PISA
Platforma pentru Inițiative de Securitate și Apărare

DCAF Geneva Centre for Security Sector Governance

Sweden
Sverige

Dinamica securității cibernetice în Republica Moldova: răspuns la amenințările complexe

Sanda SANDU,
Expertă în domeniul securității și politici de bună guvernare

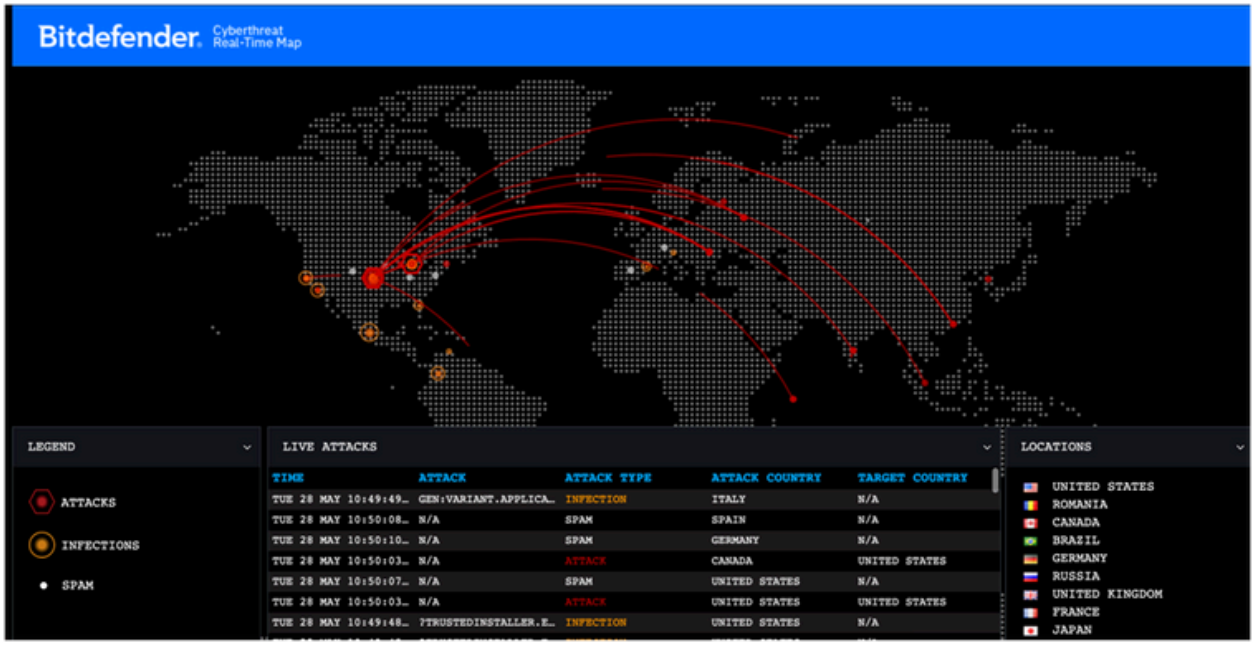
MATERIALUL ESTE ELABORAT ÎN CONTEXTUL PROIECTULUI „CAMPANIA DE INFORMARE PRIVIND OBIECTIVELE POLITICILOR DE SECURITATE ÎN REPUBLICA MOLDOVA” IMPLEMENTAT DE PLATFORMA PENTRU INIȚIATIVE DE SECURITATE ȘI APĂRARE (PISA) ȘI SUSȚINUT DE CENTRUL DE LA GENEVA PENTRU GUVERNAREA SECTORULUI DE SECURITATE (DCAF), ÎN CADRUL PROIECTULUI „CONSOLIDAREA GUVERNĂRII SECTORULUI DE SECURITATE ÎN MOLDOVA”, FINANȚAT DE SUEDIA.

Securitatea cibernetică reprezintă activitatea sau procesul, abilitatea, capacitatea sau starea prin care sistemele de informații și comunicații ce susțin sau afectează rezultatele dezvoltării, precum și informațiile conținute în acestea, sunt protejate împotriva daunelor, utilizării sau modificării neautorizate sau exploatării.

În era digitală, securitatea cibernetică a devenit un aspect esențial al securității naționale și internaționale. Securitatea cibernetică implică un set de măsuri și practici concepute pentru a proteja sistemele informatice, rețelele și datele împotriva accesului neautorizat, utilizării abuzive, divulgării, perturbării, modificării sau distrugerii. Este un domeniu multidisciplinar care necesită colaborare între guverne, sectorul privat și cetățeni, pentru a asigura un mediu digital sigur și de încredere.

Peisajul amenințărilor cibernetice este dinamic și în continuă evoluție. Acesta include o gamă variată de atacuri și tehnici utilizate de actori rău intenționați, inclusiv:

- **Atacuri Phishing.** Email-uri și mesaje frauduloase care încearcă să obțină informații sensibile, cum ar fi parole și date bancare, prin păcălirea utilizatorilor. Potrivit unui raport de la PhishMe [1], 91% din toate atacurile cibernetice încep cu un email de phishing.
- **Ransomware.** Software malițios care criptează datele victimelor și solicită o recompensă pentru decriptare. Potrivit Cybersecurity Ventures, costul anual global al criminalității cibernetice este estimat să ajungă la 9,5 trilioane USD în 2024. La aceasta se adaugă costul în creștere al daunelor rezultate din criminalitatea cibernetică, care se așteaptă să ajungă la 10,5 trilioane USD până în 2025 [2].
- **Atacuri DDoS** (Distributed Denial of Service). Inundarea unui server sau a unei rețele cu trafic excesiv pentru a le face indisponibile. Atacurile DDoS au crescut continuu în dimensiune și sofisticare, dar 2023 a accelerat această tendință într-un ritm neprevăzut [3].



Sursa: Bitdenender [5], Amenințări cibernetice, Hartă în timp real

Dezvoltarea rapidă a tehnologiei a adus beneficii semnificative, dar și provocări în ceea ce privește securitatea cibernetică. Tehnologiile emergente, cum ar fi Internetul Lucrurilor (IoT) [6], inteligența artificială (AI) [7] și

---

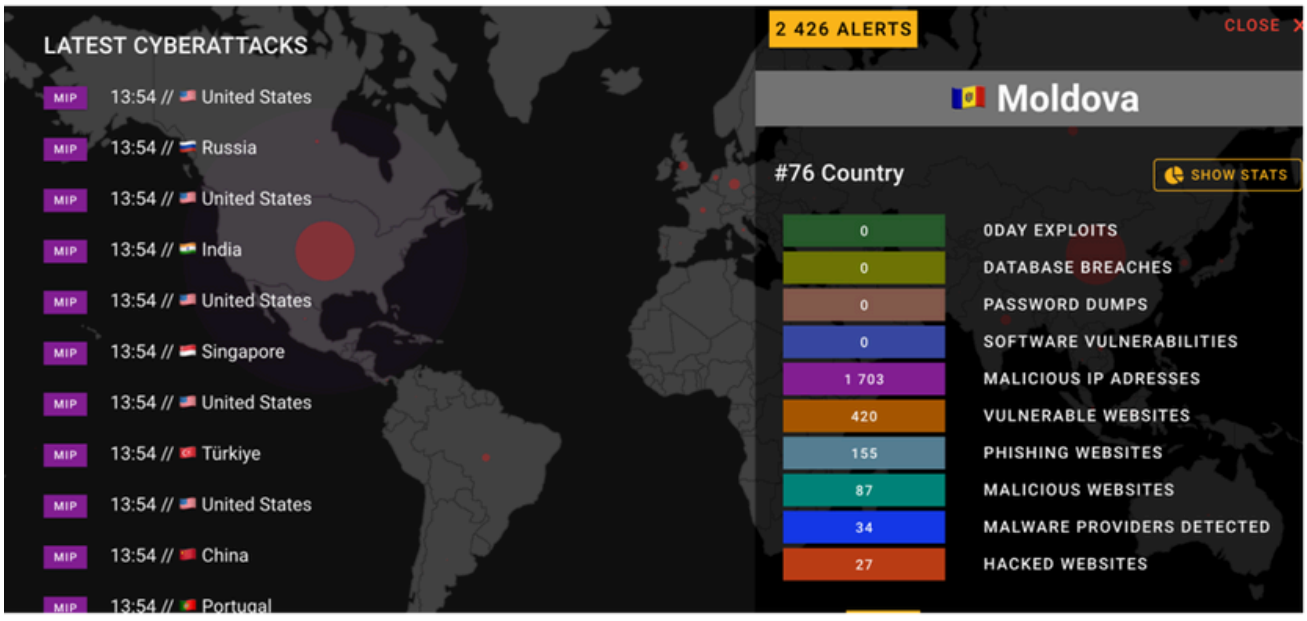
[1] COFENSE / PhishMe - Human Phishing Defense Solution. Protectie anti-phishing prin educarea utilizatorului. https://www.netsafe.ro/phishme-solutie-antiphishing/
[2] 2023 Official Cybercrime Report
https://www.esentire.com/resources/library/2023-official-cybercrime-report
[3] A Retrospective on DDoS Trends in 2023 and Actionable Strategies for 2024
https://www.akamai.com/blog/security/a-retrospective-on-ddos-trends-in-2023
[4] 2023 in Review: DDoS Attacks Report by StormWall. https://stormwall.network/ddos-attack-report-2023
[5] Bitdefender. https://threatmap.bitdefender.com/
[6] IoT este o rețea de dispozitive electronice (așa-numite și „lucruri"), care conțin senzori, software și alte tehnologii care sunt conectate la internet pentru a face schimb de date și pentru a interacționa cu alte dispozitive și oameni (denumiți, de asemenea, și „utilizatori").https://courses.minnalearn.com/ro/courses/emerging-technologies/the-internet-of-things/an-introduction-to-the-internet-of-things/
[7] Inteligența artificială. https://pisa.md/wp-content/uploads/2023/07/inteligenta-artificiala.jpg

blockchain [8], au deschis noi oportunități pentru inovare, dar au creat și noi vectori de atac și vulnerabilități. Este esențial ca dezvoltarea tehnologică să fie însoțită de măsuri de securitate robuste pentru a asigura protecția împotriva amenințărilor cibernetice.

Numărul mare de atacuri cibernetice, care se desfășoară simultan și sunt coordonate de actori statali și non-statali reprezintă o provocare majoră pentru securitatea globală. Aceste atacuri sunt adesea bine finanțate și executate cu precizie, având scopuri variate, de la spionaj economic și militar la sabotaj și perturbarea sistemelor critice.

1. ***Actori statali*** - statele folosesc atacurile cibernetice ca instrumente de război hibrid și spionaj împotriva altor state, pentru a obține informații strategice sau pentru a perturba infrastructurile critice. Un exemplu notabil este atacul asupra rețelei energetice ucrainene în anul 2015, atribuit grupului APT Sandworm [9], despre care se spune că are legături cu guvernul rus. Acest grup și-a intensificat semnificativ operațiunile cibernetice pe fondul conflictului din Ucraina. Într-adevăr, ele prezintă un amestec strategic de spionaj, perturbare și dezinformare pentru a submina adversarii. Mai mult, amenințarea imediată reprezentată de APT 44 subliniază o provocare critică la adresa rezistenței globale a securității cibernetice și a stabilității relațiilor internaționale [10].
2. ***Actori non-ntatali*** - grupurile de hackeri și organizațiile criminale cibernetice utilizează atacurile cibernetice pentru a obține beneficii financiare sau pentru a promova agende politice. Doar în SUA, conform FBI's Internet Crime Complaint Center (IC3), pentru anul 2023 [11] a fost înregistrat un număr record de plângeri din partea publicului american: 880.418 plângeri cu pierderi potențiale și care depășesc 12,5 miliarde USD, ceea ce reprezintă o creștere de aproape 10% a reclamațiilor și o creștere cu 22% a pierderilor față de 2022.

Republica Moldova ca parte a comunității internaționale, se confruntă cu provocări crescânde în domeniul securității cibernetice. Transformarea digitală rapidă și adaptarea tehnologiilor moderne expun statul și cetățenii săi la un număr tot mai mare de atacuri cibernetice. Acestea variază de la atacuri de tip phishing și ransomware la amenințări avansate și persistente (APT) care vizează infrastructurile critice ale statului.



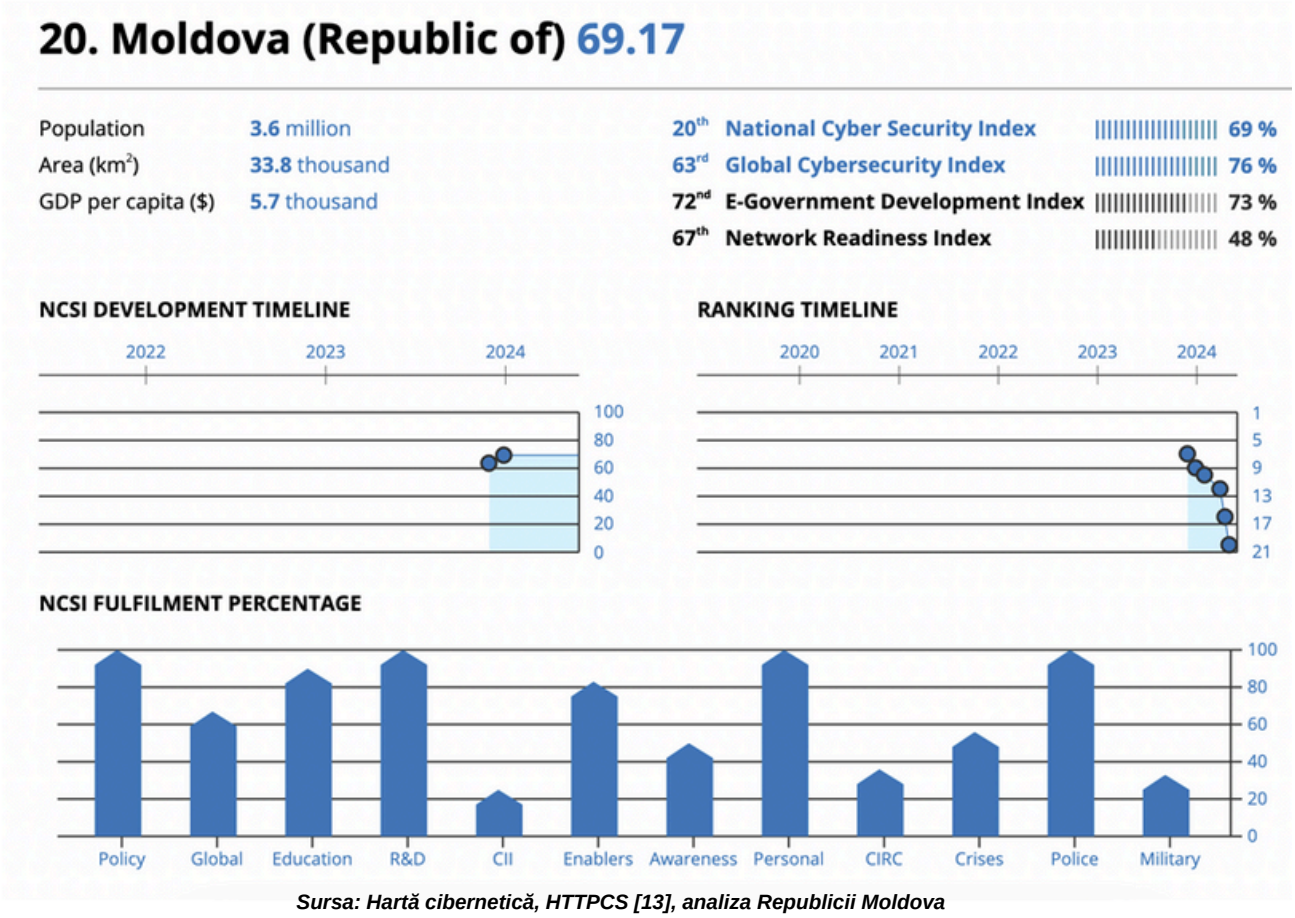
Sursa: Hartă cibernetică, HTTPCS [12], analiza Republicii Moldova

[8] Blockchain este un registru partajat, imuabil, care facilitează procesul de înregistrare a tranzacțiilor și de urmărire a activelor într-o rețea de afaceri https://www.ibm.com/topics/blockchain
[9] Sandworm Cyberattackers Down Ukrainian Power Grid During Missile Strikes.
https://www.darkreading.com/ics-ot-security/sandworm-cyberattackers-ukrainian-power-grid-missile-strikes
[10] The APT44 Sandworm: A Threat Assessment. https://greydynamics.com/the-apt44-sandworm-a-threat-assessment/
[11] Internet Crime report 2023. https://www.ic3.gov/media/pdf/annualreport/2023_ic3report.pdf
[12] Global Cybersecurity Index.
https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx

Conform Global Cybersecurity Index (GCI) — Republica Moldova este plasată pe locul 63. GCI clasifică nivelul de dezvoltare al fiecărei țări în funcție de măsurile juridice, tehnice și organizaționale ale acesteia, precum și de dezvoltarea capacității și cooperării în domeniul securității cibernetice.

Deși GCI evaluează măsurile tehnice de securitate cibernetică ale Moldovei ca fiind „relativ puternice", organizarea și dezvoltarea capacității sale trebuie îmbunătățite. Alte recomandări din partea GCI sunt: dezvoltarea unei strategii privind protecția infrastructurii critice și implementarea sistematică a sistemelor de management al securității informațiilor, care va necesita o creștere a numărului de ministere de resort certificate cu standardul ISO 27001.

Conform Global Cybersecurity Index (GCI) — Republica Moldova este plasată pe locul 63. GCI clasifică nivelul de dezvoltare al fiecărei țări în funcție de măsurile juridice, tehnice și organizaționale ale acesteia, precum și de dezvoltarea capacității și cooperării în domeniul securității cibernetice. Deși GCI evaluează măsurile tehnice de securitate cibernetică ale Moldovei ca fiind „relativ puternice", organizarea și dezvoltarea capacității sale trebuie îmbunătățite. Alte recomandări din partea GCI sunt: dezvoltarea unei strategii privind protecția infrastructurii critice și implementarea sistematică a sistemelor de management al securității informațiilor, care va necesita o creștere a numărului de ministere de resort certificate cu standardul ISO 27001.



Sursa: Hartă cibernetică, HTTPCS [13], analiza Republicii Moldova

Conform raportului USAID și datelor furnizate de CERT-GOV-MD (Computer Emergency Response Team of the Government of Moldova), numărul atacurilor cibernetice a crescut semnificativ în ultimii ani [14].
Tipologia atacurilor:

- **Phishing**: Email-uri frauduloase menite să obțină informații sensibile de la utilizatori. În 2023, a fost raportată o creștere de 45% a atacurilor de phishing față de anul anterior.

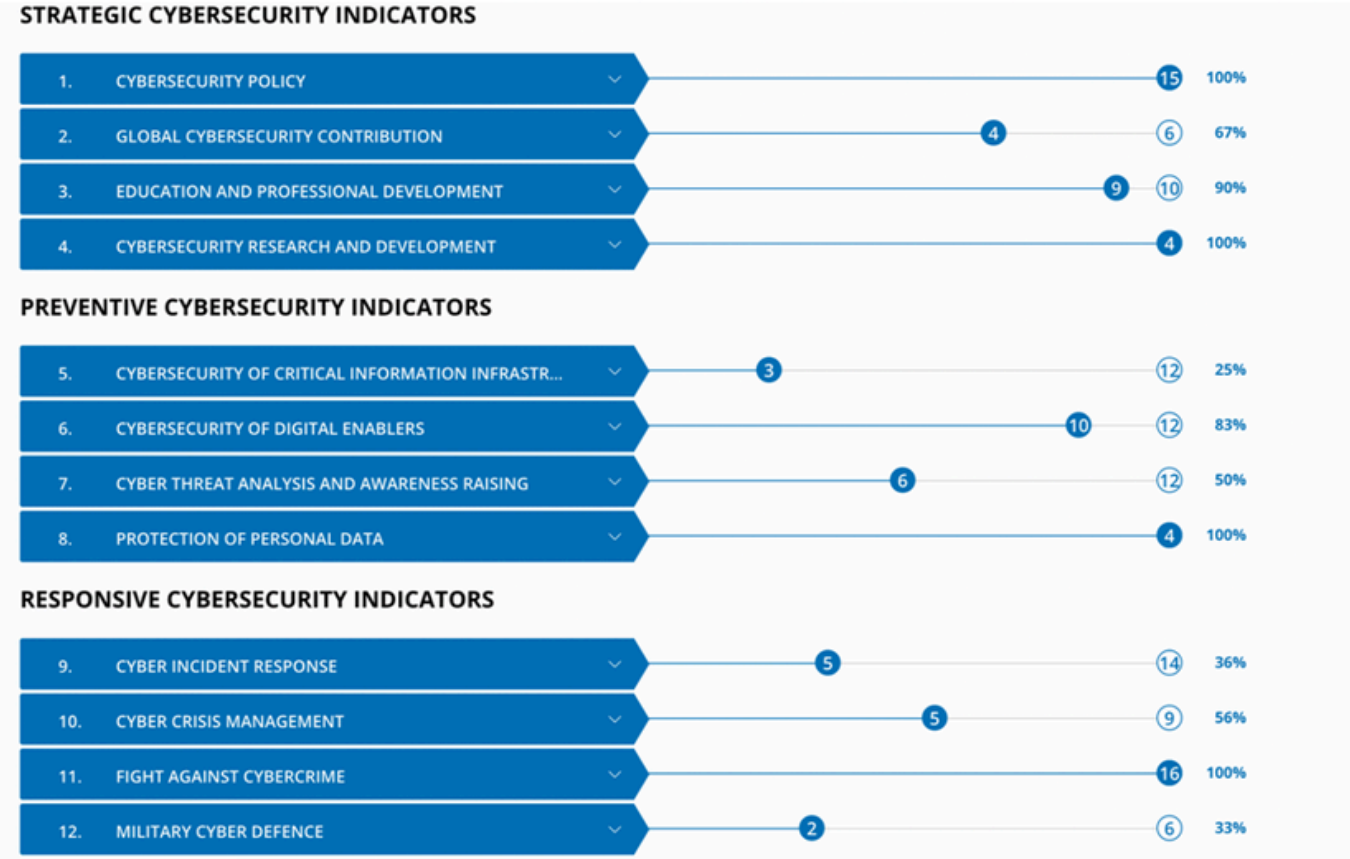
[13] Global Cybersecurity Index.
https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx
[14] Evaluarea ecosistemului digital la nivel de țară digital ecosystem country assessment (DECA)
https://www.usaid.gov/sites/default/files/2023-01/Moldova%20DECA%20%28Romanian%29.pdf

- **Ransomware**: Software malițios care blochează accesul la date până la plata unei recompense. Cazurile de ransomware au crescut cu 50% în ultimii doi ani, afectând atât instituții publice, cât și companiile private.
- **DDoS (Distributed Denial of Service)**: Atacuri care inundă serverele cu trafic pentru a le face indisponibile. Atacurile DDoS au crescut în intensitate, cu un număr de 250 de incidente raportate doar în primul trimestru al anului 2023.
- **APT (Advanced Persistent Threats)**: Atacuri bine finanțate și orchestrate, de obicei de către state sau grupuri organizate. APT-urile sunt dificil de detectat și pot cauza daune semnificative infrastructurilor critice.

Statistici relevante:

- În 2023, au fost raportate peste 1,000 de incidente cibernetice majore.
- Creșterea cu 30% a atacurilor de tip phishing față de anul precedent.

Implementarea și capacitatea securității cibernetice nu au ținut pasul cu dezvoltarea politicilor. Guvernul a introdus constant măsuri de reglementare și politici privind securitatea cibernetică într-un efort de armonizare la protocoalele UE. Cu toate acestea, când vine vorba de implementare, este nevoie de un sprijin sporit, care se explică parțial printr-un ecosistem de securitate cibernetică fragmentat, o disponibilitate redusă de specialiști în domeniul securității cibernetice și lacune în capacitatea tehnică guvernamentală. Alocarea resurselor financiare și umane este, de asemenea, inadecvată pentru nevoile crescânde și schimbătoare de securitate cibernetică. Echipa guvernamentală de intervenție în caz de urgență computerizată (CERT) este una mică și totuși servește drept punct de legătură pentru toate comunicările și pentru raportarea incidentelor de securitate cibernetică. Alte organisme guvernamentale, cum ar fi cele din cadrul Procuraturii Generale și Ministerului Afacerilor Interne, abordează problemele de securitate cibernetică [15].



Sursa: NCSI, Moldova, Raport decembrie 2023, https://ncsi.ega.ee/country/md/?pdfReport=1

[15] Evaluarea ecosistemului digital la nivel de țară digital ecosystem country assessment (DECA) https://www.usaid.gov/sites/default/files/2023-01/Moldova%20DECA%20%28Romanian%29.pdf

Răspunsul la amenințările cibernetice moderne din orice țară necesită un efort coordonat al numeroaselor instituții. Coordonarea necesită desemnarea unor roluri și responsabilități clare instituțiilor relevante și capacitatea acestora de a le îndeplini. Echipele naționale de intervenție în caz de urgență informatică sau incidente de securitate (CERT/CSIRT) acționează ca puncte unice importante de contact pentru toate părțile interesate (guvernamentale, sectorul privat și cel societal). De regulă, aceștia sunt responsabili pentru schimbul de informații și gestionarea coordonată a răspunsurilor guvernamentale la incidentele de securitate cibernetică. În luna februarie 2024, Republica Moldova a lansat Agenția Națională pentru Securitate Cibernetică, care are obiectivul de a proteja infrastructura critică a statului și a societății de atacuri cibernetice și va asigura un nivel ridicat de securitate pentru rețelele și sistemele IT ale instituțiilor publice și private [16]. De asemenea, cadrul instituțional privind asigurarea securității cibernetice este partajat între următoarele instituții: Ministerul Economiei, Serviciul Tehnologia Informației și Securitate Cibernetică (STISC), Echipa de intervenție în caz de urgență informatică din cadrul STISC (CERT-GOV-MD), Agenția de Guvernare Electronică, Ministerul Apărării, Ministerul Afacerilor Interne, Serviciul Informații și Securitate, Procuratura Generală, Cancelaria de Stat și Comisia securitate națională, apărare și ordine publică a Parlamentului Republicii Moldova.

Atacurile DDOS și ingineria socială sunt cele mai frecvente tipuri de amenințări cibernetice. Serviciul de Informații și Securitate al Republicii Moldova descrie patru tipuri predominante de amenințări de securitate cibernetică: atacuri DDOS, phishing prin e-mailuri de stat, atacuri prin forță brută (brute force) pentru obținerea accesului la sistemele de informații guvernamentale și deturnarea paginilor web oficiale. CERT-GOV-MD a confirmat că cele mai frecvente amenințări cibernetice în Moldova includ atacuri DDOS, plăți frauduloase (legate de serviciile digitale), inginerie socială (phishing, momeală, știri false, dezinformare) și furturi ale datelor.

RECOMANDĂRI

- **Reziliența cibernetică** este capacitatea de a rezista și de a se recupera rapid în urma atacurilor cibernetice. În Republica Moldova, dezvoltarea acestei reziliențe este necesară pentru protejarea infrastructurii critice, cum ar fi rețelele energetice, sistemele financiare și comunicațiile. Multe dintre aceste infrastructuri utilizează tehnologii vechi, vulnerabile la atacuri, necesitând implementarea unor protocoale stricte de securitate și sisteme eficiente de backup. Un audit continuu al securității și adoptarea celor mai bune practici internaționale sunt esențiale pentru consolidarea securității acestor infrastructuri.
- **Capacitatea de răspuns rapid și eficient la atacurile cibernetice** este esențială pentru minimizarea impactului acestora prin consolidarea echipelor CERT la nivel național, dotarea acestora cu resurse și tehnologie de ultimă oră, și organizarea de exerciții și simulări regulate. Parteneriatele internaționale cu organizații precum ENISA și NATO oferă acces la informații și resurse esențiale pentru prevenirea și combaterea atacurilor cibernetice, în timp ce schimbul de informații cu alte state ajută la abordarea amenințărilor comune.
- **Educația și conștientizarea publicului sunt esențiale** pentru protejarea cetățenilor împotriva atacurilor cibernetice. Inițierea unor campanii naționale de conștientizare, crearea de ghiduri și resurse accesibile pentru cetățeni și întreprinderi mici, precum și introducerea securității cibernetice în curriculumul școlar și universitar contribuie la creșterea nivelului de protecție. Programele de formare continuă pentru profesioniștii IT și publicul larg, alături de investițiile în start-up-uri și colaborarea cu sectorul privat, sunt esențiale pentru dezvoltarea unui ecosistem de securitate cibernetică în Moldova.

[16] Moldova launches new national cybersecurity bodies during first Cybersecurity Forum.
https://eufordigital.eu/moldova-launches-new-national-cybersecurity-bodies-during-first-cybersecurity-forum/