DIRECTORATUL NAȚIONAL
DE SECURITATE CIBERNETICĂ

Nr. DGS/R/58 din 30.04.2025

Riscurile cibernetice în sectorul educației - învățământul liceal din România

- Raport workshop -

30 aprilie 2025

TLP:GREEN

Sumar executiv

Nivelul de risc cibernetic al sectorului, rezultat în urma workshop-ului, a fost evaluat la un **nivel MEDIU**, ceea ce denotă o expunere semnificativă la amenințările cibernetice existente. Situația actuală impune necesitatea adoptării unor măsuri de securitate cibernetică și a intensificării eforturilor pentru creșterea nivelului de **conștientizare și instruire** la nivel instituțional.

Este necesar să fie acordată o atenție sporită asupra principalelor **trei riscuri** rezultate: (1) riscul unei posturi de securitate cibernetică slabe din cauza bugetului, resurselor și lipsei de prioritate pentru domeniul securității cibernetice; (2) risc de răspândire a malware-ului prin dispozitive de stocare portabile, utilizate fără măsuri de control sau scanare și (3) risc de compromitere a datelor și sistemelor informatice din cauza lipsei de conștientizare și instruire a personalului.

Pentru reducerea nivelului de risc și creșterea nivelului de securitate cibernetică în sectorul liceal, a fost elaborat un set de **recomandări** ce vizează formarea profesională, utilizarea de noi tehnologii, standardizarea practicilor și consolidarea cunoștințelor în domeniul securității cibernetice.

Introducere

Nivelul ridicat al amenințărilor cibernetice care vizează sectorul liceal, precum și introducerea rapidă a tehnologiilor digitale au condus la necesitatea planificării unui workshop destinat îmbunătățirii posturii de securitate cibernetică a sectorului.

Directoratul Național de Securitate Cibernetică (DNSC), cu sprijinul **Ministerului Educației și Cercetării** și cu participarea a peste 150 de persoane din mai mult de 100 de licee și inspectorate școlare județene, inclusiv directori, profesori de informatică, administratori de rețea și personal administrativ, a organizat un workshop pentru identificarea și evaluarea principalelor riscuri de securitate cibernetică.

Activitatea s-a desfășurat în data **23 aprilie 2025** și a inclus interpretarea și prezentarea rezultatelor chestionarului completat anterior workshop-ului de către participanți, dezbaterea principalelor riscuri de securitate cibernetică specifice sectorului liceal, precum și a măsurilor de gestionare a acestora. De asemenea, au fost evaluate riscurile de securitate cibernetică, stabilit nivelul de risc al sectorului și formulate recomandări pentru îmbunătățirea posturii generale de securitate cibernetică.

Menționăm că au fost analizate aspecte privind securitatea cibernetică a infrastructurii educaționale, urmând ca dezvoltarea culturii de securitate cibernetică în mediul educațional să fie abordată într-o activitate viitoare.

Motivația activității

Sectorul educațional reprezintă un pilon pentru dezvoltarea durabilă a societății, contribuind direct la formarea generațiilor viitoare și la pregătirea acestora pentru provocările unei societăți digitale. În ultimii ani, sectorul a cunoscut o sporire fără precedent a gradului de dependență de tehnologiile informației și comunicațiilor, fenomen accelerat inclusiv de pandemia de COVID-19, care a forțat digitalizarea rapidă a proceselor educaționale. Această tranziție a adus cu sine noi vulnerabilități și a amplificat suprafața de expunere la atacuri cibernetice. La nivelul Uniunii Europene, au fost semnalate incidente majore de securitate cibernetică ce au afectat procese educaționale, inclusiv perturbarea unor examene naționale, aspect ce evidențiază impactul potențial al acestor riscuri asupra funcționării sistemelor de învățământ.

Nivelul de maturitate cibernetică al sectorului este redus. Provocările actuale nu țin doar de tehnologii, ci și de lipsa unei culturi organizaționale solide în domeniul securității cibernetice, a formării continue a personalului și a conștientizării riscurilor în rândul elevilor și angajaților. În același timp, resursele dedicate securității cibernetice sunt limitate, iar prioritizarea acestui domeniu este adesea insuficientă.

Creșterea dependenței de platforme educaționale digitale, aplicații online, echipamente conectate și sisteme informatice utilizate zilnic în procesul educațional, cât și în procesele administrative, amplifică riscurile de securitate cibernetică la care sunt expuse liceele. În acest context, consolidarea capacității de identificare, evaluare și gestionare a riscurilor cibernetice devine o necesitate pentru protejarea integrității și continuității procesului educațional.

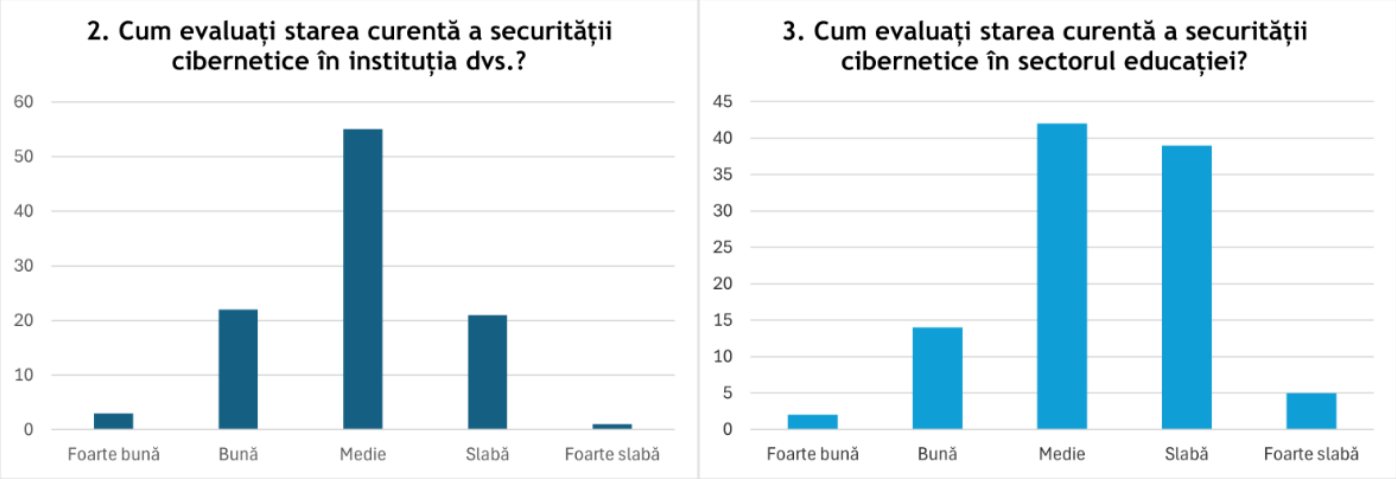
Peisajului amenințărilor

Printre cele mai frecvente amenințări se regăsesc atacurile de tip ransomware, care pot bloca accesul la date și sisteme necesare pentru desfășurarea activității educaționale. Phishing-ul și spear-phishing-ul rămân metode uzuale de compromitere a conturilor utilizatorilor, prin care atacatorii urmăresc obținerea accesului la platforme, informații personale sau instituționale.

La nivel global, se constată o creștere a atacurilor DoS și DDoS care vizează sectorul, afectând platformele de cursuri online și sistemele pentru predare și examene. Aceste atacuri perturbă activitatea instituțiilor, în timp ce eroarea umană este un factor major, favorizată de absența unor măsuri minime de securitate.

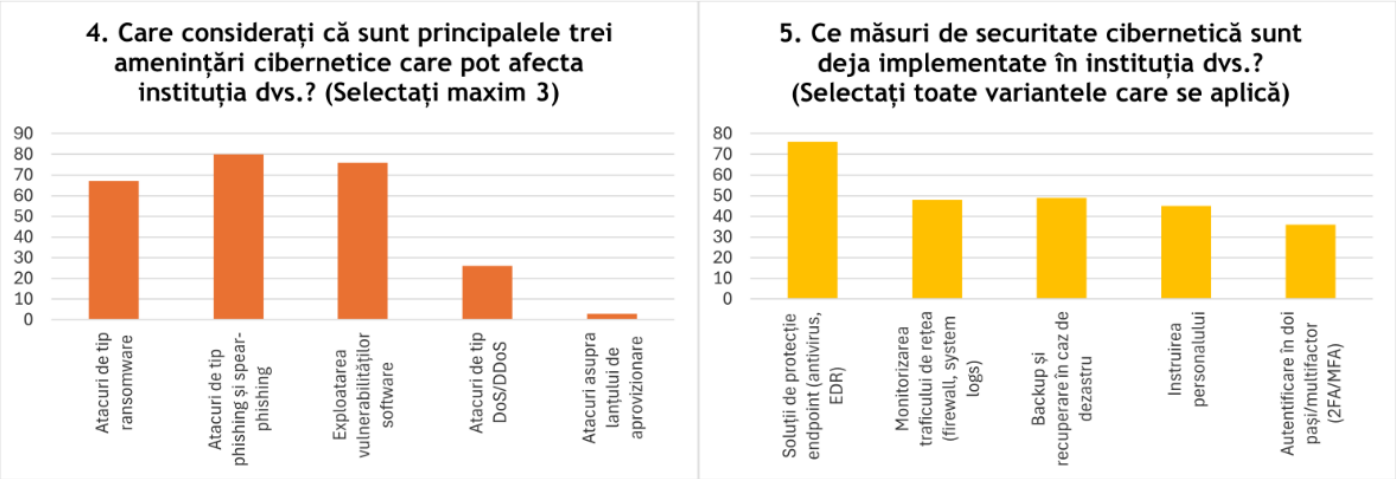
Rezultatele chestionarului

Premergător primei etape a fost transmis către participanți un **chestionar cu 15 întrebări** cu răspuns unic, multiplu sau deschis cu scopul de a obține o imagine inițială privind provocările și nivelul de maturitate al sectorului. Pe baza celor **102 răspunsuri colectate**, concluziile au fost structurate pe următoarele cinci paliere: (1) evaluarea securității la nivel instituțional și sectorial, (2) amenințările și măsurile de securitate implementate, (3) nivelul de conștientizare, (4) provocări organizaționale și (5) activități de pregătire.



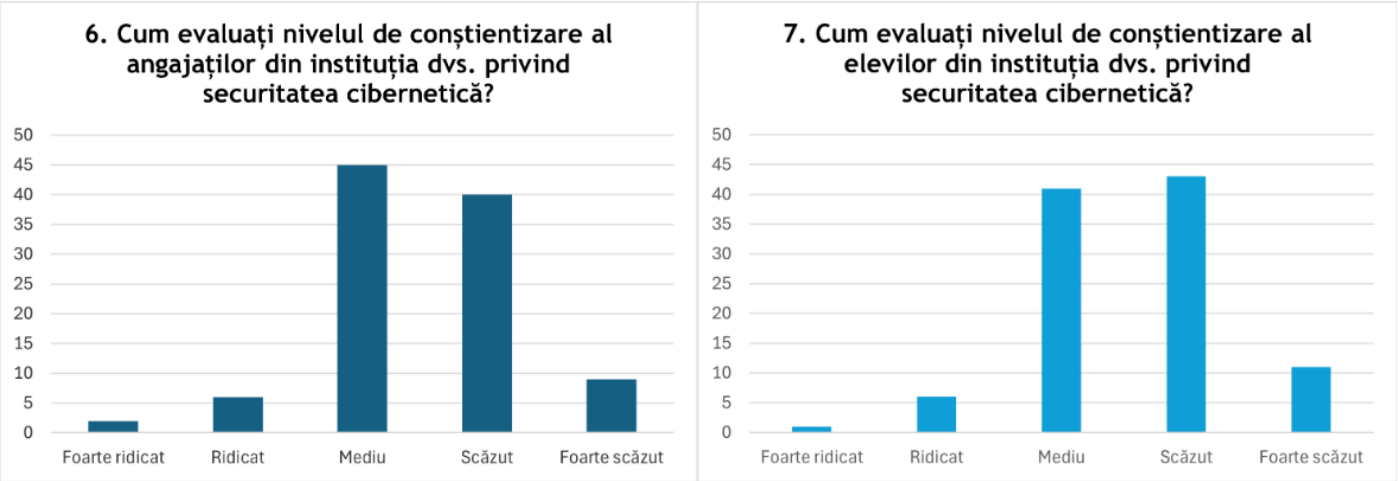
Figură 1 - Percepția stării de securitate cibernetică

Percepția asupra securității cibernetice este mai favorabilă la nivelul propriei instituții decât la nivel sectorial, sugerând fie o supraevaluare a capacităților interne, fie o conștientizare mai clară a provocărilor sistemice. Majoritatea respondenților au indicat un nivel mediu de maturitate, iar evaluările sectoriale tind să fie semnificativ mai ridicate.



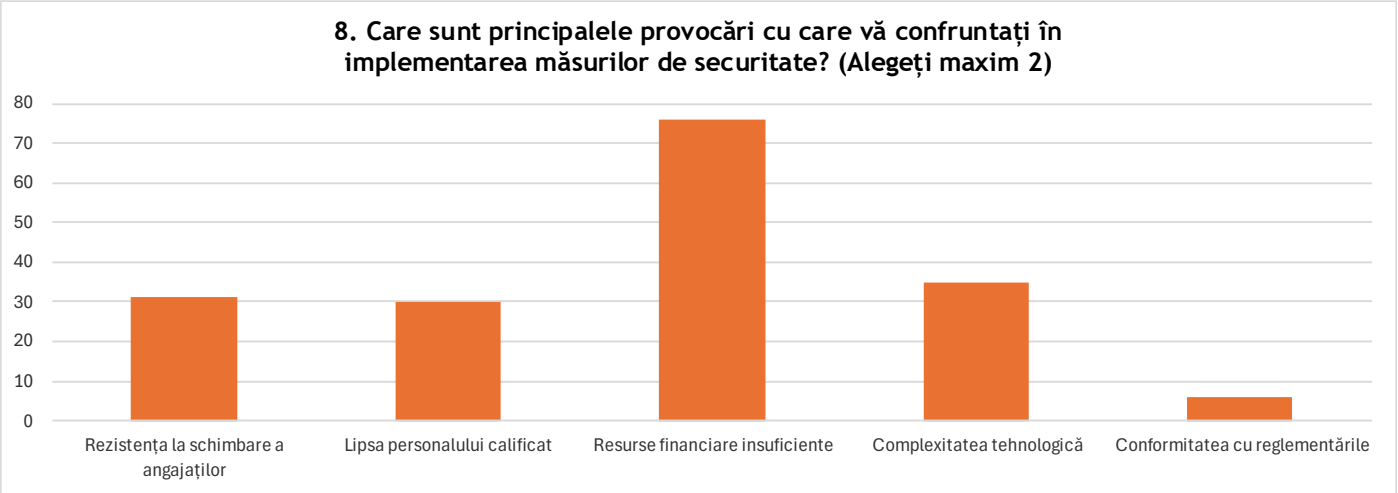
Figură 2 - Amenințări și măsuri de securitate implementate

Phishingul și spear phishingul sunt principalele amenințări, urmate de exploatarea vulnerabilităților software și ransomware, în timp ce atacurile DoS, DDoS și cele asupra lanțului de aprovizionare sunt mai rare. Deși multe instituții folosesc soluții tehnice precum protecția endpoint și backup, măsurile centrate pe factorul uman, precum instruirea personalului și autentificarea multifactor, sunt mai puțin răspândite, indicând o abordare dezechilibrată, insuficient adaptată riscurilor ce exploatează vulnerabilități umane.



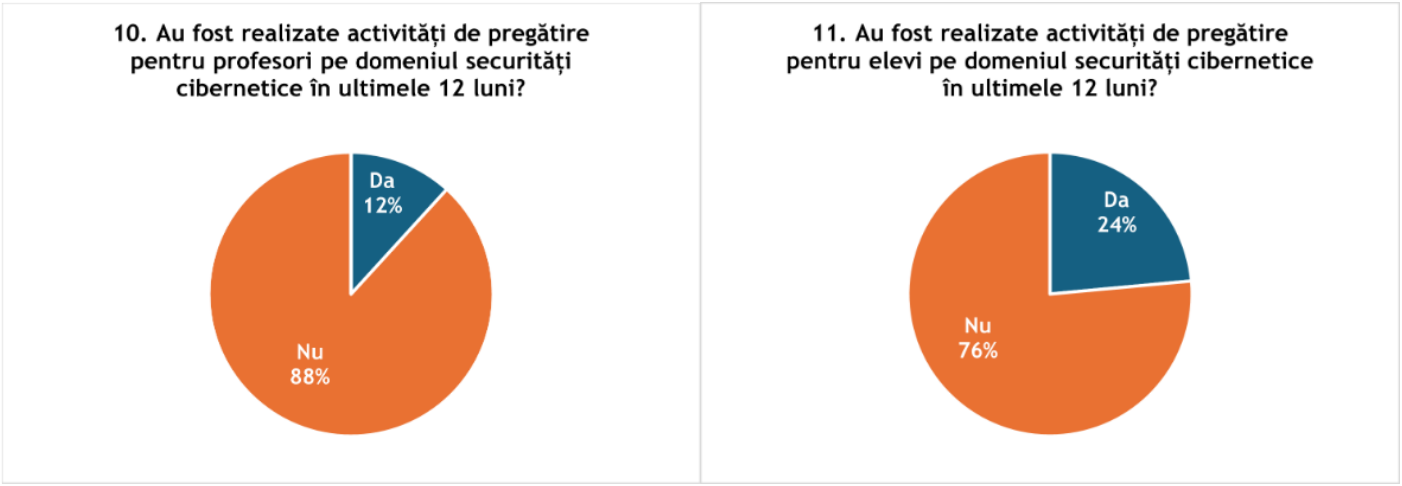
Figură 3 - Aspecte organizaționale privind conștientizarea și provocările

Nivelul de conștientizare privind securitatea cibernetică este, în general, perceput ca moderat scăzută în rândul angajaților și, mai ales, al elevilor, evidențiind lacune în cultura organizațională. Această vulnerabilitate a factorului uman afectează capacitatea de prevenție și reacție, subliniind nevoia de formare continuă și educație digitală adaptată.



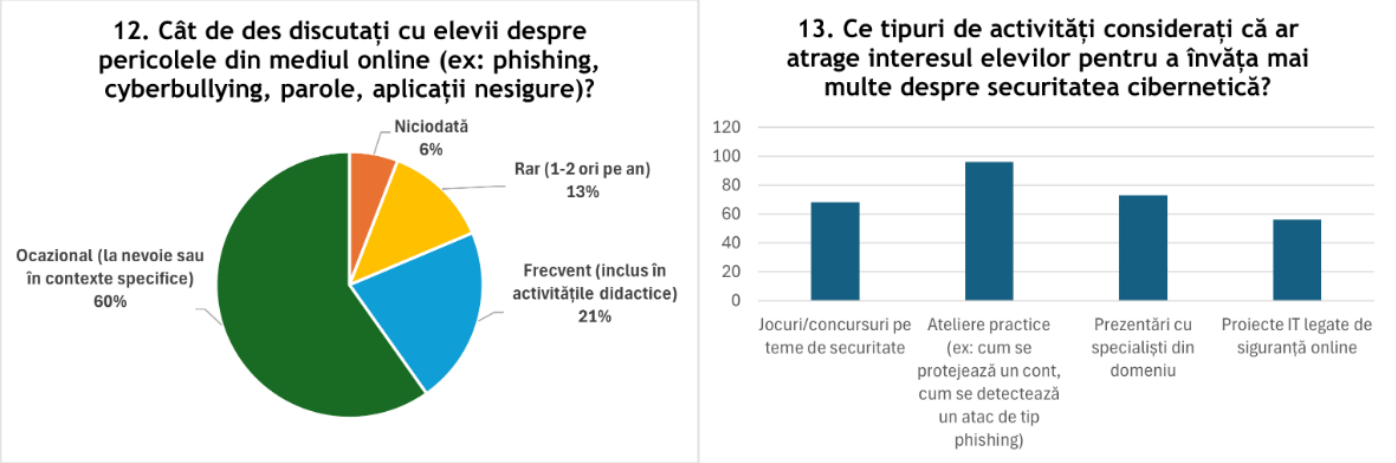
Figură 4 - Principalele provocări în implementarea măsurilor de securitate cibernetică

Resursele financiare insuficiente se conturează ca principala provocare în implementarea măsurilor de securitate, urmate de complexitatea tehnologică. Rezistența la schimbare și lipsa personalului calificat rămân, de asemenea, factori relevanți. Aceste limitări evidențiază nevoia de investiții și formare pentru consolidarea capacității de răspuns cibernetic.



Figură 5 - Activități de pregătire pentru profesori și elevi

Participarea la activități de instruire în domeniul securității cibernetice este redusă, cu doar 12% dintre profesori și 24% dintre elevi implicați în ultimul an. Nivelul redus de formare evidențiază o vulnerabilitate semnificativă și subliniază necesitatea unor programe de conștientizare adaptate și recurente în licee.



Figură 6 - Discuții și activități privind securitatea online

Discuțiile despre riscurile online au loc preponderent ocazional, fiind rareori integrate constant în activitățile didactice. Totuși, interesul elevilor este puternic asociat cu formate interactive, precum ateliere practice sau concursuri. Aceasta evidențiază oportunitatea de a consolida cultura de securitate prin metode educaționale dinamice și aplicate.

Desfășurare

Workshopul a fost organizat sub forma unei întâlniri, în care participanții au participat activ la dezbaterea și evaluarea riscurilor de securitate cibernetică specifice sectorului liceal.

S-a urmărit conturarea unei imagini realiste și coerente a posturii de securitate cibernetică în licee, prin:

- identificarea principalelor riscuri specifice;
- înțelegerea percepției participanților asupra acestor riscuri;
- formularea unor recomandări și direcții de îmbunătățire aplicabile la nivel sector.

Activitatea nu a avut caracter de audit individual, ci a urmărit o analiză comună, orientată spre învățare, colaborare și consolidarea securității cibernetice la nivel sectorial.

Identificarea, dezbaterea și evaluarea riscurilor

Pe baza unor rapoarte de specialitate, articole relevante, precum și a unui chestionar transmis anterior întâlnirii, a fost întocmită următoarea listă de riscuri:

1. Risc de compromitere a datelor și sistemelor informatice din cauza lipsei de conștientizare și instruire a personalului
2. Risc de a compromite infrastructura instituției din cauza măsurilor neexistente sau insuficiente a dispozitivelor destinate elevilor
3. Risc de perturbare a activităților educaționale și administrative din cauza infrastructurii IT învechite și neactualizate
4. Risc de interceptare și compromitere a datelor din cauza utilizării rețelelor Wi-Fi nesigure sau configurate necorespunzător
5. Risc de acces neautorizat și expunere a datelor din cauza utilizării dispozitivelor personale (BYOD) fără politici clare și măsuri de securitate
6. Risc de acces neautorizat și compromitere a conturilor din cauza gestionării inadecvate a parolelor și credențialelor de acces la platforme specifice

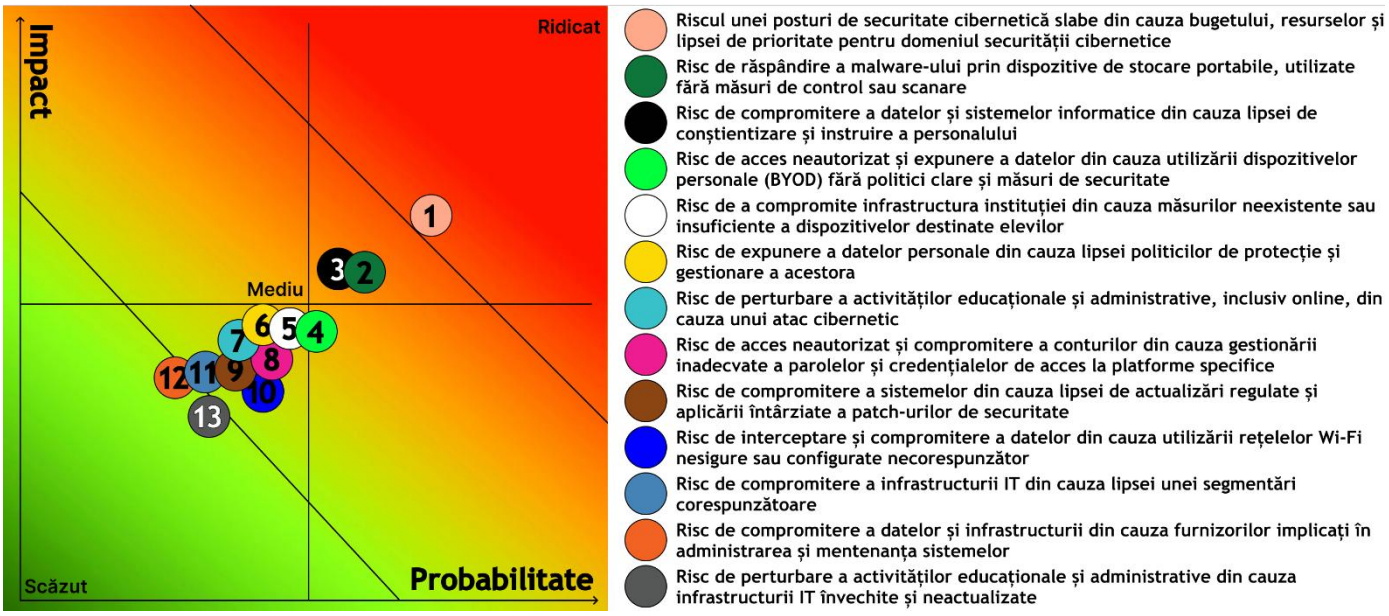
7. Risc de expunere a datelor personale din cauza lipsei politicilor de protecție și gestionare a acestora
8. Risc de perturbare a activităților educaționale și administrative, inclusiv online, din cauza unui atac cibernetic
9. Risc de compromitere a datelor și infrastructurii din cauza furnizorilor implicați în administrarea și mentenanța sistemelor
10. Risc de compromitere a sistemelor din cauza lipsei de actualizări regulate și aplicării întârziate a patch-urilor de securitate
11. Risc de răspândire a malware-ului prin dispozitive de stocare portabile, utilizate fără măsuri de control sau scanare
12. Risc de compromitere a infrastructurii IT din cauza lipsei unei segmentări corespunzătoare
13. Riscul unei posturi de securitate cibernetică slabe din cauza bugetului, resurselor și lipsei de prioritate pentru domeniul securității cibernetice

Pe baza unei înțelegeri comune a terminologiei și conceptelor din domeniul securității cibernetice, participanții au realizat o evaluare a acestor riscuri folosind o matrice formată din două criterii:

- **Impact** (financiar, operațional și asupra reputației) – evaluat ca **Scăzut, Mediu sau Ridicat**
- **Probabilitate** (în funcție de istoricul de materializare) – evaluată ca **Scăzută, Medie sau Ridicată**

Evaluarea s-a realizat online, în timp real, prin intermediul unei platforme interactive, iar scorurile au fost acordate pe o scală de la **1 (scăzut) la 3 (ridicat)**, în mod anonim, fiecare participant având în vedere instituția pe care o reprezenta și măsurile existente în prezent.

În urma evaluării a rezultat următorul **grafic al riscurilor** și **clasamentul acestora**, care reflectă percepția colectivă a participanților privind principalele riscuri cibernetice cu care se confruntă sectorul liceal:



Figură 7 - Graficul riscurilor de securitate cibernetică la nivelul sectorului liceal

Nr	Scor	Risc
1	2,36	Riscul unei posturi de securitate cibernetică slabe din cauza bugetului, resurselor și lipsei de prioritate pentru domeniul securității cibernetice
2	2,15	Risc de răspândire a malware-ului prin dispozitive de stocare portabile, utilizate fără măsuri de control sau scanare
3	2,13	Risc de compromitere a datelor și sistemelor informatice din cauza lipsei de conștientizare și instruire a personalului
4	1,95	Risc de acces neautorizat și expunere a datelor din cauza utilizării dispozitivelor personale (BYOD) fără politici clare și măsuri de securitate
5	1,94	Risc de a compromite infrastructura instituției din cauza măsurilor neexistente sau insuficiente a dispozitivelor destinate elevilor
6	1,90	Risc de expunere a datelor personale din cauza lipsei politicilor de protecție și gestionare a acestora
7	1,85	Risc de perturbare a activităților educaționale și administrative, inclusiv online, din cauza unui atac cibernetic
8	1,84	Risc de acces neautorizat și compromitere a conturilor din cauza gestionării inadecvate a parolelor și credențialelor de acces la platforme specifice
9	1,80	Risc de compromitere a sistemelor din cauza lipsei de actualizări regulate și aplicării întârziate a patch-urilor de securitate
10	1,80	Risc de interceptare și compromitere a datelor din cauza utilizării rețelelor Wi-Fi nesigure sau configurate necorespunzător
11	1,75	Risc de compromitere a infrastructurii IT din cauza lipsei unei segmentări corespunzătoare
12	1,71	Risc de compromitere a datelor și infrastructurii din cauza furnizorilor implicați în administrarea și mentenanța sistemelor
13	1,64	Risc de perturbare a activităților educaționale și administrative din cauza infrastructurii IT învechite și neactualizate

Figură 8 – Clasamentul riscurilor de securitate cibernetică la nivelul sectorului liceal

După prezentarea clasamentului final, discuțiile s-au concentrat asupra celor **mai importante trei riscuri identificate**. Pentru acestea au fost analizate:

- **cauzele principale** care le determină sau le amplifică;
- **barierele întâlnite** în gestionarea eficientă a acestora;
- cele mai relevante **măsuri și bune practici** ce pot fi aplicate.

Această etapă de dezbatere a contribuit la formularea unor concluzii și la evidențierea unor direcții viitoare de acțiune care pot susține consolidarea posturii de securitate cibernetică.

Rezultate

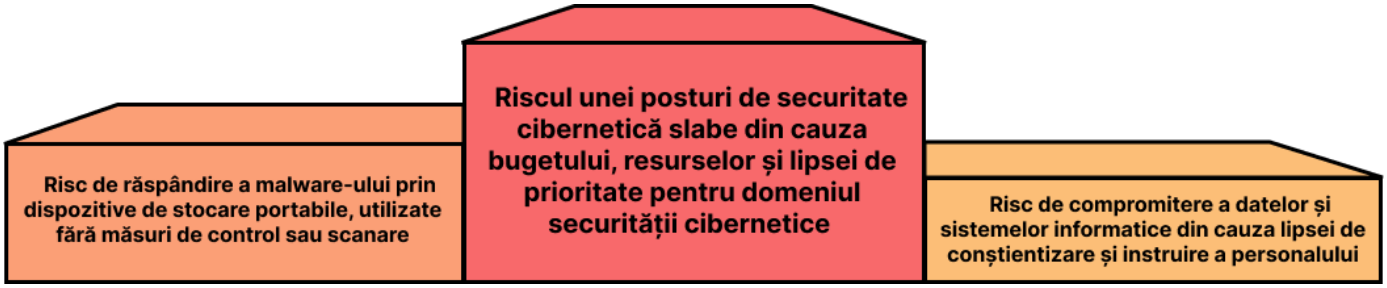
În urma evaluării a reieșit clar că nivelul general de risc cibernetic în sectorul liceal este **MEDIU**, iar riscurile prioritare identificate reflectă deficiențe critice în alocarea resurselor, aplicarea măsurilor tehnice de bază și în pregătirea personalului.

Primul risc identificat ca având un nivel de risc **ridicat**, atât din punct de vedere al impactului cât și al probabilității, este cel referitor la postura slabă de securitate cibernetică generată de **lipsa de resurse financiare, umane și de o prioritizare insuficientă** a securității cibernetice la nivel instituțional.

Următoarele două riscuri au fost evaluate cu nivel de risc **mediu spre ridicat**, necesitând atenție și măsuri adecvate din partea instituțiilor:

- **Răspândirea malware-ului prin dispozitive de stocare portabile**, care continuă să fie utilizate pe scară largă în absența unor politici clare și a mecanismelor de control și scanare automată;
- **Lipsa de conștientizare și insuficiența formării personalului**, ceea ce conduce la comportamente neadecvate în gestionarea datelor, conturilor sau echipamentelor.

Aceste constatări evidențiază faptul că principalele riscuri cu care se confruntă liceele sunt lipsa de fonduri dedicate, utilizarea necontrolată a unor tehnologii de bază și un nivel scăzut de educație în domeniul securității cibernetice în rândul personalului. În lipsa unor intervenții clare și coordonate, aceste riscuri pot afecta grav desfășurarea activităților educaționale și protejarea datelor instituționale și personale.



Figură 9 - Principalele 3 riscuri de securitate cibernetică din sectorul liceal

Riscul unei posturi de securitate cibernetică slabe din cauza bugetului, resurselor și lipsei de prioritate pentru domeniul securității cibernetice

Acest risc a fost clasat pe primul loc, indicând un nivel **ridicat** de probabilitate și impact. Evaluările și discuțiile din cadrul workshopului au evidențiat în mod clar faptul că **lipsa bugetului și a resurselor specializate** reprezintă una dintre cele mai mari provocări pentru licee în eforturile de protejare a infrastructurii IT și a datelor.

Securitatea cibernetică nu este tratată ca o prioritate în cadrul multor instituții de învățământ, fiind percepută mai degrabă ca o problemă secundară. Deciziile strategice nu includ, de regulă, elemente legate de protecția digitală, iar **conducerea instituțiilor rareori alocă resurse dedicate** în mod formal.

La nivelul personalului, **reticența față de schimbare**, în special în rândul cadrelor didactice cu vechime, îngreunează adoptarea unor practici adaptate noilor tehnologii utilizate. Lipsa motivației și interesului pentru instruirea în domeniul securității cibernetice, coroborată cu absența unor materiale ușor de înțeles și aplicat, menține acest risc la un nivel ridicat.

Această combinație de factori, precum bugetele limitate, resursele umane insuficiente și lipsa unei culturi organizaționale orientate spre securitate, definește o postură cibernetică vulnerabilă, care expune liceele la un risc semnificativ de atacuri sau incidente cu impact major.

Risc de răspândire a malware-ului prin dispozitive de stocare portabile, utilizate fără măsuri de control sau scanare

Acest risc a fost evaluat cu un nivel mediu spre ridicat de prioritate, reflectând o vulnerabilitate frecvent întâlnită în mediul liceal. Dispozitivele portabile continuă să fie utilizate pe scară largă, în special pentru transferul de materiale atât didactice cât și administrative, fără a fi supuse unor măsuri tehnice sau politici clare.

Participanții au subliniat că lipsa soluțiilor de scanare automată, combinată cu absența unor reguli stricte privind conectarea dispozitivelor externe, favorizează introducerea de programe malițioase în rețelele școlare. Această practică nesecurizată este adesea tolerată sau ignorată, fiind percepută ca o necesitate operațională și nu ca un factor de risc.

Utilizarea necontrolată a acestor medii portabile, în lipsa unor măsuri de protecție de bază, contribuie semnificativ la creșterea riscului de infectare cu malware și la compromiterea infrastructurii IT din licee.

Risc de compromitere a datelor și sistemelor informatice din cauza lipsei de conștientizare și instruire a personalului

Acest risc evidențiază un nivel mediu spre ridicat de vulnerabilitate cauzat de lipsa formării continue în rândul personalului didactic și administrativ pe domeniul securității cibernetice. Participanții au menționat că mulți angajați nu sunt familiarizați cu practicile de bază și nu conștientizează impactul acțiunilor proprii.

În lipsa instruirii periodice, riscul de erori umane și comportamente nesigure rămâne semnificativ, contribuind direct la compromiterea conturilor, datelor sau infrastructurii IT.

Recomandări

Având în vedere importanța sectorului liceal și rezultatele evaluării realizate în cadrul workshopului, instituțiile de învățământ, împreună cu autoritățile competente și partenerii din domeniu, trebuie să adopte o abordare strategică și proactivă în gestionarea riscurilor identificate. Recomandările următoare constituie un set minim de măsuri, fără a fi limitative, oferind un punct de plecare pentru consolidarea securității sectorului:

1. **Crearea unui plan de investiții în securitatea cibernetică:** Elaborarea unui plan de alocare a bugetelor dedicate infrastructurii IT, soluțiilor de protecție și instruirii personalului. Planul trebuie să fie susținut la nivel de conducere instituțională și încurajat prin politici sectoriale clare, pentru a sprijini tranziția către o postură cibernetică matură.
2. **Standardizarea cerințelor minime de securitate la nivelul sectorului:** Definirea și adoptarea, la nivel central, a unui set de cerințe tehnice și organizaționale pentru toate liceele, care să asigure un cadru unitar de protecție a datelor și a infrastructurii informatice din sistemul educațional.
3. **Creșterea protecției pentru platformele educaționale și sistemele administrative:** Consolidarea securității aplicațiilor administrative utilizate în mediul școlar, precum cataloagele online sau platformele pentru gestionarea datelor elevilor și profesorilor, prin dezvoltarea acestora cu cerințe de securitate încă din faza de proiectare, auditarea periodică a furnizorilor și aplicarea unor politici stricte de acces și utilizare.
4. **Activarea autentificării multifactor (2FA) pentru toate conturile instituționale:** Activarea autentificării multifactor pentru toate conturile utilizate de personalul didactic și administrativ în cadrul instituției, inclusiv cele aferente platformelor educaționale, aplicațiilor administrative și serviciilor cloud. Această măsură contribuie la reducerea riscului de compromitere a conturilor prin interceptarea sau reutilizarea credențialelor.
5. **Optimizarea și consolidarea strategiilor de back-up:** Implementarea unor politici de backup care să includă utilizarea combinată a soluțiilor online și offline, verificarea periodică a copiilor de siguranță și protejarea acestora împotriva ștergerii sau modificării neautorizate. Procedurile de restaurare trebuie să fie testate și documentate.
6. **Implementarea unor măsuri restrictive privind utilizarea dispozitivelor de stocare portabile:** Limitarea accesului la porturile USB pe echipamentele utilizate în instituție, acolo unde nu sunt absolut necesare, și introducerea unei politici stricte de utilizare a dispozitivelor externe, inclusiv inventarierea, scanarea automată și controlul administrativ al acestora.

7. **Implementarea unor mecanisme de segmentare și control al accesului:** Segmentarea rețelelor în funcție de nivelul de sensibilitate al datelor și configurarea riguroasă a politicilor de acces și autentificare. Se recomandă utilizarea de soluții EDR, antivirus și firewall-uri actualizate, precum și monitorizarea permanentă a traficului de rețea.
8. **Implementarea unui program de conștientizare și formare în securitate cibernetică:** Dezvoltarea unui cadru educațional continuu, adresat personalului din învățământ, axat pe înțelegerea riscurilor digitale, recunoașterea amenințărilor și utilizarea în siguranță a platformelor digitale. Acest program trebuie să includă cursuri accesibile, cu conținut adaptat nivelului utilizatorilor.
9. **Motivarea și implicarea personalului în dezvoltarea unei culturi organizaționale de securitate:** Promovarea unei culturi a responsabilității în domeniul securității cibernetice, prin implicarea activă a conducerii și includerea obiectivelor de securitate în evaluările anuale. Recunoașterea și încurajarea implicării personale pot avea un impact pozitiv asupra comportamentelor de securitate.
10. **Promovarea raportării incidentelor și a greșelilor operaționale:** Crearea unui mediu de încredere în care personalul să fie încurajat să raporteze rapid incidentele sau comportamentele suspecte, fără teama de consecințe. Instruirile trebuie să includă componente dedicate identificării timpurii și raportării eficiente.

Concluzii

Workshopul a evidențiat vulnerabilitățile persistente din sectorul liceal în fața amenințărilor cibernetice, precum și necesitatea unei abordări strategice și coordonate pentru îmbunătățirea posturii de securitate. Participanții au contribuit la conturarea unei imagini realiste asupra principalelor riscuri, iar analiza comună a dus la identificarea unor direcții concrete de acțiune.

Factorul uman a fost reafirmat ca una dintre cele mai mari vulnerabilități, lipsa de conștientizare și instruire a personalului fiind un element recurent în toate etapele evaluării. Totodată, lipsa resurselor – atât financiare, cât și umane – a fost identificată ca o barieră critică în implementarea măsurilor de protecție, în timp ce securitatea cibernetică nu este încă percepută ca o prioritate la nivel decizional în multe instituții.

Participanții au subliniat importanța dezvoltării unui cadru coerent de formare și educație digitală, adaptat specificului personalului din învățământ și elevilor, precum și necesitatea unor standarde minime și uniforme de securitate cibernetică la nivel sectorial. De asemenea, a fost evidențiată oportunitatea valorificării formatelor educaționale interactive pentru implicarea activă a elevilor în cultura de securitate.

În concluzie, workshopul a consolidat înțelegerea colectivă a provocărilor actuale și a generat un angajament comun pentru reducerea riscurilor cibernetice în sectorul liceal. Crearea unui ecosistem cibernetic educațional rezilient impune investiții, leadership activ, măsuri continue și o colaborare strânsă între autorități, conducerea unităților de învățământ și partenerii din domeniu.

Informațiile și concluziile din prezentul document au scop exclusiv informativ și nu rezultă dintr-un proces de audit formal. Acestea NU au valoare juridică și nu pot fi interpretate sau utilizate drept comunicare oficială din partea DNSC privind obligațiile și/sau măsurile ce trebuie luate de către organizațiile identificate ca entitate esențială sau importantă în temeiul OUG nr. 155/2024.

TLP:GREEN = Divulgare limitată, destinatarii pot transmite informația în cadrul comunității lor. TLP:GREEN se poate folosi atunci când informațiile sunt utile pentru a crește gradul de conștientizare în cadrul comunității extinse. Destinatarii pot partaja informații TLP:GREEN cu colegi și organizații din cadrul comunității lor, **dar nu prin canale accesibile publicului**. Când "comunitatea" nu este definită, se va presupune comunitatea de securitate cibernetică/apărare.