UNIVERSITATEA „POLITEHNICA” din BUCUREȘTI

ȘCOALA DOCTORALĂ ETTI-B

Nr. Decizie 531 **din** 28.07.2020

REZUMATUL TEZEI DE DOCTORAT

SECURITATE CIBERNETICĂ: VULNERABILITĂȚILE SISTEMELOR INFORMATICE ALE VIITORULUI

CYBER SECURITY: THE VULNERABILITIES OF FUTURE INFORMATION SYSTEMS

Doctorand: **Ing. Ionuț-Daniel BARBU**

COMISIA DE DOCTORAT

Președinte	**Prof. dr. ing. Gheorghe BREZEANU**	de la	**Universitatea POLITEHNICA din București**
Conducător de doctorat	**Prof. dr. ing. Ioan BACIVAROV**	de la	**Universitatea POLITEHNICA din București**
Referent	**Prof. dr. ing. Mircea POPA**	de la	**Universitatea Politehnica Timișoara**
Referent	**Prof. dr. ing. Gheorghe ȘERBAN**	de la	**Universitatea din Pitești**
Referent	**Conf. dr. ing. Marian VLĂDESCU**	de la	**Universitatea POLITEHNICA din București**

BUCUREȘTI 2020

Mulțumiri

În primul rând doresc să mulțumesc coordonatorului științific al studiilor mele doctorale, domnul Prof. em. dr. ing. Ioan BACIVAROV, pentru permanenta îndrumare de-a lungul stagiului de doctorat.

Mulțumesc comisiei de îndrumare (Prof. em. dr. ing. Marin DRĂGULINESCU, Prof. dr. ing. Angelica BACIVAROV, CP1 dr. ing. Marius BÂZU) pentru coordonarea activității mele pe parcursul întregului program de doctorat. De asemenea, doresc să îmi exprim gratitudinea față de membrii comisiei de evaluare a lucrării, pentru evaluarea tezei, comentariile și sugestiile oferite.

Doresc să mulțumesc membrilor Laboratorului EUROQUALROM și întregului Departament Tehnologie Electronică și Fiabilitate din cadrul Facultății de Electronică, Telecomunicații și Tehnologia Informației, Universitatea POLITEHNICA din București, departament condus de dl. Conf. dr. ing. Marian VLĂDESCU, pentru mediul de lucru asigurat, evaluarea preliminară a tezei de doctorat și recomandările făcute.

Mulțumesc în mod special domnilor Conf. dr. ing. Ioan-Cosmin MIHAI și Dr. ing. Gabriel PETRICĂ, specialiști care m-au introdus în lumea securității informatice și m-au sprijinit constant pe toată perioada studiilor. De asemenea, adresez mulțumiri colegilor doctoranzi din colectivul de cercetare pentru prietenia arătată de-a lungul timpului. Lor le datorez bucuria și împlinirile unui drum de excepție.

Țin să mulțumesc echipelor în care am lucrat (și în mod special echipelor mele din cadrul companiilor Xperi și Adobe), îndeplinind diverse roluri ce au contribuit la dezvoltarea mea profesională.

Tuturor celor care m-au sprijinit le ofer cele mai bune gânduri și recunoștință.

Mulțumesc soției mele, Ioana, care m-a sprijinit necondiționat pe toată perioada studiilor doctorale și de-a lungul întregului meu parcurs profesional și părinților care mi-au subliniat importanța educației.

Mulțumesc Anei și lui Tudor!

Rezultatele prezentate în această lucrare au fost obținute cu sprijinul Ministerului Fondurilor Europene prin Programul Operațional Sectorial Dezvoltarea Resurselor Umane 2007-2013, Contract nr. POSDRU/159/1.5/S/132397.

Cuprins

Cuprins teză

Capitolul 1. Introducere

În ultimul deceniu tehnologia în general și tehnologia informației în mod special au transformat profund mediul de afaceri global, cu progrese continue în toate domeniile, de la lucrul în echipă, stocarea datelor în cloud și blockchain la inteligența artificială (AI - Artificial Intelligence) și Internetul lucrurilor (IoT - Internet of Things). Odată cu creșterea vitezei cu care tehnologiile digitale evoluează și modifică modelele tradiționale de afaceri, riscurile legate de securitatea cibernetică par să evolueze și mai repede. Riscul cibernetic a trecut la un nivel superior, dincolo de deja „clasicele" breșe de securitate și scurgeri de date sensibile, ajungând la scheme sofisticate care pot perturba o întreagă companie sau industrie, gestionarea unui lanț logistic de aprovizionare sau chiar, la nivel guvernamental, pot afecta funcționarea unui stat. Pagubele se ridică la miliarde de euro și afectează companiile din orice sector de activitate și economiile naționale.

1.1. Prezentarea domeniului și a oportunității tezei de doctorat

Domeniul tehnologiei informației se schimbă constant, apar noi tehnologii hardware, se îmbunătățește software-ul și se optimizează procesele de afaceri. Istoria sistemelor de calcul constă într-un flux constant de avansări tehnologice. Calculatoarele mainframe au fost urmate de mini-computere, care la rândul lor au fost urmate de computere personale și apoi de dispozitive mobile. Dezvoltarea software-ului a urmat o traiectorie similară, cu o evoluție de la aplicații orientate pe loturi (batch), specifice sistemelor mainframe, trecând prin modelele client-server spre arhitecturi de servicii distribuite și aplicații Web. Procesele de afaceri s-au schimbat, iar prelucrările de date s-au extins dincolo de nivelul sistemelor back-office orientate către operațiunile de bază, spre aplicații de colaborare și productivitate adoptate pe scară largă.

Studiul „*2019 Global Cyber Risk Perception Survey*" elaborat de Marsh și Microsoft investighează percepțiile asupra riscurilor cibernetice și managementului riscului în cadrul organizațiilor din întreaga lume, în special în contextul unui mediu tehnologic de afaceri cu evoluție rapidă [1]. Concluziile acestui studiu, prezentate succint în continuare, subliniază starea riscului cibernetic în organizații în momentul actual.

1. Conștientizarea riscurilor cibernetice a crescut. Motivate de frecvența și severitatea incidentelor recente cu impact major asupra securității datelor, prioritățile organizațiilor referitoare la riscurile de securitate și amenințări au crescut semnificativ în 2019 față de 2017 în rândul organizațiilor.

2. Riscurile asociate unor atacuri sau amenințări cibernetice au depășit net toate celelalte riscuri. În 2019, cei mai mulți respondenți au clasat riscul cibernetic drept o preocupare de top, în timp ce incertitudinea economică a fost pe locul al doilea.

3. Majoritatea organizațiilor iau în considerare sau folosesc o serie de tehnologii noi. Întreprinderile împrumută inovația tehnologică și majoritatea nu consideră riscul cibernetic ca o barieră. Cel puțin 70% din respondenții sondajului din 2019 au menționat

cel puțin o tehnologie operațională inovatoare - inclusiv cloud computing, produse digitale proprii și dispozitive conectate / IoT - pe care le-au adoptat sau le iau în considerare.

În contextul prezentat mai sus, oportunitatea temei alese este dată de actualitatea și impactul securității cibernetice, considerată drept cel mai important aspect din punct de vedere tehnologic în Raportul de Risc Global al World Economic Forum pentru anul 2020 [2]. Introdus în 2015 de Klaus Schwab, fondator și președintele executiv al World Economic Forum, în articolul „*The Fourth Industrial Revolution. What It Means and How to Respond*" [3], termenul „*A patra revoluție industrială*" face referire la tehnologii care combină domeniile hardware, software și biologie (sisteme cyber-fizice), bazate pe progresele înregistrate în telecomunicații și conectivitate. Astfel, se estimează ca epoca 4IR (Fourth Industrial Revolution) să fie marcată de descoperiri în tehnologiile emergente din domenii precum robotica, inteligența artificială, nanotehnologiile, calculul cuantic, biotehnologia, IoT, IIoT (Industrial IoT), tehnologiile tip decentralized consensus (blockchain), tehnologiile wireless și rețele de telecomunicații mobile 5G, imprimare 3D și vehicule complet autonome. Acest val de tehnologii 4IR va remodela dramatic economiile și societățile: pentru medicina de precizie, vehiculele autonome și drone se estimează o piață cu creștere rapidă, în timp ce inteligența artificială este de așteptat să stimuleze creșterea globală cu 14% până în 2030 [4].

1.2. Scopul tezei de doctorat

Lucrarea „*Securitate cibernetică: vulnerabilitățile sistemelor informatice ale viitorului*" analizează contextul global al securității cibernetice actuale, prezintă considerațiile autorului referitoare la perspectivele de evoluție a amenințărilor și vulnerabilităților cibernetice și propune mai multe soluții de securizare, aplicabile atât sistemelor actuale, cât și celor ce vor ne guverna activitatea în viitorul apropiat.

Toate entitățile implicate (de la utilizatori individuali la mici organizații, mari companii sau națiuni întregi) trebuie să accepte o axiomă unanim acceptată, valabilă în momentul de față și de la care am pornit cercetările în cadrul tezei de doctorat. Vulnerabilitățile informatice există, amenințările cibernetice pot fi abordate proactiv, impactul atacurilor poate fi atenuat, pierderile de informații pot fi minimizate, se pot aplica politici de disaster recovery la nivel de organizație. În acest context, *riscul de securitate cibernetică poate fi gestionat / minimizat, însă nu poate fi eliminat* (fig. 1.5).

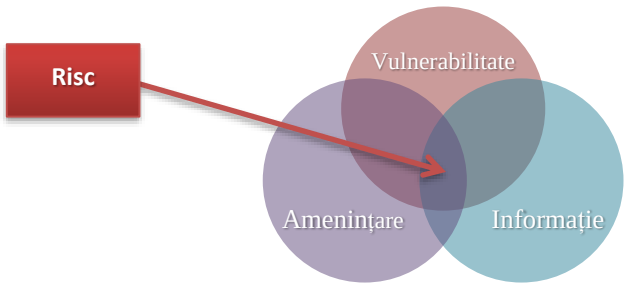

Fig. 1.5 Riscul de securitate cibernetică

Tematica acestei lucrări a fost abordată din două puncte de vedere care, doar implementate complementar, vor avea impact în organizație. Dată fiind formarea mea profesională duală, am analizat situația curentă atât din perspectivă managerială, prin propunerea unui model de implementare a unui program de securitate informațională adaptat industriei și provocărilor în continuă schimbare, cât și din punct de vedere tehnic, aplicând un model de analiză a securității în profunzime. Astfel, analizând impactul vulnerabilităților asupra sistemelor de calcul, rețelelor și dispozitivelor IoT, am observat ariile mai puțin mature ale sistemelor de securitate și am dezvoltat soluții tehnice scalabile pentru a aborda probleme de securitate și a reduce suprafața de atac odată implementate.

Capitolele lucrării oferă o imagine de ansamblu și aduc un plus referitor la nivelul de conștientizare a implicațiilor asigurării securității în sisteme cibernetice de tip „honeypot" și în orașe inteligente pentru a acoperi o plajă diversă de aplicabilitate. Cercetarea a fost condusă de o sesiune de teste efectuate într-un mediu de dezvoltare destinat proiectării și construirii de proiecte IoT de mici dimensiuni pentru a studia limitele hardware și software în analiza pachetelor de date.

Rezultatele prezentate în cadrul lucrării au condus și la obținerea de inteligență cibernetică despre actorii care conduc atacuri informatice asupra rețelelor locale de calculatoare și platformelor de tip e-learning. Deoarece se dorește o promovare a accesului la educație cu costuri foarte scăzute, hardware-ul folosit în elaborarea studiului a presupus prețuri reduse, iar software-ul a fost de tip open-source sau educațional.

Scopul final al lucrării este de a atrage atenția asupra nevoii unor implementări de securitate și standarde de conformitate pentru atenuarea riscurilor în zonele de aplicabilitate, având în vedere tipurile de vulnerabilități și amenințări specifice tehnologiilor folosite curent, într-un context fizic, psihic, tehnic și organizațional / managerial total modificat de pandemia COVID-19 cu care omenirea se confruntă la momentul actual.

1.3. Organizarea pe capitole și conținutul lucrării

Teza de doctorat a fost structurată în 5 capitole și o secțiune finală formată din 3 anexe.

Capitolul 1 face o introducere în tematica abordată, prezentând domeniul securității cibernetice, contextul în care a fost elaborată lucrarea și oportunitatea alegerii acestui subiect, actual și în special de perspectivă, chiar în viitorul imediat.

Capitolul 2 abordează aspecte generale despre securitatea informațiilor: este realizată încadrarea acestui concept în cadrul unui termen mai complex (siguranța în funcționare a sistemelor) și sunt prezentate standarde și reglementări în acest domeniu (inclusiv corelate cu IoT și protecția datelor personale). Un subcapitol special este dedicat analizei și managementului riscului de securitate. În finalul capitolului sunt prezentate metodologii și strategii de elaborare a politicilor de securitate la nivel de organizații. Se regăsesc de asemenea o analiză comparativă a centrelor de securitate cibernetică de tip SOC și SIC și un profil al analistului în securitate cibernetică.

Capitolul 3 prezintă amenințările la adresa securității cibernetice a sistemelor. Am expus separat aspecte ce țin de tipurile de atacuri informatice, profilurile și motivațiile

atacatorilor cibernetici și vulnerabilitățile actuale ale aplicațiilor. Într-un alt subcapitol am analizat detaliat două tipuri de amenințări actuale (APT și ransomware), cu perspective de creștere în complexitate și ca impact în viitorul apropiat, și am efectuat două tipuri de analize (detecție statică și dinamică) pentru aplicațiile malware. Tot în acest capitol am implementat un sistem de analiză a atacurilor și a atacatorilor cibernetici, care a constat în mai multe honeypot-uri (platforme e-learning de tip Moodle) distribuite la nivel mondial într-un honeynet în vederea obținerii de inteligență cibernetică.

Capitolul 4 debutează cu 3 categorii de modele teoretice folosite pentru analiza și implementarea securității sistemelor informatice. Pe baza modelului apărării în adâncime am propus soluții pentru securizarea celor 7 niveluri considerate la nivel de organizație. Pentru securizarea la nivelul rețelei locale am elaborat o aplicație de detecție a intruziunilor bazată pe o analiză preliminară a resurselor hardware și software disponibile. Ca suport hardware a fost folosită inițial o arhitectură Raspberry Pi, iar ca suport software, în urma unui studiu critic privind siguranța în funcționare a platformelor de tip cloud computing, am ales serviciile DigitalOcean Public Cloud.

Capitolul 5 prezintă concluziile cercetărilor și rezultatele obținute în urma stagiului doctoral. Sunt indicate lucrările științifice elaborate și activitatea de cercetare desfășurată, inclusiv în cadrul proiectului POSDRU/159/1.5/S/132397, în a cărui echipă de cercetare am participat. În final sunt analizate câteva direcții de dezvoltare a unor contribuții și de readaptare a întregii societăți la noul context global generat de pandemia de coronavirus.

Capitolul 2. Securitatea informațiilor

În capitolul al doilea al lucrării am prezentat aspecte corelate conceptului de securitate informatică, concept care vizează protejarea informației și a sistemelor de calcul în fața accesului ilegal și a încălcării unor principii referitoare la confidențialitatea, integritatea sau disponibilitatea acestora.

Capitolul a debutat cu introducerea teoretică a unor concepte de bază în siguranța în funcționare a sistemelor informatice. O componentă fundamentală a acestui concept este reprezentată de fiabilitatea unui sistem, adică probabilitatea bunei sale funcționări în timp. Pentru analiza fiabilității au fost enumerate succint cele mai utilizate metode, dintre care am putea menționa RBD (Reliability Block Diagram) din categoria metodelor bazate pe starea de funcționare a sistemului, respectiv FTA (Fault Tree Analysis) din categoria metodelor bazate pe defectare.

ISO/IEC 27001:2013 abordează securitatea informațiilor prin următoarele trei componente ale siguranței în funcționare: confidențialitatea, integritatea și disponibilitatea, aspecte prezentate detaliat în subcap. 2.1.2. Confidențialitatea este definită de ISO 27001:2013 drept „proprietatea că informațiile nu sunt puse la dispoziție sau dezvăluite persoanelor, entităților sau proceselor neautorizate” [24], integritatea se referă la protejarea exactității și informațiilor active, iar disponibilitatea unui sistem reprezintă probabilitatea ca acel sistem să fie operațional (în stare de funcționare) la momentul curent.

În subcap. 2.2 am sintetizat standarde relevante și reglementări în domeniul securității informatice. Pentru standardul ISO/IEC 27001:2013 „*Tehnologia Informației - Tehnici de securitate - Sisteme de management al securității informației - Cerințe*" am prezentat structura și modificările comparativ cu o versiune anterioară, 27001:2005. Cadrul NIST pentru securitate cibernetică, prezentat în continuare, este o colecție de ghiduri în domeniul securității sistemelor de calcul, folosite la nivel de organizație pentru evaluarea și îmbunătățirea capacității de prevenire, detecție și răspuns la atacurile cibernetice.

Referitor la problematica protecției datelor personale au fost amintite două regulamente relevante: GDPR (*Regulamentul general privind protecția datelor (UE) 2016/679*) valabil în Uniunea Europeană și Spațiul Economic European, respectiv legea privind confidențialitatea consumatorilor din California (CCPA - California Consumer Privacy Act). Din studiul comparativ al celor două acte legislative reies mai multe similitudini, dar putem sublinia în special diferențele la nivelul sferei de aplicabilitate și, evident, al spațiului geografic căruia i se aplică respectivele prevederi. Este important de menționat că există o îmbunătățire a înțelegerii importanței valorii datelor. Pe lângă abordări la nivel global, precum adoptarea celor două decizii legislative, care au ca scop protecția datelor confidențiale la nivel de individ (consumator), un rol important îl are faptul că utilizatorii cunosc și conștientizează faptul că pot exista informații importante în orice sistem, care pot duce la compromiterea întregii infrastructuri.

Ultima parte a acestui subcapitol prezintă reglementări avute în vedere pentru standardizarea domeniului IoT. Această standardizare este necesară pentru dezvoltarea coerentă, compatibilă și în siguranță a aplicațiilor specifice domeniului IoT. Printre organizațiile care abordează astfel de standardizări sunt prezentate ISO și IEC cu standardul *ISO/IEC CD 27030 - Tehnologia informației - Tehnici de securitate - Linii directoare pentru securitate și confidențialitate în Internetul obiectelor (IoT)*, aflat în fază de dezvoltare la momentul realizării acestei lucrări.

Subcap. 2.3 a avut drept temă principală analiza și managementul riscului de securitate. Scopul unei astfel de evaluări este de a crește nivelul de securitate în proiectarea și implementarea unui proiect. O inițiativă critică pentru apărarea rețelelor este conceptul „zero-trust". Încrederea zero se referă la un set de paradigme de securitate a rețelei care restrânge apărările de la perimetrele largi ale rețelei la persoane sau grupuri mici de resurse. Accentul său pe protejarea resurselor mai degrabă decât pe segmentele de rețea este un răspuns la tendințele care includ utilizatorii la distanță și activele bazate pe cloud, care nu sunt situate în limita unei rețele deținute de companie. În cadrul subcapitolului, o atenție deosebită a fost acordată problematicii managementului timpului prin metoda matricei de decizie Eisenhower. O contribuție personală a constat în conceperea unei matrice personalizate pentru îmbunătățirea activității unei companii, în care sarcinile au fost organizate pe baza a 2 criterii: urgența și importanța (metoda Eisenhower) [39].

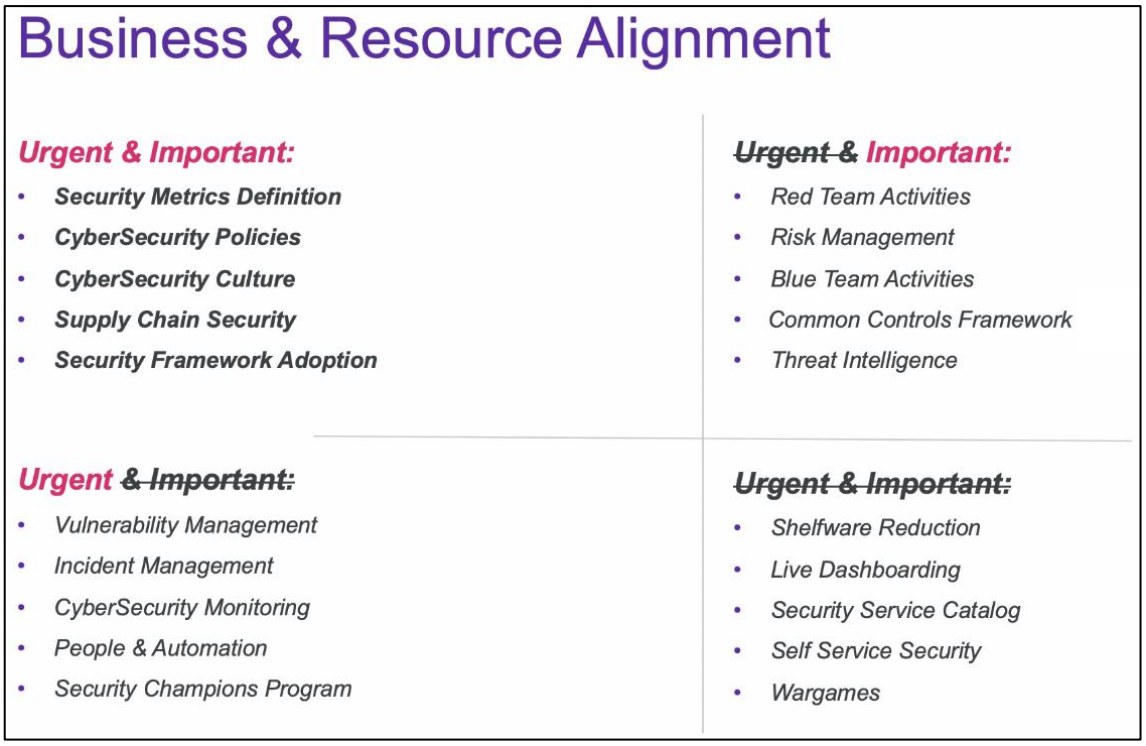

Fig. 2.7 Propunerea unei matrice Eisenhower pentru îmbunătățirea activității unei companii

O altă contribuție personală se regăsește în subcap. 2.4.2, unde am realizat un chestionar al cărui scop a fost determinarea gradului de conștientizare a securității informaționale în cadrul organizațiilor. Chestionarul (prezentat integral în Anexa A.1) este format din 20 de întrebări cu două sau mai multe răspunsuri posibile, iar fiecărui răspuns i s-a alocat un coeficient de risc între 1 (risc de securitate minim) și 10 (risc de securitate maxim). Rezultatele obținute în urma completării acestui chestionar (calculul nivelului de risc în ceea ce privește componenta umană a unei organizații) pot fi folosite în cadrul programelor de informare, avertizare și instruire a angajaților sau în politicile de securitate elaborate la nivel de organizație.

În subcap. 2.4.3 am realizat o analiză comparativă SOC vs. SIC și am subliniat avantajele tranziției de la clasicele centre de operațiuni de securitate (SOC - Security Operations Centers) la un model avansat (SIC - Security Intelligence Center) care folosește inteligența pentru a înțelege și anticipa amenințările care vizează o organizație [48]. O comparație între cele două modele poate avea la bază modul de abordare a securității cibernetice, reactivă vs. proactivă. SIC se concentrează pe capacitatea de a anticipa amenințările înainte ca acestea să devină incidente și, de asemenea, pe dezavantajele SOC clasice, inclusiv postura și monitorizarea reactivă a securității. Impactul unei astfel de tranziții asupra proceselor, dar și asupra utilizatorilor și organizațiilor, este unul benefic. Merită menționat aspectul automatizării migrației care permite resurselor umane să se separe de activitățile de rutină, permițându-le să se concentreze asupra informațiilor adunate. Deoarece instrumentele diverșilor furnizori, orientate către întreprinderi, sunt destinate să funcționeze pentru toată lumea, dar nu sunt optimizate în particular pentru nimeni, a fost subliniată importanța implementării unor

instrumente personalizate, susținute de echipe de inginerie care dețin cunoștințe avansate în domeniu.

În domeniul tehnologiei informaționale de astăzi automatizarea este aspectul care conduce înainte orice afacere. Fără nicio îndoială, un centru de informații de securitate ar trebui să își bazeze operațiunile pe automatizare. Aplicarea automatizării în activitățile zilnice permite analiștilor să vadă, să identifice, să urmărească și, mai important, să răspundă la amenințări înainte ca acestea să afecteze sistemele. În această analiză globală privind automatizarea este esențială abordarea honeypot-urilor ca unul dintre cele mai de succes instrumente utilizate pentru colectarea informațiilor despre amenințări.

Avantajul unei soluții de apărare bazate pe inteligență este deosebit de important în mediile dinamice în care fluxul de informații este rapid și anomaliile trebuie identificate rapid. În peisajul amenințărilor cibernetice ale zilelor noastre trebuie să existe o înțelegere profundă a evenimentelor trecute și actuale pentru a încerca chiar apărarea în fața atacurilor viitoare. Prin urmare, un analist SIC trebuie să se concentreze pe comparațiile SOC vs. SIC și să-și dezvolte capacitatea de a obține o viziune completă [49]. Având în vedere că toate rolurile „CxO" (CIO, CISO etc.) vizează o postură de securitate evoluată, managerii echipelor de monitorizare trebuie să se pregătească pentru tranziția abordării echipelor lor într-una de detecție activă a amenințărilor. Deși nu există o rețetă standard predefinită de migrare de la un centru de operații de securitate la un centru de securitate inteligent, este recomandată o trecere cât mai curând posibil având în vedere amenințările avansate persistente ca o certitudine a prezentului și în special a viitorului.

În subcap 2.4.4 am realizat un profil al analistului în securitate cibernetică [51], un job provocator care, deși la început poate părea greu și solicitant, este susținut, pe lângă permanentul schimb de cunoștințe dintre angajații acestei categorii profesionale, de instrumente de monitorizare a sistemelor de securitate mapate la toate nivelurile de apărare în cadrul strategiei Defense in Depth. Acest analist trebuie să fie permanent la curent cu știri, concepte, amenințări și tendințe în materie de securitate și beneficiază de susținerea altor specialiști din domenii conexe de securitate, cum ar fi evaluarea vulnerabilităților, criminalistică, prevenirea pierderilor de date, testarea penetrărilor, securitatea rețelei etc.

Capitolul 3. Amenințări la adresa securității cibernetice

Capitolul 3 a abordat tema amenințărilor la adresa securității cibernetice, iar componentele analizate au fost: atacurile informatice, atacatorii cibernetici, vulnerabilitățile informatice ale momentului și estimările referitoare la amenințările prezente și cu perspectivă de evoluție imediată.

În debutul capitolului am clasificat atacurile informatice după o serie de criterii și am detaliat principalele categorii de aplicații rău intenționate, printre care: malware, phishing, SQL injection, XSS (Cross-Site Scripting), DoS (Denial of Service). În

continuare am analizat cele mai importante 15 breșe de securitate cibernetică din istoria recentă și impactul lor asupra organizațiilor.

Contribuția realizată în subcap. 3.1.3 abordează riscurile de securitate datorate atacurilor de tip ARP spoofing [69]. S-a folosit un hardware cu costuri reduse, asociat cu capabilitățile software existente pentru analiza pachetelor și detectarea intruziunilor. Soluția propusă, formată din dispozitivul de monitorizare împreună cu aplicația creată și scripturile Python, a fost realizată ca un concept care poate fi utilizat de către analiștii de securitate în testare, scopul final fiind ca producătorii de echipamente de rețea să adopte soluții similare pentru a oferi capacități de detectare a atacurilor rău intenționate pentru dispozitivele care fac parte din segmentul de piață SOHO (Small Office Home Office).

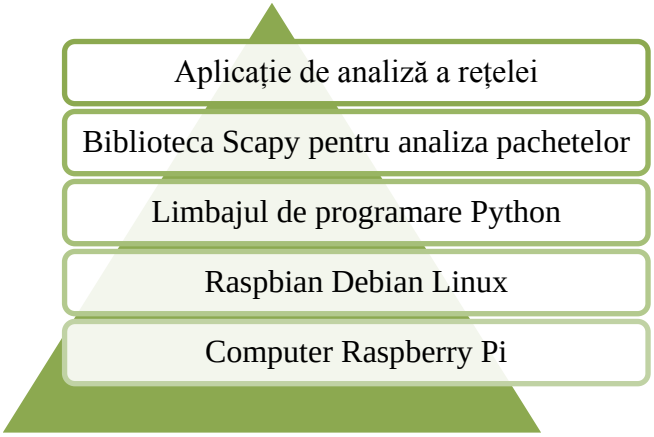

Fig. 3.5 Stiva software și hardware a soluției de monitorizare [69]

Atacatorii cibernetici au fost analizați în subcap. 3.2. Am realizat o clasificare a acestora și am descris profilul caracteristic, principalele atribute și specificul țintelor vizate de către aceștia. În continuare, pentru o mai bună înțelegere a comportamentului și instrumentelor folosite de atacatori și a studia complexitatea tehnicilor, tacticilor și procedurilor utilizate în atacuri, am conceput și implementat o rețea honeynet. După ce am analizat mai multe industrii și am evaluat riscurile în fiecare dintre ele, ne-am îndreptat atenția spre mediul de învățare electronică. Universitățile reprezintă locul de naștere al cercetării și dezvoltării, însă ele constituie, de asemenea, ținte de valoare ridicată pentru actorii cu intenții malițioase.

În subcap. 3.3 am efectuat o cercetare [78] privind colectarea informațiilor despre actorii care lansează atacuri împotriva platformelor de e-learning, în scopul de a completa profilurile acestor atacatori. Un honeypot reprezintă un sistem (computer sau rețea) care are scopul de a detecta și devia atacatorii prin atragerea lor în rețea. Importanța desfășurării punctelor honeypot ca modalitate de înțelegere a atacatorilor platformelor de e-learning a fost studiată prin implementarea unor honeypot-uri într-un mediu public de tip cloud. Astfel, am dezvoltat o infrastructură bazată pe 3 regiuni geografice: America de Nord, Europa și Asia, alcătuită din puncte honeypot de cercetare cu interacțiune redusă și cu interacțiune ridicată pentru a înțelege tactica atacatorilor. După analiza datelor culese, concluziile sunt că acest tip de cercetare este extrem de relevant pentru a înțelege starea actuală și viitoare a securității cibernetice în mediul de învățare electronică.

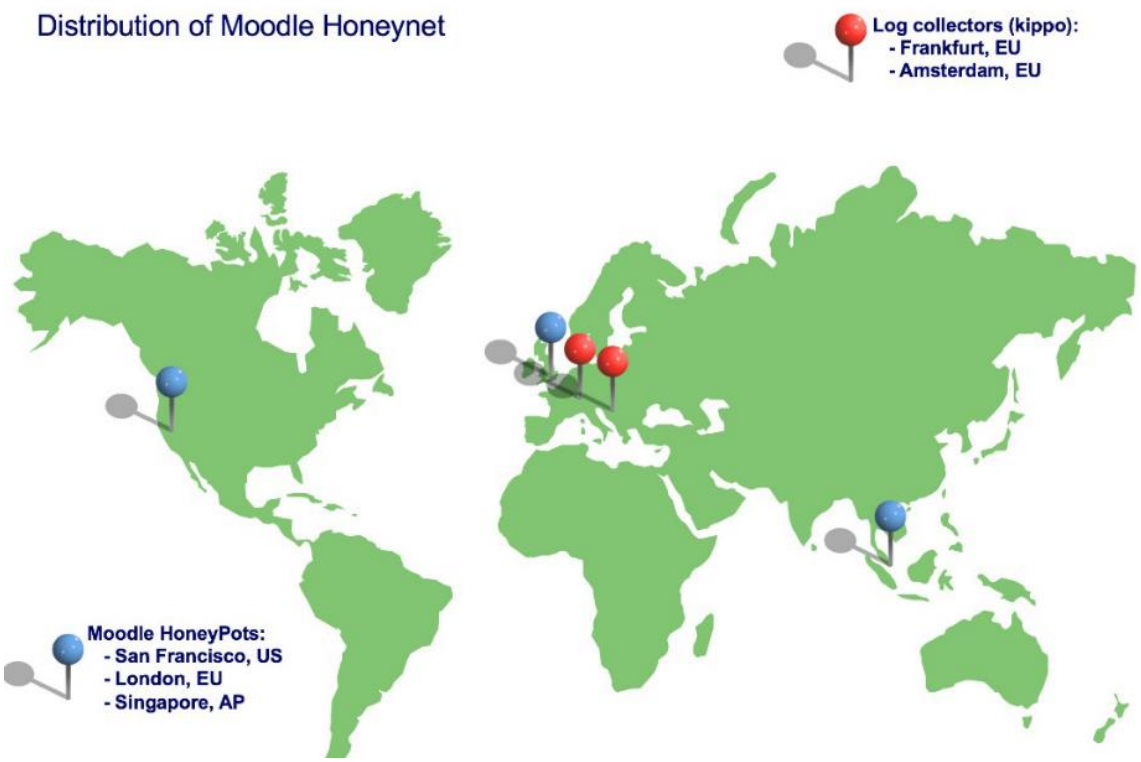

Fig. 3.8 Harta honeypot [78]

Top 10 Usernames

Username	Count
	122
root	97
admin	58
user	12
pi	9
test	8
guest	7
ubuntu	6
apache	5
alex	5

Top 10 Passwords

Password	Count
root	138
123456	40
password	20
admin	20
123	15
default	14
1234	12
admin123	7
Passw0rd@123	7
1	6

Top Username/Password Combinations

Username/Password Combination	Count
/root	122
root/root	16
root/admin	9
admin/admin	8
root/default	7
root/Passw0rd@123	7
admin/admin123	7
admin/password	6
admin/default	6
pi/raspberry	5

Fig. 3.10 Informații privind username și parole utilizate de atacatori [78]

Latest Successful Logins

Source IP	Country	Login Time
117.247.189.120	India	07/04/18 13:46:05
195.3.147.49	Latvia	07/04/18 13:16:56
93.170.114.251	Ukraine	07/04/18 13:03:09
82.208.139.2	Romania	07/04/18 13:03:08
91.135.212.13	Russia	07/04/18 12:32:35
194.85.135.14	Russia	07/04/18 12:20:37
93.170.108.240	Russia	07/04/18 12:09:52
14.245.117.94	Vietnam	07/04/18 11:55:01
195.3.147.49	Latvia	07/04/18 11:54:11
182.100.67.237	China	07/04/18 11:40:40

Fig. 3.11 Bază de date pentru monitorizarea autentificărilor [78]

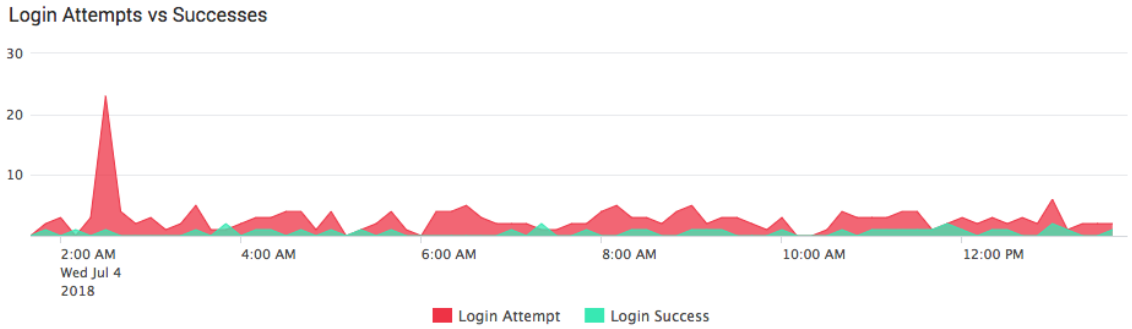

Fig. 3.12 Informații privind conexiunile reușite / nereușite ale atacatorilor [78]

Vulnerabilitățile sistemelor informatice, discutate în subcap. 3.4, reprezintă un domeniu foarte vast despre care se poate vorbi foarte mult și ce este și mai interesant este că mereu va fi ceva nou care va pune la încercare atacatorii, dar și personalul de securitate. Studiile ce privesc viitorul în domeniul vulnerabilităților sistemelor informatice se referă la dispozitivele mobile care sunt în creștere ca utilizare. Chiar dacă dispozitivele mobile sunt percepute ca fiind amenințarea numărul unu pentru perioada curentă, dispozitivele în sine nu reprezintă un risc, ci datele importante pe care acestea le pot stoca sau modul lor de utilizare ca rampă de lansare a noi atacuri.

După o clasificare a vulnerabilităților și prezentarea celor 6 pași în managementul acestora, am studiat detaliat și adus 2 contribuții pentru vulnerabilitățile de tip Buffer Overflow și Heartbleed. Pentru primul caz am prezentat un atac de tip Buffer Overflow asupra unei aplicații vulnerabile - FreeFloat FTP Server. „Atacatorul a folosit concepte de bază din programare și rețelistică pentru a obține accesul la mașina țintă. Din punctul de vedere al securității ofensive am analizat atacul asupra unui server FTP, care a dus la obținerea de drepturi asupra sistemului țintă utilizând instrumente software gratuite, la care oricine poate avea acces. Este evident că atacurile asupra sistemelor informatice pot fi foarte complexe, dar, după cum am arătat, un astfel de atac poate fi pus în practică fără un efort foarte mare, ceea ce demonstrează că un atacator nu trebuie să fie neapărat foarte instruit, iar susținerea materială de care are nevoie este minimă” [84].

Subcap. 3.4.2 a abordat subiectul vulnerabilității informatice Heartbleed, un bug care a lăsat numeroase chei private și alte informații sensibile disponibile pe Internet. Având în vedere expunerea îndelungată, ușurința de exploatare și atacurile care nu lasă vreo urmă, această vulnerabilitate trebuie considerată una extrem de periculoasă. Ca studiu de caz am simulat un atac Heartbleed asupra unei mașini (o imagine Linux pentru arhitectura ARM instalată pe un dispozitiv tip Raspberry Pi). Atacul a fost lansat dintr-o mașină virtuală ce rulează Kali Linux folosind scannerul de rețea NMAP și alte scripturi scrise în limbajul de programare Python. Datorită cererilor criptate, diferențierea între utilizarea legitimă și atac nu se poate baza pe conținutul acestora, ci comparând dimensiunea cererii cu dimensiunea răspunsului. Acest lucru implică faptul că un IDS / IPS poate fi programat pentru a detecta atacul, dar pentru a-l bloca este necesară blocarea completă a verificării. Patch-ul vulnerabilității Heartbleed este doar un prim pas în securizarea sistemelor și aplicațiilor. În practică, după aplicarea patch-urilor, este necesară generarea unei noi perechi de chei publice / private.

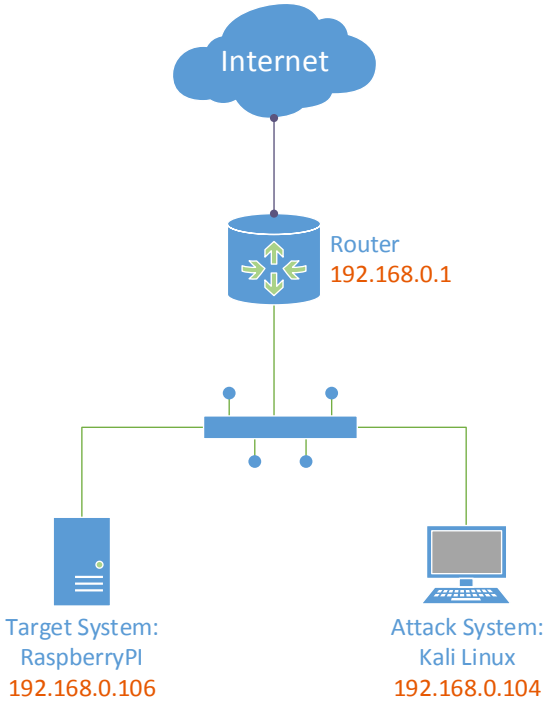

Fig. 3.21 Configurație propusă pentru implementarea unui atac Heartbleed [95]

În finalul capitolului am făcut o serie de aprecieri referitoare la două tipuri de amenințări actuale, cu certe perspective de creștere în complexitate și care se anunță a avea noi efecte devastatoare: amenințările persistente avansate (APT) și malware-ul de tip ransomware [102] [111]. APT, cu un nivel complex de acțiune și tehnici sofisticate, atacă în special mari organizații sau instituții ale statului, fiind necesară o apărare cibernetică bazată pe inteligență, pe colectarea informațiilor despre amenințări combinată cu interpretarea corectă a indicatorilor IoC privind compromiterea sistemelor. Pericolul unor atacuri lansate de aplicațiile ransomware este în momentul de față pe un trend ascendent, fiind folosiți algoritmi de criptare evoluați și chei de lungimi tot mai mari.

Contribuțiile originale din finalul capitolului 3 au constat în propunerea a două soluții utile în prevenirea atacurilor lansate de aplicațiile ransomware. Prima soluție constă în detecția statică a acestor aplicații, folosește un script Python și se bazează pe o infrastructură hardware cu costuri reduse care rulează tehnologii open-source standardizate, având ca principale avantaje o executare rapidă și un spectru larg de potențiali utilizatori.

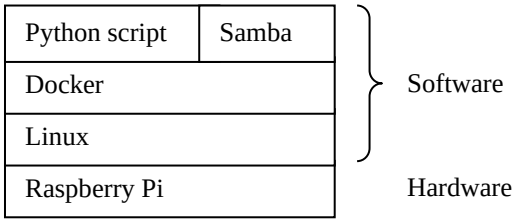

Fig. 3.27 Stiva tehnologică propusă pentru detecția ransomware-ului [112]

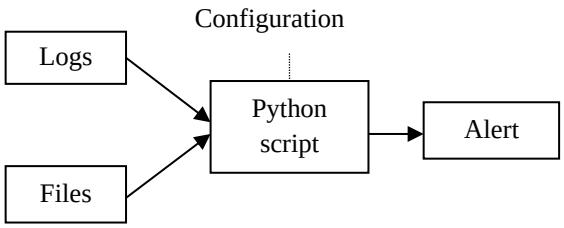

Fig. 3.28 Principiul de funcționare a scriptului Python [112]

Ulterior am dezvoltat arhitectura unei soluții dinamice de detecție și analiză a aplicațiilor ransomware bazată pe analiza comportamentală a malware-ului.

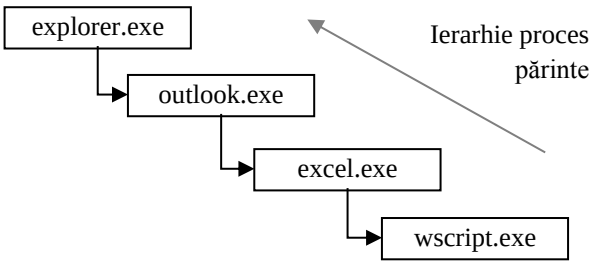

Fig. 3.33 Ierarhia proceselor [103]

Unul din modurile de utilizare a sistemului inteligent prezentat în subcap. 3.5.4 ar fi drept componentă de bază a unei soluții antivirus, ea putând fi integrată pentru a monitoriza procesele nou create și a furniza date celorlalte componente principale ale antivirusului. Un alt mod de utilizare a aplicației ar fi în timpul procesului de analiză malware. Dacă Sysmon este instalat pe un sistem informatic sau există o imagine a memoriei volatile a computerului, acestea pot fi utilizate ca intrări în aplicație și analizate pe baza pattern-urilor bine / rău intenționate. În ceea ce privește rețelele de calcul mari, sistemul inteligent poate fi rulat simultan pe mai multe calculatoare, în acest scenariu fiind necesară o consolă de administrare globală astfel încât rezultatele să poată fi centralizate și analizate. Rezultatul ar trebui să ofere o perspectivă deosebită asupra comportamentului sigur, suspect sau rău intenționat al întregului grup de calculatoare prin monitorizarea tendințelor în executarea proceselor.

Capitolul 4. Strategii de asigurare a securității cibernetice

Capitolul 4 al tezei de doctorat, intitulat „*Strategii de asigurare a securității cibernetice*”, analizează modele teoretice și aduce contribuții practice în sfera tehnicilor care îmbunătățesc securitatea sistemelor complexe abordată din mai multe puncte de vedere, atât fizic, cât și logic.

Prima parte a capitolului este dedicată modelelor teoretice de implementare și analiză a securității sistemelor informatice. Analiza modelelor multi-nivel a presupus descompunerea conceptului de securitate în nivelurile fizic și logic și descrierea individuală a acestora. Cele două niveluri sunt elemente cheie și o securitate eficientă implică asigurarea ambelor niveluri: securitatea fizică, a accesului neautorizat la echipamente, și securitatea logică, la nivelul accesului la sistem și securitatea serviciilor.

Scopul unui audit de securitate IT al sistemelor informatice este de a identifica integral vulnerabilitățile unui astfel de sistem, de a-i evalua necesitățile, a cunoaște riscul la care este supus și de a furniza o soluție pentru eliminarea vulnerabilităților. Una dintre politicile practice de diminuare a riscurilor este limitarea sau eliminarea drepturilor inutile ale utilizatorilor, păstrându-se privilegiile minime pentru un cont de acces (*least-privileged user account*).

În continuare este prezentat modelul Cyber Kill Chain, un model de securitate tradițional care descrie un scenariu clasic - un atacator din exterior care urmează câțiva pași bine definiți pentru a pătrunde într-o rețea și a fura datele sale - descompunând pașii atacului pentru a ajuta organizațiile să se pregătească. Cyber Kill Chain reușește într-un mod remarcabil să descrie vectorii de amenințare și atacurile cu care se confruntă cu organizațiile actuale.

Dezvoltat de echipa de răspuns la incidente de securitate informatică (CSIRT - Computer Security Incident Response Team) de la Lockheed Martin, scopul modelului este de a înțelege mai bine etapele prin care un atacator dezvoltă un atac și de a ajuta echipele de securitate să oprească un astfel de atac în oricare din etapele identificate. Subcapitolul 4.2 descrie cele 3 etape principale ale modelului (pre-compromitere, compromitere și post-compromitere) și detaliază etapele (fazele) componente ale fiecăreia. Atacatorul efectuează recunoașterea, intruziunea în perimetrul de securitate, exploatarea vulnerabilităților, obținerea și escaladarea privilegiilor, mișcarea laterală pentru a obține acces la ținte mai valoroase, încearcă să-și ofere activitatea și, în final, să extragă date de la organizație.

Aplicarea principiului securității stratificate (Defense in Depth) prezentat în subcap. 4.3 are drept scop principal obținerea unei protecții a datelor pe mai multe niveluri, atât a datelor în stare de repaus, cât și a celor în tranzit [128]. Scopul acestei tehnici nu este neapărat să prevină încălcările de securitate, ci mai degrabă să întârzie acțiunile unui atacator, astfel încât victima (de obicei o organizație) să câștige timp pentru a identifica și a răspunde la un atac cibernetic. O rețea de calculatoare nu poate fi protejată printr-o singură măsură de securitate. Atacurile cibernetice au avut o evoluție impresionantă în ultimele două decenii. Ingineria socială, amenințările din interiorul organizațiilor și tehnologia cloud au schimbat modul în care definim perimetrul de securitate și, conform unor opinii, au făcut ca definirea acestuia să nu mai fie relevantă. Un firewall protejează rețeaua împotriva atacurilor din exterior, dar nu este eficient atunci când atacurile vin din interior. De asemenea, punerea în aplicare a politicilor și procedurilor de control al securității conexiunilor interne vor fi ignorate de un atac din afara rețelei.

În acest context, unul dintre conceptele cheie în asigurarea securității informației este principiul apărării în adâncime, adică instituirea unui sistem de apărare multistrat folosind metode independente (asigurarea unei securități pe mai multe niveluri) care să poată:

- preveni exploatarea;
- detecta și intercepta atacul;
- afla agenții de amenințare și urmările unui atac.

O abordare de succes presupune introducerea mai multor bariere de securitate pentru a se asigura apărarea împotriva diferitelor tipuri de amenințări. Astfel, în acest subcapitol am ilustrat o imagine de ansamblu a tehnicii de apărare în adâncime aplicată conform analizei de risc efectuate în capitolul 2 pentru a asigura securitatea datelor. Am detaliat exemple de „straturi" de protecție și am prezentat, organizate pe categorii, măsurile care trebuie luate la nivelul unei companii pentru o apărare în adâncime eficientă și solidă. Elementele de bază pentru aplicarea apărării în adâncime într-o organizație sunt personalul (angajații), tehnologia (la nivel hardware și software) și nivelul de operare (activități periodice de monitorizare / actualizare, dar și recuperarea după incidente).

Asigurarea securității sistemelor informaționale constă nu doar în achiziționarea de hardware puternic sau software modern. La nivel organizațional este nevoie de o politică puternică și coerentă pentru controlul accesului la date și implementarea strategiilor care asigură securitatea datelor, indiferent de tehnologia utilizată. La nivelul conștiinței individuale a angajatului trebuie să fie formate reflexe care să minimizeze încălcările de securitate și să asigure securitatea și confidențialitatea datelor: accesarea cu atenție a link-urilor, ignorarea programelor sau a aplicațiilor provenite din surse incerte, parole complexe și diferite. O contribuție personală în acest capitol a fost dezvoltarea unui program de extragere a parolelor nesigure folosind funcția crypt() și un atac brute-force de tip dicționar.

În subcap. 4.5 am realizat un sistem pentru detecția intrușilor într-o rețea locală. Am prezentat pentru început mediul hardware și software în care această aplicație a fost implementată. Suportul hardware a constat într-un model Raspberry Pi de generație recentă, ales datorită costurilor reduse și performanțelor ridicate, potrivite pentru specificul aplicației și puterea de calcul cerută. Limbajul de programare Python a fost ales datorită avantajelor sale (open-source, versatil, ușor de utilizat și cu numeroase biblioteci incluse).

În subcap. 4.5.2 am analizat comparativ soluțiile oferite de mediul cloud computing și am prezentat aspecte specifice celor 3 lideri de pe piața serviciilor online în cloud: Amazon Web Services, Microsoft Azure și Google Cloud. Fiecare furnizor vine cu avantaje, dar și dezavantaje, astfel încât soluția optimă trebuie aleasă în funcție de specificul fiecărei organizații, nevoile de servicii și prețul corelat cu necesarul de resurse hardware și software oferite. Trebuie luate în calcul mai multe considerente atunci când se stabilește modelul de implementare în cloud potrivit unei anumite organizații. Criteriile abordate pot fi nevoile de conformitate cu reglementările organizației, resursele financiare, modelul preferat de cheltuieli, locațiile geografice ale utilizatorilor sau predictibilitatea cererii. Nu toate modelele de cloud pot aborda în mod egal aceste cerințe,

criteriile analizate reprezentând un ghid inițial pentru a stabili dacă un cloud privat, public, hibrid sau comunitar este cel mai potrivit pentru organizația în discuție.

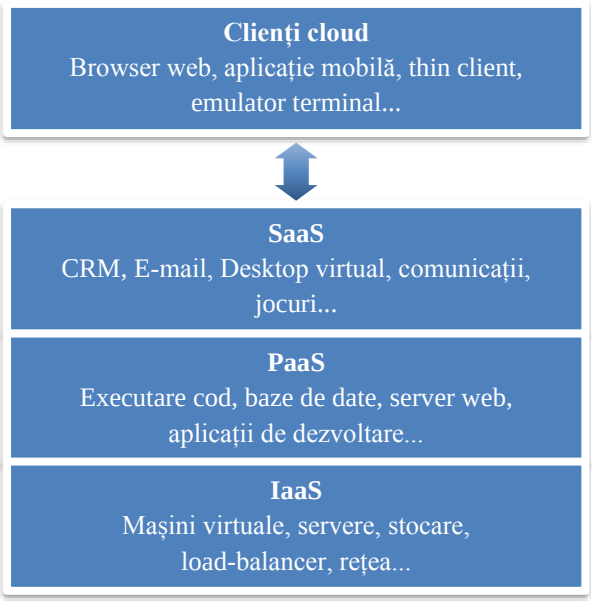

Fig. 4.7 Modele de servicii cloud computing [149]

Soluțiile pentru detecția intruziunilor, disponibile pe piață în momentul de față, au scopul de a proteja rețelele de mari dimensiuni și au un preț ridicat. Soluția open-source pentru rețelele locale de mici dimensiuni, concepută în subcap. 4.5.3, are capabilitățile de a detecta o intruziune în rețeaua locală prin analizarea IP-urilor din mediu [159]. Configurat pentru a funcționa manual sau automat, acest software construiește o listă de referință de bază și își compară constant elementele cu IP-urile existente în rețea. Când apare o anomalie, acesta avertizează administratorul și oferă, de asemenea, posibilitatea de a determina porturile deschise și vulnerabilitățile echipamentului respectiv. Soluția propusă se bazează pe tehnologii gratuite și open-source. Scopul proiectării unei soluții cu cerințe de resurse de calcul foarte scăzute este faptul că nivelul software poate fi portat pe echipamente de rețea pentru consumatori, cum ar fi routere proiectate pentru uz casnic și birouri mici, oferind capabilități de detecție ransomware care să completeze soluția antivirus.

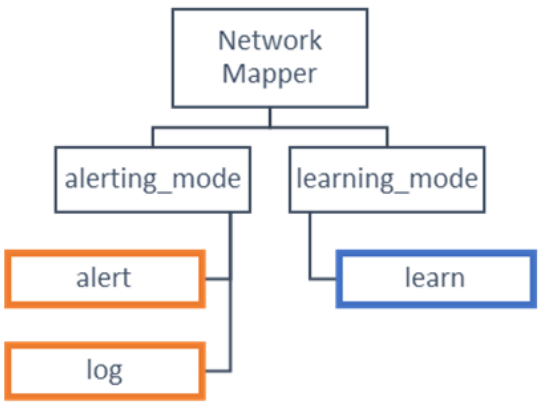

Fig. 4.8 Network Mapper - moduri de lucru [159]

Capitolul 5. Concluzii finale

Ultimul capitol al tezei conține sinteza aspectelor prezentate în lucrare și lista contribuțiilor originale, respectiv a lucrărilor publicate pe parcursul stagiului doctoral. Am indicat activitățile pe care le-am desfășurat pe parcursul programului de doctorat și am identificat câteva direcții ulterioare în care contribuțiile aduse ar putea fi dezvoltate. În finalul capitolului am făcut o analiză a contextului complex generat de pandemia de coronavirus în care ne aflăm la acest moment și am estimat atât vectorii de atac specifici perioadei imediat următoare, cât și prioritățile cărora organizațiile vor trebui să le acorde atenție maximă în vederea reluării și adaptării activităților la o „nouă normalitate".

5.1. Principalele aspecte expuse în cadrul tezei

Rezultatele originale obținute în cadrul acestui stagiu doctoral pot fi considerate atât din punct de vedere ingineresc, printr-o serie de contribuții tehnice în domeniul științific al temei studiate, cât și dintr-o perspectivă managerială, prin propunerea și implementarea unui program de securitate cibernetică pentru optimizarea activității unei organizații multinaționale de mari dimensiuni.

Obiectivul principal al tezei de doctorat a fost reprezentat de dezvoltarea unei serii de produse compatibile și eligibile pentru securitatea cibernetică a viitorului prin studiul atacurilor informatice și al evoluției acestora pentru a înțelege impactul unei abordări proactive comparativ cu o abordare reactivă. Obiectivele secundare au constat în elaborarea unor analize teoretice, comparative, și conceperea unor configurații hardware și aplicații software destinate minimizării impactului atacurilor cibernetice și optimizării costurilor în cadrul unor organizații.

Capitolul 2 al lucrării abordează problematica securității informației prezentată la nivelul teoretic al conceptelor implicate, standardelor și reglementărilor legale privind securitatea informatică, managementul riscului de securitate și al politicilor de securitate în cadrul organizațiilor. În debutul capitolului am descris noțiunile generale de sistem și dependabilitate (siguranță în funcționare) a unui sistem, aceasta din urmă reprezentând caracteristica unui sistem prin care acesta furnizează cu încredere serviciul pentru care a fost conceput, evitând defectările mai frecvente sau mai severe decât un nivel considerat acceptabil. Am detaliat componentele de bază ale siguranței în funcționare, punând accent pe trei dintre ele și anume confidențialitatea, integritatea și disponibilitatea, esențiale în asigurarea securității informațiilor.

În continuare, în subcap. 2.2 am analizat câteva standarde relevante și reglementări în domeniul securității informatice:

- ISO/IEC 27001:2013, standard care specifică „cerințele pentru stabilirea, implementarea, menținerea și îmbunătățirea continuă a unui sistem de management al securității informațiilor și cerințele pentru evaluarea și tratarea riscurilor de securitate a informațiilor adaptate nevoilor tuturor organizațiilor, indiferent de tip, dimensiune sau natură" [24];

- NIST Cybersecurity Framework, cadrul care „integrează standardele industriei și cele mai bune practici pentru a ajuta organizațiile să dezvolte o înțelegere comună și să își gestioneze riscurile de securitate cibernetică” [29];
- două regulamente destinate protecției datelor personale ale utilizatorilor: GDPR, pentru Uniunea Europeană și Spațiul Economic European, respectiv CCPA pentru statul California (Statele Unite ale Americii), studiate comparativ și care au subliniat măsurile luate pentru protecția datelor confidențiale ale individului (consumatorului), drepturile și obligațiile sale, dar și ale companiilor, în relațiile de interacțiune mutuală;
- activitățile de standardizare în domeniul IoT inițiate de mai multe organizații internaționale și aflate în diverse stadii de lucru, în vederea asigurării unui limbaj comun de abordare a provocărilor din domeniul securității cibernetice ce vizează dispozitivele IoT.

Din punctul de vedere al abordării managementului riscului din mai multe perspective, considerate pe toată durata stagiului doctoral, am studiat evoluția atacurilor cibernetice, am elaborat și am aplicat un cadru de definire și analiză a riscului de securitate cibernetică la nivel organizațional. Astfel, am definit și am implementat un departament și un program de management de securitate cibernetică în cadrul unor companii și, în special, în cadrul unei fuziuni a două companii globale prin aplicarea metodei defensivei stratificate (*Defense in Depth*). Am studiat în mod deosebit implicațiile și vulnerabilitățile pe care o astfel de fuziune - între o companie certificată PCI DSS (Payment Card Industry Data Security Standard) și SOX (Sarbanes-Oxley Act) și o companie care doar adera la câteva practici de implementare a securității cibernetice - le are pentru organizația rezultată. Am identificat astfel o serie de puncte de risc și, în urma evaluărilor tehnice, am dezvoltat o metodologie și am creat o matrice de analiză bazată pe metoda Eisenhower de concentrare a eforturilor, prezentată în subcap. 2.3.1. Am concluzionat că o abordare proactivă bazată pe scenarii și anticiparea evenimentelor a avut o rată de succes mai mare în reducerea suprafeței de atac și a costurilor generate de incidentele cibernetice.

Din punct de vedere tehnic am urmărit proiectarea, dezvoltarea și implementarea unor soluții pentru a parcurge procesul de convertire a datelor în înțelepciune. O metodă de a extrage datele necesare a fost realizarea unui chestionar privind gradul de conștientizare a securității cibernetice în cadrul unor organizații, pentru a obține informații și cunoștințe în ceea ce privește principalele arii de risc din punct de vedere al personalului angajat. În Anexa A.1 am prezentat in extenso acest chestionar format din 20 de întrebări, iar fiecărui răspuns posibil i-a fost alocat un coeficient de risc original cu valori între 1 (risc de securitate minim) și 10 (risc de securitate maxim). Folosind explicațiile și procedura de calcul a scorului general indicate în subcap. 2.4.2, o organizație poate determina gradul de conștientizare a securității informatice la nivelul componentei umane - angajații - și poate îmbunătăți valoarea acestuia prin programe de informare, avertizare și instruire, prin elaborarea unor ghiduri de bune practici sau în cadrul politicilor interne de securitate.

Din punct de vedere organizațional, în subcap. 2.4.3 am realizat un studiu comparativ în ceea ce privește impactul și rezultatele centrelor de securitate de tip SOC și SIC și, pe baza acestei analize, am redefinit subdepartamentele în cadrul departamentului de

securitate al organizației nou formate. De asemenea, în subcap. 2.4.4, dezvoltând profilul profesional al analistului în securitate cibernetică, am determinat necesarul din punct de vedere al resurselor umane și am definit palierele de dezvoltare profesională pentru angajați.

Capitolul 3 prezintă principalele categorii de amenințări la adresa securității cibernetice, iar pentru fiecare dintre acestea am subliniat aspectele relevante și am adus contribuții originale la nivel teoretic și/sau practic (hardware / software). Atacurile informatice au fost clasificate în funcție de mai multe criterii de bază: tipul amenințării, modul de acțiune, intenția, originea sau ținta vizată. De asemenea, sunt relevante instrumentele folosite în desfășurarea unui atac și nivelul de acces obținut în urma unui atac reușit. Principalele categorii de amenințări (malware, phishing, SQL injection, XSS, DoS, Session Hijacking, Man-in-the-Middle sau reutilizarea credențialelor) au fost prezentate detaliat, după care am realizat o analiză a celor mai importante breșe de securitate cibernetică din istoria recentă, observând că a crescut nu doar numărul acestor incidente, cât în special valoarea impactului atât asupra organizațiilor, cât și a utilizatorilor afectați de scurgerile de date confidențiale.

Un tip de atac asupra căruia am insistat în subcap. 3.1.3 a fost atacul ARP spoofing. După o prezentare tehnică a acestui atac, am propus o soluție de detecție a atacurilor de tip ARP spoofing folosind o platformă hardware bazată pe Raspberry Pi și sistem de operare Linux drept dispozitiv de monitorizare ce va fi conectat la un port SPAN al unui smart switch prin care tot traficul din rețea va fi copiat și trimis pentru analiză. Scriptul, scris în limbajul de programare Python, detectează activitățile de scanare (interogarea adreselor IP dintr-o rețea locală), fiind eficient în cazul rețelelor LAN de mici dimensiuni (SOHO), însă limitat din cauza interfeței de rețea la 100 Mb/s. Soluția prezentată acționează la nivelul etapei de recunoaștere (*Reconnaissance*) din cadrul modelului Cyber Kill Chain (dezvoltat ulterior în cap. 4) deoarece scanarea rețelei echivalează cu activitatea în care atacatorul adună informații despre dispozitivele existente în rețea.

În subcap. 3.2 am analizat profilurile, atributele și motivațiile atacatorilor cibernetici. Conform statisticilor pentru prima parte a anului 2020, criminalitatea cibernetică a rămas pe primul loc (86,6%) în topul motivațiilor din spatele atacurilor, ceea ce a condus la concluzia că atacatorii cibernetici ce au în principal scopuri economice (financiare) sau de distrugere sunt cei mai activi pe această piață. Astfel de atacatori posedă atribute avansate, precum un nivel de cunoștințe ridicat și se bazează pe o agresivitate crescută și tehnici fine (de exemplu, ingineria socială) pentru a-și atinge scopul.

Realizarea portretului atacatorilor cibernetici pe baza criteriilor expuse mai sus este completată de contribuția originală care se regăsește în subcap. 3.3. În scopul de a colecta și centraliza date referitoare la atacurile cibernetice care au ca țintă sisteme de tip e-learning (platforme Moodle), am conceput o arhitectură de rețea honeynet implementată inițial în sisteme locale (Raspberry Pi), apoi folosind o infrastructură cloud și mai multe puncte honeypot de cercetare plasate strategic în 3 regiuni geografice: America de Nord, Europa și Asia. Am realizat de asemenea o aplicație prin care am colectat și agregat datele atacatorilor (adrese IP, parole și nume de utilizatori folosite în atacuri) corelate cu versiunile și vulnerabilitățile platformelor e-learning utilizate. Din

analiza acestor date am obținut informații, cunoștințe și inteligență despre atacatori în vederea înțelegerii modurilor lor de atac și a obiectivelor urmărite. Rezultatele obținute în urma acestui studiu pot fi folosite ca reguli IoC în cadrul unor sisteme de detecție și prevenire a intruziunilor.

O categorie extrem de importantă de amenințări la adresa securității cibernetice o reprezintă vulnerabilitățile, acestea fiind acele puncte slabe (hardware sau software) din cadrul unui sistem informatic, pe care atacatorii le pot exploata în vederea încălcării politicilor de securitate stabilite și efectuarea unor operațiuni fără a avea drepturile de acces necesare. Astfel, în subcap. 3.4 am detaliat și testat practic două tipuri de vulnerabilități software: Buffer Overflow (pentru care am simulat un atac ce a folosit această vulnerabilitate, prezentat în Anexa A.2) și Heartbleed (împreună cu propunerea unei configurații hardware folosită pentru implementarea unui atac care a exploatat acest bug). În urma studiului aspectelor tehnice ale acestor vulnerabilități și a simulărilor atacurilor - realizate local (în cadrul rețelei LAN a laboratorului) și bazate pe mașini virtuale și aplicații open-source, alese datorită costurilor și scalabilității lor - s-au obținut cunoștințe, cu ajutorul cărora am evaluat consecințele acestor tipuri de exploatări.

Subcap. 3.5 al tezei prezintă două dintre tipurile de amenințări cibernetice actuale cu efecte dintre cele mai periculoase: APT (amenințările persistente avansate) și malware-ul de tip ransomware. Din punctul de vedere al securității informației, APT reprezintă cel mai important factor al mediului tehnologic informațional actual datorită utilizării unor tehnici extrem de sofisticate care le permit să acționeze un timp îndelungat fără a putea fi detectate. Pe de altă parte, una din provocările actuale în securitatea cibernetică o reprezintă aplicațiile malware de tip ransomware, care criptează fișierele din hard-disk-ul sistemului și solicită plata unei răscumpărări. În continuare am propus două soluții de detecție a atacurilor malware ce au drept țintă obținerea de beneficii financiare: o detecție statică, prin dezvoltarea unui script Python original pe o infrastructură hardware cu costuri reduse care rulează tehnologii open-source standardizate (în subcap. 3.5.3), respectiv o soluție dinamică bazată pe analiza comportamentală a malware-ului (în subcap. 3.5.4). Sistemul inteligent ar putea servi drept componentă a unei aplicații antivirus, ea putând fi integrată pentru a monitoriza procesele nou create și a furniza date celorlalte componente ale antivirusului. Totuși, soluția dinamică este într-o stare incipientă de abordare, necesitând aprofundarea cercetărilor și studiul mai multor idei propuse (aceste dezvoltări ulterioare sunt indicate în subcap. 5.4).

Capitolul 4 debutează cu abordări la nivel teoretic privind modelele de implementare, analiză și asigurare a securității informației. Dintre acestea se remarcă două modele pe care le-am prezentat în detaliu: modelul Cyber Kill Chain și modelul apărării în adâncime (Defense in Depth). Modelul Cyber Kill Chain este un model de securitate tradițional structurat în 3 etape (pre-compromitere, compromitere efectivă și post-compromitere), acestea fiind la rândul lor descompuse într-un număr total de 7 etape. Rolul unui astfel de model este de a descompune pașii unui atac (cibernetic în cazul acestei analize) și a ajuta organizațiile să se apere împotriva vectorilor de amenințare.

Modelul Defense in Depth are drept scop principal nu neapărat să prevină încălcările de securitate, ci mai degrabă să întârzie acțiunile unui atacator, astfel încât organizația

victimă să câștige timp pentru a identifica și a răspunde la un atac cibernetic. Securitatea stratificată introduce mai multe bariere de securitate pentru a se asigura apărarea împotriva diferitelor tipuri de amenințări. Unul din aceste straturi de protecție poate fi reprezentat de tehnicile de autentificare (parole, tokens sau date biometrice). În acest sens, folosind și rezultatele chestionarului din Anexa A.1 referitoare la parolele utilizate (complexitate, măsuri de păstrare în siguranță, grad de reutilizare etc.) am realizat în subcap. 4.3.2 o aplicație folosită pentru verificarea nivelului de securitate asigurat de parole, aplicație ce exploatează vulnerabilități ale procesului de criptare prin simularea unui atac brute-force de tip dicționar.

Un alt strat de protecție în aplicarea modelului Defense in Depth constă în detecția activităților care ar duce la încălcări de securitate, iar un astfel de sistem de detecție a intruziunilor a fost dezvoltat în subcap. 4.5. Pentru început am analizat oportunitățile oferite implementarea soluției software proiectate și dezvoltate pe arhitecturile hardware de tip ARM având la bază un sistem Raspberry Pi (subcap. 4.5.1). Ulterior, soluția software a fost implementată și în cadrul unei infrastructuri computaționale de tip cloud, analizând și prezentând comparativ avantajele și limitările unor astfel de abordări comparativ cu dezvoltările pe configurații hardware low-cost (sisteme Raspberry Pi, rețele locale SOHO). În vederea implementării soluțiilor online am realizat în subcap. 4.5.2 un studiu critic privind siguranța în funcționare a platformelor de tip cloud computing punând un accent deosebit pe raportul cost / beneficiu din perspectiva conceptelor fundamentale în securitatea informațiilor: confidențialitate, integritate, disponibilitate. În final, sistemul propus pentru detecția intruziunilor într-o rețea locală de mici dimensiuni (prezentat conceptual în subcap. 4.5.3 și extins în Anexa A.3) este destinat atenuării amenințărilor de tip Man-in-the-middle. Avantajele acestei soluții constau în utilizarea unor tehnologii gratuite și open-source, a unor resurse de calcul foarte scăzute și, nu în ultimul rând, este portabilă pe alte echipamente de rețea.

5.2. Contribuții originale

În continuare prezint succint lista contribuțiilor personale în cadrul tezei de doctorat. Acestea, împreună cu perspectivele de dezvoltare ulterioară reprezintă o fundație pentru reducerea riscului generat de vulnerabilitățile sistemelor informatice ale prezentului și viitorului. Pe lângă aceste sisteme informatice în sine, adaptarea și realinierea unui program de management al riscului de securitate cibernetică sunt critice în contextul în care mediul de lucru și infrastructura se redefinesc ca urmare a pandemiei generate de COVID-19. Apreciez că aceste măsuri vor trebui luate în considerare încă de acum, pentru o atitudine proactivă în abordarea riscurilor de securitate cibernetică prezente și viitoare și asigurarea continuității afacerilor.

1. Am elaborat și aplicat un cadru de definire și analiză a riscului de securitate cibernetică în cadrul unei companii globale care dezvoltă și licențiază tehnologie și proprietate intelectuală în domenii precum ICT (Information and Communication Technology), inteligența artificială, audio/video, circuite integrate și auto.

2. Am definit și implementat un departament și un program de management de securitate cibernetică în cadrul unei fuziuni a două companii globale prin aplicarea metodei de defensivă stratificată. În cadrul acestei contribuții am organizat peste 100 de interviuri de tip 1 la 1 și întâlniri de echipă cu colegi dintr-un spectru cât mai larg de roluri și responsabilități, de la inginerii implicați în proiectarea și dezvoltarea produselor, arhitecți de infrastructură și sisteme, cât și lideri ai organizațiilor de testare, dezvoltare, resurse umane și departamentul financiar. În urma evaluării atât tehnice, cât și din punct de vedere organizațional, am propus o matrice bazată pe metoda Eisenhower de reducere a riscului, un buget anual pentru integrarea tehnologică, investiții în tehnologii și personal și am preluat o echipă în cadrul departamentului condus de CFO (Chief Financial Officer).

3. Am conceput un chestionar privind gradul de conștientizare a securității cibernetice în cadrul unei organizații pentru a determina principalele arii de risc din punctul de vedere al personalului angajat, știind fiind că suprafața de atac cea mai vulnerabilă în cadrul organizațiilor este reprezentată de componenta umană. Rezultatele obținute în urma diseminării chestionarului au contribuit la îmbunătățirea programului de securitate în cadrul organizației-pilot considerate și elaborarea unor ghiduri de bune practici pentru alte organizații similare care activează în industria ICT.

4. Am realizat un studiu comparativ în ceea ce privește impactul și rezultatele unor centre de securitate cibernetică de tip SOC (Security Operations Center) și SIC (Security Intelligence Center). În urma acestui studiu a rezultat redefinirea subdepartamentelor în cadrul departamentului de securitate întrucât am concluzionat că o implementare bazată pe analiza măsurătorilor și inteligenței colectate prin diverse metode are o rată mai mare de succes în reducerea suprafeței de atac și a costului generat de către incidente. Acest fapt este datorat abordării proactive bazată pe scenarii și anticiparea evenimentelor de securitate cibernetică versus abordării reactive bazată pe așteptare și răspuns la incidente de securitate informațională [B1] [C5].

5. Am dezvoltat un profil profesional al analistului în securitate cibernetică pentru a determina necesarul din punctul de vedere al resurselor umane în cadrul departamentului de securitate și am definit etape de dezvoltare în carieră pentru angajați [B4].

6. Am elaborat un sistem de analiză a atacurilor și atacatorilor pe baza unei rețele de honeypot-uri implementată atât în sisteme locale (precum Raspberry Pi), cât și în diverse arii geografice prin folosirea capacității computaționale din cloud ca etapă în aplicarea modelului Cyber Kill Chain [A2].

7. Am realizat un studiu privind aspectele tehnice și impactul vulnerabilității Heartbleed, în care am evaluat consecințele exploatării acesteia în momentul în care a fost publicată, cât și răspunsul companiilor globale pentru a reduce expunerea la această vulnerabilitate prin testarea în sisteme locale în cadrul laboratorului și prin monitorizarea resurselor disponibile online conținând informații despre răspunsurile la acest eveniment [B3].

8. Am studiat implicațiile și vulnerabilitățile pe care o fuziune între o companie certificată PCI DSS și SOX și o companie care doar adera la câteva practici de implementare a securității cibernetice o are pentru organizația rezultată. Am identificat astfel o serie de puncte de risc și am conceput și implementat un program de management pentru a reduce suprafața de atac.

9. Am dezvoltat arhitectura unei soluții dinamice de detecție și analiză a aplicațiilor malware de tip ransomware prin implementarea cunoștințelor dobândite în urma absolvirii cursului Machine Learning (din cadrul University of Washington) [A4].

10. Am dezvoltat un sistem de detecție a intrușilor și intruziunilor ca etapă în aplicarea modelului Defense in Depth pentru a determina necesarul din punctul de vedere al monitorizării și răspunsului la evenimente de securitate. Acest program a reprezentat cea mai importantă etapă în înțelegerea ecosistemului ce trebuie protejat [A1] [B2] [C4].

11. Am realizat o soluție de detecție statică în urma analizei impactului aplicațiilor malware ce au ca țintă obținerea de beneficii financiare [B5] [B6]. Soluția constă într-un script Python original [A6] și folosește o infrastructură hardware cu costuri reduse care rulează tehnologii open-source standardizate, ceea ce o face atât rapidă, cât și accesibilă unui public larg.

12. Am realizat un studiu critic privind siguranța în funcționare a platformelor de tip cloud computing [C3] și am pus un accent deosebit pe analiza opțiunilor privind raportul cost / beneficiu din punctul de vedere al conceptelor principale din securitatea informatică: confidențialitatea, integritatea și disponibilitatea datelor.

13. Am realizat un program și o arhitectură pentru colectarea și centralizarea datelor referitoare la atacuri cibernetice asupra unor end-point-uri de tip honeypot construite ca bază pentru platforme e-learning de tip Moodle [A2] [A3]. Astfel, a fost definită și realizată o rețea honeynet folosind o infrastructură cloud și s-au analizat datele atacatorilor (adrese IP, parole și nume de utilizatori folosite în atacuri) corelate cu versiunile și vulnerabilitățile platformelor e-learning utilizate.

14. Am aplicat metoda studiată de analiză a atacurilor cibernetice „Cyber Kill Chain” și am propus o soluție de contracararea atacurilor de tip ARP spoofing [B7].

15. Folosind o suită de aplicații open-source, alese datorită costurilor și scalabilității lor, am studiat impactul atacului cibernetic de tip Buffer Overflow prin simularea acestuia în cadrul infrastructurii din laborator [C1].

16. Am proiectat și realizat un program folosit pentru verificarea nivelului de securitate al parolelor folosind limbajul de programare Python, ce exploatează vulnerabilități ale procesului de criptare prin simularea unui atac brute-force de tip dicționar [C2].

17. Am implementat soluțiile software proiectate și dezvoltate pe arhitecturi hardware de tip ARM atât cu ajutorul platformelor Raspberry Pi, cât și în cadrul unei infrastructuri computaționale de tip cloud, analizând și prezentând comparativ avantajele și limitările unor astfel de abordări.

5.3. Activitatea pe parcursul stagiului doctoral

În continuare este prezentată sintetizat activitatea mea pe parcursul stagiului doctoral: articolele cu care am participat la conferințe științifice recunoscute sau publicate în reviste indexate în baze de date internaționale, rezultatele obținute în urma participării la proiectul POSDRU/159/1.5/S/132397 „*Excelență în cercetare prin burse doctorale și postdoctorale" (ExcelDOC)* și alte activități relevante pentru domeniul tezei de doctorat.

Toate acestea au reprezentat elemente cheie care mi-au permis nu doar definitivarea lucrării de doctorat și a întregului stagiu, ci au adus și un aport esențial în îmbunătățirea expertizei personale în domeniul cybersec și perfecționarea mea profesională ca specialist în domeniu, atât pe plan tehnic, cât și managerial.

5.3.1. Lista lucrărilor realizate

A. Articole științifice în publicații indexate ISI / IEEE Xplore

A1. I.D. Barbu, C. Pascariu, I.C. Bacivarov, S.D. Axinte, M. Firoiu, *Intruder monitoring system for local networks using Python*, 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Targoviste, Jun 29 - Jul 01, 2017, eISBN 978-1-5090-6458-8, doi: 10.1109/ECAI.2017.8166457, WOS: 000425865900073

A2. I.D. Barbu, G. Petrică, S.D. Axinte, I. Bacivarov, *Analyzing cyber threat actors of e-learning platforms by the use of a honeynet cloud based infrastructure*, Proc. of the 13th International Scientific Conference "eLearning and Software for Education", Bucharest, 2017, Vol. 3, pp. 352-357, doi: 10.12753/2066-026X-17-226

A3. G. Petrică, **I.D. Barbu**, S.D. Axinte, I. Bacivarov, I.C. Mihai, *E-learning platforms identity using digital certificates*, Proc. of the 13th International Scientific Conference "eLearning and Software for Education" Bucharest, 2017, Vol. 3, pp. 366-373, doi: 10.12753/2066-026X-17-228

A4. C. Pascariu, **I.D. Barbu**, *Dynamic analysis of malware using artificial neural networks. Applying Machine Learning to identify malicious behavior based on parent process hierarchy*, 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Targoviste, Jun 29 - Jul 01, 2017, eISBN 978-1-5090-6458-8, doi: 10.1109/ECAI.2017.8166505, WOS: 000425865900121

A5. G. Petrică, **I.D. Barbu**, S.D. Axinte, C. Pascariu, *Reliability analysis of a web server by FTA method*, The 10th International Symposium on Advanced Topics in Electrical Engineering (ATEE), Bucharest, 2017, pp. 683-686, doi: 10.1109/ATEE.2017.7905101, WOS: 000403399400133

A6. C. Pascariu, **I.D. Barbu**, *Ransomware honeypot. Honeypot solution designed to detect a ransomware infection identify the ransomware family*, 11th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Pitesti, June 27-29, 2019, eISBN 978-1-7281-1624-2, doi: 10.1109/ECAI46879.2019.9042158

B. Articole științifice în publicații indexate BDI

B1. I.D. Barbu, C. Pascariu, I.C. Bacivarov, *Migration of a SOC to SIC. Security Operations Center vs. Security Intelligence Center. The use of honeypots for threat intelligence*, Proc. of the 15th International Conference on Quality and Dependability Sinaia, Romania, September 14th-16th, 2016, pp. 150-155, ISSN 1842-3566

B2. I.D. Barbu, G. Petrică, *Defense in Depth principle to ensure information security*, IJISC - International Journal of Information Security and Cybercrime, Vol. 4, No. 1, 2015, pp. 41-46, doi: 10.19107/IJISC.2015.01.06

B3. I.D. Barbu, I.C. Bacivarov, *The Heartbleed bug - a vulnerability in the OpenSSL cryptographic library*, Proc. of the 14th International Conference on Quality and Dependability Sinaia, Romania, September 17th-19th, 2014, pp. 100-109, ISSN 1842-3566

B4. I.D. Barbu, C. Pascariu, *Information security analyst profile*, IJISC - International Journal of Information Security and Cybercrime, Vol. 3, No. 1, 2014, pp. 29-36, doi: 10.19107/IJISC.2014.01.03

B5. C. Pascariu, **I.D. Barbu**, I.C. Bacivarov, *WannaCry ransomware analysis. 1 day, 150 countries, >57k infected computers*, Asigurarea Calității - Quality Assurance, Anul XXIII, Numărul 90, Aprilie-Iunie 2017, pag. 4-7, ISSN 1224-5410

B6. C. Pascariu, **I.D. Barbu**, *Ransomware - an emerging threat*, IJISC - International Journal of Information Security and Cybercrime, Vol. 4, No. 2, 2015, pp. 27-32, doi: 10.19107/IJISC.2015.02.03

B7. C. Pascariu, **I.D. Barbu**, I.C. Bacivarov, *Network security monitoring with embedded platforms*, Proc. of the 16th International Conference on Quality and Dependability Sinaia, Romania, September 26th-28th, 2018, pp. 243-246, ISSN 1842-3566

C. Rapoarte științifice în cadrul programului de doctorat

C1. Raportul științific nr. 1, iunie 2014: *Buffer Overflow vulnerability exploitation using open-source tools*

C2. Raportul științific nr. 2, decembrie 2014: *Studiul metodelor de programare utilizând Python în vederea dezvoltării unui program de verificare a parolelor*

C3. Raportul științific nr. 3, iunie 2015: *Studiul programelor de tip OpenStack în vederea implementării în sistemul de securitate dezvoltat. Studiu comparativ între securitatea informațiilor on premise sau în cloud*

C4. Raportul științific nr. 4, decembrie 2015: *Intruder monitoring system for local networks using Python*

C5. Raportul științific nr. 5, iunie 2016: *Studiu comparativ între implementarea unui centru de securitate cibernetică de tip SOC (Security Operations Center) și SIC (Security Intelligence Center)*

5.3.2. Proiectul POSDRU/159/1.5/S/132397

În perioada aprilie 2014 - decembrie 2015 am participat în echipa de cercetare a proiectului POSDRU/159/1.5/S/132397 „*Excelență în cercetare prin burse doctorale și postdoctorale" (ExcelDOC)*.

Obiectivul general al acestui proiect a constat în „creșterea competitivității și a performanței profesionale a viitorilor doctori în științe și a cercetătorilor care au obținut titlul de doctor în științe, prin participarea și implicarea activă în programe doctorale și post-doctorale, contribuind la dezvoltarea unui corp de cercetători-experți capabili să adopte o abordare interdisciplinară în domeniul cercetării, dezvoltării și inovării" [160].

5.3.3. Alte activități în domeniul tezei de doctorat

Participări la evenimente

1. Am participat la conferințele științifice internaționale „International Symposium on Advanced Topics in Electrical Engineering" (2017), „eLearning and Software for Education Conference" (2017), „Electronics, Computers and Artificial Intelligence" (2017, 2019), „Calitate și Siguranță în Funcționare" (2014, 2016, 2018).
2. Am participat la Simpozionul Anual al Doctoranzilor în Electronică, Telecomunicații și Tehnologia Informației, ediția 1 (2018).
3. Am avut o implicare activă în domeniul cybersecurity prin:

- crearea de echipe și comunități;
- susținerea educației și instruirii la nivel național / internațional;
- organizarea unor evenimente destinate publicului larg (BSidesBucharest, conferințele OWASP România, mai multe hackathon-uri și workshop-uri), mediului universitar și mediului de afaceri (prezentări de produse, servicii, tehnologii).

Alte lucrări publicate

1. Am publicat în revista IJISC - International Journal of Information Security and Cybercrime recenzii ale unor evenimente în domeniul securității cibernetice la care am participat în calitate de speaker sau invitat (Black Hat USA, Defcamp, OWASP, BSides, SPARKS).
2. Am avut o contribuție activă la îmbunătățirea culturii cybersecurity prin elaborarea unor studii și analize personale privind securitatea cibernetică, materiale diseminate prin intermediul website-ului personal sau publicate pe site-uri de specialitate (reviste, bloguri, forumuri și comunități tehnice).

Bibliografie selectivă

[1] Marsh & Microsoft, 2019 Global Cyber Risk Perception Survey, Marsh LLC, 2019, https://www.microsoft.com/security/blog/wp-content/uploads/2019/09/Marsh-Microsoft-2019-Global-Cyber-Risk-Perception-Survey.pdf.
[2] World Economic Forum, The Global Risks Report 2020, http://www3.weforum.org/docs/WEF_Global_Risk_Report_2020.pdf.
[3] K. Schwab, The Fourth Industrial Revolution. What It Means and How to Respond, Foreign Affairs, 2015, https://www.foreignaffairs.com/articles/2015-12-12/fourth-industrial-revolution.
[4] World Economic Forum, Wild Wide Web. Consequences of Digital Fragmentation, 2020, https://reports.weforum.org/global-risks-report-2020/wild-wide-web/.
[24] International Standard ISO/IEC 27001:2013 Information technology - Security techniques - Information security management systems - Requirements, 2nd edition, 2013.
[29] NIST, Framework for Improving Critical Infrastructure Cybersecurity, Version 1.1, April 2018, https://nvlpubs.nist.gov/nistpubs/CSWP/NIST.CSWP.04162018.pdf.
[39] B. McKay, K. McKay, The Eisenhower Decision Matrix: How to Distinguish Between Urgent and Important Tasks and Make Real Progress in Your Life, 2013, https://www.artofmanliness.com/articles/eisenhower-decision-matrix/.
[48] I.D. Barbu, C. Pascariu, I.C. Bacivarov, Migration of a SOC to SIC Security Operations Center vs. Security Intelligence Center. The use of honeypots for threat intelligence, Proceedings of the 15th International Conference on Quality and Dependability Sinaia, Romania, September 14th-16th, 2016, pp. 150-155, ISSN 1842-3566.
[49] I.D. Barbu, Studiu comparativ între implementarea unui centru de securitate cibernetică de tip SOC (Security Operations Center) și SIC (Security Intelligence Center), Raportul științific nr. 5, iunie 2016.
[51] I.D. Barbu, C. Pascariu, Information Security Analyst Profile, IJISC - International Journal of Information Security and Cybercrime, Vol. 3, No. 1, 2014, pp. 29-36, doi: 10.19107/IJISC.2014.01.03.
[69] C. Pascariu, I.D. Barbu, I.C. Bacivarov, Network security monitoring with embedded platforms, Proceedings of the 16th International Conference on Quality and Dependability Sinaia, Romania, September 26th-28th, 2018, pp. 243-246, ISSN 1842-3566.
[78] I.D. Barbu, G. Petrică, S.D. Axinte, I. Bacivarov, Analyzing cyber threat actors of e-learning platforms by the use of a honeynet cloud based infrastructure, Proc. of the 13th International Scientific Conference "eLearning and Software for Education", Bucharest, 2017, Vol. 3, pp. 352-357, doi: 10.12753/2066-026X-17-226.
[84] I.D. Barbu, Buffer Overflow vulnerability exploitation using open-source tools, IJISC - International Journal of Information Security and Cybercrime, Vol. 2, No. 2, 2013, pp. 43-54, doi: 10.19107/IJISC.2013.02.05.
[95] I.D. Barbu, I.C. Bacivarov, The Heartbleed bug - a vulnerability in the OpenSSL cryptographic library, Proceedings of the 14th International Conference on Quality and Dependability Sinaia, Romania, September 17th-19th, 2014, pp. 100-109, ISSN 1842-3566.
[102] C. Pascariu, I.D. Barbu, I.C. Bacivarov, WannaCry Ransomware Analysis. 1 day, 150 countries, > 57k infected computers, Asigurarea Calității - Quality Assurance, Anul XXIII, Numărul 90, Aprilie-Iunie 2017, pag. 4-7, ISSN 1224-5410.
[103] C. Pascariu, I.D. Barbu, Dynamic analysis of malware using artificial neural networks Applying Machine Learning to identify malicious behavior based on parent process hierarchy, 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Targoviste, Jun 29 - Jul 01, 2017.
[111] C. Pascariu, I.D. Barbu, Ransomware - an emerging threat, IJISC - International Journal of Information Security and Cybercrime, Vol. 4, No. 2, 2015, pp. 27-32, doi: 10.19107/IJISC.2015.02.03
[112] C. Pascariu, I.D. Barbu, Ransomware honeypot. Honeypot solution designed to detect a ransomware infection identify the ransomware family, 11th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Pitesti, June 27-29, 2019, eISBN 978-1-7281-1624-2, doi: 10.1109/ECAI46879.2019.9042158.
[128] I.D. Barbu, G. Petrică, Defense in Depth Principle to Ensure Information Security, IJISC - International Journal of Information Security and Cybercrime, Vol. 4, No. 1, 2015, pp. 41-46, doi: 10.19107/IJISC.2015.01.06.
[149] E. Gorelik, Cloud Computing Models, Working Paper CISL# 2013-01, MIT, 2013.
[159] I.D. Barbu, C. Pascariu, I.C. Bacivarov, S.D. Axinte, M. Firoiu, Intruder monitoring system for local networks using Python, 9th International Conference on Electronics, Computers and Artificial Intelligence (ECAI), Targoviste, Jun 29 - Jul 01, 2017.
[160] Proiectul POSDRU/159/1.5/S/132397 (ExcelDoc), http://cempdi.pub.ro/exceldoc/.