PISA
Platforma pentru Inițiative de Securitate și Apărare

DCAF Geneva Centre for Security Sector Governance

Sweden
Sverige

Moldova și securitatea cibernetică: intețirea atacurilor pe fundal de război pune sub lupă politicile pentru asigurarea unui ecosistem digital de nădejde

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.

În 2023, în Republica Moldova au fost raportate peste 1,000 de incidente cibernetice majore. Este cel mai mare număr înregistrat până acum, creșterea cea mai mare revenindu-le atacurilor phishing. În general, Moldova se confruntă cu patru tipuri predominante de amenințări cibernetice, potrivit Serviciului de Informații și Securitate acestea sunt: atacurile 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. Cele mai periculoase sunt considerate atacurile DDOS (Distributed Denial of Service), ce semnifică inundarea unui server sau a unei rețele cu trafic excesiv pentru a le face indisponibile. Acestea au crescut constant în dimensiune și sofisticare, dar 2023 a accelerat tendința de creștere într-un ritm neprevăzut. Geopolitica este un factor-cheie ce explică frecvența lor fără precedent și în țări precum SUA, Rusia, Ucraina, Israel, Germania, Franța, Polonia și Emiratele Arabe Unite. Numărul mare de atacuri cibernetice, care se desfășoară simultan și sunt coordonate de actori statali și non-statali reprezintă actualmente o provocare majoră pentru securitatea globală.

În aceste condiții, Republica Moldova a luat măsuri care să asigurare un ecosistem digital de încredere. În luna februarie 2024, bunăoară, a fost creată Agenția Națională pentru Securitate Cibernetică. Obiectivul acesteia e să protejeze infrastructura critică a statului și a societății de atacuri cibernetice și să asigure un nivel ridicat de securitate pentru rețelele și sistemele IT ale instituțiilor publice și private. Cadrul instituțional privind asigurarea securității cibernetice este partajat în prezent 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.

Într-un efort de armonizare la protocoalele UE, guvernul a introdus constant măsuri de reglementare și politici privind securitatea cibernetică. Implementarea acestora și crearea de capabilități nu au ținut, însă, pasul cu dezvoltarea politicilor. Astfel, se poate constata că Republica Moldova are astăzi 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.

Ce recomandă în primul rând - nevoia de sporire a rezilienței cibernetice (capacitatea de a rezista și de a se recupera rapid în urma atacurilor cibernetice) e necesitatea acută de protejare a 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 publicului pentru conștientizarea necesității de protejare a cetățenilor împotriva atacurilor cibernetice devine esențială. Astfel, se impune inițierea unor campanii naționale de conștientizare a importanței acestei securități, crearea de ghiduri și resurse accesibile pentru cetățeni și întreprinderi mici, precum și introducerea securității cibernetice în curriculumul școlar și universitar. Programele de formare continuă pentru profesioniștii IT și publicul larg, alături de investițiile în start-up-uri și colaborarea cu sectorul privat, ar contribuie hotărâtor la dezvoltarea unui ecosistem de securitate cibernetică în Moldova.

Află mai multe la acest subiect din opinia integrală:
bit.ly/3RYXgUu