilor de infrastructuri publice cât și private. Michigan (Michigan Cyber Range, 2020) și Florida (Florida Cyber Range, 2020) au infrastructură asociată publică, privată și federativă.

- utilizarea de implementări bazate pe: *cloud*/*cloud* + VPN/fără *cloud*;

Unele PC implementează VPN, iar altele se bazează pe rețeaua virtuală de clonare (*Virtual Clone Network* - VCN). În general, PC care utilizează platforma *cloud*, implementează și VPN. PC de la Universitatea din Delaware implementează un VPN fără infrastructură *cloud*. PC Virginia, IBM și Florida utilizează platforma *cloud*. CISCO, DoD, Michigan, CRATE, NATO etc. acceptă *cloud* și VPN.

- după tipurile de echipe incluse (roșie, albastră, verde, galbenă, violet, albă, gri);

PC includ grupuri diferite de utilizatori: studenți, profesioniști, clienți și pot accepta mai multe tipuri diferite de instrumente și platforme. În funcție de mediul de funcționare și de scopul declarat, pot fi găzduite diferite tipuri de echipe. Echipele roșii și albastre sunt comune pentru toate PC. NCR include o echipă gri. NATO include echipă galbenă, albă și verde. PC de la Universitatea Delaware (Delaware Cyber Range, 2020) include o echipă violet.

- implementarea bazată pe mașini virtuale/mașini virtuale + *sandbox*-uri (*sandboxes*- este un mecanism de securitate care separă programele care rulează, pentru a atenua eșecurile sistemului / vulnerabilitățile software, fiind folosit pentru rularea de cod, fără a deteriora mașina gazdă / sistemul de operare).

Ambele modalități oferă izolare și este posibil să nu poată evita activitățile dăunătoare care au loc în cadrul unei aplicații, ele pot fi diferențiate din anumite motive. Deoarece sunt implementate în moduri diferite, ele posedă software diferit, fișiere și sisteme de operare. Mașinile virtuale oferă o izolare completă, cu un contact limitat la aplicații, *browsere* și depozite. *Sandbox*-urile oferă o izolare flexibilă. În general, PC sunt implementate pe mașini virtuale iar unele dintre ele iau în considerare și *sandbox*-urile. Testarea *malware*-urilor pe mașini virtuale este mai sigură decât testarea pe *sandbox*-uri, deoarece acestea din urmă sunt insuficiente pentru testarea cazurilor complexe. PC care sunt implementate numai pe mașini virtuale sunt: Virginia, CRATE, CISCO, Universitatea Delaware, Baltimore, Florida, iar PC implementate pe mașini virtuale și *sandbox*-uri sunt: Michigan, IBM, NATO, DoD.

5. Parametrii de caracterizare ai PC

PC sunt orientate spre operare; de aceea, performanța lor depinde de anumiți parametri. O serie dintre ei sunt considerați esențiali pentru caracterizarea poligoanelor și au o anumită semnificație pentru acestea. Fiecare parametru poate fi reprezentat pe o scală de reprezentare: foarte mare, mare, mediu, mic, foarte mic (vezi Figura 4). Pentru fiecare dintre parametrii prezentați se precizează valoarea calitativă. Acești parametri sunt:

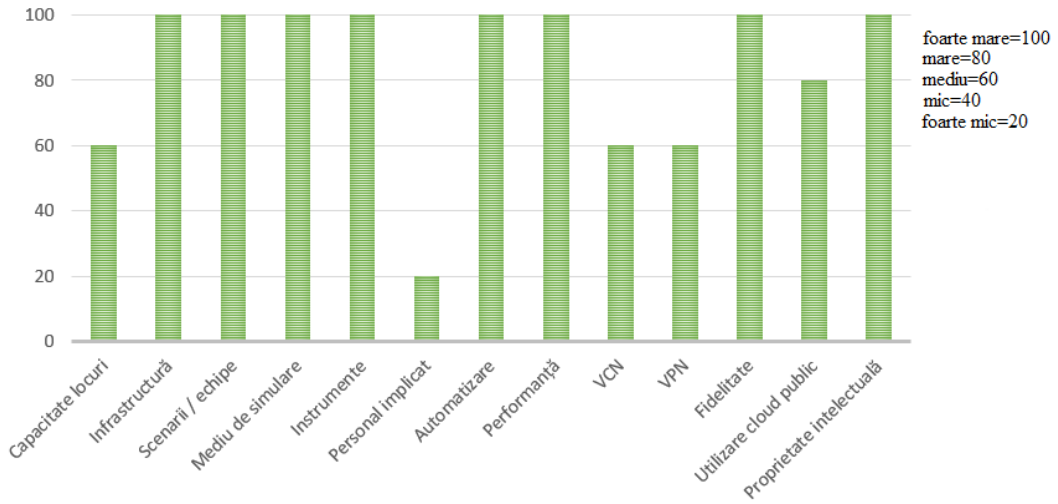

Figura 4. Reprezentarea parametrilor de caracterizare ai unui PC (cercetare proprie)

- **Capacitate** – Se referă de numărul de locuri (24–320) și la sistemele incluse. Unele PC sunt disponibile pentru utilizatori la distanță (**mediu**);
- **Infrastructură** – Este specifică, în concordanță cu funcția PC; permite separarea mediilor de testare și permite capacitățile de testare hardware în buclă. Combinarea diferitelor infrastructuri contribuie la mărirea scalabilității și a fiabilității. (**foarte mare**);
- **Scenarii/echipe** – Fiecare echipă are propriile cerințe specifice. Un poligon mai mare presupune echipe mai numeroase. Atacul echipei roșii este esențial în descoperirea lacunelor din sistem (de exemplu, trimiterea de trafic rău intenționat - atacuri de rețea și *spyware*). Echipa albastră este responsabilă de gestionarea infrastructurii de rețea utilizând servere de aplicații antivirus, pe un dispozitiv fizic (ca mecanism de contracarare pentru repararea și consolidarea sistemului, în vederea neutralizării viitoarelor atacuri). Echipa verde simulează utilizatorii și traficul bun care accesează aplicațiile găzduite pe infrastructura de rețea administrată de echipa albastră. Echipa violet stabilește obiective cu privire la atac și apărare. Echipa albă monitorizează componentele infrastructurii critice utilizând DNS, sisteme de detectare a intruziunilor, simulatoare de trafic și servere de aplicații. PC oferă o platformă pentru a acoperi toate funcțiile esențiale ale fiecărei echipe. Toate aceste echipe sunt esențiale pentru PC. (**foarte mare**);
- **Mediu de simulare –** Un PC ar trebui să poată simula tot ceea ce înseamnă Internet și operațiuni, făcând uz de platforme de simulare precum (Metova, 2020), Cyberbit (Cyberbit, 2020), Tintri (Tintri, 2020). O problemă importantă este furnizarea de scenarii din viața reală pentru instruire și testare; simulatoarele sunt un element important deoarece ajută la analiza datelor confidențiale, precum și la procesul de luare a deciziilor. PC lucrează cu trei tipuri de simulare: reală (efectuată pe sisteme reale sub formă de exerciții cibernetice într-un mediu fizic al rețelelor izolate), virtuală (evaluarea capacităților practice, de control și de cooperare prin simularea sistemelor reale), constructivă (sistemele simulate sunt operate de obiecte simulate). Instrumentele de simulare pot îmbunătăți fidelitatea traficului, analiza activelor, capacitățile de virtualizare. (**foarte mare**);
- **Instrumente** – Unele PC includ instrumente complexe, cum ar fi: SAST - *Systems Administrator Simulation Trainer* și ANTS - *A Network Traffic Synthesizer*, pentru intruire și testare intense. Alte instrumente de bază pot fi: Wireshark (Wireshark, 2020), John the Ripper (incorporabile în sisteme de operare) (John the Ripper, 2020), Encase (Encase, 2020), Sleuth Kit (instrumente criminalistice) (Sleuth, 2020). (**foarte mare**);
- **Personal implicat –** Utilizatorii pot fi: studenți, profesioniști, clienți, personal, oficiali guvernamentali, militari, cercetători, profesioniști în drept etc. PC poate include mai multe servere, instrumente și platforme ce permit accesul la distanță, ceea ce elimină necesitatea implicării directe a persoanelor. Personalul semnificativ, cum ar fi un administrator sau alt personal tehnic, este o componentă indispensabilă cu implicare directă în toate aspectele, din punct de vedere tehnic. Totuși, este posibil ca accesul să poată fi realizat de la distanță, ceea ce face ca necesitatea personalului în PC să fie redusă. (**foarte mic**);
- **Automatizare** – PC includ un număr mare de dispozitive, servere, operațiuni, trafic de rețea. Un mediu automatizat poate contribui la consolidarea stabilității, securității și infrastructurii PC, la configurarea rapidă și eliminarea mediilor de testare, crearea rapidă a infrastructurii de testare pentru topologie și corelarea sistemului, consolidarea controlului și aprovizionarea automată a mediului. Automatizarea conduce la testarea mediilor complexe. Astfel, automatizarea este esențială pentru PC, ceea ce face ca această cerință să fie foarte ridicată. (**foarte mare**);
- **Performanță –** PC pot gestiona simultan site-uri web cu trafic ridicat, supraîncărcarea serverelor conducând la o degradare a funcționării. Echilibratoarele de sarcină pot surmonta întreruperile prin distribuirea eficientă a traficului între mai multe servere. În

cazul rulării de operațiuni în *cloud* cu mai multe servere, vizibilitatea în timp real este o necesitate pentru că ajută la înțelegerea alocării resurselor și la stabilirea necesarului de resurse suplimentare. Echilibrarea sarcinii oferă disponibilitate ridicată, depinde de dimensiunea PC și de numărul de platforme și instrumente acceptate. (**foarte mare**);

- **Rețea virtuală de clonare –** Oferă într-un mediu realist, instruire și evaluare, luând în considerare gestionarea riscurilor și testarea ipotezelor pentru incidente cibernetice în timp real. Analiza comparativă a soluțiilor actuale conduce la soluții mai bune pentru viitor. Pe de-o parte, această rețea face PC relativ mai eficient, deoarece VCN nu sunt limitate la rețele mici, asigură scalabilitate și fiabilitate. Pe de altă parte, sunt consumatoare de resurse numeroase și se ridică problema fiablității. (**mediu**);
- **VPN** – Prin implementarea VPN, Cisco și DoD încurajează îmbunătățirea securității, a performanțelor, deoarece se pot partaja fișiere, este permis accesul la distanță, se pot obține adrese diferite IP. În cazul când din motive de securitate adresele de protocol Internet au fost mascate, se pot accesa site-uri web blocate, se poate ocoli conținutul, este permis anonimatul on-line, este disponibil un mecanism performant pentru derularea de activități ofensive/defensive. (**mediu**);
- **Fidelitatea –** Este o măsură de acuratețe, corectitudine, autenticitate. Mediile PC de înaltă fidelitate permit testarea independentă și obiectivă, evaluarea caracteristicilor avansate, instruirea și testarea complexă în toate fazele ciclului de viață al sistemului, testarea sistemelor complexe. (**foarte mare**);
- **Utilizarea infrastructurii *cloud* public –** Permite reproducerea scenariilor din lumea reală; se adaugă un strat suplimentar de hipervizor care oferă izolare (pentru experimentarea *malware*, alte tehnici distructive) și auto-routare; se pot furniza PC preconfigurate și personalizate ca medii izolate. Utilizarea *cloud*-ului conduce la unele neajunsuri; este blocată difuzarea, se oferă acces de la nivelul 3 în sus, în condițiile în care multe implementări se bazează pe protocoale de nivel 2, nu este acceptată oglindirea porturilor ceea ce conduce la o dificultate în monitorizarea traficului. (**mediu - mare**);
- **Proprietatea intelectuală** – Constă în realizarea de scenarii, jocuri sau provocări pentru îndeplinirea unor sarcini. Ca exercițiu pentru echipa roșie/albastră, utilizatorul poate include provocări (distrugerea unui sistem, securizarea acestuia, un sistem ca un întreg pentru a construi un sistem *open source*). (**foarte mare**).

Este posibil ca viitoarele cercetări să reliefeze nevoia de noi parametri pentru a-i adăuga în această analiză. Toate acestea trebuie să pună în evidență furnizarea de: feedback în timp real cu simulare de înaltă fidelitate; mediul în care echipele se pot angaja pentru a sprijini experimentele; mediul în care echipele pot testa diverse ipoteze; metricile și datele de evaluare bazate pe performanță.

6. Utilitatea PC

PC sunt platforme interactive, simulate și reprezentări ale rețelelor, sistemelor, instrumentelor și aplicațiilor care pot oferi: învățare și evaluare bazate pe performanță; simularea experienței la locul de muncă; un mediu simulat în care echipele pot lucra împreună pentru a îmbunătăți munca în echipă și capacitățile echipei; un mediu în care ideile noi pot fi testate și echipele pot lucra pentru a rezolva probleme cibernetice complexe; *feedback* în timp real.

Fiind medii virtuale, PC nu sunt limitate la rețeaua locală a unei organizații, astfel încât pot fi utilizate de către organizații publice și private (universități, guvern, industrie, mici afaceri, public, media), împreună cu cercetători, studenți, furnizori de educație, formatori.

Profesorii pot implementa cursuri și programe de învățământ de bază în domeniul securității cibernetice. Sunt organizații sau persoane interesate de pregătire și educație continuă pentru

operațiuni de securitate; analize și specializare criminalistică; testarea de produse noi; lansări de software și restructurare organizațională. Există organizații sau persoane care urmăresc validarea abilităților de securitate cibernetică în vederea evaluării candidaților pentru ocuparea unor funcții în domeniul securității cibernetice. Există persoane care caută pregătire pentru forța de muncă pentru personalul care se transferă în domenii și poziții legate de securitatea cibernetică.

Utilizarea PC în domenii specifice de aplicații include sistemele de control industrial, rețelele mobile ad-hoc și sistemele cibernetice.

În funcție de scopul pentru care sunt utilizate, PC pot avea următoarele destinații:

În domeniile **militar**, **apărare** și **informații**, organizațiile militare sau agențiile guvernamentale solicită personal cu abilitățile necesare pentru combaterea terorismului cibernetic (Figura 5). Vulnerabilitățile și punctele slabe sunt esențiale pentru infrastructura unei națiuni. Astfel, armata fiecărei țări trebuie să implementeze PC pe scară largă (NCR Cyber Range, 2020).

Figura 5. Poligon cibernetic. Mediu de antrenare (https://www.cyberbit.com/)

Un PC pentru **educație** este o idee apărută în 2015 pentru a oferi instruire militarilor și veteranilor, dar și instruire pe subiecte legate de atacuri cibernetice, apărare și detectare, dezvoltarea certificărilor, colaborare cu mediul industrial, cercetare.

Întreprinderile și **organizațiile comerciale** implementează PC pentru a realiza simulări și exerciții în vederea consolidării capacității de apărare împotriva atacurilor cibernetice. Întreprinderile trebuie să desfășoare pregătire la standarde cât mai înalte, pentru a putea face față aplicațiilor, amenințărilor și volumelor de trafic aflate într-o continuă creștere. Soluțiile de PC implementate trebuie să creeze un mediu relevant din punct de vedere operațional pentru a reflecta rețeaua globală de informații (*Global Information Grid* - GIG) și pentru a permite simulări sofisticate dar și gestionarea unei rețele distribuite de PC.

Formarea în domeniul securității cibernetice poate fi realizată prin crearea de noi linii de afaceri și înființarea de centre de formare, de simulare a securității cibernetice și de furnizare de **servicii avansate** de formare și testare.

Un mediu sigur de învățare, *hacking*, testare, jocuri de război, practici *malware* și provocări reale ale adversarilor ajută profesioniștii în securitate să capete experiență practică pentru acțiunile din lumea reală. Dacă acesta este și gratuit (*open source*), accesibil pe Internet și sigur, constituie pentru începători și experți un mod de testare a abilităților și de exersare a practicilor de securitate.

Aplicațiile în domeniul militar cu **respectarea legii** sunt dezvoltate și testate în PC, garantând fezabilitatea și eficacitatea lor practică. Fiecare dispozitiv utilizat crește vulnerabilitatea unei infracțiuni cibernetice. Autoritățile legitime pot răspunde infracțiunilor informatice rezultate și asigură asistență tehnică în domeniul criminalistică și investigații, pe lângă instruire, ajutor acordat victimelor și educație în rândul comunității.

7. Concluzii

În timp ce tehnologia cunoaște o dezvoltare continuă, infracțiunile informatice au devenit tot mai sofisticate. Zi de zi, breșele din sistemele informatice pun în pericol securitatea datelor care pot include informații personale ale cetățenilor. Securitatea cibernetică reprezintă o provocare globală de actualitate prin prisma faptului că, pe parcursul ultimelor decenii, numărul de atacuri cibernetice au înregistrat o creștere deosebită. Spațiul cibernetic este considerat domeniu de război; de aceea, lupta împotriva crimelor din acest domeniu presupune o pregătire adecvată în domeniul securității cibernetice.

În lucrare a fost prezentat poligonul cibernetic, un concept relativ nou în domeniul securității cibernetice, o platformă fizică/virtuală ce poate fi folosită pentru pregătirea specialiștilor sau pentru experimentări în domeniul securității cibernetice. Au fost prezentate componentele tehnice și taxonomia PC, arhitectura și specificațiile funcționale, tipurile cunoscute de PC și clasificarea lor, parametrii de caracterizare, utilitatea PC.

În viitor, cercetarea se va concentra pe tipurile de exerciții și competiții de apărare cibernetică care pot fi folosite pentru antrenarea specialiștilor, studiul celor mai cunoscute platforme de tip PC, studiul uneltelor care permit definirea de scenarii și *deployment*-ul automat al mașinilor virtuale necesare derulării unui exercițiu.

Mențiuni

Prezenta lucrare are la bază parte din activitățile și rezultatele temei de cercetare PN 19370102/2019 – „*Poligon cibernetic pentru sisteme de control industrial - ROCYRAN*”, proiect ce a fost finanțat în cadrul Programului Național Nucleu 2019-2022.

BIBLIOGRAFIE

1. Baltimore Cyber Range. https://www.baltimorecyberange.com/, accesat septembrie 2020.
2. Barbu, C.D. (2016). *Îmbunătățirea protecției infrastructurilor critice din sectorul TIC prin creșterea rezilienței.* În Revista Română de Informatică și Automatică (Romanian Journal for Information Technology and Automatic Control), vol. 26, nr. 4/2016.
3. CISCO Cyber Range. https://www.ciscolive.com/, accesat septembrie 2020.
4. CRATE Cyber Range. https://www.foi.se/en/foi/resources/crate, accesat septembrie 2020.
5. Cyberbit. https://www.cyberbit.com/, accesat septembrie 2020.
6. Delaware Cyber Range. https://udspace.udel.edu/, accesat septembrie 2020.
7. DoD Cyber Range. https://www.hqmc.marines.mil/doccsr/, accesat septembrie 2020.
8. Encase. https://www.guidancesoftware.com/encase-forensic, accesat octombrie 2020.
9. Florida Cyber Range. https://www.floridacyberrange.org, accesat septembrie 2020.
10. IBM Cyber Range. https://www.ibm.com/security/services/managed-security-services/security-operations-centers, accesat septembrie 2020.
11. John the Ripper. https://www.openwall.com/john/, accesat octombrie 2020.
12. Metova. https://metova.com/, accesat octombrie 2020.
13. Michigan Cyber Range. www.merit.edu/cyberrange, accesat septembrie 2020.

14. Mudassar, M., Y. B. Katt, & V. Gkioulos (2020). *Cyber ranges and security testbeds: Scenarios, functions, tools and architecture*. În „Computers & Security" Volume 88, January 2020, https://doi.org/10.1016/j.cose.2019.101636.
15. National Initiative for Cybersecurity Education, Cyber Ranges (2017). *National Institute of Standards and Technology (NIST)*. US Department of Commerce, nvlpubs.nist.gov., accesat septembrie 2020.
16. NATO Cyber Range. https://www.nato.int/nato_static_fl2014, accesat septembrie 2020.
17. NCR Cyber Range. https://www.peostri.army.mil/national-cyber-range-ncr, accesat septembrie 2020.
18. Priyadarshini, I. (2018). *Features and Architecture of the Modern Cyber Range: A Qualitative Analysis and Survey*, https://www.researchgate.net/publication/327835952.
19. Raytheon Cyber Range - Cyber Range | Raytheonwww.raytheon.com › cyber, accesat septembrie 2020.
20. SCADA. https://www.sielcosistemi.com/en/what-is-scada.html, accesat septembrie 2020.
21. Sleuth. http://www.sleuthkit.org/, accesat octombrie 2020.
22. Tintri. https://tintri.com, accesat octombrie 2020.
23. Virginia Cyber Range. https://www.virginiacyberrange.org/, accesat septembrie 2020.
24. Wireshark. https://www.wireshark.org/, accesat octombrie 2020.

Electra MITAN este cercetător științific în Departamentul „Modelare, Simulare, Optimizare" în cadrul Institutului Național de Cercetare-Dezvoltare în Informatică – ICI București. A absolvit Facultatea de Matematică din cadrul Universității București. Principalele domenii de interes pentru activitatea de cercetare includ: modelare matematică, optimizare, e-business, e-learning, securitate cibernetică, Big Data, Machine Learning and Statistics, dezvoltarea de sisteme informatice. A publicat peste 30 de articole științifice în reviste și o carte.

Electra MITAN is a scientific researcher in the "Modeling, Simulation, Optimization" Department within the National Institute for Research and Development in Informatics – ICI Bucharest. She graduated Mathematics Faculty, University of Bucharest. The main areas of interest for research activities include: mathematical modeling, optimization, e-business, e-learning, cyber security, Big Data, Machine Learning and Statistics, development of computer systems. She published over 30 articles in scientific journals and conferences proceedings and a book.