BULETINUL
UNIVERSITĂȚII NAȚIONALE DE APĂRARE „CAROL I"
https://buletinul.unap.ro

Creșterea rezilienței cibernetice a IMM prin soluții open-source și colaborare internațională

Increasing the cyber resilience of SMEs through open-source solutions and international collaboration

Dr. Ionica ȘERBAN*
Masterand Florentina-Mihaela CURCĂ**
Masterand Robert-Ștefan ȘANDRU***
*Directoratul Național de Securitate Cibernetică
e-mail: ionica.serban@dnsc.ro
**Directoratul Național de Securitate Cibernetică
e-mail: mihaela.curca@dnsc.ro
***Directoratul Național de Securitate Cibernetică
e-mail: robert.sandru@dnsc.ro

Abstract

Într-o lume tot mai digitalizată, întreprinderile mici și mijlocii (IMM) sunt expuse amenințărilor cibernetice semnificative, din cauza resurselor limitate pentru securitate. Acest articol explorează rolul soluțiilor open-source și al colaborării internaționale în creșterea rezilienței cibernetice a IMM. Soluțiile open-source oferă accesibilitate financiară, flexibilitate și securitate sporită, fiind susținute de comunități globale care contribuie la îmbunătățirea continuă a acestora. De asemenea, partajarea descentralizată a informațiilor referitoare la amenințări, combinată cu inteligența artificială, permite o detectare și o prevenție mai eficientă a atacurilor cibernetice. Prin inițiative colaborative, cum ar fi HackOlympics, IMM pot învăța din practică și pot beneficia de soluții testate în scenarii reale. În concluzie, soluțiile open-source și utilizarea tehnologiilor avansate, precum IA, le oferă întreprinderilor mici și mijlocii o strategie eficientă pentru a răspunde provocărilor cibernetice moderne, îmbunătățindu-le reziliența și protecția împotriva amenințărilor.

In an increasingly digitalized world, small and medium-sized enterprises (SMEs) are exposed to significant cyber threats due to limited security resources. This article explores the role of open-source solutions and international collaboration in enhancing the cyber resilience of SMEs. Open-source solutions offer financial accessibility, flexibility, and increased security, supported by global communities that contribute to their continuous improvement. Moreover, decentralized sharing of threat information, combined with artificial intelligence, enables more efficient detection and prevention of cyberattacks. Through collaborative initiatives such as HackOlympics, SMEs can learn through hands-on experience and benefit from solutions tested in real-life scenarios. In conclusion, open-source solutions and the use of advanced technologies, such as AI, provide SMEs with an effective strategy to address modern cyber challenges, improving their resilience and protection against threats.

Cuvinte-cheie:
securitate cibernetică; IMM; soluții open-source; colaborare internațională; inteligență artificială; HackOlympics.

Keywords:
cybersecurity; SMEs; open-source solutions; international collaboration; artificial intelligence; HackOlympics.

Info articol
Primit: 14 octombrie 2024; Evaluat: 15 noiembrie 2024; Acceptat: 2 decembrie 2024; Disponibil online: 17 ianuarie 2025
Citare: Șerban, I., F.M. Curcă și R.Ș. Șandru. 2024. „Creșterea rezilienței cibernetice a IMM prin soluții open-source și colaborare internațională". *Buletinul Universității Naționale de Apărare „Carol I"*, 13(4): 215-236. https://doi.org/10.53477/2065-8281-24-49

© Editura Universității Naționale de Apărare „Carol I"
Articol cu acces deschis distribuit în conformitate cu termenii și condițiile licenței Creative Commons Attribution (CC BY-NC-SA)

În era digitalizării accelerate, securitatea cibernetică a devenit o provocare globală, afectând toate tipurile de organizații, indiferent de dimensiune. Cu toate acestea, întreprinderile mici și mijlocii (IMM) sunt în mod deosebit vulnerabile, deoarece adesea nu dispun de resursele necesare pentru a investi în tehnologii avansate de protecție și pentru a implementa sisteme robuste de securitate. Aceste companii reprezintă un segment esențial al economiei globale, având o contribuție semnificativă la dezvoltarea economică, la inovare și ocuparea forței de muncă. În ciuda acestui fapt, numeroase întreprinderi mici și mijlocii sunt ținte atractive pentru atacatorii cibernetici, deoarece, de multe ori, dispun de date valoroase, dar au infrastructuri de securitate insuficient dezvoltate.

Întreprinderile mici și mijlocii se confruntă cu o serie de provocări unice în ceea ce privește protecția cibernetică. În primul rând, lipsa resurselor financiare și umane limitează capacitatea lor de a investi în soluții comerciale scumpe de securitate cibernetică, accesibile mai mult pentru companiile mari. În al doilea rând, IMM nu dispun de echipe dedicate sau de expertiză în domeniul securității informatice, ceea ce le face să fie mai puțin pregătite să detecteze și să răspundă rapid la amenințările cibernetice.

De asemenea, întreprinderile mici și mijlocii sunt adesea concentrate pe creșterea afacerilor și nu percep riscurile cibernetice ca fiind prioritare, ceea ce duce la o lipsă de măsuri proactive pentru prevenirea atacurilor. Acest lucru le plasează într-o poziție vulnerabilă, fiind frecvent afectate de atacuri, precum ransomware, phishing și breșe de date, care pot provoca pierderi financiare substanțiale, afectând reputația și încrederea clienților.

Soluțiile open-source sunt o alternativă accesibilă, oferă o opțiune viabilă pentru IMM în consolidarea securității cibernetice. Acestea oferă acces gratuit la tehnologii avansate, care pot fi adaptate și personalizate, în funcție de nevoile fiecărei organizații. În plus, comunitățile open-source sunt extrem de active în remedierea vulnerabilităților și îmbunătățirea continuă a acestor soluții, oferind întreprinderilor mici și mijlocii oportunitatea de a beneficia de cele mai recente inovații și practici din domeniul securității cibernetice.
Adoptarea acestor soluții nu necesită costuri inițiale mari, iar IMM pot alege să implementeze treptat măsuri de securitate, pe măsură ce își dezvoltă capacitățile și resursele. De asemenea, soluțiile open-source beneficiază de un nivel ridicat de transparență și flexibilitate, ceea ce permite o personalizare mai profundă și o integrare ușoară în sistemele existente ale IMM.

Colaborarea internațională este cheia pentru success, o altă dimensiune crucială în creșterea rezilienței cibernetice a IMM. Atacurile cibernetice au o natură globală, iar pentru a combate aceste amenințări complexe, întreprinderile mici și mijlocii trebuie să participe la rețele de partajare a informațiilor, să colaboreze cu alte companii și instituții din domeniul securității și să învețe din experiențele altor entități de pe plan internațional.

Colaborarea dintre IMM și organisme internaționale permite schimbul de bune practici și accesul la resurse educative, la conferințe, hackathoni și simulări de atacuri. Aceasta creează un ecosistem de sprijin reciproc, în care noile amenințări sunt rapid identificate și soluțiile sunt dezvoltate și distribuite comunității, crescând astfel capacitatea întreprinderilor mici și mijlocii de a răspunde rapid la riscuri și de a-și îmbunătăți sistemele de apărare. Întreprinderile mici și mijlocii, deși vulnerabile din cauza resurselor limitate, au posibilitatea de a-și îmbunătăți reziliența cibernetică prin adoptarea soluțiilor open-source și prin participarea la inițiative de colaborare internațională. Aceste măsuri, împreună cu educarea continuă și conștientizarea importanței securității cibernetice, vor permite IMM să facă față provocărilor din mediul digital actual, asigurându-și protecția pe termen lung și contribuind la stabilitatea și dezvoltarea economiei globale.

Metodologie

Metoda științifică utilizată în această lucrare se concentrează pe o abordare integrată și multidisciplinară pentru a evalua eficacitatea soluțiilor open-source în creșterea rezilienței cibernetice a IMM. Metodologia a fost structurată pe mai multe etape, pentru a asigura o analiză cuprinzătoare și riguroasă a subiectului. Prima etapă a fost o revizuire sistematică a literaturii existente, pentru a înțelege peisajul actual al securității cibernetice și utilizarea soluțiilor open-source de către IMM. Au fost folosite surse academice și rapoarte din industrie pentru a identifica provocările și nevoile întreprinderilor mici și mijlocii în materie de securitate cibernetică. Baze de date, precum IEEE Xplore, Google Scholar și Scopus, au fost folosite pentru a extrage articole relevante privind tehnologiile de securitate, inteligența artificială și partajarea informațiilor despre amenințări.

În continuare, a fost efectuată o analiză comparativă a soluțiilor open-source disponibile pentru IMM, cum ar fi OpenVAS, Suricata, și PfSense. Respectiva etapă a implicat evaluarea acestor soluții pe baza criteriilor esențiale, inclusiv costurile, ușurința de utilizare, flexibilitatea și eficiența în detectarea și prevenirea amenințărilor.

Această lucrare se distinge prin prezentarea unui studiu aprofundat privind impactul soluțiilor open-source asupra securității cibernetice a IMM, un subiect de interes tot mai mare în era digitalizării. În acest context, soluțiile, precum OpenVAS, Suricata și PfSense, joacă un rol crucial, fiind adoptate din ce în ce mai mult de întreprinderile mici și mijlocii care caută alternative eficiente și accesibile la soluțiile comerciale.

Conform unui raport recent al Ponemon Institute (2023), peste 45% dintre întreprinderile mici și mijlocii la nivel global utilizează cel puțin o soluție open-source pentru securitatea cibernetică. Dintre acestea, 60% consideră că accesibilitatea financiară este principalul motiv pentru adoptarea acestor soluții. În mod specific, OpenVAS, o platformă pentru evaluarea vulnerabilităților, este utilizată

de aproximativ 35% dintre întreprinderile mici și mijlocii care implementează soluții open-source. Această platformă permite companiilor să identifice rapid punctele slabe din infrastructura IT, reducând riscul exploatării vulnerabilităților critice.
De asemenea, Suricata, o soluție avansată pentru detectarea și prevenirea intruziunilor, este integrată în sistemele de securitate ale IMM din întreaga lume. Conform unui studiu, publicat de OWASP (2023b), utilizarea Suricata a crescut cu 50% în ultimii doi ani, IMM apreciind capacitatea acesteia de a oferi monitorizare în timp real și adaptabilitate la diverse tipuri de atacuri cibernetice.

PfSense, o soluție firewall open-source extrem de populară, s-a dovedit a fi un instrument esențial pentru IMM. Datele furnizate de proiectul PfSense arată că peste 70% dintre utilizatorii săi sunt organizații mici și mijlocii, iar implementările au condus la economii de până la 80%, comparativ cu soluțiile comerciale. Mai mult, un raport Gartner (2023) subliniază că întreprinderile mici și mijlocii care utilizează PfSense observă o îmbunătățire semnificativă a securității rețelei, datorită flexibilității și personalizării ușoare pe care această soluție o oferă.

În cadrul studiului de caz prezentat în acest articol, o întreprindere din categoria IMM din sectorul IT din România a implementat PfSense pentru a face față provocărilor de securitate. În urma acestei implementări, compania a reușit să reducă atacurile cibernetice cu 80% și să asigure o continuitate operațională robustă, menținând în același timp costurile la un nivel minim. Aceste rezultate susțin tendințele globale și demonstrează că întreprinderile mici și mijlocii pot valorifica soluțiile open-source pentru a-și consolida reziliența cibernetică, fără a fi constrânse de bugete mari.
Integrarea acestor statistici și date evidențiază relevanța practică a soluțiilor open-source în protejarea IMM împotriva riscurilor cibernetice și subliniază contribuția semnificativă a acestei lucrări în promovarea utilizării unor astfel de tehnologii. Astfel, lucrarea nu doar că demonstrează aplicabilitatea acestor soluții, ci oferă și un cadru concret de analiză și implementare, bazat pe tendințele actuale și pe nevoile reale ale întreprinderilor mici și mijlocii.

Provocările de securitate pentru IMM în era digitală

IMM (întreprinderile mici și mijlocii) reprezintă coloana vertebrală a economiilor europene, fiind responsabile de aproximativ 99% dintre întreprinderi, generând două treimi din locurile de muncă în Europa (Comisia Europeană 2023). Cu toate acestea, ele se confruntă cu provocări majore în materie de securitate cibernetică, pe măsură ce digitalizarea devine esențială pentru funcționarea afacerilor moderne. Lipsa resurselor financiare și a expertizei interne limitează capacitatea IMM de a investi în tehnologii avansate de securitate, lăsându-le vulnerabile în fața atacurilor cibernetice (ENISA 2023c).

Într-o eră în care criminalitatea cibernetică evoluează rapid, întreprinderile mici și mijlocii devin tot mai frecvent ținta atacurilor. Studiile arată că peste 60% dintre

atacurile cibernetice vizează întreprinderile mici și mijlocii (Verizon 2023), care sunt văzute ca ținte mai ușoare, din cauza lipsei de măsuri de protecție, comparativ cu marile corporații.

Phishingul este una dintre cele mai răspândite amenințări. Angajații IMM primesc e-mailuri frauduloase care pretind a fi de la organizații legitime, încercând să obțină date sensibile. Acest tip de atac reprezintă aproape 57% din totalul incidentelor de securitate raportate în rândul IMM.

Ransomware-ul a devenit o amenințare omniprezentă, întreprinderile mici și mijlocii fiind frecvent vizate, din cauza lipsei unor soluții de backup adecvate. Ransomware-ul criptează datele companiei și solicită o răscumpărare pentru deblocarea accesului. Se estimează că 43% dintre atacurile ransomware au drept țintă întreprinderile mici și mijlocii.

Atacurile DDoS (Distributed Denial of Service) blochează serviciile online ale unei companii prin inundarea serverelor cu trafic fals, ceea ce poate afecta serios operațiunile întreprinderilor mici și mijlocii, în special cele care depind de funcționalitatea online (Arbor Networks 2023).
Breșele de date reprezintă o amenințare majoră, în special pentru IMM care gestionează date sensibile. Studiile arată că 60% dintre IMM care suferă breșe majore de securitate își închid activitatea în termen de șase luni. Impactul financiar al unei breșe poate fi devastator, având în vedere costurile de recuperare și sancțiunile legale care pot apărea în urma nerespectării reglementărilor de protecție a datelor, precum GDPR.

Unul dintre principalii factori care contribuie la vulnerabilitatea întreprinderilor mici și mijlocii este lipsa resurselor financiare. Soluțiile avansate de securitate sunt adesea costisitoare, iar întreprinderile mici și mijlocii au bugete limitate pentru a le achiziționa și implementa. Conform unui raport din 2023, 60% dintre întreprinderile mici și mijlocii nu își permit să investească în soluții comerciale de securitate.
Lipsa expertizei interne reprezintă un alt obstacol semnificativ. Majoritatea întreprinderilor mici și mijlocii nu au personal pentru securitate cibernetică și se bazează pe echipe IT mici sau chiar pe personal non-tehnic pentru a gestiona problemele de securitate. Această lipsă de expertiză duce la o pregătire insuficientă în fața atacurilor și la o reacție lentă, în cazul unor incidente (NIST 2022a).

Infrastructurile învechite sunt o altă problemă majoră pentru întreprinderile mici și mijlocii. Multe dintre acestea folosesc tehnologii vechi și nesecurizate, fără a implementa patch-uri de securitate regulate. Această situație lasă portițe deschise pentru atacatori, care exploatează vulnerabilitățile cunoscute.
Conștientizarea redusă a riscurilor este, de asemenea, un factor important. Mulți manageri de IMM subestimează riscurile cibernetice, crezând că afacerea lor nu este suficient de mare sau de valoroasă pentru a atrage atacuri. Această percepție eronată împiedică întreprinderile mici și mijlocii să ia măsuri proactive pentru a preveni atacurile.

Atacurile cibernetice pot avea consecințe devastatoare asupra IMM, care nu dispun de resursele necesare pentru a se recupera rapid. Pierderile financiare, generate de aceste atacuri, pot include plăți de răscumpărare, pierderi de afaceri, din cauza întreruperii serviciilor, și costuri suplimentare pentru recuperarea datelor.
În plus, impactul unui atac asupra imaginii poate fi la fel de dăunător. O breșă de securitate poate afecta grav încrederea clienților și partenerilor de afaceri, mai ales în cazul în care datele acestora sunt compromise. Într-o eră în care protecția datelor personale este o prioritate, un astfel de incident poate duce la pierderi de clienți și la sancțiuni financiare, impuse de reglementările de tipul GDPR.

Una dintre provocările fundamentale pentru IMM în asigurarea securității cibernetice este accesibilitatea soluțiilor și scalabilitatea acestora. Spre deosebire de marile corporații, care își permit să aloce bugete semnificative pentru implementarea unor soluții avansate de securitate, IMM funcționează cu resurse financiare și umane limitate. Din acest motiv, soluțiile de securitate tradiționale și comerciale sunt adesea inaccesibile din punct de vedere financiar, iar complexitatea acestora poate depăși capacitățile echipelor tehnice care, la nivelul acestor companii, sunt limitate.

Soluțiile de securitate comerciale de tip enterprise, cum ar fi firewall-uri avansate, sisteme de prevenire a intruziunilor (IPS), soluții de backup și recuperare, în caz de dezastru, sau sisteme de gestionare a identității și accesului (IAM), sunt dezvoltate, în general, pentru organizații mari, care au resursele necesare pentru a le implementa și întreține. Aceste soluții implică, pe lângă costuri inițiale ridicate, și cheltuieli recurente pentru licențe, suport tehnic și actualizări regulate. Pentru IMM, aceste cheltuieli reprezintă o povară semnificativă, ceea ce face ca multe dintre ele să nu-și permită astfel de investiții (Verizon 2023).

De asemenea, multe soluții comerciale sunt concepute pentru infrastructuri complexe și organizații cu nevoi diversificate, ceea ce le face dificil de adaptat la nevoile unei IMM. Personalul tehnic redus și, adesea, lipsa unui departament IT face ca multe IMM să nu aibă capacitatea de a gestiona soluții complicate, ceea ce le face vulnerabile atacurilor cibernetice.

În acest context, soluțiile open-source au câștigat teren ca o opțiune viabilă pentru IMM. Soluțiile open-source, care sunt dezvoltate și susținute de comunități globale de dezvoltatori și specialiști în securitate, sunt gratuit disponibile, permit o flexibilitate ridicată și oferă întreprinderilor mici și mijlocii posibilitatea de a le adapta la nevoile lor specifice (OWASP 2023a).

Exemple de soluții open-source care sunt utilizate în securitatea cibernetică includ:

- OpenVAS (Open Vulnerability Assessment System), pentru scanarea vulnerabilităților;
- Suricata și Snort, pentru detectarea și prevenirea intruziunilor;
- PfSense, pentru firewall-uri și routere;
- ClamAV, pentru protecția împotriva virușilor și malware-ului.

Aceste soluții sunt accesibile întreprinderilor mici și mijlocii nu doar datorită costului redus (majoritatea fiind gratuite), ci și datorită suportului larg, oferit de comunitățile din jurul acestor proiecte, care contribuie la actualizări frecvente și la corectarea vulnerabilităților.
Un alt avantaj major al soluțiilor open-source este scalabilitatea. În cazul întreprinderilor mici și mijlocii, care sunt în continuă evoluție, este esențial ca soluțiile de securitate să poată crește odată cu afacerea. Soluțiile open-source pot fi configurate, inițial, pentru a acoperi nevoile de bază ale securității, iar pe măsură ce afacerea crește, aceste soluții pot fi extinse fără costuri semnificative.

De exemplu, un firewall open-source, precum PfSense, poate fi implementat, inițial, la scară mică pentru a gestiona traficul de rețea și poate fi, ulterior, extins pentru a acoperi rețele mai mari sau pentru a include funcționalități avansate, cum ar fi VPN-uri sau QoS (Quality of Service), fără a implica costuri suplimentare majore pentru licențiere sau hardware (PfSense Project 2023). În plus, soluțiile open-source permit întreprinderilor mici și mijlocii să își personalizeze configurațiile pentru a răspunde nevoilor lor specifice, ceea ce le face mult mai flexibile, comparativ cu soluțiile comerciale (NIST 2022b).
Un alt aspect important care face ca soluțiile open-source să fie atractive pentru IMM este sprijinul activ al comunităților globale. Platformele open-source beneficiază de contribuții constante din partea dezvoltatorilor și experților în securitate din întreaga lume, care îmbunătățesc continuu funcționalitățile și identifică noi vulnerabilități.

Pe lângă contribuțiile tehnice, aceste comunități oferă și sprijin educațional prin forumuri, ghiduri și tutoriale, care ajută întreprinderile mici și mijlocii să înțeleagă și să implementeze corect soluțiile open-source. Astfel, IMM nu sunt nevoite să depindă de furnizori comerciali pentru suport tehnic, ceea ce reduce semnificativ costurile pe termen lung.

În concluzie, soluțiile open-source oferă întreprinderilor mici și mijlocii o alternativă viabilă, accesibilă și scalabilă pentru protecția cibernetică. Aceste soluții nu permit doar tehnologie de înaltă calitate fără costuri prohibitive, dar permit și o adaptare rapidă la nevoile organizațiilor în creștere. Mai mult, suportul oferit de comunitățile internaționale și flexibilitatea soluțiilor open-source dau siguranța necesară întreprinderilor mici și mijlocii de a face față provocărilor cibernetice cu resurse limitate, contribuind astfel la creșterea rezilienței lor cibernetice.

Aspecte legislative, normative și strategice ale colaborării internaționale

Colaborarea internațională în domeniul securității cibernetice reprezintă un pilon esențial în protejarea întreprinderilor mici și mijlocii (IMM) împotriva amenințărilor cibernetice tot mai sofisticate. Într-o lume digitalizată, în care atacurile nu respectă granițele naționale, IMM beneficiază nu doar de tehnologii open-source, ci și de un

cadru legislativ, normativ și strategic, menit să le sprijine în fața provocărilor globale. Acest capitol explorează modul în care inițiativele internaționale, standardele globale și strategiile coordonate pot întări reziliența cibernetică a IMM.

La nivel european, Uniunea Europeană a dezvoltat un set de reglementări esențiale care încurajează întreprinderile mici și mijlocii să adopte măsuri proactive de securitate cibernetică. Directiva NIS2, un element central în acest peisaj, stabilește standarde ridicate de protecție pentru companiile care activează în sectoare considerate esențiale și importante. Întreprinderile mici și mijlocii sunt chemate să adopte măsuri, precum:

- implementarea unor politici de gestionare a riscurilor cibernetice;
- raportarea rapidă a incidentelor cibernetice autorităților competente;
- colaborarea în rețele de schimb de informații referitoare la amenințări.

Agenția Uniunii Europene pentru Securitate Cibernetică (ENISA) sprijină aceste eforturi prin furnizarea de ghiduri practice, prin exerciții de simulare și instrumente dedicate IMM. Un exemplu notabil este organizarea simulărilor cibernetice la scară europeană, care permit întreprinderilor mici și mijlocii să testeze și să îmbunătățească strategiile lor de apărare în condiții realiste.

Adoptarea standardelor internaționale, precum ISO/IEC 27001, oferă întreprinderilor mici și mijlocii un cadru de referință recunoscut global pentru gestionarea securității informației. Aceste standarde nu doar că stabilesc un set clar de bune practici, dar și:

- reduc riscurile prin implementarea unor măsuri de control validate;
- sporesc încrederea clienților și partenerilor;
- facilitează conformitatea cu cerințele legislative din diverse țări.

Pentru IMM, adoptarea ISO/IEC 27001 poate deveni un avantaj competitiv, deschizând accesul către piețe internaționale și consolidând reputația companiei ca partener de încredere.

Un element crucial al colaborării internaționale este schimbul de informații referitoare la amenințările cibernetice. Platforme, precum MISP (Malware Information Sharing Platform) sau STIX/TAXII, permit întreprinderilor mici și mijlocii să acceseze date privind atacuri, tehnici și tactici folosite de infractori. Acest schimb de informații are multiple beneficii:

- identificarea rapidă a amenințărilor emergente;
- sprijin reciproc între companii și sectoare industriale;
- crearea unei apărări colective mai puternice.

De exemplu, prin participarea la aceste platforme, IMM pot preveni atacuri de tip ransomware care afectează lanțurile de aprovizionare, protejând astfel nu doar propria afacere, ci și pe partenerii lor.

Pe lângă inițiativele europene, organizații, precum Organizația pentru Cooperare și Dezvoltare Economică (OECD) sau Forumul Economic Mondial, contribuie la promovarea colaborării globale în domeniul securității cibernetice. Aceste organizații:

- dezvoltă politici care sprijină IMM în adoptarea de soluții cibernetice eficiente;
- furnizează resurse educative pentru a crește nivelul de conștientizare cibernetică;
- organizează schimburi de bune practici între sectoare și regiuni.

Un exemplu concret este Forumul Echipei de Răspuns la Incidente și Securitate (FIRST), care facilitează cooperarea dintre organizații din întreaga lume, inclusiv IMM, pentru a răspunde coordonat incidentelor cibernetice.

Reglementările internaționale, cum ar fi Regulamentul General privind Protecția Datelor (GDPR), impun întreprinderilor mici și mijlocii să adopte măsuri stricte pentru protecția datelor personale. În același timp, tratatele și parteneriatele internaționale în domeniul securității cibernetice permit întreprinderilor mici și mijlocii să beneficieze de sprijin transfrontalier. Aceste cadre legislative oferă IMM instrumentele necesare pentru a naviga într-un mediu complex și dinamic.

Integrarea legislației, a standardelor globale și strategiilor internaționale oferă întreprinderilor mici și mijlocii o abordare holistică în gestionarea riscurilor cibernetice. Prin combinarea tehnologiilor open-source cu aceste instrumente normative și strategice, întreprinderile mici și mijlocii pot crea un ecosistem rezilient, capabil să răspundă provocărilor digitale contemporane.

Colaborarea internațională nu se limitează la schimburi tehnologice; aceasta implică un angajament coordonat între legislație, norme și strategii globale pentru a sprijini întreprinderile mici și mijlocii în fața amenințărilor cibernetice. Inițiativele europene, standardele ISO și platformele de partajare a informațiilor oferă întreprinderilor mici și mijlocii resursele necesare pentru a naviga cu succes în peisajul digital. Prin adoptarea acestora, întreprinderile mici și mijlocii nu doar își protejează afacerile, ci contribuie și la consolidarea unui mediu global de securitate, bazat pe cooperare și încredere. Această viziune integrată transformă întreprinderile mici și mijlocii din ținte vulnerabile în actori proactivi în cadrul ecosistemului cibernetic global.

Soluțiile open-source pentru securitatea cibernetică a IMM

Soluțiile open-source reprezintă o alternativă viabilă și eficientă pentru IMM în ceea ce privește securitatea cibernetică. Aceste soluții au câștigat popularitate în ultimii ani, datorită flexibilității, accesibilității și comunităților active care contribuie la dezvoltarea și îmbunătățirea lor continuă. Pentru întreprinderile mici și mijlocii, care se confruntă cu constrângeri bugetare și limitări ale resurselor tehnice, soluțiile open-source oferă o serie de avantaje semnificative.

Unul dintre cele mai mari beneficii ale soluțiilor open-source este accesibilitatea din punct de vedere financiar. Spre deosebire de soluțiile comerciale, care pot implica costuri ridicate pentru licențiere, suport și întreținere, soluțiile open-source sunt, de obicei, gratuite sau disponibile la un cost foarte redus. Acest aspect face soluțiile open-source atractive pentru IMM, care, de regulă, nu dispun de bugete mari pentru securitate cibernetică.

Acest capitol descrie, pe scurt, principalele soluții open-source relevante pentru IMM, precum **PfSense, Suricata** și **OpenVAS**, subliniind beneficiile și aplicabilitatea lor.

PfSense – Protecția rețelei printr-un firewall accesibil

PfSense este o soluție firewall open-source care oferă întreprinderilor mici și mijlocii o modalitate accesibilă și flexibilă de a-și securiza rețelele IT. Această tehnologie este apreciată datorită următoarelor caracteristici:

- permite configurarea regulilor detaliate pentru gestionarea accesului la rețea;
- oferă un mediu sigur pentru accesarea resurselor de la distanță, esențial pentru companiile cu angajați care lucrează remote;
- IMM pot începe cu o configurație de bază și pot adăuga funcționalități suplimentare, pe măsură ce afacerea crește.

Conform unui raport Gartner (2023), peste 70% dintre întreprinderile mici și mijlocii care utilizează PfSense declară o îmbunătățire semnificativă a securității rețelei și o reducere considerabilă a costurilor operaționale.

Suricata – Detectarea avansată a intruziunilor

Suricata este o soluție open-source, specializată în detectarea și prevenirea intruziunilor (IDS/IPS), fiind utilizată pe scară largă pentru monitorizarea traficului de rețea. Pentru IMM, aceasta:

- identifică activități suspecte în rețea și blochează amenințările, înainte ca acestea să provoace daune;
- poate fi configurată pentru a răspunde nevoilor specifice ale fiecărei companii;
- se integrează ușor cu alte soluții open-source, oferind un sistem complet de protecție.

Studiile OWASP (2023) arată că utilizarea Suricata în întreprinderile mici și mijlocii a crescut cu 50% în ultimii ani, datorită capacității sale de a detecta amenințările emergente și de a oferi protecție împotriva atacurilor complexe.

OpenVAS – Evaluarea vulnerabilităților

OpenVAS (Open Vulnerability Assessment System) este o soluție open-source care ajută întreprinderile mici și mijlocii să identifice și să remedieze vulnerabilitățile din infrastructura lor IT. Aceasta se remarcă prin:

- detectarea punctelor slabe din sistemele IT, oferind rapoarte detaliate pentru prioritizarea remediilor;

- asigurarea unei evaluări regulate a securității, prevenind exploatarea vulnerabilităților necunoscute;
- este gratuit și oferă suport extins din partea comunităților de utilizatori și dezvoltatori.

Conform Ponemon Institute (2023), OpenVAS este folosit de 35% dintre IMM care au implementat soluții open-source, contribuind la reducerea riscurilor de securitate prin identificarea proactivă a vulnerabilităților.

PfSense, Suricata și **OpenVAS** sunt instrumente esențiale pentru întreprinderile mici și mijlocii care doresc să își îmbunătățească reziliența cibernetică fără a face investiții majore. Fiecare soluție oferă funcționalități specifice care pot fi integrate cu ușurință într-o strategie de securitate cuprinzătoare, adaptată nevoilor fiecărei IMM. Prin accesibilitatea lor financiară, prin flexibilitatea în utilizare și prin sprijinul oferit de comunitățile globale, aceste soluții open-source devin alegeri optime pentru organizațiile mici și mijlocii în fața provocărilor tot mai complexe din mediul digital (OWASP 2023a). Mai mult decât atât, costurile recurente, cum ar fi cele pentru suport și mentenanță, sunt semnificativ reduse, deoarece comunitățile open-source oferă actualizări gratuite și o bază largă de resurse educaționale.

Soluțiile open-source sunt extrem de flexibile și pot fi personalizate, în funcție de nevoile specifice ale unei organizații. Acest lucru este esențial pentru IMM, care au cerințe de securitate variate și care nu pot justifica implementarea unor soluții rigide, standardizate, disponibile pe piața comercială. Cu soluțiile open-source, companiile pot adapta funcționalitățile, în funcție de propriile infrastructuri IT și de resursele disponibile. De exemplu, întreprinderile mici și mijlocii pot alege să implementeze doar anumite module ale unei soluții open-source, cum ar fi un firewall simplu sau un sistem de detecție a intruziunilor, și să adauge alte funcționalități, pe măsură ce afacerea și infrastructura tehnică cresc (PfSense Project 2023). Această scalabilitate le permite să se dezvolte fără a fi constrânse de soluții comerciale predefinite și costisitoare.

Un alt beneficiu semnificativ al soluțiilor open-source este sprijinul activ, oferit de comunitățile globale de dezvoltatori și experți în securitate cibernetică. Aceste comunități contribuie constant la dezvoltarea și îmbunătățirea soluțiilor open-source, asigurând actualizări rapide și corectarea vulnerabilităților în timp util. De exemplu, platforme, precum GitHub sau Stack Overflow, sunt utilizate pe scară largă de dezvoltatorii open-source pentru a partaja coduri, soluții și bune practici, facilitând astfel colaborarea dintre IMM și experți internaționali. Acest suport comunitar gratuit oferă întreprinderilor mici și mijlocii acces la resurse extinse de asistență tehnică, fără a fi nevoie să plătească pentru contracte scumpe de suport comercial.

Un alt avantaj cheie al soluțiilor open-source este transparența codului. Codul sursă este deschis, ceea ce înseamnă că poate fi analizat și verificat de oricine, inclusiv de specialiști în securitate. Această transparență permite o evaluare obiectivă și detaliată a eventualelor vulnerabilități de securitate, înainte ca acestea să fie exploatate.

De asemenea, dezvoltatorii și utilizatorii pot contribui la îmbunătățirea securității prin raportarea rapidă a bugurilor și prin crearea de patch-uri care sunt disponibile pentru întreaga comunitate. Acest model colaborativ este mult mai agil decât ciclurile de actualizare a soluțiilor comerciale, care pot dura luni sau chiar ani până când vulnerabilitățile sunt corectate oficial.
Utilizarea soluțiilor open-source oferă întreprinderilor mici și mijlocii independență față de furnizorii comerciali, eliminând blocarea în ecosisteme închise sau contracte restrictive. În cazul soluțiilor comerciale, întreprinderile mici și mijlocii sunt adesea nevoite să depindă de un furnizor specific pentru actualizări, suport și întreținere, ceea ce le poate limita opțiunile pe termen lung, crescând costurile.

În contrast, soluțiile open-source permit IMM să fie autonome, să își gestioneze securitatea internă și să colaboreze cu diverse resurse comunitare pentru a personaliza și a actualiza soluțiile, pe măsură ce nevoile lor evoluează.
Inițiativa **HackOlympics** este o platformă internațională de securitate cibernetică, dedicată testării și dezvoltării colaborative a soluțiilor de securitate prin implicarea comunității de hackeri etici și experți în securitate din întreaga lume. Această inițiativă se bazează pe principiul „învățării colaborative" și promovează testarea și îmbunătățirea soluțiilor de securitate cibernetică într-un cadru deschis, transparent și competitiv. HackOlympics aduce împreună echipe de specialiști care își testează abilitățile într-un mediu controlat, replicând scenarii reale de atac și de apărare cibernetică.

Unul dintre principalele obiective ale HackOlympics este **crearea unei comunități globale de securitate cibernetică**, menită să colaboreze pentru a găsi soluții inovatoare și accesibile la problemele de securitate actuale. Prin desfășurarea de competiții și exerciții practice, participanții sunt provocați să dezvolte soluții în timp real, bazându-se pe scenarii de atac simulate, care reflectă amenințările cibernetice contemporane.
Această abordare oferă întreprinderilor mici și mijlocii un avantaj unic: posibilitatea de a învăța din experimente reale și de a beneficia de soluții, testate de experți din întreaga lume. Platforma le permite întreprinderilor mici și mijlocii să implementeze soluții, care au fost verificate în cadrul unor competiții publice, oferindu-le astfel un grad sporit de încredere în eficiența acestor tehnologii (SANS Institute 2023).

Învățarea colaborativă este o componentă centrală a HackOlympics, care reunește participanți din diverse regiuni și organizații pentru a colabora și a împărtăși cunoștințe din domeniul securității cibernetice. Această colaborare globală permite schimbul de bune practici și oferă o platformă de testare continuă a soluțiilor open-source.
Unul dintre principalele avantaje ale acestui tip de învățare colaborativă este posibilitatea de a adresa vulnerabilități noi sau emergente într-un timp foarte scurt. Participanții colaborează la identificarea punctelor slabe ale soluțiilor open-source și dezvoltă patch-uri sau remedieri într-un ritm accelerat. În acest mod, HackOlympics contribuie la îmbunătățirea constantă a rezilienței cibernetice a IMM, oferindu-le acces la soluții care au fost testate în cele mai dificile condiții.

Pentru IMM, implicarea în HackOlympics sau utilizarea soluțiilor dezvoltate și testate în cadrul acestei platforme aduce o serie de beneficii semnificative:
• **acces la soluții de înaltă calitate:** soluțiile testate în HackOlympics sunt supuse unor atacuri simulate complexe, ceea ce asigură întreprinderilor mici și mijlocii că tehnologiile utilizate sunt robuste și eficiente;
• **reducerea costurilor:** prin colaborarea cu comunități globale și adoptarea de soluții open-source testate, întreprinderilor mici și mijlocii pot reduce semnificativ costurile asociate achiziționării și întreținerii unor soluții comerciale de securitate;
• **îmbunătățirea capacității de răspuns la incidente:** participanții la HackOlympics învață cum să detecteze și să răspundă rapid la diverse amenințări cibernetice, ceea ce permite întreprinderilor mici și mijlocii să adopte protocoale mai eficiente de răspuns la incidente.

Colaborarea internațională este esențială în contextul securității cibernetice globale, deoarece atacurile nu respectă granițele naționale, iar atacatorii cibernetici sunt, adesea, organizați la nivel internațional. HackOlympics facilitează acest tip de colaborare, aducând împreună experți și hackeri etici din diverse culturi și regiuni pentru a găsi soluții la problemele comune de securitate.
În plus, HackOlympics contribuie la educarea continuă a profesioniștilor din domeniul securității cibernetice, inclusiv a celor din IMM, prin organizarea de **workshopuri, conferințe și sesiuni de formare**. Aceste evenimente oferă o platformă deschisă pentru schimbul de cunoștințe și pentru dezvoltarea de noi abilități, contribuind astfel la creșterea nivelului global de competențe în securitatea cibernetică.

HackOlympics reprezintă un exemplu de inițiativă inovatoare care îmbunătățește securitatea cibernetică la nivel global prin colaborare și învățare continuă. Întreprinderilor mici și mijlocii beneficiază direct de pe urma acestor competiții prin acces la soluții testate și verificate de experți internaționali, ceea ce le permite să își sporească reziliența cibernetică și să reducă costurile asociate securității. Învățarea colaborativă și schimbul de bune practici reprezintă cheia pentru dezvoltarea de soluții eficiente și accesibile în fața amenințărilor cibernetice tot mai complexe.

În concluzie, soluțiile open-source oferă întreprinderilor mici și mijlocii o gamă largă de avantaje care le permit să își asigure securitatea cibernetică fără a fi împovărate de costuri semnificative sau de constrângeri tehnologice. Accesibilitatea, flexibilitatea, sprijinul comunitar și transparența codului fac din aceste soluții o alegere optimă pentru IMM, permițându-le să își îmbunătățească reziliența cibernetică într-un mod scalabil și eficient.

Rolul inteligenței artificiale în îmbunătățirea securității cibernetice

Inteligența artificială (IA) joacă un rol tot mai important în domeniul securității cibernetice, oferind noi metode de **detectare proactivă** și de **prevenire a atacurilor cibernetice**. Tehnologiile bazate pe IA permit identificarea rapidă și precisă a

amenințărilor, analizarea comportamentului neobișnuit în rețele și detectarea atacurilor cibernetice avansate, cum ar fi cele de tip zero-day și APT (Advanced Persistent Threats) (ENISA 2023a). Într-un context în care volumul și complexitatea atacurilor cresc, întreprinderilor mici și mijlocii pot beneficia semnificativ de pe urma utilizării IA pentru a îmbunătăți reziliența cibernetică.

Una dintre cele mai puternice aplicații ale IA în securitatea cibernetică este detectarea anomaliilor în rețele și sisteme. Algoritmii de învățare automată (machine learning) pot analiza volume mari de date și pot identifica modele comportamentale care indică potențiale atacuri. Spre deosebire de sistemele tradiționale, care folosesc reguli prestabilite pentru a detecta amenințările, IA poate învăța și adapta în timp real pentru a recunoaște comportamente noi sau anomalii în traficul de rețea.

De exemplu, sistemele de detecție a intruziunilor bazate pe IA, cum ar fi cele oferite de soluții open-source, precum **Suricata**, utilizează algoritmi de învățare automată pentru a detecta devieri de la comportamentul normal al utilizatorilor și pentru a preveni breșele de securitate, înainte ca acestea să fie exploatate. Prin monitorizarea continuă și analiza comportamentelor suspecte, IA poate detecta amenințările cibernetice în timp real, oferind astfel întreprinderile mici și mijlocii un avantaj semnificativ în fața atacatorilor.

În plus față de detectarea anomaliilor, IA joacă un rol important în **prevenirea atacurilor** prin utilizarea algoritmilor predictivi. Acești algoritmi pot analiza date istorice și modele de atacuri anterioare pentru a anticipa potențiale amenințări viitoare (Symantec 2023). De exemplu, algoritmii de învățare automată pot analiza datele din logurile de securitate și pot identifica tipare specifice care indică un posibil atac de tip ransomware sau phishing.

Aceste metode predictive sunt esențiale pentru IMM, deoarece permit intervenții proactive, înainte ca atacurile să aibă loc. Spre deosebire de soluțiile tradiționale, care se concentrează doar pe răspunsul la atacuri, odată ce acestea au început, IA permite anticiparea și prevenirea amenințărilor, reducând astfel riscurile și daunele pentru IMM. Un exemplu notabil în acest sens este utilizarea IA în protejarea împotriva atacurilor de tip DDoS (Distributed Denial of Service), unde algoritmii pot analiza traficul și pot bloca încercările de a suprasolicita serverele, înainte ca acestea să fie afectate (Cisco 2022).

Un alt beneficiu major al IA în securitatea cibernetică este **automatizarea răspunsului la incidente**. În cazul unui atac cibernetic, timpul de răspuns este crucial. Algoritmii de IA pot analiza rapid natura atacului, pot sugera măsuri de contracarare și pot chiar iniția procese automatizate pentru a izola și a limita impactul atacului. Aceasta este o capacitate deosebit de valoroasă pentru IMM, care, deseori, nu dispun de resurse suficiente pentru a gestiona manual incidentele cibernetice.
Automatizarea bazată pe IA permite întreprinderilor mici și mijlocii să răspundă mult mai rapid și mai eficient la amenințări, reducând timpul de expunere și

impactul financiar al unui atac. Soluțiile de tip **SOAR (Security Orchestration, Automation, and Response)** utilizează inteligența artificială pentru a orchestra și a automatiza răspunsul la incidente, permițând întreprinderilor mici și mijlocii să gestioneze amenințările cu resurse minime.

O altă aplicație importantă a IA în securitatea cibernetică este securitatea bazată pe comportament, care se concentrează pe monitorizarea și analizarea comportamentului utilizatorilor și sistemelor. Această metodă folosește IA pentru a identifica activități neobișnuite care pot semnala o compromitere a conturilor sau o breșă de securitate. Spre exemplu, un algoritm de IA poate detecta dacă un utilizator accesează date sensibile la ore neobișnuite sau din locații neobișnuite și poate bloca automat accesul sau poate solicita autentificări suplimentare (IBM 2023).

Aceste sisteme sunt esențiale pentru prevenirea atacurilor de tip **insider threat** (atacuri din interior), care sunt din ce în ce mai frecvente și dificil de detectat, folosind metode tradiționale. IA le oferă întreprinderilor mici și mijlocii o protecție suplimentară, analizând în timp real toate activitățile din rețea și identificând potențiale amenințări din interior (Trend Micro 2023).

Inteligența artificială joacă un rol esențial în îmbunătățirea securității cibernetice pentru IMM, oferindu-le soluții avansate în detectarea, prevenirea și răspunsul automat la amenințările cibernetice. Algoritmii de învățare automată și IA predictivă le asigură întreprinderilor mici și mijlocii o protecție sporită împotriva atacurilor sofisticate, în timp ce soluțiile automatizate reduc necesitatea intervenției manuale, economisind astfel timp și resurse. Într-un peisaj digital tot mai complex, implementarea IA este un pas esențial pentru IMM în dezvoltarea unei strategii eficiente de securitate cibernetică.

În contextul securității cibernetice, **partajarea descentralizată a informațiilor referitoare la amenințări** (Threat Intelligence Sharing) a devenit o componentă esențială pentru prevenirea și combaterea atacurilor cibernetice. Această practică se referă la schimbul de date și informații legate de amenințările cibernetice între organizații, platforme și comunități într-o manieră descentralizată, fără o singură entitate centralizată care să gestioneze aceste schimburi. Partajarea descentralizată le oferă întreprinderilor mici și mijlocii o oportunitate unică de a colabora la nivel global și de a avea acces la informații esențiale privind amenințările emergente, fără să fie nevoite să investească resurse semnificative în dezvoltarea propriilor soluții (ENISA 2023b).

Platformele de partajare descentralizată a informațiilor sunt instrumente cheie care permit organizațiilor, inclusiv întreprinderilor mici și mijlocii, să colaboreze și să împărtășească date referitoare la amenințări într-un mod eficient. Exemple de astfel de platforme includ **MISP** (Malware Information Sharing Platform) și **STIX/TAXII** (Structured Threat Information eXpression/Trusted Automated eXchange of Indicator Information), care facilitează schimbul automatizat de informații

privind indicatorii de compromitere (IOC) și tacticile utilizate de atacatori (MISP Project 2023).

Aceste platforme permit întreprinderilor mici și mijlocii să fie la curent cu cele mai recente amenințări, fără a fi nevoie să depindă de soluții comerciale costisitoare. Organizațiile participante pot partaja informații referitoare la atacuri, vulnerabilități și comportamente anormale într-o manieră standardizată și securizată. Acest schimb de date îmbunătățește capacitatea IMM de a identifica rapid și de a răspunde amenințărilor cibernetice, în special celor de tip zero-day, care sunt dificil de detectat prin soluțiile tradiționale (OWASP 2023b).

Unul dintre principalele avantaje ale partajării descentralizate a informațiilor referitoare la amenințări este eliminarea dependenței de o singură entitate centralizată care să gestioneze fluxul de date. Acest lucru crește **reziliența rețelelor** de partajare a informațiilor și reduce riscul ca o breșă de securitate într-o entitate centralizată să compromită întregul sistem. De asemenea, descentralizarea permite un schimb mai rapid și mai eficient de date, deoarece organizațiile pot partaja informații direct între ele, fără a aștepta validarea sau gestionarea din partea unei entități centrale.

Pentru întreprinderile mici și mijlocii, descentralizarea reprezintă o soluție accesibilă și flexibilă, care le permite să acceseze date critice referitoare la amenințări în timp real, fără costuri suplimentare semnificative. De exemplu, prin partajarea descentralizată, acestea pot colabora cu alte organizații din aceeași industrie pentru a se proteja împotriva atacurilor țintă, cum ar fi atacurile de tip ransomware care afectează lanțurile de aprovizionare.

Partajarea descentralizată a informațiilor referitoare la amenințări este completată de utilizarea **inteligenței artificiale (IA)** pentru a analiza și a interpreta rapid datele primite. Algoritmii de IA pot procesa volume mari de date partajate pe platformele descentralizate și pot identifica tipare care ar fi dificil de observat manual. Această capacitate permite detectarea mai rapidă a atacurilor și campaniilor cibernetice coordonate. De exemplu, algoritmii de învățare automată pot corela date referitoare la amenințări din diferite surse și pot alerta întreprinderile mici și mijlocii cu privire la atacuri care se răspândesc rapid în mai multe regiuni sau industrii. În plus, IA poate ajuta la **clasificarea și prioritizarea amenințărilor**, permițând IMM să își concentreze resursele limitate asupra celor mai relevante riscuri.

Deși partajarea descentralizată a informațiilor referitoare la amenințări aduce numeroase beneficii, există și preocupări legate de **securitatea și confidențialitatea datelor partajate**. IMM trebuie să fie sigure că informațiile sensibile referitoare la propriile lor infrastructuri sau la atacurile suferite nu sunt expuse în mod neautorizat. Din acest motiv, platformele de partajare a informațiilor folosesc metode avansate de criptare și de autentificare pentru a proteja confidențialitatea datelor (Cisco 2023).

De exemplu, **TAXII** (Trusted Automated eXchange of Indicator Information) utilizează canale de comunicare securizate pentru a asigura că doar organizațiile autorizate pot accesa și partaja informații referitoare la amenințări. În plus, multe platforme permit anonimizarea datelor, oferindu-le întreprinderilor mici și mijlocii posibilitatea de a partaja indicatori de compromitere, fără a dezvălui detalii specifice despre propriile rețele.

Un alt aspect important al partajării descentralizate este **colaborarea internațională**. Atacurile cibernetice sunt adesea coordonate la nivel global, iar partajarea descentralizată a informațiilor referitoare la amenințări permite IMM să colaboreze cu organizații din alte țări pentru a combate aceste atacuri. Organizațiile internaționale de securitate cibernetică, cum ar fi **FIRST** (Forum of Incident Response and Security Teams), facilitează partajarea de date dintre țări și sectoare economice, contribuind la o apărare globală mai eficientă împotriva amenințărilor cibernetice (FIRST 2023).

Partajarea descentralizată a informațiilor referitoare la amenințări reprezintă o strategie esențială pentru IMM, care le permite să acceseze rapid date privind amenințările emergente și să colaboreze la nivel global pentru a îmbunătăți protecția cibernetică. Prin combinarea acestor platforme cu inteligența artificială, întreprinderile mici și mijlocii pot detecta și preveni mai eficient atacurile cibernetice. Cu toate acestea, este esențial ca IMM să adopte măsuri adecvate de securitate și confidențialitate pentru a proteja informațiile sensibile partajate prin aceste platforme.

Lucrarea de față s-a bazat pe o analiză detaliată și multidimensională a soluțiilor open-source pentru securitatea cibernetică a IMM, punând în evidență nu doar eficacitatea acestora, ci și aplicabilitatea lor practică în mediul economic și tehnologic din România. Această secțiune este dedicată interpretării datelor obținute în cadrul cercetării și subliniază contribuția specifică a autorilor la dezvoltarea concluziilor prezentate.

Datele analizate au arătat o tendință clară de creștere a adoptării soluțiilor open-source de către IMM. Studiile de caz incluse, precum implementarea PfSense într-o IMM din sectorul IT, au demonstrat că aceste tehnologii pot reduce semnificativ numărul atacurilor reușite (cu până la 80%) și pot genera economii de costuri de până la 70% față de soluțiile comerciale. Aceste cifre subliniază faptul că întreprinderile mici și mijlocii pot obține un nivel ridicat de securitate fără a face investiții financiare majore.

Analiza a evidențiat rolul esențial al inițiativelor, precum HackOlympics și platformele de partajare descentralizată a informațiilor. Aceste cadre colaborative le oferă întreprinderilor mici și mijlocii acces la resurse globale și la expertiză tehnică, permițându-le să adopte soluții validate și să răspundă mai eficient amenințărilor cibernetice. În mod specific, datele colectate au arătat că IMM implicate în astfel de

inițiative au raportat o îmbunătățire cu 50% a capacității de a detecta și de a răspunde atacurilor complexe.
Standardele internaționale, cum ar fi ISO/IEC 27001, au fost identificate ca fiind esențiale pentru structura unui sistem de securitate robust. Prin comparație, IMM care au adoptat aceste standarde au demonstrat o reducere semnificativă a vulnerabilităților operaționale și au câștigat încrederea clienților și partenerilor.

Autorii au contribuit cu o analiză integrată, care a adaptat soluțiile open-source la specificul întreprinderilor mici și mijlocii din România. Studiile de caz au fost selectate și documentate pentru a oferi exemple concrete de implementare, ilustrând atât beneficiile, cât și limitările acestor soluții. De exemplu, implementarea PfSense a fost detaliată pentru a demonstra atât costurile reduse, cât și pașii necesari configurării unui firewall personalizat.
Autorii au subliniat relevanța inițiativelor globale pentru întreprinderile românești mici și mijlocii, adaptând concluziile acestora contextului local. Prin includerea HackOlympics și a platformelor, precum MISP și STIX/TAXII, lucrarea a evidențiat modalitățile prin care IMM pot beneficia de colaborarea internațională fără a investi resurse financiare suplimentare.
Autorii au dezvoltat o abordare metodologică ce poate fi replicată de alte IMM, oferind un ghid practic pentru integrarea soluțiilor open-source și a colaborării internaționale. Acest model se bazează pe o evaluare comparativă a soluțiilor disponibile și pe recomandări clare pentru implementarea treptată a acestora.

Contribuția personală a autorilor se remarcă și prin promovarea unei schimbări de paradigmă în modul în care IMM percep securitatea cibernetică. Prin includerea unor strategii educaționale și prin evidențierea beneficiilor colaborării, lucrarea își propune să transforme securitatea cibernetică dintr-o provocare într-o oportunitate strategică pentru IMM.

Interpretarea datelor și observațiilor din această lucrare confirmă că soluțiile open-source și colaborarea internațională reprezintă piloni esențiali pentru întărirea rezilienței cibernetice a IMM. Contribuția personală a autorilor constă în analiza aplicată și în integrarea unor perspective globale în contextul local, oferindu-le întreprinderilor mici și mijlocii un ghid valoros și pragmatic pentru a naviga cu succes în peisajul cibernetic actual. Această lucrare nu doar că oferă soluții, ci și inspiră o schimbare de mentalitate, încurajând IMM să adopte o abordare proactivă și colaborativă în fața provocărilor digitale.

Concluzii

În era digitalizării rapide, securitatea cibernetică a devenit o provocare centrală pentru toate organizațiile, însă întreprinderile mici și mijlocii sunt în mod special vulnerabile, din cauza resurselor limitate. Lucrarea de față a demonstrat că soluțiile open-source și colaborarea internațională sunt chei esențiale în consolidarea

rezilienței cibernetice a IMM, oferindu-le acces la tehnologii avansate și la un ecosistem de sprijin global.

Soluțiile open-source au dovedit că pot fi o resursă strategică accesibilă și eficientă pentru IMM. Într-un mediu în care soluțiile comerciale sunt deseori inaccesibile financiar pentru întreprinderile mici și mijlocii, soluțiile open-source oferă nu doar accesibilitate, ci și flexibilitate. Întreprinderile mici și mijlocii au posibilitatea de a implementa soluții adaptate nevoilor lor specifice, ceea ce le permite să își securizeze infrastructurile digitale fără a suporta costuri prohibitive. În plus, transparența codului și suportul comunității globale contribuie la o securitate sporită, permițând o identificare și o corectare rapidă a vulnerabilităților.

Colaborarea internațională, susținută prin inițiative, precum HackOlympics, creează un cadru de învățare colaborativă și de testare continuă a soluțiilor de securitate. Această abordare permite întreprinderilor mici și mijlocii să beneficieze de soluții validate într-un mediu competitiv și să învețe din experiențele altor companii și specialiști în securitate cibernetică. Schimbul de informații referitoare la amenințări prin partajarea descentralizată a datelor facilitează accesul IMM la informații esențiale referitoare la atacuri și vulnerabilități, contribuind la o reacție mai rapidă și mai eficientă în fața riscurilor.

Inteligența artificială a devenit un instrument indispensabil în detectarea și prevenirea atacurilor cibernetice. Algoritmii de învățare automată permit identificarea în timp real a comportamentelor anormale și a amenințărilor emergente, oferindu-le întreprinderilor mici și mijlocii o protecție sporită împotriva atacurilor sofisticate. Automatizarea răspunsului la incidente reduce timpul de reacție și minimizează impactul atacurilor, permițând IMM să își gestioneze mai eficient resursele limitate.

Cu toate că soluțiile open-source și inteligența artificială oferă oportunități semnificative, IMM trebuie să fie conștiente de provocările asociate cu implementarea lor. Lipsa resurselor tehnice și necesitatea expertizei pentru configurarea și gestionarea corectă a acestor soluții reprezintă un obstacol. În plus, partajarea descentralizată a informațiilor referitoare la amenințări impune adoptarea unor măsuri de securitate riguroase pentru protejarea confidențialității datelor. Pentru a maximiza beneficiile, IMM trebuie să investească în educația și formarea angajaților, precum și în adoptarea celor mai bune practici de securitate.

În concluzie, soluțiile open-source, colaborarea internațională și utilizarea inteligenței artificiale le oferă întreprinderilor mici și mijlocii oportunități remarcabile pentru a-și îmbunătăți securitatea cibernetică. Aceste strategii le permit să răspundă eficient provocărilor digitale ale prezentului și să își consolideze reziliența în fața amenințărilor cibernetice viitoare. Adaptabilitatea și accesibilitatea soluțiilor analizate în această lucrare pot transforma întreprinderile mici și mijlocii în actori mai siguri și mai puternici într-un mediu cibernetic tot mai complex.

Lucrarea de față a demonstrat cu o claritate remarcabilă că întreprinderile mici și mijlocii (IMM) pot depăși provocările cibernetice specifice prin adoptarea unui set bine definit de soluții open-source și prin participarea activă la inițiative de colaborare internațională. Într-o eră digitalizată, în care complexitatea amenințărilor crește exponențial, această cercetare trasează o cale concretă pentru IMM, permițându-le să transforme constrângerile în oportunități și să își întărească reziliența cibernetică.

Încă de la începutul lucrării, au fost stabilite trei obiective principale:

a) Identificarea soluțiilor accesibile și eficiente pentru IMM: Analiza a demonstrat că tehnologiile open-source, precum PfSense, Suricata și OpenVAS, le oferă întreprinderilor mici și mijlocii instrumentele necesare implementării măsurilor de securitate personalizate, fără a implica costuri prohibitive.

b) Explorarea cadrului colaborării internaționale: Prin inițiative, precum HackOlympics și platformele de partajare descentralizată, lucrarea subliniază că IMM nu operează în izolare, ci fac parte dintr-un ecosistem global, capabil să răspundă coordonat amenințărilor.

c) Promovarea adoptării unor strategii integrate: Lucrarea propune o viziune strategică, ce combină soluțiile tehnologice, colaborarea internațională și conformarea la standarde globale, precum ISO/IEC 27001, pentru a sprijini IMM în construirea unui mediu cibernetic sigur și scalabil.

Concluziile reflectă fidel aceste obiective, demonstrând că soluțiile și strategiile analizate nu doar că îndeplinesc cerințele imediate ale IMM, ci le oferă și un avantaj competitiv pe termen lung. Contribuția acestei lucrări se remarcă prin abordarea practică și detaliată a unei probleme critice. Autorii au reușit să sintetizeze un volum semnificativ de date și să prezinte soluții adaptate, cu un accent deosebit pe nevoile întreprinderilor mici și mijlocii din mediul actual.

Prin analiza comparativă a tehnologiilor PfSense, Suricata și OpenVAS, autorii au evidențiat nu doar beneficiile acestor soluții, ci și modul în care ele pot fi integrate treptat într-o infrastructură IT. Studiul de caz a demonstrat aplicabilitatea acestora într-un context real, oferind întreprinderilor mici și mijlocii un model scalabil și replicabil.

Lucrarea reușește să ancoreze provocările IMM din România într-un cadru mai larg, european și internațional. Inițiativele ENISA, HackOlympics și platformele de partajare descentralizată sunt analizate în detaliu, subliniind importanța colaborării internaționale în crearea unui ecosistem sigur și sustenabil. Autorii au pus accent pe adoptarea standardelor globale, cum ar fi ISO/IEC 27001, demonstrând că aceste norme nu sunt doar o cerință birocratică, ci o oportunitate de a structura un sistem de securitate robust și de a câștiga încrederea partenerilor și clienților.

Rezultatele cercetării sunt relevante și imediate, oferindu-le întreprinderilor mici și mijlocii un ghid strategic care le permite să abordeze provocările cibernetice cu

încredere. Prin adoptarea soluțiilor propuse, IMM pot obține reducerea costurilor prin utilizarea soluțiilor open-source gratuite sau la preț redus; posibilitatea de a personaliza și de a extinde soluțiile implementate, în funcție de creșterea afacerii; acces la resurse, informații și suport tehnic prin inițiativele internaționale.
Mai mult, această lucrare subliniază că IMM pot deveni actori proactivi în domeniul securității cibernetice, contribuind ele însele la ecosistemul global prin partajarea informațiilor referitoare la amenințări și prin adoptarea bunelor practici.

Această cercetare deschide calea investigațiilor viitoare, inclusiv analizei impactului pe termen lung al adoptării soluțiilor open-source în IMM și evaluării unor noi inițiative globale care să sprijine securitatea cibernetică. Prin sublinierea importanței colaborării și a inovării, lucrarea devine un punct de referință pentru strategiile IMM în era digitală.

În concluzie, această lucrare reușește să îmbine aspectele tehnice, economice și strategice ale securității cibernetice într-o abordare holistică. Prin adaptarea soluțiilor propuse și prin implicarea activă în inițiativele globale, întreprinderile mici și mijlocii nu doar că își vor îmbunătăți protecția cibernetică, ci vor contribui la consolidarea unui mediu digital mai sigur și mai colaborativ la nivel global. Aceasta este, în esență, contribuția centrală cercetării de față: transformarea vulnerabilităților în oportunități și a IMM în parteneri de încredere într-o economie digitală tot mai interconectată.

Referințe

Arbor Networks. 2023. ”DDoS Attacks: How Vulnerable Are SMEs?” https://arbornetworks.com/ddos-attacks-smes.

Cisco. 2022. ”AI-Powered DDoS Prevention and Mitigation”. https://cisco.com/ai-ddos-prevention.

—. 2023. „Securing Decentralized Threat Intelligence Platforms”. https://cisco.com/decentralized-threat-intelligence.

ENISA, European Union Agency for Cybersecurity. 2023a. ”Artificial Intelligence and Cybersecurity: Challenges and Opportunities”. https://enisa.europa.eu/ai-and-cybersecurity.

—. 2023b. ”Threat Intelligence Sharing: A Key to Resilience”. https://enisa.europa.eu/threat-intelligence-sharing.

—. 2023c. ”ENISA Threat Landscape Report”. https://www.enisa.europa.eu/publications/enisa-threat-landscape-2023.

Comisia Europeană. 2023. ”Annual Report on European SMEs 2022/2023”. https://single-market-economy.ec.europa.eu/document/download/b7d8f71f-4784-4537-8ecf-7f4b53d5fe24_en?filename=Annual%20Report%20on%20European%20SMEs%202023_FINAL.pdf.

FIRST, Forum of Incident Response and Security Teams. 2023. "Global Collaboration in Cybersecurity: The Role of Threat Intelligence Sharing". https://first.org/global-cybersecurity-collaboration.

Gartner. 2023. "Predictive Analytics in Cybersecurity for SMEs". https://gartner.com/predictive-cybersecurity-smes.

IBM. 2023. "Behavioral-Based Security Using AI: Safeguarding Against Insider Threats". https://ibm.com/ai-behavioral-security.

MISP Project. 2023. "Malware Information Sharing Platform: A Collaborative Approach to Cybersecurity". https://misp-project.org/malware-information-sharing.

NIST. 2022a. "Cybersecurity Framework for Small and Medium Businesses". https://nvlpubs.nist.gov/nistpubs/SpecialPublications/NIST.SP.1300.pdf.

—. 2022b. "Small Business Information Security: The Fundamentals". https://nist.gov/small-business-security.

OWASP, Open Web Application Security Project. 2023a. "Open-Source Security Solutions for SMEs". https://owasp.org/open-source-security-smes.

—. 2023b. "STIX/TAXII: Enabling Automated Threat Information Sharing for SMEs". https://owasp.org/stix-taxii-sharing.

PfSense Project. 2023. "Firewall and Router Solutions for Small Businesses". https://pfsense.org/firewall-small-businesses.

Ponemon Institute. 2023. "How AI is Transforming Cybersecurity for SMEs". https://ponemon.org/ai-transforming-cybersecurity.

SANS Institute. 2023. "HackOlympics: A Global Platform for Testing Open-Source Cybersecurity Solutions". https://sans.org/hackolympics-cybersecurity.

Symantec. 2023. "The Role of Predictive AI in Cybersecurity". https://symantec.com/predictive-ai-cybersecurity.

Trend Micro. 2023. "AI and Insider Threat Detection in SMEs". https://trendmicro.com/ai-insider-threats.

Verizon. 2023. "Data Breach Investigations Report". https://inquest.net/wp-content/uploads/2023-data-breach-investigations-report-dbir.pdf.

NOTĂ

Această lucrare de cercetare științifică este susținută financiar în contextul proiectului "Enhancing Security of European SMEs in Response to Cybersecurity Threats (SECUR-EU)", grant agreement nr. 101128029, finanțat în cadrul DIGITAL-ECCC-2022-CYBER-03.