Universitatea POLITEHNICA București

Teză de Doctorat

in Calculatoare, Tehnologia Informației și Automatică

CR-LM: Managementul unui Laborator de tip Poligon Cibernetic (Cyber Range)

ARHITECTURĂ ȘI FUNCȚIONALITĂȚILE UNUI POLIGON CIBERNETIC IDEAL

prezentată de

Drd.ing. Dragoș-George IONICĂ

Conducător Doctorat:

Prof.dr.ing. Florin POP

2021

București, România

RECUNOAȘTERE

Îmi imaginez cu greu că aș fi putut finaliza această lucrare fără ajutorul multor persoane de specialitate. Nu îi voi numi pe toți aici deoarece nu le pot mulțumi îndeajuns de mult pentru ajutor. Aș dori să le ofer mulțumirile mele Prof. Florin Pop, Prof. Ciprian Dobre, Prof. Decebal Popescu și Prof. Nirvana Popescu, îndrumătorii mei în cercetare în timpul studiului de doctorat, pentru tot ajutorul, suportul și coordonarea.

Au fost întotdeauna disponibili și mi-au oferit sfaturi în ciuda programului aglomerat. Gândirea lor analitică m-a ajutat în timpul dezvoltării cercetărilor și m-a ajutat să identific noi idei și scenarii pentru activitatea mea. Aștept cu nerăbdare să colaborez cu ei în viitor pentru a pune în practică mai multe implementări și exerciții care pot avea scopuri educaționale.

As dori să îmi exprim recunoștința tuturor colegilor mei de la Centrul National Cyberint pentru suportul necondiționat din timpul studiilor mele de doctorat. Încurajările lor au fost o sursă de inspirație pe tot parcursul meu profesional. În acești ani, m-am simțit onorat să întâlnesc atâția oameni minunați care m-u inspirat cu idei, m-au provocat și m-au ajutat să avansez în cercetare.

Aș dori să menționez aici (o listă departe de a fi finalizată) pe Mihai Predescu, Aniello Castiglione (Universitatea din Salerno), Edouard Ivanjko (Universitatea din Zagreb), prieteni și colegi de la Universitatea Politehnica din București și mulți alții.

Cuprins

Rezumat

În ultimele decenii, securitatea cibernetică devine una dintre provocările eminente la nivel mondial datorită creșterii remarcabile a înregistrărilor de atacuri cibernetice. Pentru protecția datelor cu caracter personal, pentru a garanta un mediu sigur de muncă și productivitate, este important să se acorde atenția cuvenită securității cibernetice . Însușirea cunoștințelor din domeniul securității cibernetice este esențială pentru a evita eventualele atacuri ce pot apărea atât în cadrul infrastructurilor de tip enterprise, dar și a celor cu valențe critice. Cunoștințele privind securitatea cibernetică și formarea în domeniul securității cibernetice sunt încurajate de mediile cu infrastructuri critice și importanța acestora prin implementarea unor poligoane cibernetice pentru exersarea mai multor scenarii.

Principalele obiective ale tezei au fost studierea arhitecturilor și caracteristicilor complexe care pot fi utilizate în poligoanele cibernetice, identificarea celor mai utilizate arhitecturi și caracteristici în poligoanele cibernetice la nivel mondial și aspectele cheie ale acestora care pot fi utilizate pentru a crea un concept de tip Next-Generation Cyber-Range, precum și să identifice avantajele creșterii nivelului de conștientizare în cadrul departamentelor de securitate cibernetică ale infrastructurilor cu valențe critice.

Multe dintre rezultatele prezentate în această teză sunt strâns legate sau motivate de exerciții practice și provocări din viața reală pe care le-am întâlnit în timpul activităților sau sarcinilor mele zilnice. În acest sens, contribuțiile mele științifice se referă la arhitecturi complexe și caracteristici care pot fi utilizate în poligoanele cibernetice, evaluarea scenariilor propuse atât pentru echipele de tip Red Team, respecitv Blue Team , cum se poate proiecta o platformă colaborarativă eficientă care să poată simula atacuri de la infrastructuri de bază la infrastructuri critice care ar putea conține PLC-uri sau sisteme SCADA.

1. Introducere

Această lucrare prezintă o scurtă descriere a poligoanelor cibernetice existente precum și operațiunile ce vizează rețelele de calculatoare cu valențe, ce au ca scop îmbunătățirea pregătirii în domeniul securității cibernetice. Acest capitol introductiv oferă un rezumat succint al arilor cu probleme în care dezvoltările cibernetice din cadrul unor instituții precum Ministerului Apărării (MoD) sunt introduse odată cu un astfel de poligon cibernetic pentru testarea și aprofundarea cunoștințelor în domeniu. Scopul cercetării este de a introduce limitările acestor studii și rezultatele dorite. Acest capitol este bazat **pe Capabilitățile Apărării Cibernetice în Rețelele Complexe**.

Provocările din domeniu

În planurile sale de pregătire și apărare, instituții cu astfel de responsabilități precum Ministerele Apărării (MA) ale mai multor țări au considerat reducerea masivă a costurilor pentru operațiunile realizate, iar această dorință a înclinat spre domeniul rezilienței digitale și a operațiunilor din domeniul securității cibernetice.

Sunt câteva exemple de guverne, precum guvernul Regatului Unit al Marii Britanii și guvernul Olandei, care au dedicat aproximativ 50 milioane de euro pentru investiții în domeniul rezilienței digitale și operațiilor digitale pentru a fi utilizate în întărirea arsenalului din domeniul securității cibernetice în anul 2016 [1].

Din perspectiva guvernului Statelor Unite, care poate fi generalizată, strategia unui mediu cibernetic al unui Minister al Apărării bine pregătit are șase obiective:

1. Realizarea unui abordări coerente și a unei evaluări bune din punctul de vedere al securității cibernetice;
2. Creșterea rezistenței securității cibernetice a MA și a altor infrastructuri critice;
3. Dezvoltarea capabilității MA de a executa operații cibernetice (atât de apărare cât și de atac);
4. Dezvoltarea mai multor capabilități informaționale în domeniul securității cibernetice;
5. Dezvoltarea cunoștințelor și acumularea capabilităților inovative în domeniul securității cibernetice;
6. Dezvoltarea națională și internațională a cooperărilor cu alte MA sau CSIRTS.

Viitoarea structură guvernamentală a unui MA va fi asemănătoare cu cea specificată mai sus [2]. Prima entitate din structură este reprezentată de Comanda Cibernetică (Cyber Command) care va prelua operațiile cibernetice. A doua entitate este constituită pe baza operațiunilor cibernetice care conțin capabilitățile informaționale, capabilitățile de apărare și de atac. Ultima entitate este reprezentată de Centrul de Expertiză Cibernetică care se concentrează pe abilitățile și cunoștințele cu privire la operațiile cibernetice ale MA. Această entitate va oferi un poligon de testare cibernetică (PTC).

Scopul cercetării

Scopul principal al cercetării este de a proiecta o programă de dezvoltare a poligoanelor cibernetice de testare, de a studia arhitecturi complexe și caracteristici care pot fi utilizate în poligonul cibernetic, identificarea celor mai utilizate arhitecturi și trăsături din poligoanele cibernetice prezente în întreaga lume și aspectele cheie ale acestora care pot fi utilizate pentru a crea noua generație de poligon cibernetic, precum și să identifice avantajele creșterii nivelului de conștientizare în cadrul departamentelor de securitate cibernetică ale infrastructurilor cu valențe critice.

Planul tezei

Această teză se va orienta pe poligoanele cibernetice, modalitatea variată de aplicare în pregătirea din domeniul securității ciberentice prin diferite scenarii de atac și apărare. Conține de asemenea și o analiză detaliată a diferitelor poligoane cibernetice și tipurile în care se încadrează acestea. În timpul acestei cercetări am identificat diverse platforme de tip cyber-ranges care au diferite puncte forte, cât și slăbiciuni, astfel că am fost capabili să creăm un Poligon Cibernetic Ideal utilizând parametrii de clasificare.

În **capitolul 2** am descris în detaliu operațiunile cibernetice ale capabilității Cibernetice de Apărare în Rețele Complexe și care reprezintă componentele principale ale Poligonului Cibernetic al MA. Acest capitol include de asemenea o comparație între Poligonul Cibernetic al Statelor Unite, Poligonul Cibernetic NATO (Poligonul Cibernetic CCDCOE) și Poligonul Cibernetic al Angliei.

În **capitolul 3** am realizat maparea a unui poligon cibernetic, prioritățile funcționalităților unui astfel de sistem conform capabilităților operațiunilor cibernetice și cerințele necesare pentru a livra aceste funcționalități.

Capitolul 4 descrie nevoia introducerii realismului în poligoanele cibernetice și implementarea unui scenariu de atac-apărare bazat pe noile tendințe de vectori de atac.

În **capitolele 5 și 6** am introdus conceptele de poligon cibernetic fizic și virtual și am descris de asemenea și arhitectura unui poligon virtual complex și a diferitelor topologii care pot fi implementate în diferite tipuri de scenarii de tip Red Team-Blue Team.

Capitolul 7 a introdus conceptul de noua generație de poligon cibernetic și a descris parametrii esențiali care pot defini poligonul cibernetic ideal (numărul de jucători, infrastructura, scenariile, personalul implicat, mediul simulat, uneltele, automatizările, performanța, VPC, VPN, fidelitatea și proprietatea intelectuală).

În **capitolul 8** am subliniat diferitele componente, circumstanțe și caracteristici precum calcularea, valorile, uneltele, echipa și platforma Cyber Range a Exercițiului Anual CyDEx. Am făcut de asemenea și o comparație între poligonul CyDEx și conceptul de poligon cibernetic ideal.

În **capitolul 9** am descris nevoia exercițiilor cibernetice pentru angajații care sunt implicați în infrastructuri cibernetice critice precum sisteme SCADA. Am discutat despre conceptele de securitate ale sistemelor SCADA, vectorii de atac și perspectivele de apărare.

Capitolele 10 și 11 includ două scenarii complexe care au fost dezvoltate într-un exercițiu cibernetic implementat în cadrul NATO Cyber Coalition și CyDEx. Aceste scenarii au țintit către infrastructuri cibernetice complexe, sisteme SCADA afectate de atacuri distrugătoare și medii militare care au fost afectate de malware complex de tip fileless. Ambele scenarii au inclus vectori de atac, etapele de investigare pentru analiză și recomandările de protecție împotriva acestor tipuri de atac.

2. Operațiuni în cadrul securității cibernetice

Acest capitol prezintă cele mai relevante operațiuni cibernetice ale unui poligon cibernetic și este bazat pe articolul **Capabilitățile Ciberentice de Apărare în Rețele Complexe**. Operațiunile din mediul cibernetic sunt definite ca „utilizarea capabilităților cibernetice unde scopul principal este de a obține obiective militare sau efecte în spațiul cibernetic sau prin acesta”.

NATO utilizează următoarele definiții pentru a descrie capabilitățile Operațiunilor Cibernetice:

- Operațiuni de Rețele de Calculatoare – operațiunile de rețele de calculatoare (cu trei componente: Atac de Rețea Computerizată, Exploatare și Protecție) se concentrează pe obținerea accesului nelimitat la rețeaua de calculatoare pentru a perturba sau a ineficientiza capabilitățile sau utilizarea acestora ca boți.
- Apărarea Rețelei de Calculatoare – acțiuni care protejează împotriva compromiterii sau distrugerii informațiilor stocate în computere, rețele de calculatoare sau rețelele în sine.
- Atacul Rețelei de Calculatoare – acțiuni care compromit sau distrug informațiile din computer sau rețeaua de calculatoare.
- Exploatarea Rețelei de calculatoare – acțiunile întreprinse pentru a utiliza un computer sau o rețea de calculatoare precum și informațiile localizate în acestea cu scopul de a obține avantaje

Operațiunile cibernetice sunt efectuate folosind informații secrete, capabilități ofensive și defensive. Apărarea cibernetică are ca scop protejarea propriilor rețele și sisteme. Atacul cibernetic are ca scop perturbarea, compromiterea, degradarea sau distrugerea rețelei și a sistemelor de calcul [3].

Activitățile efectuate într-un atac cibernetic și obținerea de informații confidențiale/clasificate sunt similare și au ca scop accesarea sistemului pentru a conduce la un efect plănuit. Aceste activități constau în: recunoaștere, scanare, accesare, escaladare, exfiltrare, asalt, susținere și acoperire.

Activitățile conduse într-o structură defensivă urmează ciclul vieții unui incident și constau din șase activități principale care sunt parte din scheletul impus de NATO: detecția unei activități malițioase, finalizarea atacului, prevenirea migrației, evaluarea atacului, revenirea din atacul cibernetic, luarea unei decizii în timp util și managementul informațiilor de apărare cibernetică.

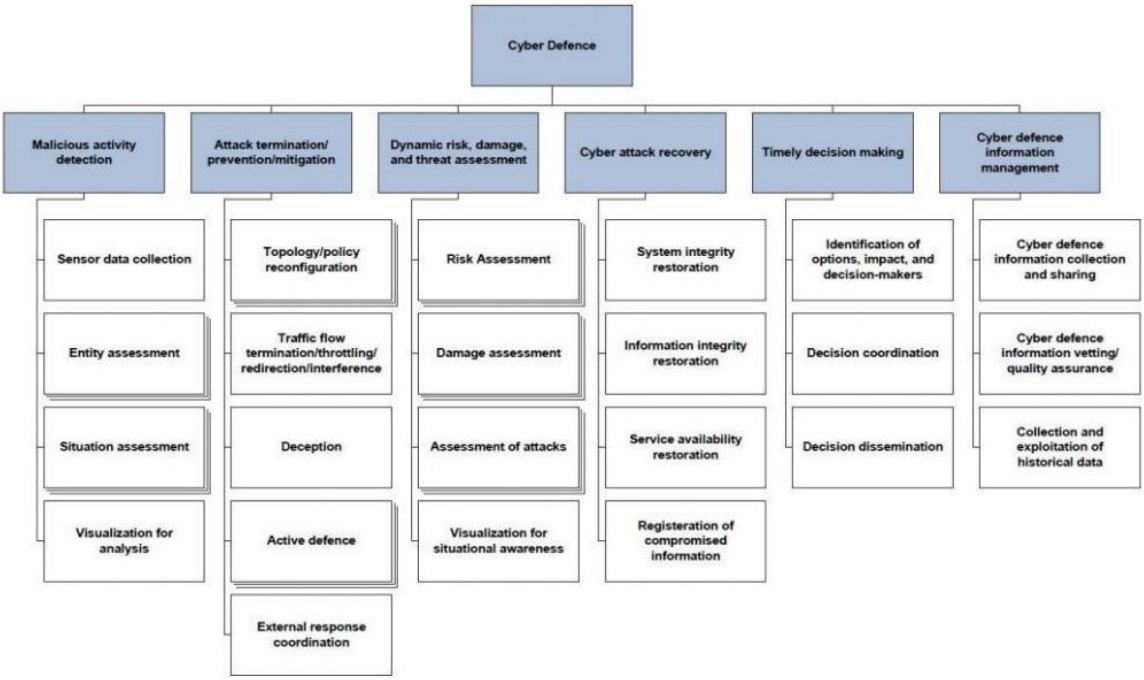

Figura 1. Capabilitățile de apărare cibernetică.

2.1. Dezvoltările poligoanelor cibernetice de test

Poligoanele cibernetice de test (CTR) sunt definite ca medii virtuale utilizate pentru cercetare, dezvoltare, evaluare și antrenare în domeniul securității cibernetice. Scopul acestor poligoane implică recrearea situațiilor din lumea reală, dar fără sa afecteze cu adevărat rețeaua de calculatoare. Cerințele CTR sunt obligatorii. Ele trebuie să reproducă rețelele și sistemele de computer, să imite operațiile esențiale efectuate în cadrul companiei/instituției și să producă trafic de date real pentru a se putea conduce testele fără a afecta mediul real.

Studiu de caz

Există un număr mare de CTR care au fost făcute operaționale sau sunt încă în proces de implementare. Aceste CTR-uri sunt bune pentru a obține caracteristicile viitoare și obiectivele unei noi implementări și, de asemenea, să se înțeleagă mai bine despre poligoanele de test și proiectarea acestora cu scopul de a lupta împotriva criminalității cibernetice și a terorismului cibernetic.

Exemple

1. CTR-ul Statelor Unite – SUA este în faza de a implementa un Poligon Cibernetic Național (NCR). Acest poligon va oferi infrastructura și uneltele software pentru o testare securizată capabilă să simuleze rapid un număr mare de rețele complexe care să se apropie de diversitatea rețelelor din mediul real.

În plus față de NCR, experții din domeniul cibernetic din SUA au început dezvoltarea în anul 2006 a unui poligon de operațiuni informatice (IO). Scopul acestuia a fost de a oferi un mediu creat din proceduri și

structuri care dezvoltă un test sensibil, un mediu de pregătire și practică pentru crearea și operaționalizarea capabilităților IO și a strategiilor, metodelor și procedurilor acestora.

2. NATO – Centrul de Excelență de Apărare Cibernetică NATO (NATO CCDCOE) conduce un laborator cibernetic creat de Directorul CCDCOE. Laboratorul cibernetic țintește ca utilizatorii operaționali să participe la cursuri tehnice de antrenare și expertiză tehnică. În acest poligon sunt dezvoltate două exerciții importante: LockShield (exerciții echipa roșie vs. echipa albastră) și Cyber Coalition [3] (exerciții bazate pe diferite scenarii care implică analiza malware, analiza traficului și reportarea incidentelor de securitate observate în urma investigațiilor) [4].

3. Regatul Unit – UK a deschis poligonul cibernetic în anul 2010 [5]. CTR-ul lor „este capabil să simuleze o infrastructură mare și globală a amenințărilor cibernetice și să evalueze aceste rețele militare, civile sau comerciale, să răspundă la un atac pentru dezvoltarea capabilităților care vor conduce la rețele mai bine securizate".

Northrop Grumman oferă facilitățile de test ale poligonului [6]. Poligonul are patru utilități comune:

- Antrenarea care țintește prevenirea victimelor în situația unui atacul cibernetic și antrenarea care presupune îmbunătățirea tratării unui astfel de atac.
- Să obțină și să înțeleagă robustețea arhitecturii IT și să înțeleagă consecințele completărilor sau modificărilor arhitecturii cibernetice.
- De a testa și de a repera componentele IT
- Dezvoltare și cercetare

2.2. Poligonul de test al Ministerului Aparării

Așteptările MA în ceea ce privește CTR-ul include funcționalități care constau din mai multe nivele. Primul nivel face legătura dintre funcționalitățile CTR și operațiunile cibernetice, astfel că funcționalitățile ușurează execuția operaților cibernetice. Nivelul doi constă în funcționalități care suportă una dintre capacitățile domeniului operațiilor cibernetice: apărare, atac sau informații confidențiale/clasificate.

Funcționalitățile generice sunt funcționalități care suportă operațiunile zilnice și permit dezvoltarea și cercetarea. Pentru a suporta astfel de operațiuni, CTR-ul încearcă să prezinte funcționalități care ajută personalul să acționeze eficient capacitățile deja existente în domeniul cibernetic. [7].

Exercițiile sunt componentele critice deoarece consolidează fiecare componentă a operațiunilor într-o activitate foarte asemănătoare cu situațiile reale. Protecția cibernetică poate fi pregătită pentru fiecare componentă în parte, în vederea identificării modului de revenire la normalitate după un atac cibernetic.

Atacul/apărarea cibernetică – descrie dorința către o perspectivă de atac/apărare. Prezentarea generală a unui atac constă din trei componente [8]:

- Capabilitățile particulare utilizate pentru atacul/apărarea cibernetică
- O altă specificație a capacităților particulare în administrarea CTR-ului îndreptat către sprijinul apărării/atacului
- O împărțire a administrării CTR-ului în segmente administrative care să susțină atacul/apărarea cibernetică.

3. Maparea Funcționalităților în Poligonul Cibernetic de Testare

Această mapare a funcționalităților va fi disponibilă în următorii ani și include livrarea funcționalităților din interiorul CTR și cerințele tehnice necesare.

Pentru a stabili această mapare sunt necesare două etape. Prima etapă este de a identifica prioritatea funcționalităților CTR in concordanță cu perspectiva capabilităților cibernetice operaționale. Cea de-a doua etapă este de a determina diverse nivele ale funcționalităților dintr-un serviciu și cerințele necesare pentru a livra aceste funcționalități [1].

Există două variabile care determină prioritățile. Prima variabilă este nivelul de urgență (care necesită utilizarea rapidă a funcționalităților) și cea de-a doua variabilă este complexitatea (care implică cunoașterea cerințelor necesare). Ambele variabile (și combinațiile dintre acestea) reprezintă prioritățile funcționalităților; funcționalitățile care au un nivel de urgență ridicat și complexitate redusă trebuie rezolvate prioritar, iar cele care au urgență redusă, dar complexitate ridicată vor fi rezolvate în continuare [9].

Modelul CTR matur este proiectat să definească diferite funcționalități și sa determine cerințele necesare. Metodologia definirii modelului de test urmează trei pași [10]:

- Să conecteze cerințele CTR-ului la serviciile individuale CTR;
- Să abstractizeze cerințele care țin de serviciile CTR la nivelul funcționalităților CTR;
- Să împartă cerințele în diferite nivele și să lege aceste cerințe la nivelul serviciilor funcționalităților

4. Scenarii reale de Atac-Apărare pentru antrenamentele din domeniul Securității Cibernetice

Acest capitol introduce nevoia poligoanelor cibernetice în practicarea scenariilor reale pentru infrastructurile cibernetice și se bazează pe articolul **Creating and Managing Realism in the Next-Generation Cyber Range.**

4.1. Ce este Poligonul Cibernetic?

Cuvântul poligon cibernetic provine de la noțiunea militară de poligon în care trupele sunt trimise pentru a-și îmbunătăți aptitudinile de luptă într-un mediu controlat în care se găsesc diferite activități care încorporează familiarizarea cu arme și muniție, tancuri, avioane de război, nave militare, etc. În acest mod, militarii sunt pregătiți pentru adevărata bătălie. Poligonul cibernetic se concentrează pe cea mai bună metodă de evaluare a circumstanțelor și aplicarea aranjamentelor/proiectării atacurilor în circumstanțe particulare [13].

4.2. Cine are nevoie de un Poligon Cibernetic?

În fiecare zi, știrile atenționează asupra atacurilor cibernetice din domeniul financiar, extorsiune, fraudă, scurgere de informații secrete și atacuri politice sau ideologice. În cazul în care ne raportăm la o organizație petrolieră a cărei bază de date este modificată în mod nefavorabil sau anihilată de un atac cibernetic care influențează capacitatea de a livra marfa, atunci specialiștii din domeniu și-ar fi dorit cu siguranță să fi investigat acea proiecție într-un poligon care are capacitatea de a identifica și elimina un astfel de atac cât mai repede.

Cine are nevoie de un poligon cibernetic? Luând în considerare toate datele, este destul de evident că pentru toate intențiile și scopurile acestuia orice companie ar avea nevoie de unul. Nimeni nu este imun la astfel de incidente

4.3. Este chiar atât de rău?

Auzim constant despre starea curentă a noilor atacuri de securitate și despre uzualele breșe de securitate. Se pare că nu este doar un capăt la care trebuie să ne uitam. Modul în care majoritatea companiilor din lume ne securizează sistemele și informațiile este într-o mare măsura o problemă greu de gestionat [14]. Direct proporțional cu mărimea și complexitatea echipamentelor și programelor marilor companii se află și breșele de securitate, cu vulnerabilitățile care sunt scoase la lumină în fiecare zi pe întreg globul.

4.4. Cum putem bloca aceste probleme de securitate?

Au fost purtate nenumărate discuții la nivel înalt cu scopul de a găsi diferite perspective despre cum pot fi descoperite aceste probleme de securitate atât pe termen scurt cât și pe termen lung. Există examinări în ceea ce privește proiectările deschise, avantajele unei structuri închise, o perspectivă nouă și strălucitoare cunoscută sub numele de sisteme „securizate de la bun început” care conțin modele, utilizări ale firewall-ului,

confirmare de atacuri de tip 0-day, cadre de administrare a riscului (UMTS) și o gamă largă de proiectări de securitate.

5. Proiectare unui poligon cibernetic

Poligonul digital poate fi proiectat din multe puncte de vedere, însă în final acestea pot fi agregate în trei clasificări: fizice, virtuale și încrucișate. Trebuie investigate toate tipurile de poligoane și punctele lor forte și slăbiciunile [15].

5.1. Arhitectura fizică de poligon cibernetic

Într-un poligon cibernetic complet fizic, se copiază întreaga fundație fizică a sistemului, switch-urile, firewall-urile, serverele, etc. Se folosesc aceste elemente copiate pentru pregătire. Această metodă este foarte bună deoarece nu se poate obține ceva mai practic decât implementarea reală și fizică a poligonului, acesta fiind cel mai aproape de adevăr.

Însă, această abordare prezintă și câteva dezavantaje, acestea fiind destul de importante:

- Cel mai mare dezavantaj este costul ridicat acordat echipamentelor si personalului pentru recreerea mediului complex al sistemului live
- Un alt dezavantaj îl constituie timpul acordat pentru crearea de situații sau scenarii noi în mediul realizat
- O altă problemă o reprezintă administrarea fizică a sistemului, costurile operaționale continue pentru răcire, puterea utilizată, etc.
- Ultimul, dar nu și cel din urmă, este dificultatea de a curăța poligonul după un exercițiu practic. Acest lucru este vital ținând cont de faptul că numeroase situații ale poligonului vor include atacuri complexe care vor lăsa artefacte nedorite în sistem.

5.2. Arhitectura Virtuală a Poligonului Cibernetic

Într-un poligon cibernetic virtual, totul este reconstituit. Fiecare segment este copiat pe mașini virtuale. Această abordare oferă o serie de avantaje. Costul capitalului necesar și costul operațiilor de realizare sunt mai mici decât cele ale unui poligon fizic.

6. Utilizarea efectivă a poligonului cibernetic

Știm că avem nevoie de un mediu încrucișat și avem o idee generală despre ce avem nevoie pentru a virtualiza și ce avem nevoie de a păstra fizic. Deoarece diferite segmente pot fi virtuale sau fizice, în funcție de ce presupune fiecare situație în parte, nu vom acoperi utilizarea autentică a poligonului digital [18], [19]. Acest capitol este bazat pe lucrarea **Creating and Managing Realism in the Next-Generation Cyber Range.**

Conexiunea de corespondență condusă poate fi oricare: asocieri ISP, coordonate prin cablu punct-la-punct, schimburi de mesaje bazate pe conexiune prin satelit, telefonie, etc. Problema este că de fiecare dată demonstrația ar trebui să fie rezonabilă și așteptările să fie conform cerințelor practice și a obiectivelor. Este posibil să existe câteva servere care necesită un sistem de bază de tip (DMZ) [20].

Un DMZ implică un sistem extern de administrare a componentelor de risc, cum este de exemplu, facilitarea accesului către un site web sau administrarea email-ului. Acestea pot avea acces unic prin firewall către alte active corporative și servere, făcându-le cel mai probabil ținta atacurilor [21].

O topologie de nivel înalt a Poligonului Cibernetic include:

- Centrul de date: Serviciile interne ale companiei (DC, DB, FileServ, Exchange etc.)
- DMZ: Serviciile externe ale companiei (web hosting, email etc.)

De la clienții interni:

- Navigarea pe internet

- Căutarea internă a clienților pe WWW
- Clienții interni care accesează resursele companiei din centrul de date

De la clienți externi:

- Clienți de pe internet care doresc să pătrundă / lovească organizația
- Utilizatorii de internet care accesează DMZ
- DNS și sincronizarea email-ului
- Clienții interni care accesează internetul prin VPN

6.1. Evaluarea Tehnologică de Dezvoltare

Vom discuta mai întâi despre cazurile de evaluare a avansării inovației. La prima vedere, acest caz are toate caracteristicile de a fi direct și fără probleme. Utilizarea poligonului furnizează un mediu de laborator important, mapează cazurile autentice care îți garantează beneficiile, arhitectura, etc.

Același lucru va fi evaluat, în cazul în care ne uităm la diferiți parametri care ar putea fi în conflict. Aceste aspecte au un efect colosal în identificarea examinărilor poligoanelor digitale. De reținut că autenticitatea este esențială într-un poligon digital. Într-un mediu în care nu există situații sensibile, care să includă activitatea fundamentală rezonabilă și practică a atacurilor, poligonul este fără nicio utilizare [22].

6.2. Antrenarea în Războiul Cibernetic Echipa roșie/Echipa Albastră

În pregătirea situațiilor, este ușor de a observa cum lucrurile pot deveni destul de rapid destul de încurcate. Utilizăm ceea ce numim echipa roșie (red-team) și echipa albastră (blue-team) pentru a separa sistemele de atac de sistemele de apărare, serverele și aplicațiile ca un aspect major al poligonului digital, regulile fiind setate de echipa albă (white-team).

Membrii echipei albe setează obiectivele pentru exercițiu. Acestea pot fi obiective bazate pe echipa roșie, obiective bazate pe echipa albastră sau pentru ambele cazuri. Aceștia se ocupă cu pregătirea exercițiului, au perceptibilitate completă asupra exercițiului și setează instrucțiunile acestuia. Echipa albă garantează de asemenea și cerințele necesare pentru desfășurarea exercițiului de pregătire.

În cea mai mare parte aceștia cer ca apărătorii (echipa albastră) să aibă un firewall interior și un aranjament perceptiv pentru a căuta corespondențe ciudate care nu există în mod normal în sistem, după care să examineze folosindu-se de software-uri de inspecție avansată a pachetelor (DPI) unde anumite fire de execuție ale unor procese sunt izolate in vederea investigațiilor amănunțite.

6.3. Atacuri de tip 0-day

Atacurile de tip 0-Day sunt atacuri definitive în lumina faptului că, prin definiție fac referire la asalturi care nu au fost încă găsite de specialiștii în securitate cibernetică. Acestea sunt create de interese răuvoitoare care preiau controlul a ceea ce se considera a fi un bun organizațional protejat.

Pot de asemenea aduce o întrerupere sau decimare a componentelor sistemului sau informațiilor. Câteodată aceste malware-uri pot sta în expectativă pentru un timp exact când sunt programate să înceapă activități distructive. Nu se poate ști exact dacă sau când se va întâmpla. Acestea se pot de asemenea șterge, transforma și pot crea un număr mare de pagube în cadrul infrastructurilor compromise.

6.4. Crearea și gestionarea realismului în poligoanele cibernetice

Există un număr mare de potențiale scenarii și situați de poligoane digitale. Noi am experimentat câteva situații actuale. Ceea ce se poate cunoaște imediat este faptul că fiecare scenariu final necesită componente umane distincte, atacuri și standarde de securitate. Ce se poate descoperi, de asemenea, este că acestea vor necesita un număr mare de resurse umane (HR) și implementări, pregătiri, timp de examinare, care se materializează într-un cost (timp și bani). Acest lucru poate obliga activitățile să devină rigide și să nu ofere rezultatele de care este nevoie. Specialiștii pot deveni cu ușurință copleșiți de aceste variabile de bază care

deservesc activitățile lor, în consecință se poate diminua calitatea exercițiului eliminând beneficiile oferite de capacitatea de a pregăti cu adevărat „câmpul de luptă”.

7. Introducerea unui poligon cibernetic ideal

În următorul capitol vom discuta despre câțiva parametrii importanți pentru poligoanele cibernetice. Apoi, vom atribui valori calitative acestor parametrii pe baza importanței lor în cadrul poligonul cibernetic. Aceste valori calitative vor contribui în realizarea poligonului cibernetic perfect.

7.1. Parametrii fundamentali ai Poligonului Cibernetic

Performanțele poligonului cibernetic se bazează pe o serie de parametrii specifici care sunt orientați pe operațiuni. Acești parametrii variază de la numărul de jucători (locuri) la infrastructură, prin urmare afectează funcționarea poligonului cibernetic într-o formă sau alta. Câțiva dintre acești parametrii vor fi detaliați în această secțiune. Pe baza importanței acestor parametrii și a riscului impus de aceștia, am decis să oferim o serie de calificative precum, deficitar, scăzut, mediu, mare și foarte mare [23].

Acești parametri sunt:

Locurile – dimensiunea poligonului cibernetic poate fi definită de numărul sistemelor și locurilor incluse. Parametrul cerut pentru poligonul cibernetic poate și mediu, din moment ce poligoanele implică funcționalități exclusive pentru acesta [24].

Infrastructura – poligoanele cibernetice dețin infrastructura lor implicită conform funcționalității. Infrastructuri multiple și arhitecturi sunt combinate pentru a crea infrastructura specifică poligonului. Din acest motiv, valoarea necuantificată asociată infrastructurii este foarte mare.

Scenariu – cum a fost menționat și anterior, există mai multe echipe: roșie, albastră, verde, galbenă, gri, mov și albă, fiecare având particularitățile sale într-un poligon cibernetic. Atacul echipei roșii urmărește găsirea vulnerabilităților din sistemul informatic. Toate funcționalitățile echipei sunt susținute de o platformă oferită de poligonul cibernetic.

Implicarea personalului – pe baza clasificărilor anterioare, putem concluziona că poligoanele cibernetice nu sunt limitate la un singur grup particular de oameni; în schimb, este de interes pentru un grup larg de oameni. Studenți, cercetători, specialiști, specialiști în drept, militari, guvern, clienți, toți pot accesa poligonul cibernetic în baza unor înțelegeri prestabilite.

Simularea mediului – un poligon cibernetic virtual ar trebui să aibă abilitatea de a simula întreg internetul și operațiunile suportate de acesta. Simulatoarele sunt elemente semnificative pentru poligoanele cibernetice având în vedere că principalul scop al acestuia este de a oferi situații reale de antrenare și testare. Având în vedere acest aspect, pentru un poligon perfect simularea mediului necesită o importanță foarte mare.

Uneltele – diferite unelte pot fi instalate în funcție de mediul necesar pentru fiecare poligon cibernetic. Uneltele sunt de asemenea o componentă importantă a poligonului cibernetic având o valoare foarte mare ca importanță.

Automatizarea – poligoanele de test trebuie să suporte un număr mare de servere, operațiuni, dispozitive și trafic de rețea. Automatizare poate conduce la testarea mediilor complexe în poligonul cibernetic, făcând acest parametru o componentă esențială a poligonului cibernetic având o cerere foarte mare [25].

Performanța – poligoanele cibernetice au uneori de-a face cu site-uri cu trafic greu. Dacă devine prea încărcat, serverele pot afecta negativ performanța poligonului cibernetic. Pentru a balansa încărcarea și pentru a face față întreruperilor, poligonul cibernetic suportă câteva operațiuni, dispozitive și servere; performanța este un parametru cu cerere forte mare.

Rețeaua clonată virtual (VCN) – această componentă este responsabilă de oferirea unui mediu realist împreună cu antrenarea și testarea. Cu toate acestea, VCN-ul folosește numeroase resurse, iar fiabilitatea lor este o problemă motiv pentru care acest parametru are o cerere medie.

Rețeaua Virtuală Privată (VPN) – o rețea virtuală privată este utilizată pentru conectarea mașinilor în managementul poligonului. Este dependent de configurație. VPN-urile nu au o varietate mare deoarece pot fi ușor înlocuite cu alte tehnici și unelte cu care se pot obține lucruri asemănătoare [26].

Fidelitatea – fidelitatea este o calitate de conformitate și corectitudine. Este un parametru vital pentru operațiunile poligonului cibernetic. Fidelitatea măsoară corectitudinea, complianța, acuratețea și autenticitatea. Pentru un poligon perfect, cererea parametrului de fidelitate este foarte mare.

Infrastructură Cloud Publică – principalul scop al infrastructurii cloud în poligoanele cibernetice este pentru a include o acoperire suplimentară a hipervizorului în ideea de a oferi izolare și auto-rutare. Implementarea unei infrastructuri cloud este ideală atunci când poligoanele cibernetice nu sunt dependente de hipvervizor ESXi și protocoale de Nivel 2.

Proprietatea intelectuală – proprietatea intelectuală poate fi definită ca un gând, o sugestie sau o propunere creată de minte datorită inteligenței sau intelectului. Cele mai multe poligoane cibernetice sunt incapabile să implementeze proprietăți intelectuale. Valoarea parametrului proprietății intelectuale este foarte mare.

7.2. Propunerea Poligonului Cibernetic Ideal

În capitolele anterioare au fost prezentate câteva poligoane cibernetice care există în prezent. Fiecare poligon cibernetic are abilitățile sale. Inconsistența cauzată de dezvoltarea unui poligon cibernetic poate apărea în cadrul tuturor parametrilor și pot împiedica construirea poligonul perfect [27].

Datele prezentate sub formă de tabel și grafice:

Parametri	Nivele
Seats	Medium
Infrastructure	Very High
Scenario (Teams)	Very High
Simulation Environment	Very High
Tools	Very High
People Involved	Low
Automation	Very High
Performance	Very High
Virtual Clone Network	Medium
Virtual Private Network	High
Fidelity	Very High
Cloud Infrastructure	High

Tabel 1. Parametrii și nivelurile respective pentru un poligon cibernetic perfect.

7.3 Reprezentarea poligonului cibernetic ideal pe baza parametrilor

Un poligon cibernetic perfect este reprezentat grafic în figura de jos. Linile indică parametrii considerați, în timp ce punctele rotunde marcate din interior spre exterior indică nivelele parametrilor [28].

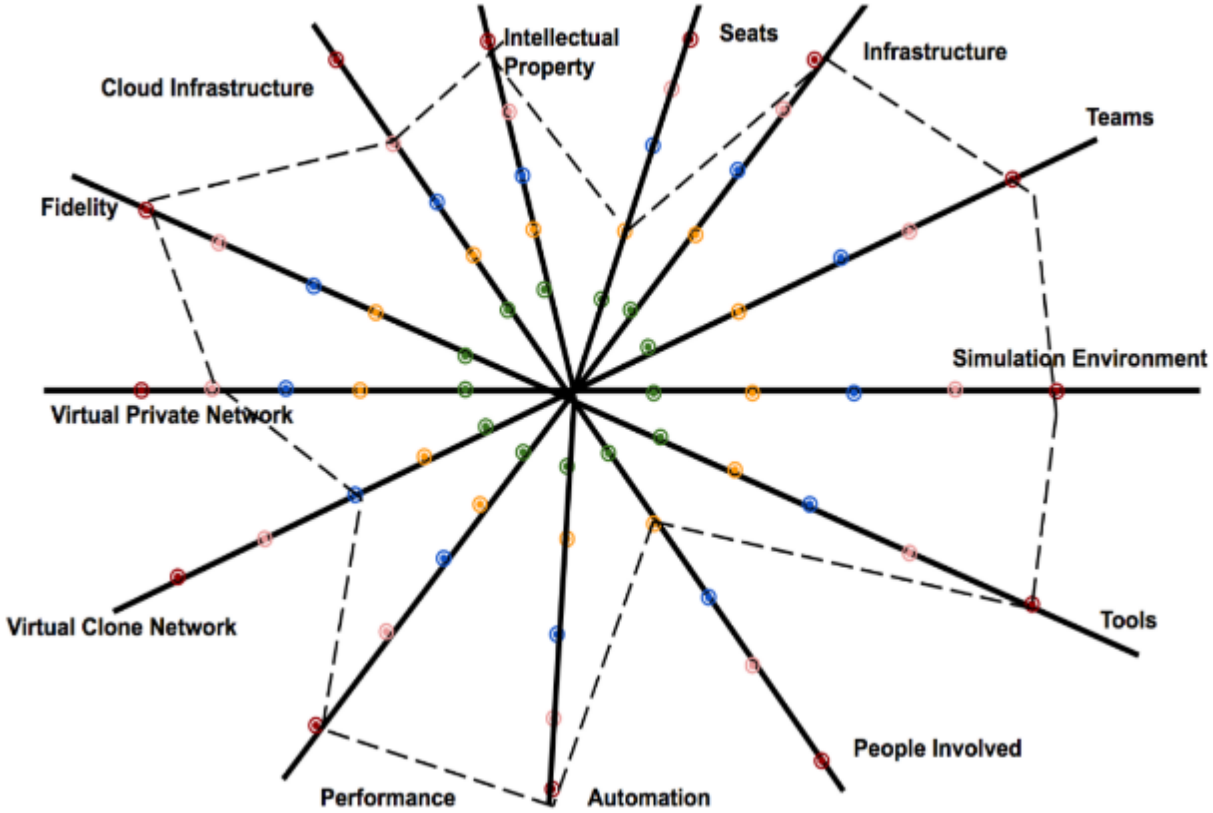

Figura 2. Reprezentarea unui poligon cibernetic perfect [29].

Poligoanele cibernetice oferă o varietate de medii de simulare precum hipervizori, mașini virtuale și componente de tip sandbox. Cu toate acestea, pentru caracteristici și operațiuni mai bune, sunt adoptate simulatoare hibride pentru un poligon cibernetic perfect. Alți parametrii, precum VPN-ul, infrastructura cloud și performanța sunt de asemenea cruciale, dar mai puțin importante. Parametrii precum clona virtuală a rețelei și numărul de locuri sunt de nivel mediu, în timp ce jucătorii au un aport mai mic la poligonul cibernetic perfect. Se poate observa că nu este niciun parametru care necesită un nivel deficitar. Cu toate acestea, parametrii a căror condiții se află într-o categorie joasă sunt considerați în continuare importanți pentru funcționarea poligonului [30].

Poligoanele cibernetice au puncte forte și limitări unice. Câțiva parametrii au fost identificați. Pe baza semnificației acestora, am oferit un nivel de importanță cu scopul de a facilita dezvoltarea unui poligon cibernetic perfect. Reprezentarea grafică ne ajută la crearea unei idei clare asupra parametrilor pe care îi luăm în considerare pentru un astfel de cyber-range [31].

8. Poligonul cibernetic CyDEx

În acest capitol vom discuta despre poligonul cibernetic de la exercițiul anual CyDEx. Acest capitol evidențiază diferitele componente, circumstanțe și caracteristici precum calcularea, metrică, uneltele, echipa și platforma poligonului cibernetic CyDEx.

Acest capitol va conține de asemenea și planul unui poligon cibernetic ideal deja proiectat și vom evalua asemănarea cu poligonul cibernetic al Exercițiului Anual CyDEx [32].

Ținând cont de ceea ce a fost deja efectuat și de care sunt posibilitățile viitoare ale acestui tip de poligon cibernetic urmărim ce este necesar pentru a putea îmbunătăți poligonul pentru viitoarele exerciții.

8.1. Poligonul Cibernetic de la Exercițiul Anual CyDEx

Poligonul cibernetic a fost inaugurat în mai 2017 la Centrul Național Cyberint la prima ediție de CyDEx. Poligonul cibernetic este prevăzut cu echipamente specifice și abilități care asigură exerciții de antrenare pentru apărare cibernetică. Poligonul cibernetic poate oferi atât exerciții predefinite, cât și antrenament. Principalele focusuri al poligonului sunt următoarele:

Planificarea și rularea exercițiilor de antrenament – poligonul cibernetic oferă facilități pentru rularea simulărilor de rețea și testarea software. Această procedură poate conduce eficient la crearea de noi unelte și tehnici de testare.

Oferă medii de testare pentru cercetare și studenți – studenții și cercetătorii folosesc poligonul cibernetic pentru diferite motive. Acest lucru va ajuta la stabilirea performanțelor de bază și la urmărirea regulată a dezvoltării acestuia [33].

Exerciții de tip Capture the Flag (CTF) – așa cum știm, poligonul cibernetic este plin de abilități de rețea. Poate de asemenea coordona exerciții de antrenare și apărare cibernetică într-un mediu de test. Aceste sarcini sunt de obicei realizate de grupuri de studenți.

8.2. Scenariile care pot fi suportate de poligonul bibernetic CyDEx (CCR)

Poligonul este eterogen deoarece este construit pe baza a diferite facilități. În această secțiune se vor prezenta posibilele circumstanțe în care operează poligonul cibernetic. În continuare sunt prezentate câteva scenarii fezabile pentru CCR.

Echipa – CCR-ul suportă idea de echipe care să realizeze diferite activități. Aceste echipe includ executarea de activități pe bază de echipă roșie, mov și albastră. Sunt o varietate de operațiuni și funcționalități pentru diferite sisteme de operație. Câteva echipe observate în CCR sunt:

ROȘU: RT (echipa roșie) este responsabilă pentru inițierea unor atacuri către alte sisteme utilizând diferiți vectori precum malware, spyware, worm sau viruși. Sistemele cu nivel de bază sunt susceptibile la multe atacuri de securitate.

ALBASTRU: BT (echipa albastră) dintr-un poligon cibernetic este responsabilă pentru analizarea sistemelor de recunoaștere a vulnerabilităților, de a garanta securitatea și de a valida eficacitatea tehnicilor defensive. BT evidențiază funcționalități precum analiza traficului, analiza jurnalului de evenimente și analizarea fluxului de date.

Echipa albastră găsește nivelul atacului efectuat de echipa roșie cu scopul de a remedia problema. Un scenariu în care sistemele sunt identice și fiecare sistem este alocat unei echipe albastre diferite [34].

MOV: PT (echipa mov) este un parteneriat între echipa albastră și echipa roșie și este de obicei motivul îmbunătățirii poligonului cibernetic. Echipa mov combină membrii din echipa albastră și din echipa roșie și colaborează în fiecare etapă.

Scanarea de Vulnerabilități a sistemului Gazdă – scanarea vulnerabilităților gazdei se referă de obicei la management-ul vulnerabilităților și auditul automatizat al sistemelor gazdă. Poligonul cibernetic poate crea o situație care poate remedia scanarea vulnerabilităților gazdei.

Scanarea Vulnerabilităților Web – aceste acțiuni ar trebui realizate pentru găsirea vulnerabilităților aplicațiilor bazate pe tehnologii web. Aceste vulnerabilități pot fi identificate de atacatori pentru a obține acces ilegal pentru a extrage informații confidențiale. Această scanare ajută la verificarea traficului dintre browser și aplicații.

Exploatarea framework-urilor – acestea se referă la exploatarea executării codului în afara mașinii considerate țintă. Pentru traficurile de rețea incerte și cod malițios, aceste framework-uri în mare parte permit folosirea diferitelor coduri-uri de exploatare (payload-uri).

Răspunsul la incidente – CCR-ul poate executa răspunsuri la evenimente precum atacuri cibernetice; poligonul cibernetic se poate confrunta cu aceste consecințe. Poate, de asemenea, să limiteze pagubele și să scadă timpul de reparare și costurile. Un plan de răspuns la incident cuprinde proceduri care permit identificarea, reacția și să restricționarea atacurilor cibernetice precum virușii sau intruziunile la nivel de rețea.

Activități de tip Network Forensics – o rețea este o acumulare enormă de vulnerabilități, care pot conduce la rezultate teribile. Sunt două tipuri de sisteme destinate activităților de network forensics.

Digital Forensics – este responsabilă de analizarea datelor, prelevarea și interpretarea acestora. Principalul scop este de a conserva orice dovadă în forma originală pentru a nu fi modificată de explorarea structurată.

Penetration Testing – CCR-ul este devotat educației și antrenării în domeniul securității cibernetice. Acest lucru motivează efortul colectiv de a realiza competiții de securitate cibernetică pentru a susține educația în acest domeniu.

Open Source Intelligence – acest lucru se referă de obicei la conținutul public și informații nespecificate disponibile pe internet. Aceste informații pot veni de pe website-uri, blog-uri, rețele de socializare, forumuri etc.

Inginerie inversă (**Reverse Engineering)** – este o tehnică de analiză care analizează software-ul pentru a ușura găsirea și interpretarea conținutului. Poligonul cibernetic CCR poate oferi un mediu propice pentru inginerie inversă.

Inginerie socială – există un număr mare de tehnici utilizate pentru a extrage informații cibernetice de la persoane. Uneori, comunicarea dintre atacatori și ținta este necesară pentru a realiza ingineria socială.

Spam – este o metodă de a trimite mesaje nedorite sau inadecvate pe internet în mod repetat. Există deferite tipuri de spam-uri, precum spamarea cu mesaje instante, spamarea email-ului, spamarea motorului de căutare etc.

Phishing-ul și Spear phishing-ul – criminalii cibernetici se prefac să fie entități oneste și atrag victimele pentru a obține date sensibile despre acestea. Datele senzitive pot fi sub formă de declarații bancare, parole, etc.

Autentificare – un poligon cibernetic funcționează prin intermediul userilor și a mașinilor, prin urmare relizarea procedurii de autentificare este importantă. Indiferent dacă este o clasă de antrenare, un exercițiu de echipă roșie sau un exercițiu de echipă albastră, autentificarea este necesară deoarece este unul dintre cele mai importante scenarii.

Autentificarea cu un singur factor – utilizatorii se pot autentifica singuri prin această metodă prin utilizarea unei perechi de credențiale (nume de utilizator și parola).

Autentificarea cu mai mulți factori – această tehnică conferă o încredere mai mare și utilizează un mix din ceea ce avem, ceea ce cunoaștem și ceea ce suntem. Ceea ce cunoaștem reprezintă un cod secret, parolă sau PIN, care se poate găsi în biometrie, simbolizând ceea ce suntem.

Amenințarea internă – se referă la amenințarea cibernetică care apare în interiorul organizației și se datorează oamenilor din interior.

Centrul de securitate operațională (Security Operations Center) – este reprezentat de o echipă de experți care examinează infrastructura cibernetică a unei organizații și o îmbunătățesc. Aceștia sunt responsabili pentru evitarea, recunoașterea și răspunderea la evenimentele de securitate.

Analiza jurnalului de log – aceasta este o condiție de bază a unui poligon cibernetic. Fiecare acțiune condusă este înregistrată în fișierul de log. Analiza jurnalului de log are scopul de a analiza aceste înregistrări. În cazul unei vulnerabilități în sistem, sunt examinate pentru a înțelege ce activități au condus la acțiunea malițioasă a sistemului.

Scenarii de business – majoritatea organizațiilor sunt lovite de probleme de securitate. Atacurile sunt inițiate în diferite industrii, companii sau bănci pentru a accesa informații sensibile sau pentru a cauza evenimente de tip fraudă.

8.3. Componentele Poligonului Cibernetic CyDEx (CCR)

Poligoanele cibernetice sunt setări virtuale realiste care promovează educația în domeniul securității cibernetice, combaterea atacurilor și dezvoltarea acestui domeniu. Poligoanele cibernetice sunt pregătite cu câteva funcționalități și proceduri. Caracteristicile funcționale și procedurale ale unui poligon cibernetic sunt diferite în funcție de poligon exemplu: componentele poligonului cibernetic.

Router-ul – într-un CR poate fi observat un volum mare de flux de informații în fiecare secundă. Un router poate fi definit ca un dispozitiv de rețea expert în direcționarea traficului și transmiterea pachetelor de date.
Swich-ul – acesta lucrează spre formarea rețelei, la fel ca routerele care conectează rețele. Este utilizat pentru a lega diferite echipamente precum computere, servere, imprimante etc.
Puncte de acces (Access Point) – acestea sunt de obicei localizate în in Wireless Local Area Networks (WLAN). Punctul de acces este un dispozitiv de rețea utilizat ca punct de trecere din aria locală în rețea și dispozitivele de rețea.
Numele Domeniului (DNS) – este o metodă de accesare a datelor pe internet. Pentru a accesa paginile web, comunicarea este necesară între browser și adresa Protocolului de Internet (IP). DNS-ul este răspunzător pentru alocarea adreselor IP către domeniile accesate.
Rețea locală virtuală – VLAN – este definită ca o subrețea care cuprinde o varietate de servere, stații de lucru, dispozitive de rețea care par a fi limitate la un LAN specific, indiferent de poziția geografică.
Firewall – acesta ar putea fi o idee a unei partiționări care alege ce pachete de date pot trece sau pot pleca în rețea. Scopul este de a filtra traficul neobișnuit și de a evita transmisii malițioase prin rețea.
Sistem de detecție a Intruziunilor – IDS-ul asigură securitatea prin monitorizarea datelor din rețea de activități suspicioase și alertează atunci când găsește astfel de activități. Poate găsi și acționa împotriva acestor activități.
Sistem de detecție a intruziunilor bazate pe sistemul gazdă – într-un astfel de sistem, componentele de securitate (exemplu IDS-ul, antivirusul, firewall-ul) sunt instalate pe fiecare sistem din rețea. Observă jurnale de log, evenimente, servere, host-uri și fișiere critice ale sistemului.
Sistem de detectare a intruziunilor din rețea – funcționează pe plasarea strategică a IDS-urilor pe întreaga rețea pentru a evalua traficul și migrarea datelor prin rețea.

Pachetele de Inspecție Avansată (DPI) – este o tehnică de filtrare a datelor care cercetează un nivel înalt de analize și controlează traficul de rețea. Filtrarea tradițională a pachetelor nu poate redirecționa pachetele bazate pe date particulare pe care DPI le poate detecta, controla și clasifica.

Email – Poligonul cibernetic a adoptat tehnica de trimitere a mail-ului pentru a facilita rutarea dintre rețele. Este limitat la platforma UNIX și multe protocoale sunt suportate de acesta.

Filtrarea spam-ului – este unul din scenariile suportate de CCR. Fiind conectat la multe stații, servere și mașini, spam-urile sunt inevitabile, iar consecințele pot fi severe.

Rețeaua Virtuală Privată – pentru securizarea comunicațiilor rețele, poligoanele cibernetice trebui să conțină operațiuni atât ofensive cât și defensive. Ca rezultat, CCR folosește o rețea viruală privată pentru a asigura siguranța comunicării din rețea.

Achiziționarea Datelor și Controlul Supervizat (SCADA) – poate fi sub formă de software, hardware sau o combinație între cele două. Puterea mare de procesare este necesară datorită numărului mare de sisteme,

platforme, și servere în poligonul cibernetic, motiv pentru care optimizarea este esențială pentru a menține eficacitatea.

Securitatea – ambele componente sunt prezente în poligon, inclusiv una care este esențială pentru securitatea cibernetică și pentru cei care oferă securitate standard. Deoarece poligonul cibernetic nu este limitat doar în interior, este obligatoriu ca utilizatori să dispună de siguranță.

Ieșiri – sunt multe ieșiri din poligon. Cele trei ieșiri pot fi utile în momentul unor incidente neplăcute acolo unde este necesar pentru eliberarea poligonului online.

Alarme – sistemele de detecție de intruziuni pot utiliza poligonul cibernetic să declanșeze alerte dacă este detectat un comportament suspicios. Protecțiile standard și securitatea sunt de asemenea obligatorii într-un poligon cibernetic.

Supravegherea video sau CCTV-ul (televiziunea cu circuit închis) – semnalele sunt transmise către un monitor, astfel încât pot fi vizualizate diferitele atacuri. Ajută la observarea cercetătorilor și a studenților cu scopul de a preveni atacurile de securitate.

Single sign-on – controlul accesului este una dintre cele mai importante aspecte ale securității cibernetice. Este vorba despre autentificare, ceea ce înseamnă că sistemul poate fi accesat doar de anumite entități. Termenul „single sign-on” (SSO) se referă la o proprietate web care permite utilizatorilor să acceseze un website sau un sistem separat. Permite acestora să folosească același set de date de autentificare pentru a accesa câteva sisteme dintr-un poligon cibernetic.

Servere Web – în poligonul cibernetic, serverele, mașinile, platformele și stațiile de lucru rulează în același timp. Serverul web este responsabil de cererile de procesare a rețelei și asigură execuția operațiunilor poligonului. Un server web poate fi o piesă de software, o piesă de hardware sau o combinație între cele două dedicată să îndeplinească cerințele clientului.

Baza de date – este o compilație de informații care permit adăugarea, ștergerea, modificarea, și recuperarea datelor. Baza de date conține un număr mare de funcții de procesare pentru a opera asupra datelor.

Managementul – deoarece există atât de multe operații care rulează pe CCR, este important să se controleze eficient poligonul

SIEM – se ocupă cu analiza în timp real a poligonului cibernetic și generează alarme de fiecare dată când este detectat un comportament suspicios. Controlul accesului pe baza identității și managementul vulnerabilității sunt două dintre cele mai importante caracteristici de management suportate de SIEM.

Nagios – are abilitatea de a analiza sistemul, rețeaua și infrastructura. Nagios, asemenător SIEM-ului, poate genera alerte atunci când este detectat un comportament discutabil. Când problema este rezolvată, trimite înapoi o alertă că totul este în regulă. Nagios este o aplicație de monitorizare care poate monitoriza cu ușurință serviciile de rețea (precum FTP, HTTP si SSH), scripturi și resursele gazdei.

Antiviruși bazați pe sistemul gazdă – aceștia sunt necesari pentru maximizarea eficienței și disponibilității serverului. În plus, antivirușii bazați pe sistemul gazdă se ocupă de managementul serverului și problemelor de securitate.

Sisteme terminale de protecție – acestea pot fi aplicații sau programe software care sunt utilizate pentru identificarea, controlul și managementul dispozitivelor care cată acces către server sau alte servicii.

Firewall – aceste firewall-uri monitorizează traficul de intrare și ieșire dintr-un dispozitiv cu scopul de a evalua dacă un pachet ar trebui sa fie permis sau nu. Firewall-ul poate fi configurat și personalizat conform cerințelor sistemului

Uneltele de securitate cibernetică – unul dintre cele mai cruciale aspecte ale poligonului cibernetic sunt uneltele de securitate cibernetică. CCR oferă suport pentru un număr vast de unelte. Unele unelte sunt

compatibile cu o varietate de sisteme de operare, în timp ce altele sunt restricționate la un singur sistem de operare.

8.4. Caracteristicile principale ale Poligonului Cibernetic CyDEx

Sunt câteva caracteristici ale poligonului cibernetic:

Cloud – activitățile din mediul poligonului cibernetic și copierea scenariilor de exercițiu din viața reală consumă o cantitate semnificativă de resurse. Implementarea framework-ului gazdă în poligonul cibernetic este o metodă excelentă pentru depășirea acestei limitări.
Site Metrics – poligonul cibernetic este localizat într-un centru de înaltă performanță. În ciuda faptului că serverele pot fi localizate la distanță, obiectivul principal al anunțării numărului de participanți în poligonul cibernetic este de a accesa mașinile și uneltele care vor fi utile pentru studenți și cercetători din exteriorul poligonului.
Site Computing – se referă la operațiile computaționale din poligonul cibernetic. Deoarece un poligon cibernetic implică mai multe task-uri, computerele trebuie să fie capabile să facă față atribuțiilor.
Per Seat Metrics – determină abilitățile computaționale a unui sistem desemnat unui singur loc din poligon. Aria în care se găsește un sistem computațional, reprezentată în inch este de 1x34" (21:9).
Toolurile – uneltele de operare, uneltele de detectare a intruziunilor, uneltele de criptare și alte unelte de rețea sunt utilizate de poligonul cibernetic CyDEx pentru exercițiile de securitate cibernetică, antrenare și testare.
Capabilitățile – capabilitățile poligonului cibernetic pot fi descrise ca potențialul de a realiza o sarcină eficient. Câteva trăsături care contribuie la integritatea poligonului cibernetic sunt afișate mai jos.
Setările reale – mediul real de risc și mediul hiper-realistic sunt utilizate pentru a realiza instrucțiunile de apărare și antrenare al poligonului. Poate fi realizat prin replicarea configurațiilor rețelei, angajarea uneltelor de securitate și simularea vizitatorilor din rețea.
Automatizarea completă – o automatizare a poligonului asigură securizarea, stabilitatea și îmbunătățește performanțele. Câteva componente sunt considerate sisteme de operare, conectare, aplicații și stocare pentru a produce rapid medii mari, conducând la scalabilitate.
Mediu de testare controlabil – pentru a suporta capabilitățile unui sistem client-server, câteva stații de lucru și configurații, poligonul cibernetic trebuie să conțină un mediu ușor gestionabil de test.
Fidelitatea – prin utilizarea uneltelor în poligonul cibernetic, acesta asigură o fidelitate bună. Aceste unelte pot fi utilizate într-un cadru federat.
Reconfigurarea Arhitecturii Rețelei – asigură comunicarea dintre un număr mare de gazde. Se ia în calcul analizarea protocoalelor, captarea pachetelor de date și monitorizarea rețelei.
Antrenarea individuală și în echipă – antrenarea atât individuală cât și în echipă este disponibilă în CCR. Antrenarea individuală necesită un cadru care să efectueze teste de penetrare, apărarea sistemului și capabilitățile pe care indivizii le posedă deja.
Suportul echipelor pe platformă – CCR-ul suportă trei echipe diferite: echipa roșie, echipa mov și echipa albastră, fiecare fiind identificate după gradul de expertiză, domeniu și scară.

Infrastructura de tip Cloud – este recunoscută ca fiind următorul pas semnificativ în dezvoltarea avansată a poligoanelor cibernetice. Astfel este necesar să fie introdusă scalabilitatea unui poligon cibernetic cu toate caracteristicile menționate mai sus, operațiuni, scenarii și componente.

Federația – poligonul cibernetic din cadrul CyDEx este cunoscut în momentul de față pentru contribuțiile oferite de cercetători, studenți și experți în domeniul securității cibernetice . În momentul de față este utilizată pentru sesiuni de instruire precum și pentru organizarea evenimentelor cu mai mulți participanți din domenii critice pentru siguranța națională. Datorită nivelului de securitate ridicate, operațiunea federală nu este planificată.

8.5 Comparația dintre CyDex CR și poligonul cibernetic ideal pe baza parametrilor

În decursul lucrării, au fost luați în considerare câțiva parametrii cu scopul de a dezvolta ideea de poligon cibernetic ideal. Unii dintre parametrii cruciali, precum și semnificația acestora într-un poligon cibernetic ideal au fost deja evidențiate. Deoarece parametrii nu au putut fi cuantificați, a fost utilizată o metodă calitativă de atribuire a valorilor, cu calificative ce variază de la Foarte Mare, Mare, Mediu, Scăzut și Extrem de Scăzut. Aceste valori au fost oferite pe baza contribuției și semnificației acestora pentru poligonul cibernetic. Astfel vom analiza același set de parametrii și vom observa cât de aproape este poligonul CyDEx de un poligon cibernetic ideal.

Locurile (numărul de participanți) – poligonul cibernetic ideal atribuie o valoare medie numărului de locuri. Unele poligoane cibernetice au, comparativ mai multe locuri decât CCR, care are doar douăzeci și patru de locuri, ceea ce reprezintă un număr mic.

Infrastructura – pentru CCR există o infrastructură robustă. Sistemele de detecție a intruziunilor, inspecția avansată a pachetelor și firewall-urile oferă toate o varietate de niveluri de protecție și securitate. Pentru a asigura eficiența și performanța, se utilizează mecanisme de control, cum ar fi Superfisory Control and Data Acquisition (SCADA) și componente precum componentele de balansare a traficului.

Scenariul – diferitele situații care sunt utilizate pentru a efectua funcționalități sau pentru a efectua o operațiune sunt descrise de scenariul poligonului cibernetic. Întrucât obiectivul principal al unui poligon cibernetic este de a crea un mediu dinamic și puternic de securitate cibernetică, o serie de entități funcționează fără întrerupere.

Uneltele - este esențial să se ofere o experiență practică pentru a transmite abilități de securitate cibernetică, educație și formare. Dacă sunt furnizate numai echipamente, platforme și mașini, experiența practică va fi insuficientă.

Oamenii implicați - persoanele sunt angajate în mod obișnuit pentru administrarea securității poligonului cibernetic. Ar putea fi un administrator de rețea sau un personal tehnic care se concentrează în primul rând pe asistarea cercetătorilor și studenților din domeniul cibernetic sau persoane care sunt responsabile pentru restaurarea dispozitivelor în cazul unor defecțiuni tehnice.

Mediul simulat - o replică sau o copie a unui mediu dat poate fi descrisă ca un mediu simulat. Fără un mediu simulat, nu se poate crea un poligon cibernetic.

Automatizarea - starea în care sistemele funcționează sau operează automat este denumită automatizare. O serie de componente cibernetice, cum ar fi sistemele de control și sistemele de detectare a intruziunilor, sunt capabile să îndeplinească funcționalitățile în mod sistematic.

Performanța - în lumea computerelor, performanța este definită ca timpul de răspuns rapid al unui sistem, utilizarea redusă a resurselor sau randamentul ridicat al resurselor. Comutatoarele, routerele, serverele complicate și aplicațiile sunt printre componentele CCR.

Rețeaua clonată virtual - în CCR, nu există o rețea clonată virtual (VCN). VCN valorifică puterea unei platforme cloud pentru a oferi o platformă cibernetică care poate fi preconfigurată și modificată după cum este necesar.

Rețeaua Privată Virtuală – poligonul cibernetic ideal evaluează importanța rețelelor private virtuale (VPN), deoarece VPN-urile pot fi înlocuite cu o varietate de strategii și instrumente.

Fidelitate – poligonul cibernetic ideal trebuie să prezinte un nivel mai ridicat de comportament de fidelitate. Sistemele sunt bine cunoscute pentru oferirea unui răspuns realist în timpul testării [35]. Sistemele de înaltă fidelitate, cum ar fi CCR, manifestă de obicei scenarii în timp real.

Infrastructura Cloud - CCR, spre deosebire de majoritatea poligoanelor cibernetice, nu are o infrastructură cloud. Implementarea infrastructurii în cloud este de preferat lansării poligonului cibernetic în cloud [36].

Proprietatea Intelectuală - în poligonul cibernetic, un motor de căutare sau un nume ar putea constitui proprietate intelectuală.

8.6 Reprezentarea CyDEx Cyber-Range pe baza parametrilor de bază

Secțiunea anterioară a detaliat parametrii care au fost deja luați în considerare pentru poligonul cibernetic CyDEx Cyber-Range. Deși anumiți parametri au valori echivalente, alții sunt complet contradictorii. În această secțiune, vom crea o reprezentare grafică a parametrilor.

Parameters	Levels
Seats	Medium
Infrastructure	Very High
Scenario (Teams)	Very High
Simulation Environment	High
Tools	Very High
People Involved	Very Low
Automation	Very High
Fidelity	Very High
Cloud Infrastructure	Very Low
Intellectual Property	Very High
Performance	Very High
Virtual Clone Network	Very Low
Virtual Private Network	High

Tabel 2. Importanța parametrilor CyDEx Cyber-Range.

Se poate crea un grafic pentru a ilustra liniile ca parametri și nivelul propus în index, în funcție de valorile prezentate în tabel.

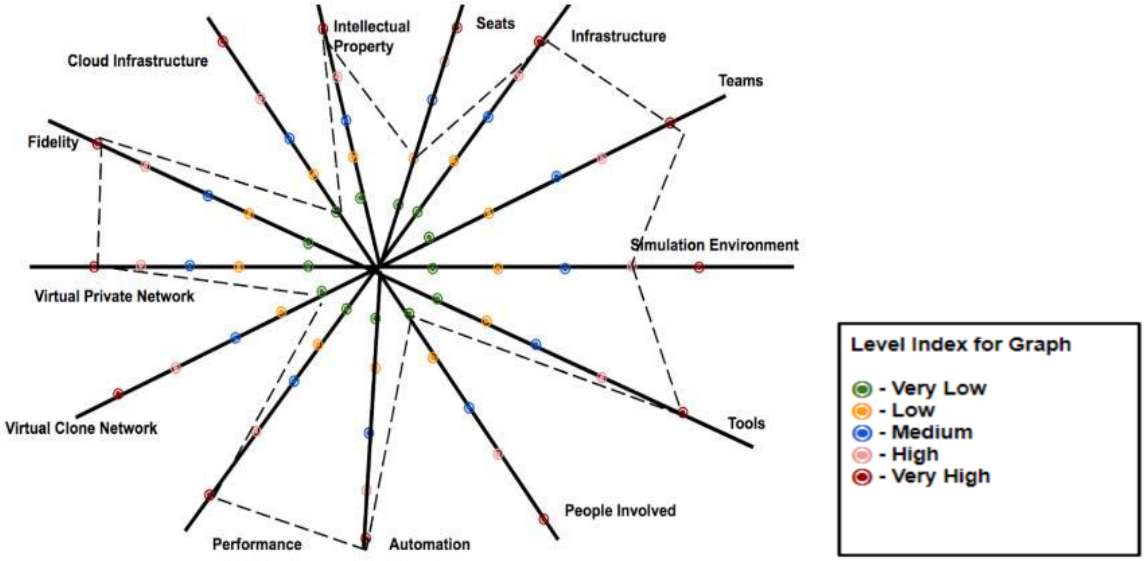

Figura 3. Illustration of the Cyber Range [37].

8.7. Studiul calitativ al poligonului cibernetic

Am reprezentat anterior poligonul cibernetic ideal bazat pe principiul calitativ al atributelor variabilelor luate în considerare. Având în vedere circumstanțele, am considerat că este necesar să ilustrăm grafic CyDEx Cyber-Range pentru a urmări legătura puternică a poligoanelor cibernetice. Vom aplica în mod constructiv principiul calitativ pentru a stabili vecinătatea celor două ramuri din această secțiune.

Cât de capabil este CyDEx Cyber-Range

Am oferit mai devreme Cyber-rage-ul adecvat, bazat pe câteva variante disponibile. Am folosit aceleași variabile pentru a compara CyDEx Cyber-Range cu poligonul cibernetic ideal. În ciuda faptului că CyDEx Cyber-Range simulează un număr mare de valori ai parametrilor găsiți în căutarea poligonului cibernetic ideal, există câteva elemente care sunt complet diferite [38].

Uneltele, locurile, VPN, Infrastructura, Fidelitatea, Performanța, Scenariul, Automatizarea și Proprietatea Intelectuală sunt parametri care au aceleași valori, în timp ce Mediul Simulat, Infrastructura Cloud, VCN și Implicarea Personalului sunt diferite. Valorile atribuite nu sunt cantitative, dar putem calcula valoarea cantitativă sub forma procentului pentru a măsura proximitatea ambelor poligoane cibernetice pe baza unor valori similare. Numărul de valori parametrice la fel împărțit la numărul total de parametrii înmulțiți cu 100 poate fi folosit pentru a calcula procentul de proximitate.

% Proximitate = (Numărul de parametrii la fel/ Nr. Total de parametrii) * 100 = (9/13) * 100 = aprox. **69.23%**

Credem că CCR este cel puțin 69,23% asemănător cu Cyber-Rage-ul ideal. Valoarea poligonului cibernetic va crește probabil, deoarece se urmărește dezvoltarea infrastructurii cloud în viitor.

9. Concepte și recomandări de securitate SCADA

Pentru a înțelege securitatea SCADA, trebuie să înțelegem câte ceva despre sistemele SCADA și securitatea cibernetică în cadrul unor astfel de sistem. Acest capitol se bazează pe lucrarea **SCADA Security: Concepts and Recommendations.**

Sistemele SCADA sunt computerele care controlează procesele fizice importante, complexe și, de multe ori periculoase, multe dintre acestea constituind infrastructura fizică critică pentru societatea modernă. Aceste procese fizice sunt unelte puternice și utilizarea lor greșită are, în general, consecințe grave. Prevenirea unei astfel de utilizări necorespunzătoare este scopul securității SCADA. Pentru a înțelege utilizarea greșită și pentru a o preveni, avem nevoie de o înțelegere a ceea ce este un sistem SCADA și cum funcționează.

Sistemele industriale de control sunt vechi – personalul controla procesele fizice cu cadrane și instrumente de măsură înainte de apariția computerelor și am rămas la acest control asistat aproape de când au fost inventate prima dată computerele. Ca în cazul oricărui domeniu vechi, terminologia este similară. Ce numește mass-media de specialitate un „sistem SCADA" este eronat [39].

Procesele industriale pot fi de asemenea divizate. Cele mai multe infrastructuri critice sunt exemple de „procese industriale" [40]. În procesele industriale, manipularea materialelor este mai mult sau mai puțin „posibilă", într-un anumit punct din lanțul de procesare fizică: sistemele de purificare a apei manipulează apa, rafinăriile manipulează uleiul, iar conductele conduc fluidul. Rețelele electrice sunt, de asemenea, considerate procese industriale, deoarece electricitatea este produsă într-un spațiu continuu care poate fi modificat. Chiar și sistemele de cale ferată și de control al traficului sunt considerate sisteme de proces, însă acest lucru forțează puțin conceptul.

Un aspect important al tuturor sistemelor SCADA este operatorul uman. Sistemele de control din instalațiile industriale, au aproape întotdeauna au unul sau mai mulți operatori care au fost pregătiți să asigure siguranța și funcționarea fiabilă a procesului fizic. Acești operatori folosesc unelte cunoscute ca software de „interfață mașină-om" (HMI). Acest software include aproape întotdeauna o vizualizare grafică a stării procesului fizic și, de multe ori, include și alte elemente, cum ar fi manageri de alarmă și unelte care arată istoricul proceselor.

Acest lucru înseamnă că cel mai adesea, cel mai simplu lucru pentru un atacator pentru a provoca consecințe fizice este acela de a afecta funcționarea unei anumite părți a operatorului HMI sau a sistemului care susține HMI-ul. Cele mai simple consecințe fizice ale unor astfel de atacuri sunt închiderea procesului fizic. Multe procese industriale pot fi închise pentru mult mai repede decât își pot relua activitatea, și pot avea nevoie de zile întregi pentru refacerea completă după o închidere de urgență. În unele cazuri, trebuie să se obțină autorizări de reglementare înainte de reînceperea proceselor fizice, întârziind procesul de repornire chiar și câteva luni. În plus, închiderile de urgență pot pune adesea stres fizic pe echipamentele industriale, ducând la erori ale echipamentului sau la îmbătrânirea prematură a acestuia.

9.1. Securitatea cibernetică în sistemele SCADA

Securitatea cibernetică se focusează pe prevenirea unor astfel de atacuri. Securitatea SCADA ce concentrează pe prevenirea oricărei operațiuni neautorizate a sistemelor computaționale SCADA. Securitatea SCADA este o disciplină recentă față de sistemele SCADA sau sistemele automatizate, dar nu este mai puțin confuză. Noii veniți în domeniul securității văd o varietate uluitoare de tipuri de vulnerabilități, atacuri și sisteme defensive [41].

Combinați acest lucru cu imaginea permanentă că „un lanț este la fel de puternic cum este cea mai slabă verigă" și sarcina de apărare a sistemelor interne poate părea imposibilă. Această varietate uluitoare este o iluzie. Toate vulnerabilitățile din software și într-adevăr, din sistemele de hardware și rețele, sunt erori sau defecte. Varietatea uluitoare este pur și simplu rezultatul încercării de a clasifica unele defecte - toate defectele posibile – toate metodele prin care se pot produce sisteme si software-uri la modul incorect. Toate aceste sisteme de clasificare sunt sortite eșecului - oamenii pot greși în numeroase metode [42].

9.2. Trei Reguli ale Securității SCADA

Cu scopul de a simplifica domeniul securității cibernetice până în punctul în care practicienii SCADA pot crea o rutină în aplicarea bunelor practici de securitate, propunem trei reguli ale securității SCADA. În vremuri moderne, oamenii de știință preferă termenii „principiu" și „teorie" până la „reguli", dar încercăm să simplificăm lucrurile în aceasta lucrare.

1) Nimic nu este sigur

Securitatea este o practică continuă, nu o valoare binară. Având suficient timp, bani și inspirație, orice problemă de securitate poate fi evitată [39]. Oricine folosește termeni precum „comunicări securizate", „securizat" sau „sistem securizat de operare" fie vinde ceva, fie tocmai a vândut. Acest lucru este important.

Se schimbă conversația de la „nu te îngrijora, am securitatea acoperită„ la „cât de siguri suntem noi?" și, în cele din urmă, "cât de siguri trebuie să fim?"

2) Toate software-urile pot fi piratate

Toate uneltele software au erori. Este posibil ca echipele de dezvoltare să elimine erorile pe care le pot rezolva, dar în ciuda celor mai bune eforturi ale lor, toate software-urile au bug-uri, chiar și cele de siguranță. Unele erori rezultă din vulnerabilități de securitate ce pot fi exploatate de atacatori. Pentru dovezi în acest sens, pur și simplu căutați secțiunea de suport a oricărui site web al vânzătorului și veți vedea câte actualizări de securitate au fost făcute în ultimul timp. În concluzie, în practică, toate produsele software pot fi exploatate.

3) Fiecare informație poate fi atacată

Chiar și un singur bit de informație – un 1 sau un 0 - poate fi atacat. Dacă un operator are o încercare de a închide un echipament cu un 0, dar un atacator schimbă ceea ce este 0 în 1, acesta este un atac. Parolele și intențiile malițioase ale unui operator pot fi considerate un atac. Malware-ul poate fi instalat și pe computere complet noi sau în cel mai mic computer incorporat în tastatură.

9.3. Atacurile Cibernetice ale Sistemelor SCADA

Dacă protecțiile IT sunt inadecvate, atunci cum ar trebui să protejăm sistemele SCADA? Pentru a aborda aceste întrebări, trebuie mai întâi să înțelegem atacurile cibernetice. Prea mulți specialiști în securitatea SCADA nu studiază tehnicile moderne de atac producând astfel sisteme de securitate SCADA vulnerabile.

În locul atacurilor, prea mulți specialiști de securitate SCADA și IT petrec mult timp concentrându-se la vulnerabilități. Calculele clasice de evaluare a riscului mențin acest risc deoarece el este o funcție de amenințări, vulnerabilități, exploatări și consecințe. Oricare dintre practicanții din acest domeniu poate concluziona faptul că jobul lor este de a elimina vulnerabilitățile. Modul de gândire din spatele acestei teorii este că, dacă am putea să eliminăm toate vulnerabilitățile, atunci sistemele noastre ar fi invulnerabile. Acest mod de gândire se transformă rapid în preocupare cu vulnerabilități cunoscute și programe de securitate actualizate.

Prima regulă de securitate cibernetică afirmă că nimic nu este vreodată sigur. De exemplu, actualizările de securitate repară numai vulnerabilitățile cunoscute ale produsului, lăsând libere numeroase elemente necunoscute să fie descoperite și exploatate. În general, sistemele SCADA, care pot avea vulnerabilități care se nasc din modul în care au fost implementate și configurate, independent de orice defecte de securitate din codul produsului [43].

Persoanele din interior

Persoanele din interior sunt persoanele care accesează rețelele IT și în care sunt considerați de încredere de către organizație. Aceștia pot fi angajați, contractori, parteneri de afaceri sau chiar vânzători. Insiderii au, în general, o parte din conturi, parole și alte date de acces care îi lasă să utilizeze în mod legitim echipamente și aplicațiile din rețeaua IT.

Persoanele din interior, au tendința de a ști puțin despre securitate și mai puțin despre sistemele industriale de control. Cei mai mulți oameni care se interesează de atacurile din interior sunt sistemele IT, producând fie o scurgere de informații, fie o fraudă financiară.

Crima Organizată

Crima Organizată este responsabilă pentru majoritatea spam-urilor din email și a malware-urilor comune precum viruși, viermi, troieni etc. Organizațiile criminale plătesc dezvoltatori de malware pentru a crea aceste unelte de atac, respectiv să le îmbunătățească constant pentru a fi cu un pas înaintea dezvoltatorilor profesionali de combatere a acestor malware-uri care produc antiviruși, detecția intruziunilor și alte unelte de combatere.

Crima Organizată are banii și talentul pentru a produce malware care se răspândește fără discriminare și infectează și compromite cât mai multe mașini posibile. Aceste grupări criminale extrag în medie câțiva dolari din fiecare mașină compromisă. Această valoare poate lua forma unui card de credit furat, credențiale bancare, sau utilizarea computerelor compromise pentru a trimite milioane de spam-uri [42].

O excepție a acestei reguli de „low impact" este ransomware-ul. Acesta este un malware care criptează fișierele și cere o valoare în bani pentru a le restaura. Este ușor să vă imaginați cum criptarea fișierelor de pe computerele SCADA ar putea face fișierele importante inutilizabile. Acest lucru ar putea afecta sistemul suficient pentru a afecta nivelurile de confidențialitate ale operatorului, conducând la o închidere sigură. Așa cum malware-ul devine mai intruziv, aceste atacuri pe SCADA vor deveni o amenințare din ce în ce mai mare pentru sistemele industriale [44].

Personal cu acces la sisteme SCADA (din interior)

La fel ca persoanele din interiorul departamentului IT, persoanele ce au acces la soluțiile de tip SCADA, au acces la rețele și sisteme și dispun de încredere acordată din partea companiei.

Din nou, pot fi persoane angajate, contractori sau vânzători intermediari. Persoanele ce se ocupa de sistemele SCADA au, în general, acces la conturi, la parole și la alte date de acces care le permit să folosească echipamente și aplicații în rețeaua SCADA. Ca și în cazul persoanelor din interiorul IT, persoanele din interiorul SCADA au tendința de a fi bine poziționați pentru a utiliza atacuri sociale pentru a obține privilegii adiționale.

Hacktiviștii

Hactiviștii sunt persoane fizice sau grupuri cu o motivație extremistă, care pot conduce/lansa atacuri cibernetice. Hactiviștii au adesea un grad mediu de cunoștințe în materie de securitate și pot fi extrem de calificați - petrec mult timp intrând în alte computere și rețele. Cu toate acestea, hactiviștii sunt amatori în sensul în care nu profită personal din spargerea sistemelor de securitate [45].

Rapoartele publicate indică totuși faptul că nu contează care sunt atacatorii, însă tehnicile și uneltele sunt preluate de la hacktiviști:

- O campanie specială de phishing împotriva angajaților de distribuire a electricității din Ucraina au capturat datele de acces de la distanță pentru cel puțin trei companii de distribuție
- Apoi au apelat la computerele din rețeaua SCADA peste o perioadă de mai mulți ani, studiind modul în care au funcționat aceste sisteme. Se presupune că au folosit, de asemenea, internetul și alte resurse pentru a înțelege cum au fost concepute aceste sisteme SCADA.
- În ziua atacului, s-au conectat în cel puțin trei companii de distribuție. Rapoartele publicate includ doar câteva informații despre câte companii au fost țintite și câte persoane au fost afectate. Pe două sisteme, au activat elemente ale software-ului SCADA care au dezactivat mouse-urile și tastaturile și au oferit atacatorilor control asupra HMI SCADA. Pe cel de-al treilea sistem de distribuție, atacatorii au obținut o copie a sistemului SCADA HMI pe computerele proprii. Pentru ultimul atac, ei au utilizat un VPN pentru a conecta copia lor la SCADA HMI la infrastructura sistemelor de distribuție SCADA.
- Pe o durată de peste 30 de minute, atacatorii au folosit software-ul pentru a naviga pe ecrane pentru cel puțin 30 de stații și pentru a închide fluxul de curent prin aceste stații compromise.

Cel puțin 200.000 de persoane au fost afectate până la câteva ore. În timpul acestui atac, atacatorii au inundat personalul companiei de distribuție cu telefoane false. În acest mod, consumatorii țintiți nu au putut raporta faptul că nu au curent, ceea ce a prelungit durata penei de curent. Acest tip de atac este cunoscut ca un atac de tip „Advanced Persistent Threat" (APT). APT se diferențiază de atacul crimei organizate prin:

1) Atacul a fost probabil cel mai probabil motivat de conflictul Ucraina/ Rusia și a avut un anumit scop: companiile de distribuție care servesc consumatorii ucraineni.
2) Atacul a folosit controlul de la distanță - atacatorii au stat la tastatură și au oferit comenzi pentru compromiterea sistemelor pentru câteva luni înainte de cele 30 de minute de atac.

De amintit faptul că și crima organizată este cunoscută pentru utilizarea tehnicilor care țintesc victima. Grupurile care lansează atacuri de tip ransomware au început să arunce fragmente de malware în rețea, pentru a extrage sume mai mari de bani pentru decriptarea unei întregi rețele țintă care altfel ar fi putut afecta multiple sisteme individuale [46], [13].

Servicii de intelligence

Serviciile de intelligence naționale sau regionale, sunt grupări disciplinate de atacatori care folosesc atât tehnici de control la distanță, cât și malware-uri sofisticate atunci când este nevoie. Diferite servicii de informații din China sunt acuzate de pionierat utilizând aceste metode pentru spionajul cibernetic și multe alte națiuni sunt acuzate că folosesc aceste tehnici [47]. În prezent, aceste atacuri sunt folosite în mod obișnuit pentru a fura informații despre disidenți, guverne, corporații competitive, proiectarea de produse, cod sursă, și chiar și modele pentru site-uri și site-uri industriale [2], [48].

Multe guverne și autorități și-au exprimat îngrijorarea de faptul că aceste tehnici ar putea fi folosite pentru a efectua sabotaj mai mult decât pentru spionaj. Unele guverne au declarat că sabotarea infrastructurilor critice naționale vor fi considerate declarații de război [14].

Un atac uzual de acest tip are mai multe etape:

1) Atacatorii urmăresc rețelele de socializare pentru a strânge informații despre personal și folosesc tehnici de phishing special pentru a înșela un individ care lucrează la organizația țintită să acceseze sau să descarce un fișier care activează malware-ul.
2) Antivirusul (AV) din organizația țintă este inutil la atac deoarece activarea malware-ului a fost făcută ușor, în cantități mici. Senzorii AV sunt proiectați să combată un volum mare de malware al crimei organizate. Noile semnături AV sunt create atunci când se detectează un număr mare de copii ale unei noi variante de malware pe mașina respectivă. Malware-urile agențiilor de informații secrete sunt de obicei dezvoltate pentru câteva victime.
3) Malware-ul încărcat „sună acasă”. Se conectează și raportează prin internet căte un centru de control și comandă (C&C). Operatorii profesioniști folosesc C&C-ul să se conecteze la malware și să opereze de la distanță. Această clasă de malware de obicei are trăsături similare cu tooluri de tip „secure shell” și uneltele de acces de la distanță.
4) Operatorii malware folosesc computerele optimizate pentru a urmări în liniște rețeaua compromisă, împrăștie malware-ul către alte mașini unde contul compromis poate avea permisiunea de a crea și rula fișiere executabile și cel mai important, să fure numele contului și parola.
5) Atunci când atacatorii capturează credențialele administratorului de Windows, aceștia creează, de cele mai multe ori, noi administratori și conturi VPN pentru ei înșiși, pentru a nu mai avea nevoie de malware-ul special să continue atacul.
6) Când își ating scopul, se află într-o poziție bună pentru a începe să colecteze/exfiltreze un număr mare de informații, care să modifice sau să conducă la operare disfuncțională a sistemelor industriale.

Pentru țintele cu valoare mare, atacatorii pot introduce mai multe tipuri de malware-uri în organizația țintă, fiecare raportând către un centru de control diferit. Cel mai puțin valoros și mai puțin sofisticat malware este utilizat inițial.

Atacurile la nivel militar

După cum am menționat în această teză, nimic nu este sigur. Atacurile militare dovedesc această idee. Atacurile militare presupun accesul la toate tehnicile de atac utilizate de toate celelalte clase de atacatori, dar ele și dispun de asemenea și de resurse mari tehnice și financiare.

Atacurile la nivel militar se pot face fizic prin pătrunderea în organizația țintă și furarea cheilor criptate și alte date de autentificare. Ei pot intercepta echipamente și programe software aflate în drum spre client și pot introduce echipamente hardware și malware în acele echipamente ce vor fi livrate. Atacatorii la nivel militar pot plăti o sumă mare de bani pentru descoperirea noilor vulnerabilități de tip „0-Day” în aplicațiile și

produsele ce securitate cibernetică și pot plăti o sumă considerabilă de bani pentru a produce un malware personalizat pentru a exploata acele vulnerabilități.

Transmiterea Atacurilor

Fiecare piesă de informație poate fi atacată, chiar și un singur bit / bitul zero, și chiar informațiile transmise utilizând semnale analogice. Ce înseamnă asta? Aproape toată lumea știe că un cod de atac sofisticat poate fi încorporat și fișierele complexe, cum ar fi fișierele PDF. Orice mecanism de comunicare care transmite fișiere, inclusiv persoanele care cară aceste fișiere pe suporturi mobile precum telefonul pot transmite atacuri. Cei mai mulți oameni știu că orice flux continuu de mesaje complexe pot coda atacuri, precum mesajele care vin prin internet.

9.4. Eșecul apărării avansate

În ceea ce privește atacurile descrise anterior, și orice alte tipuri de atacuri, abordarea IT a securității cibernetice a fost considerată „standardul de aur" pentru securitatea SCADA, cam de când a apărut securitatea SCADA. Securitatea SCADA a apărut ca disciplină numai după atacul World Trade Center din 2001 și, în mod natural, a fost inspirat din ceea ce a fost atunci cel mai matur domeniu de securitate IT. Această tendință de a se inspira din securitatea IT a fost reintrodusă de către produse software și hardware IT care au devenit omniprezente în sistemele de control de la începutul anilor 2000.

Apărarea avansată a dat greș. Atacurile moderne de rutină compromit atât domeniul IT cât și rețelele SCADA protejate de sistemele IT de apărare avansate. Standardele de securitate SCADA, reglementările și recomandările evoluează pe lângă sistemele IT de apărare avansată, dar încet. În ciuda deficiențelor sale clare, mulți experți și, în special, experți în IT, continuă să mențină că apărarea în avansată IT este cea mai bună abordare pentru securitatea SCADA.

Pentru a înțelege de ce a dat greș apărarea avansată, examinăm în acest capitol abordarea în stil IT a securității SCADA. Proiectarea vectorilor de atac este un concept de securitate fizică. Un astfel de document descrie cea mai mare dificultate pe care un site trebuie să îl depășească cu un grad mare de încredere. Pentru multe site-uri, acest document este confidențial.

Personal din interior în corporații

Apărarea IT avansată începe cu cea mai mică amenințare - inserații corporative. Calculatorul recepționerului dintr-un birou de pe un alt continent nu ar trebui să poată trimite mesaje care să ducă în eroare sistemul de control. Și, așadar, prima apărare dezvoltată de cele mai multe site-uri este un firewall.

Atunci când filtrul eșuează în identificarea unui atac, firewal-ul transmite mesajele de atac, în general, chiar în rețeaua SCADA, considerând că firewall-ul îl protejează. În realitate, există multe metode de a depăși firewall-ul.

Apărarea avansată, prin urmare, ne învață să dezvoltăm mai multe straturi de firewall, între sistemele SCAD și Internet, fiecare de la un furnizor diferit și de a folosi diferite tipuri de comunicări între fiecare strat. Motivul aici este că atunci când se găsesc vulnerabilități în firewall, protocoalele de comunicare și în alte sisteme, acest design care prezintă o singură vulnerabilitate, va oferi o probabilitate mai mică pentru un atacator să treacă de toate aceste straturi de firewall.

Crima Organizată

Apoi, apărarea în stil IT avansat recomandă dezvoltarea sistemelor antivirus și actualizări de securitate sau „pachete" în limbajul sistemelor SCADA. Sistemele antivirus ar trebui să poată captura majoritatea a volumului mare de malware care trece de firewall sau se introduc prin USB, iar actualizările de securitate ar trebui să blocheze restul. Cea mai mare parte a volumului mare de malware din întreaga lume exploatează vulnerabilitățile cunoscute și, de obicei, actualizările elimină astfel de vulnerabilități.

Există mulți oameni care stau în fața sistemelor SCADA 24x7, ani de zile deoarece țintim către zero timpi morți. Scanarea AV este o problemă reală pe cele mai importante computere SCADA. Actualizările de securitate sunt și mai dificile. Luați o rafinărie pentru un exemplu. Rafinăria tipică se închide complet la fiecare câțiva ani pentru o inspecție, reparare și îmbunătățire. Componentele uzate sunt reparate sau înlocuite. Grupul SCADA folosește oportunitatea de a înlocui toate componentele computerului și îmbunătățirea sistemelor software, atât cât este posibil, la nivel de sistem, pentru a introduce cele mai recente versiuni stabile, cu cele mai recente adaptări.

După o lună completă, fabrica se află la cote de 100% din capacitate și totul revine la normal. Următoarea zi, Microsoft emite de 73 actualizări de securitate pentru 73 de componente ale sistemului de operare Windows care rulează pe computerele fabricii. Microsoft oferă foarte puține detalii, despre cât de mult s-a schimbat, sau cum s-a modificat codul.

Insiderii SCADA

Intrarea în sistem a persoanelor din interior este, în cele din urmă, însoțită de acces fizic legitim și este permis accesul la echipamentele de sistem. Aceste persoane pot fi o amenințare unică. Pe de alta parte, dacă acționează pentru a dăuna echipamentelor sau de a scădea securitatea, este propria lor sănătate și bunăstare pe care o pun în pericol. Securitatea cibernetică clasică sugerează că cel mai bun mod de a aborda acest risc este cu o combinație de măsuri.

- Implementarea controalelor de acces fizic, pentru a asigura că numai persoanele autorizate din interior au acces fizic la echipamentele industriale și la introducerea echipamentelor de sistem
- Plătiți și tratați bine și în mod echitabil oamenii și, prin urmare, reduceți drastic probabilitatea ca o persoană din interior să dezvolte cu intenții rele,
- Efectuați verificări și monitorizați antecedentele personalului, pentru a identifica indivizii care ar putea avea un risc mai mare decât cel obișnuit de a deveni nemulțumiți sau contracarați,
- Configurați monitorizarea video pentru a oferi unele șanse de a depista sabotarea fizică în acțiune, dar mai mult pentru prezentarea dovezilor pentru investigațiile post atac
- Configurați un audit cibernetic detaliat pentru a avea dovezi pentru investigațiile post atac

În practică, persoanele din interiorul SCADA sunt cele mai de încredere persoane din afaceri atunci când vine vorba de echipamentul industrial pe care îl operează. În practică, aceste recomandări detaliate de monitorizare pot fi utilizate și ar trebui utilizate cu scopul de a cerceta incidentele de siguranță și de a închide fabrica la nevoie. Vizionarea video și alte înregistrări de audit pot îmbunătăți siguranța și increarea și pot minimiza atacul din interior.

Hackiviștii

În acest moment, în proiectarea noastră de apărare avansată în stilul IT, am acumulat un risc rezidual și nu am abordat decât măsuri de compensare, care nu au fost implementate. La acest moment în proiectare și pentru a aborda hackviștii, apărarea avansată în stilul IT scoate „armele mari”: sisteme de detectare intruzive (IDS). Având în vedere riscurile reziduale din sistemele noastre defensive, și având în vedere capabilitățile inamicilor, IT-știi susțin că compromiterea rețelelor cele mai importate este inevitabilă.

Sună convingător, nu? Sunt probleme serioase ale acestei abordări

Începem cu ultimul paragraf de mai sus. IDS este o măsură de detecție, nu o metodă preventivă - IDS-urile nu împiedică compromiterea. Un sondaj recent al sectorului de energie Nord American au arătat că un executiv mediu a fost convins că sistemele lor SCADA de detecție a intruziunilor ar detecta orice intruziune în 24 de ore ale acesteia. Alte studii arată că o intruziune ia în medie 6 luni să fie detectată și remediată.

10. Studiu de caz – Scenariul SCADA (Scenariu SCCR)

Acest capitol este bazat pe lucrarea **SCADA Security: Concepts and Recommendations**.

De ce să includem SCADA în scenariu?

- Peste tot în lume există un sistem SCADA rulând în spatele sistemelor critice
- Sistemele SCADA sunt coloana vertebrală a industriei moderne
- Totul de la rețelele de răspuns, cum ar fi și gazele, sistemele de gestionare a traficului, sistemele de tratare a apei, sistemele de control al construcțiilor utilizează SCADA
- Arhitectură foarte complexă (RTU-uri, PLC-uri, date relaționale, servere de date și servere web, HMI-uri)
- Vulnerabile prin proiectare
- Uzual sunt conectate într-o formă sau alta la internet (dar nimeni nu recunoaște asta)
- Fără update-uri
- De obicei sunt o cutie neagra pentru personal

Scenariul SCADA se bazează pe un sistem de monitorizare a rezervorului de combustibil:

- Versiune virtualizată a sistemului de monitorizare AST Monitoring (Sistem SCADA)
- Protocol simplu cu text clar
- Comenzi de bază precum l20100 în inventarul rezervoarelor
- Conexiune la internet (simulată)
- Amenințarea este grupul APT (Blueweeder)

Inamicul rațional: perturbă direct misiunea și provoacă dileme politice în interiorul trupelor, care poate contribui negativ în cadrul națiunilor, provocând o problemă cu populația.

Pentru a îndeplini scopul un grup de hackeri de la Stellaria au atacat sistemul SCADA cu scopul de a perturba baza militară aeriană Tytan localizată la Lastopol (în Tytan) care găzduiește de asemenea și evacuarea medicală MATO, avioanele tactice, precum și trupele care susțin misiunile locale. Atacuri similare împotriva sistemelor SCADA sunt planificate împotriva trupelor națiunilor.

10.1. Calendarul scenariului – Secvența de evenimente:

O lună înainte de STARTEX

- Blueweeder a identificat o anumită vulnerabilitate care afectează un control de combustibil foarte popular care intră în sistemul SCADA utilizat de națiunile MATO care vine în sprijinul misiunii MATO din Tytan
- Atacatorii au reușit să obțină acces la numeroase rețele naționale (nu în misiune) care utilizează sistemul vulnerabil SCADA și au plasat o bombă logică în HMI (interfața mașină-om). Bomba logică va fi activată automat (fără a necesita interacțiuni suplimentare) pe STARTEX + 1
- Bomba logică, atunci când este activată, interferează cu sistemul de măsurare a volumului și prezintă până la 30% mai puțin volum decât volumul actual din rezervoare.

6 zile înainte de STARTEX

- Blueweeder câștigă accesul la sistemul SCADA din baza Lastopol. Aceștia infectează sistemul cu bomba logică, care este activată mai târziu în aceeași zi.

5 zile înainte de STARTEX

- Explozie în baza Lastopol cauzată de umplerea prea mare a rezervoarelor cu combustibil. Doi angajați locali sunt uciși. Operațiunile aeriene sunt afectate deoarece avioanele nu mai au combustil. Ca rezultat, baza nu mai este operațională timp de 7 zile.

4 zile înainte de STARTEX

- Oficialii Tytanului după investigația inițială suspectează un atac cibernetic și colicită suport RRT de la MATO
- Tytan oferă informații cu privire la sistemul SCADA care a fost atacat tuturor națiunilor contribuabile. Națiunile pornesc o investigație pentr a identifica utilizarea acestui tip de SCADA

STARTEX (ziua 1)

- Ajung RRT în baza Lastopol și ăncep investigațiile sub direcția MATO CERT
- Blueweeder își asumă responsabilitatea pentru atac. Cer ca națiunile să oprească sprijinul operațiilor și oferă 48 de ore trupelor militare sau alte atacuri vor continua în capitală.
- Națiunile încep să investigheze sistemele SCADA similare

STARTEX Ziua 2

- Bomba logică este activată în sistemele naționale SCADA
- Valori greșite sunt prezentate pe monitor, iar rezervoarele conțin mai mult combustibil decît este reportat

STARTEX Ziua 3

- Întrucât națiunile nu și-au retras forțele militare iar umplerea rezervoarelor poate dura de la ore la zile, Blueweeder încearcă să se conecteze la sistemele SCADA și să modifice valorile astfel încât să umple rezervoarele mai repede.
- În cazul în care Blueweeder reușește (jucătorii nu au eliminat bomba logică și nu au identificat modul în care atacatorii au obținut accesul la rețea), acțiunile vor exploda la 13:00 Zulu
- Dacă Blueweeder nu reușesc să câștige un acces, dar bomba logică este încă activă, rezervoarele vor exploda la 15:00 Zulu
- Explozia este simulată prin închiderea mașinilor virtuale SCADA

10.2. Arhitectura segmentelor naționale și calea de atac

Există 29 de segmente de rețea (Țări) pentru care va trebui să simulați pașii de atac. Prin urmare, trebuie să repetați această secțiune de 29 de ori. Cea mai ușoară soluție este să obțineți X segmente fiecare lucrând în paralel.

Ca plan de atac, Blueweeder (echipa de atacatoru) va compromite mai multe sisteme de control ale combustibilului SCADA din mai multe țări și le vor infecta cu o bombă logică, care va interfera cu sistemul de măsurare a volumului din rezervoare. Acest lucru va conduce la umplerea peste măsură a rezolvoarelor și explodarea acestora. Ei au identificat faptul că un server vulnerabil VNC (versiunea de VNC este vulnerabilă la autentificare pe bază de parolă) rulează pe infrastructura țintei. Prin exploatarea acetsui serviciu, ei au câștigat acces la un sistem de pe LAN (VM1) cu privilegii locale de administrator.

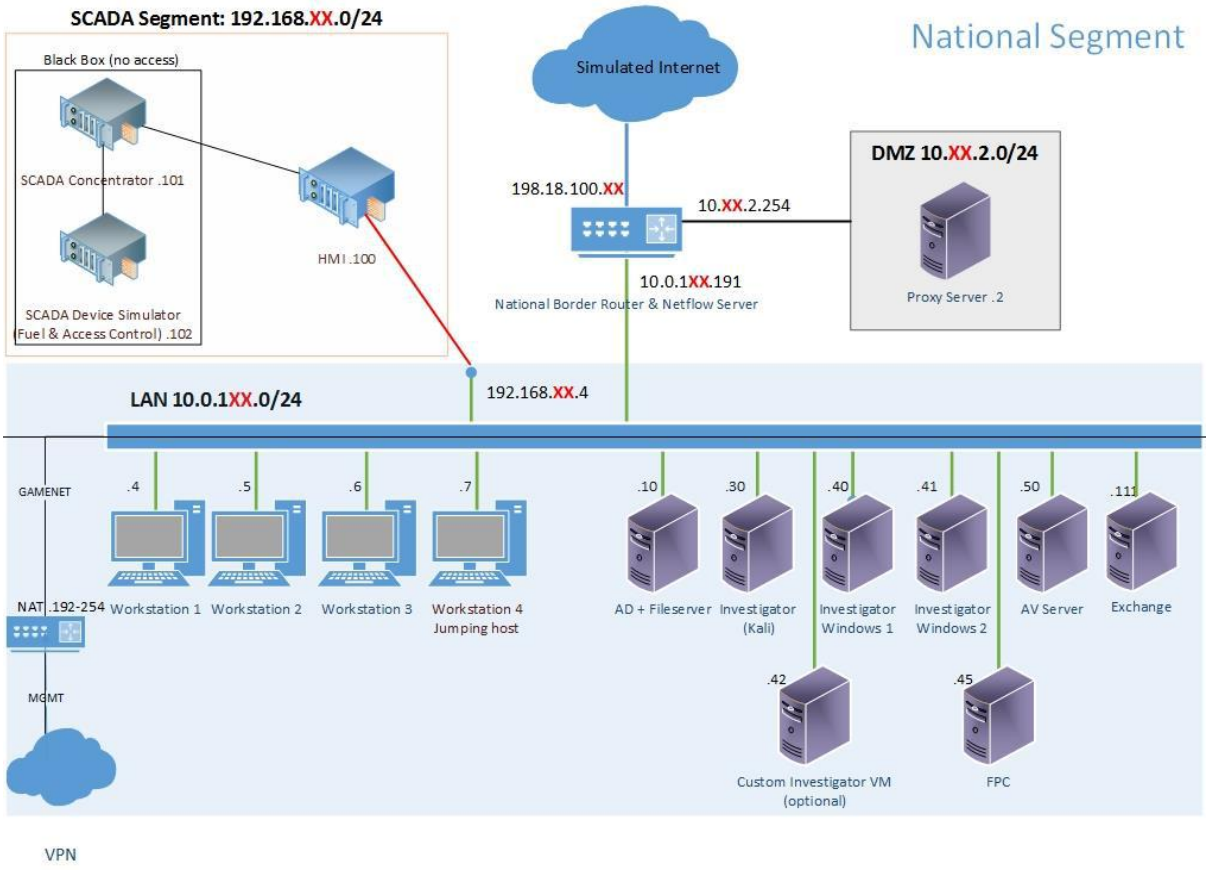

Figura 4. Arhitectura rețelei pentru fiecare segment.

Ei folosesc mimikatz pentru a lăsa credențialele capturate din memorie și, ca domeniu administrator, a fost conectat anterior la această stație de lucru, obținând drepturi de admin.
Apoi enumeră LAN-ul și identifică faptul că există o VM care are două interfețe de rețea. Această VM le permite să acceseze segmentul SCADA. Trimit RDP către acesta, scanează segmentul SCADA și identifică sistemele SCADA și HMI (interfața admin). Aceștia exploatează o vulnerabilitate injectabilă SQL pe HMI, câtigp accesul la server și instalează bomba logică (cod PHP pe interfața web).
Pentru monitorizarea rețelei există o soluție numită ***nfsen***, folosită pentru statisticile de rețea, pentru conexiunile interne (între VM-urile LNA) și către/de la Internet și două Windows VM și investigatorul Linux (kali) oferit pentru investigație.

Soluții potențiale

- Conectare de la un IP stelar la (netflow)
- Jurnalele Proxy cu uneltele pe care atacatorul le-a descărcat pe sistemele interne (rputer de frontieră se comportă ca un server proxy)
- Conectarea de la o stație de lucru compromisă la toate sistemele interne (netflow) în timpul procesului strângere a informațiilor
- Jurnalele de evenimente Windows (autentificările)
- Jurnalele serverului Web pe HMI (fără acces la VM SCADA)

Obiectivele acoperite

Incidentele cibernetice SCADA afectează direct și indirect misiunea MATO (amenințarea trupelor pentru contribuirea la națiuni în propria lor țară). Audiențele naționale de transport ar trebui să ia în considerare raportarea linilor naționale și MATO.
Mediul SCADA de antrenament necesită analiza unui: trafic netflow, jurnale proxy, jurnale de evenimente și criminalistica OS, pentru a identifica și rezolva vulnerabilitatea sistemului SCADA. Descoperirile tehnice ale analizei SCAD trebuie să fie administrate și redate în conformitate cu procedurile naționale / MTA. Rezultatele trebuie să fie împărtășite cu toate părțile relevante naționale / MATO, care urmăresc rapoartele. În funcție de contextul național creat pentru acest incident SCADA, acțiunile pot exercita consultanța cu industria. Consultarea industriei ar putea fi disponibilă pentru a stabili acorduri sau proceduri care ar putea fi exercitate pentru a crea acorduri de urgență pentru o amenințare eminentă.

11. Identificarea și analiza unui malware „fileless” (fără fișier)

Numeroase organizații consideră că utilizarea unor solutii antivirale bine-cunoscute ajută la protejarea terminalelor lor de toate tipurile de atacuri. O scanare săptămânală și o actualizare rapidă a semnăturii sunt la fel de bune ca amenințările pe care știe să le detecteze. Mecanismele de prevenire ale companiilor antivirus se bazează pe o varietate de metode, inclusiv euristică (ceea ce face fișierul), semnături (o copie a fișierului) și alți indicatori (reputație, DNS sau modificări de registru și așa mai departe). Se utilizează firewall și pentru a evita descărcarea fișierelor, executarea codurilor malițioase, exfiltrarea malware-ului în speranța prevenirii comportamentului neașteptat când se rulează scripturi sau fișiere ce conțin malware.

11.1. Ce este un malware de tip „fileless” (fără fișier)?

Protejarea dvs. implică mai mult decât actualizarea regulată a AV-ului și efectuarea scanărilor în mod regulat și există câteva provocări principale în tratarea atacurilor fără fișier folosind numai AV tradiționale și Firewall-uri:

- Atacurile fără fișier nu creează un fișier, făcând metodele de detectare bazate pe fișiere depășite;
- Atacurile fără fișier sunt utilizate în atacuri vizate și ca primă etapă a infecției cu malware se folosește un browser, însă atacurile complete sunt acum fără fișiere;

- Atacurile fără fișier, de multe ori pivotează din exploatarea memoriei către codul PowerShell pe care cele mai multe soluții terminale nu le inspectează;
- Procesele de scanare nu sunt suficient de rapide pentru a ține pasul cu programele de browser sau programele de aplicații;
- Multe soluții AV pretind că protejează împotriva exploatărilor de memorie și a scripturilor, dar cel mai mult sunt vagi în ceea ce privesc detaliile, lucru care face dificilă compararea soluțiilor pentru cumpărător.

În câteva cuvinte, PowerShell este:

- Microsoft a introdus cadrul PowerShell în 2005
- Oferă un limbaj de scriptare și o linie de comandă, ideal pentru automatizarea și gestionarea sarcinilor
- Deoarece este puternic, este de asemenea rapid adoptat de atacatori

PowerShell este de asemenea o platforma foarte bună pentru atac :

- Utilizat în principal pentru descărcare și pentru mișcare laterală
- Codul este ușor de acoperit
- Codul acoperit este greu de analizat
- Semnăturile statice ale AV sunt ineficiente pe un cod obfuscat
- Adesea tratat superficial de produsele de securitate tradiționale și de apărători atunci când își consolidează sistemele
- Are o comunitate în creștere cu scripturi disponibile

11.2. Detectarea și prevenire malware-ului fără fișier

Ce face atât de dificilă detectarea atacurilor malware fără fișiere? Aceste atacuri sunt complet în memorie și folosesc sisteme legitime de administrare pentru a executa și a se propaga, făcând identificarea a ceea ce este utilizare legitimă a PowerShell și a ceea ce este activitatea atacatorului extrem de dificilă. PowerShell este utilizat de administratorii IT pentru a efectua zilnic o varietate de sarcini, de aceea este necesară o cantitate mare de PowerShell.

Administratorii IT utilizează PowerShell pentru a efectua zilnic o varietate de sarcini, prin urmare, o cantitate mare de utilizare a PowerShell nu ridică semne de întrebare. Și pentru că PowerShell este atât de utilizat pe scară largă, profesioniștilor în securitate le lipsește timpul necesar pentru a studia jurnalele, pentru a identifica comportamentul suspect și pentru a investiga apariția.

Dezactivarea PowerShell este o concepție greșită des întâlnită care va preveni atacurile malware fără fișiere. Din păcate, această abordare doar va îngreuna munca celor din domeniul IT. PowerShell este necesar pentru a îndeplini cele mai simple funcții. În plus, PowerShell va fi utilizat în cele din urmă de toate produsele Microsoft.

Administratorii care devin competenți în PowerShell vor putea gestiona majoritatea produselor noi Microsoft. Utilizarea PowerShell este restricționată, limitând abilitățile administratorilor la talentele obținute care le-ar putea ajuta cariera.

11.3. Studiu de caz – Scenariul malware fără fișier (Scenariul FMW)

Liniile de bază ale scenariului

Blueweeder țintește rețelele Gvernamentale implicate în proiectare, testând și epuizând Sistemul de Apărare a Aeriană (ADS) al lui NTAO în Tytan.

Obiective

- Încerinirea proiectului prin pierderea datelor
- Chiar și datele neclasificate programul de livrare, livrarea etc) pot fi utile pentru Stellaria
- Câștigarea informațiilor despre sistemul aerian de apărare

Problemele tehnice

- Criminalistica computațională
- Criminalistica rețelei
- Analiza malware

Calendarul scenariului – secvențe de evenimente

3 săptămîni înainte de STARTEX

– Blueweeder începe să trimită email-uri de phishing
– Infectează ai multe stații de lucru cu malware care rămâne adormit

1 zi înainte de STARTEX

– Malware se activează. Exfiltrează și șterge fișierele încet.
– Userul începe să raporteze lipsa fișierelor

STARTEX

– Echipa tehnică începe investigația

Arhitectura Segmentului Național & Planul de atac

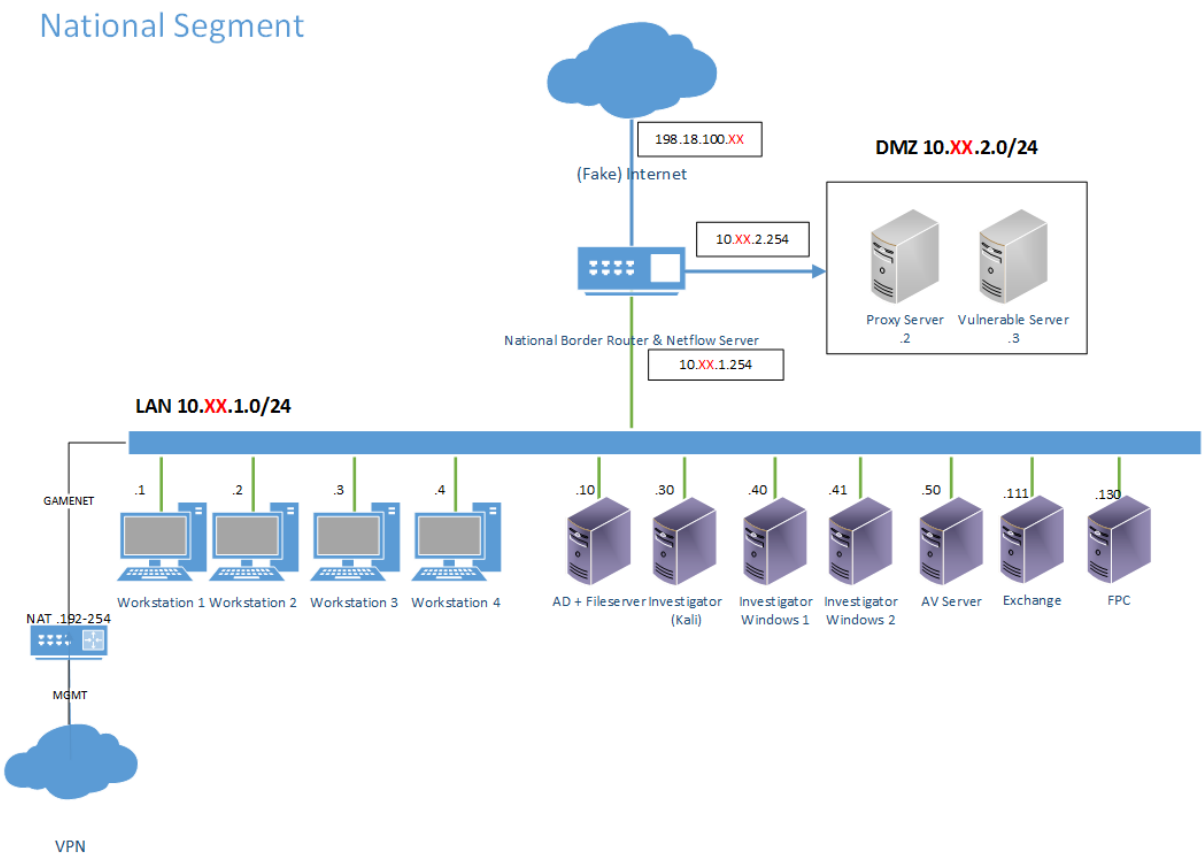

Figure 15. Diagrama unui segment național.

Infectarea inițială

Atacul de phishing împotriva a 2 utilizatori per națiune. Email-uri cu documente Word. Documentul va conține un scurt script powershell (Etapa 1) codat în macros ce va fi trimis în directorul AppData și o sarcină programată va fi adăugată să execute la fiecare 2 ore, începând din STARTEX – 1.

Etapa 1

De fiecare dată când va fi executat va:

– lua numele domeniului

– va face trei cereri către BadIP (Blueweeder)

- URL va fi folosit asemănător unei chei
- acets lucru va permite rularea firewall-ului pe BadIP pentru a permite conexiunile de la IP-ul respectiv

– va face o cerere HTTP către BadIP portul 80/TCP trimițând numele domeniului

- BadIP va returna scriptul PowerShell din Etapa 2 și va fi executat în memorie

– unic pentru fiecare națiune

– se conectează la un server C&C diferit în fiecare țară

Etapa 2

Acțiunile care se realizează în etapa 2 sunt:

– Căutarea în hardurile locale și maparea driverelor de rețea pentru MS Office și fișierele PDF și selectează 5 aleator

– Generează o cheie aleatoare (256 biți)

– Trimite numele fișierelor, amestecuri de fișiere și chei criptate către C&C, criptate cu cheia publică a C&C-ului.

– Criptează (AES 256) cele 5 fișiere, le trimite către serverele C&C, le șterge apoi iese (va începe din nou la un interval prestabilit)

Etapele așteptate din timpul executării:

- Identificarea infectării inițiale
- Identificarea stațiilor de lucru infectate și a proceselor malițioase (Etapa 1)
- Realizarea analizei malware în Etapa 1&2
- Colaborarea cu națiunile în care au fost încărcare fișiere (luarea fișierelor criptate și a cheilor)
- Împărtășirea informațiilor identificate

12. Concluzii și direcții viitoare

12.1. Concluzii

În această teză am analizat numeroase poligoane cibernetice și tipurile lor. Deoarece acum putem susține că diferitele poligoane cibernetice au puncte tari și puncte slabe distincte, putem crea un poligon cibernetic ideal utilizând parametrii de clasificare. Diferite tabele și figuri au fost folosite pentru a reprezenta aceste clasificări. Am atribuit un nivel de importanță fiecărui parametru pe baza semnificației acestuia.

În continuare, am introdus conceptul de „Next-Generation Cyber Range”. Poligonul cibernetic este responsabil pentru inițierea unor scenarii de securitate cibernetică, care au fost, de asemenea, recunoscute ca centre de instruire și conștientizare a securității cibernetice.

Ca parte a funcționalităților și arhitecturii, scenariul SCADA a fost dezvoltat și rulat cu 30 de echipe (echipa roșie și echipa albastră).

Un alt scenariu important care să poată pune în valoare caracteristicile și funcționalitățile unui poligon cibernetic de generație următoare și care să poată îmbunătăți conștientizarea în orice echipă de securitate cibernetică (roșu, albastru și mov) este scenariul dezvoltat cu malware fără fișier prezentat în teză.

12.2. Contribuții principale

Am fost implicat în procesul de cercetare și dezvoltare a diverselor poligoane cibernetice ce pot fi considerate un rezultat solit al acestei teze. Am evaluat poligoanele cibernetice actuale și le-am clasificat pe baza anumitor factori ca parte a lucrării, deoarece observ că diferite game cibernetice au puncte tari și diferite limitări.

Folosind parametrii de clasificare, am prezentat un Cyber-Range ideal. Pentru a reprezenta clasificarea, au fost utilizate mai multe tabele și figuri. Am atribuit un nivel de prioritate fiecărui parametru pe baza rezultatului acestuia. Graficele însoțitoare oferă o imagine bună a parametrilor care trebuie luați în considerare pentru un poligon cibernetic perfect.

O parte importantă a acestei cercetări a fost proiectarea și dezvoltarea activității cibernetice pentru exercițiul NATO Cyber Coalition (2015-2018) bazat pe infrastructura Ministerului Apărării din Estonia. Pentru a crea o bună dovadă a conceptului, am fost implicat și în dezvoltarea scenariului SCADA pentru exercițiul NATO Cyber Coalition 2017, în care am putut simula un mediu critic care poate fi atacat de actori rău intenționați.

Am fost, de asemenea, implicat în dezvoltarea scenariului și dezvoltarea infrastructurii pentru exercițiul NATO Cyber Coalition 2018, care se bazează pe un scenariu de tip Fileless Malware. În România am făcut parte din echipa care a organizat (implementarea infrastructurii exercițiilor și contribuția la scenariu) exercițiile CyDEx în 2017 și 2018 și în 2019 am făcut parte din echipa Deloitte care a creat scenariul echipei roșii și a jucat acest scenariu în timp real în timpul exercițiului CyDEx 19.

Putem concluziona că principalele contribuții la această lucrare de cercetare sunt:

- Am studiat arhitecturi și caracteristici complexe care pot fi utilizate în poligoanele cibernetice și am comparat trei dintre cele mai importante poligoane cibernetice existente - între SUA Cyber Test Range, NATO Cyber Range (CCD COE Cyber Range) și UK Cyber Range. Rezultatele sunt prezentate în Capitolul 2;
- Am identificat cele mai utilizate arhitecturi și caracteristici din poligoanele cibernetice la nivel mondial și am descris diferite topologii care ar putea fi implementate în diferite tipuri de scenarii de echipă roșie-echipă albastră. Rezultatele sunt prezentate în capitolele 5 și 6;
- Am identificat aspectele cheie ale unui poligon cibernetic de generație următoare și am descris parametrii esențiali care pot defini poligonul cibernetic perfect (setări, infrastructură, scenariu, personal implicat, mediu simulat, instrumente, automatizare, performanță, VPC, VPN, fidelitate și proprietate intelectuală). Toți acești parametri au fost evidențiați pe poligonul cibernetic al exercițiului anual CyDEx. De asemenea, am făcut o comparație între CyDEx Cyber Range și conceptul de Cyber-Range ideal. Rezultatele sunt prezentate în capitolele 7 și 8;
- Am identificat avantajele creșterii gradului de conștientizare pentru departamentele de securitate cibernetică și infrastructura critică, cum ar fi sistemele SCADA. De asemenea, au fost identificate principalele concepte și preocupări de securitate privind sistemele SCADA, vectorii de atac și perspectiva apărării. Toate rezultatele sunt prezentate în capitolul 9;
- Am propus scenarii practice pentru infrastructuri critice de securitate cibernetică care au fost dezvoltate în exerciții cibernetice din lumea reală, pe NATO Cyber Coaliton și CyDEx. Scenariile includ

vectori de atac, pași de investigație pentru analiză și recomandări de protecție împotriva acestui tip de atacuri, toate acestea fiind prezentate în detaliu în capitolele 10 și 11.

12.3. Lista publicațiilor

1. **Dragos-George Ionica**, Florin Pop and Aniello Castiglione - ***Creating and Managing Realism in the Next-Generation Cyber Range***. Published in Network and System Security12th International Conference, NSS 2018, Hong Kong, China, August 27-29, 2018,
2. **Dragos-George Ionica**, Nirvana Popescu, Decebal Popescu, Ciprian Dobre - ***SCADA Security: Concepts and Recommendations***: 10th International Symposium, CSS 2018, Amalfi, Italy, October 29–31, 2018
3. **Dragos-George Ionica**, Nirvana Popescu, Decebal Popescu, Florin Pop - ***Cyber Defence Capabilities in Complex Networks*** - INTERNET OF EVERYTHING - ALGORITHMS, METHODOLOGIES, TECHNOLOGIES AND PERSPECTIVES 2018
4. Andrei Stoicu, **Dragos-George Ionica** - ***Social Media Avatar: My Dear Virtual Assistant***. Published in: 2018 IEEE 16th International Conference on Embedded and Ubiquitous Computing (EUC)
5. Marius Marian, Adelin Cusman, Dan Popescu, **Dragos Ionica** - ***A DNP3-based SCADA Architecture Supporting Electronic Signatures***. Published in: 2019 20th International Carpathian Control Conference (ICCC)
6. Marius Marian, Adelin Cusman, Florin Stinga, Dan Popescu, ***Dragos Ionica*** - ***Experimenting with Digital Signatures over a DNP3 Protocol in a Multitenant Cloud-Based SCADA Architecture*****.** Published in: August 2020 IEEE Access PP(99):1-1

12.4. Alte activități

- Participarea la conferința BlackHat USA și Defcon în 2017
- Participarea la Offensive Con 2019 & 2020
- Red Team Operator (Certificare emisă de Zero Point Security) în 2020
- Adversary Tactics: Red Team Operations (Certificare emisă de Specter Ops)
- Parte din Programul COE Cybercrime
- Top 5 Cercetători/Pentesteri din Cobalt Core în anul 2020 pe platforma Cobalt PaaS https://blog.cobalt.io/exploring-valuable-pentester-traits-top-cobalt-core-pentesters-of-2020-e8d1fc0389ae

12.5. Direcții viitoare

Am fost eficient în clasificarea poligoanelor cibernetice în mai multe categorii pe baza cercetărilor realizate. Există mult mai multe poligoane cibernetice care funcționează într-o varietate de moduri, crescând posibilitatea apariției mai multor astfel de parametrii în viitor. Nivelul de importanță atribuit pentru fiecare parametru al unui poligon cibernetic ideal poate varia în conformitate cu analiza altor poligoane cibernetice. Evaluarea nu poate fi făcută decât pe logică și convingere, deoarece datele colectate nu sunt cantitative, ci doar calitative. În viitor, pot afla mai multe despre modul în care funcționează poligoanele cibernetice și pot colecta date pentru o varietate de poligoane cibernetice, reușind astfel să furnizez date cantitative pentru un poligon cibernetic perfect.

S-a dezvăluit că următoarea generație Cyber-Rage este comparabilă cu Cyber-Rage-ul perfect atunci când este utilizat într-un context real. Mai mulți parametrii, cum ar fi Infrastructura Cloud, Simularea, Personalul Implicat și Rețeaua de tip VCN, au valori diferite, rezultând discrepanțe. În timp ce infrastructura cloud este în curs de implementare, pot fi utilizate unelte sofisticate pentru a îmbunătăți simularea, iar oamenii pot fi introduși în viitor în exerciții. Pe de alta parte, parametrii precum VCN ar putea să nu mai facă parte din gama cibernetică în curând. Ca urmare, apropierea procentuală între intervalele cibernetice ar putea crește semnificativ. La analiză pot fi adăugați și noi parametri.

Referințe bibliografice

[1] "Defence Minister opens UK cyber security test range - GOV.UK," [Online]. Available: https://www.gov.uk/government/news/defence-minister-opens-uk-cyber-security-test-range. [Accessed January 2021].

[2] N. Wiener, Cybernetics or Control and Communication in the Animal and the Machine, Cambridge: MIT Press, 1948.

[3] "NATO Cooperative Cyber Defence Centre of Excellence. CCD COE Training Courses -CCD COE.," [Online]. Available: https://ccdcoe.org/training/. [Accessed July 2020].

[4] M. . J. West-Brown , D. Stikvoort , K.-P. Kossakowski , G. Killcrece, R. Ruefle and M. Zajicek , "Handbook for Computer Security Incident Response Teams (CSIRTs)," Software Engineering Institute, April 2003.

[5] NC3A, "Cyber Defence Capability Framework," December 2010.

[6] P. A. Bauxbaum, "Building a Better 'Cyber Range'," August 2011.

[7] R. H. T. K. a. P. C. E. Powell, "The Information Assurance Range," *ITEA Journal,* vol. 31, pp. 473-477, 2010.

[8] Welshans, "History of Cyber Testing and Evaluation - A Voice From the Front Lines," *ITEA Journal,* vol. 31, pp. 449-452, 2010.

[9] UK Ministry of Defence, "Defence Minister opens UK cyber security test range.," [Online]. Available: http://www.mod.uk/DefenceInternet/DefenceNews/DefencePolicyAndBusiness/Defence Minister OpensUkCyberSecurityTestRange.htm.

[10] J. e. a. Mirkovic, "The DETER Project; Advancing the Science of Cyber Security Experimentation and Test," *IEEE,* 2010.

[11] "DARPA. National Cyber Range. DARPA. 21. Defense Information Systems Agency. Department of Defense Information Assurance Range: A Venue for Test and Evaluation In Cyberspace.," [Online]. Available: http://www.darpa.mil/Our_Work/STO/Programs/National_Cyber_Range_(NCR).aspx. [Accessed August 2011].

[12] W. e. a. He, "A game theoretical attack-defense model oriented to network security risk assessment," *Computer Science and Software Engineering,* 2008.

[13] R. a. L. P. Ottis, "Cyberspace: Definitions and Implications," in *5th International Conference on Information Warfare and Security*, Dayton OH, US, 2010.

[14] D. D. S. H. S. a. L. K. W. F. D. K. Kuehl, " Cyberpower and National Security," in *From Cyberspace to Cyberpower: Defining the Problem.*, 2009.

[15] Ministry of Security and Justice, "Cyber Security Beeld Nederland," June 2012. CSBN-2. .

[16] D. L. D. C. a. C. Y. Paul Cornish, "On Cyber Warfare," *Chatham House,* November 2010.

[17] Ginter, "13 ways through a firewall: What you don't know can hurt you. ISA Intech," 2013. [Online]. Available: https://www.isa.org/standards-publications/isa-publications/intech-

magazine/2013/april/special-section-13-ways-through-firewall-what-you-dont-know-can-hurt-you/ .

[18] US Department of Defence, "Joint Publication 3-0, Joint Operations.," August 2011.

[19] E. Ferrara, " Determine the business value of an effective security program - information security economics 101," *Forrester Research,* 2002.

[20] A. W. B. Conklin, "E-Government and Cyber Security: The Role of Cyber Security Exercises," in *39th Hawaii International Conference on Systems Sciences*, 2006.

[21] The White House, "International Strategy for Cyberspace," 2011. [Online]. Available: http://bruteforcelab.com/wp-content/uploads/HILJ-Online_54_Schmitt.pdf.

[22] NATO, "Allied Joint Doctrine for Information Operations," vol. AJP 3.10, November 2009.

[23] J. D. a. S. Magrath, "A survey of Cyber Ranges and Testbeds," *Cyber and Electronic Warfare Division Defence Science and Technology Organisation, Australian Government Department of Defence,* 2013.

[24] "Enisa - European Network and Information Security Agency," *Good Practice Guide on National Exercises,* 2009.

[25] D. A. S. Sr, "'Communications-Electronics Command cyber training range launches', Logistics and Readiness Center, CECOM," 23 June 2015. [Online]. Available: https://www.army.mil/article/150996/communications_electronics_command_cyber_t.

[26] "National initiative for Cybersecurity Education, Cyber Ranges, National Institute of Standards and Technology (NIST),US Department of Commerce, 2017.".

[27] "The Role of Local Law Enforcement Agencies In Preventing and Investigating," April 2014.

[28] "Standing up a Cyber Range Capability in Michigan Centre for Secure Computing (CSC), De Montfort University Partnered with the Michigan Cyber Security Center (MCC)," 21 Dec 2017.

[29] "Image for Cisco Cyber Range," [Online]. Available: http://www.manetic.org/images/stories/events/20170424/20170424.JPG .

[30] Cyberbit, "Cybershield Training and Simulation, Live training for cyber-security professionals," 2016. [Online]. Available: https://www.cyberbit.com/wpcontent/uploads/2016/09/CB-TnS-Print.pdf.

[31] M. Gürtler, "'NATO Cooperative Cyber Defence Centre of Excellence', Locked Shields," 27 June 2012. [Online]. Available: https://www.enisa.europa.eu/events/cyber-exercise-conference/presentations/7.%20Conf%20Paris%20-June%202012%20-%20-%20M.%20GURTLER%20-NATO-CCDCOE.pdf .

[32] Department of Defense, "National Cyber Range, Test resource Management Center," 24 February 2015. [Online]. Available: https://www.acq.osd.mil/dte-trmc/docs/20150224_NCR%20Overview_DistA.pdf.

[33] "Baltimore Cyber Range (About), August 2017," [Online]. Available: https://www.baltimorecyberange.com/about .

[34] E. Tate Emily, "Regent University opens stand-alone cyber range," Regent Cyber Range, October 2017. [Online]. Available: https://edscoop.com/regent-university-opens-stand-alone-cyber-range.

[35] J. Curry, "CyberSecurity Range (CSR) v2.0 Architecture and Capability," Defense Information Systems Agency (DISA), April 2016. [Online]. Available: http://www.disa.mil/~/media/Files/DISA/News/Conference/2016/AFCEASymposium/5-Curry20Improving_Cyber_Security.pdf.

[36] " Georgia Cyber Range," [Online]. Available: http://cyber.augusta.edu/au/wp-content/uploads/2017/01/videobgtest.png.

[37] "Image for NATO cyber range," [Online]. Available: https://www.nato.int/nato_static_fl2014/assets/pictures/stock_2017/20170406_170406.

[38] R. C. Range. [Online]. Available: https://www.raytheon.com/index.php/cyber/news/feature/ready-aim-test.

[39] Ponemon Institute, "2016 Ponemon Cost of Data Breach Study," Ponemon Institute, 2017. [Online]. Available: https://www.ibm.com/security/data-breach/.

[40] Tripwire, "Tripwire Critical Infrastructure Study," 2015. [Online]. Available: Available: https://www.tripwire.com/company/press-releases/2015/01/study-critical-infrastructure-executives-complacent-about-internet-of-things-secu/. [Accessed January 2017].

[41] "The Georgia Cyber Range," [Online]. Available: https://gov.georgia.gov/sites/gov.georgia.gov/files/related_files/press_release/Georgia%20Cyber%20Innovation%20and%20Training%20Center.pdf.

[42] CBC News, "University of Calgary paid $20K in ransomware attack," 2016. [Online]. Available: http://www.cbc.ca/news/canada/calgary/university-calgary-ransomware-cyberattack-1.3620979.

[43] Mandiant, "Mandiant APT1 – Exposing One of China's Cyber Espionage Units," 2013. [Online]. Available: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

[44] S.Gallagher, "Two more healthcare networks caught up in outbreak of hospital ransomware," Arstechnica, 2016. [Online]. Available: https://arstechnica.com/security/2016/03/two-more-healthcare-networks-caught-up-in-outbreak-of-hospital-ransomware/.

[45] R. Eller, "Black Hat Japan 2004 - capture the flag games/ measuring skill with hacking contests," 15 October 2004. [Online]. Available: http://www.blackhat.com/presentations/bh-asia-04/bh-jp-04-pdfs/bh-jp-04- eller/bh-jp-04-eller.pdf. [Accessed July 2018].

[46] M. o. Defence., "Ministry of Defence. Defense after the credit crisis: a smaller armed forces in a troubled world," BS2011011591, 2011.

[47] Mandiant, "Mandiant APT1 – Exposing One of China's Cyber Espionage Units," 2013. [Online]. Available: https://www.fireeye.com/content/dam/fireeye-www/services/pdfs/mandiant-apt1-report.pdf.

[48] T. Scott, "March 17 1948: William Gibson , Father of Cyberspace," [Online]. Available: Wired.com. [Accessed March 2011].