ROMÂNIA
SERVICIUL ROMÂN DE INFORMAŢII
ACADEMIA NAŢIONALĂ DE INFORMAŢII
„MIHAI VITEAZUL"
Program studii universitare de masterat
profesional dedicat formării ofițerilor de informații
„Analiză de Intelligence"

2024

PROBĂ SCRISĂ PENTRU EVALUAREA APTITUDINILOR NECESARE FORMĂRII OFIȚERILOR DE INFORMAȚII

VARIANTA 2

Citiţi informaţiile de mai jos:

Informația 1

Numărul adreselor IP (protocol de internet) utilizate pentru atacuri cibernetice în contextul războiului Ucraina-Rusia a crescut din nou, odată cu atacurile de tip Distributed Denial of Service (DDoS) care au vizat site-urile unor instituții publice/organizații private din România, revendicate de gruparea de hackeri Killnet afiliată Rusiei, a anunțat Directoratul Național de Securitate Cibernetică (DNSC). Peste 11.400 de adrese IP au fost utilizate până marți, 3 mai 2022, unele și din România. Adresa IP este un număr unic atribuit fiecărui computer sau altui dispozitiv care se conectează la internet. Adresele IP sunt atribuite dispozitivelor de internet de către furnizorii de servicii de internet și de foarte multe ori, furnizorii de internet atribuie aceeași adresă IP unui număr mare de computere. Ca atare, este posibil ca mai multe computere să aibă adrese IP identice. Numărul adreselor IP utilizate pentru atacuri cibernetice, inclusiv cele de tip DDoS, împotriva instituțiilor publice și private din România, a crescut de la 3.521 de adrese IP în data de 1 mai, la peste 11.400 de adrese IP în data de 3 mai, arată datele DNSC. Mai multe adrese IP folosite în aceste atacuri sunt din România și sunt în continuare active, potrivit raportului DNSC.

Atacul cibernetic de tip DDoS implică generarea unui val de cereri de conexiune la adresa unui site web, ceea ce conduce la funcționarea semnificativ încetinită sau oprirea activității site-ului țintă, potrivit DNSC. Mai multe site-uri web guvernamentale, inclusiv site-ul Guvernului ori Ministerului Apărării, site-uri ale unor aeroporturi, dar și ale unor bănci ori firme private au fost recent ținta unor atacuri cibernetice de tip DDoS revendicate de gruparea de racheți ruși Killnet. În cadrul unui astfel de atac, atacatorii utilizează mai multe dispozitive conectate la internet și deja compromise (botnet) pentru a ataca o anumită țintă. Prin utilizarea unui botnet, atacatorii au la dispoziție o „putere de atac" mai mare și sursa reală a atacului este dificil de identificat. „Un atac DDoS face ca un website sau o resursă online să nu fie accesibilă prin direcționarea multor dispozitive care să încerce accesul în același timp. Daunele sunt foarte variate, în funcție de profilul site-ului afectat. Dacă este vorba de o companie care își desfășoară activitatea online, simpla lipsă a accesului consumatorilor provoacă pierderi financiare", a declarat Silviu Stahie, specialist în

securitate informatică la Bitdefender. Acesta a subliniat că atacurile DDoS nu necesită cunoștințe tehnice considerabile și nici resurse financiare complexe, iar astfel de resurse de atac împotriva unui site web pot fi cumpărate de pe dark web, la prețuri care încep de la 15 dolari pe oră împotriva unui site neprotejat, cu până la 50.000 de accesări pe secundă. Atacul împotriva unui site protejat poate ajunge până la 200 de dolari.

Informația 2

Grupul Rompetrol anunță că în cursul zilei de 7 martie 2022 serviciul Fill & Go Manager a înregistrat o serie de disfuncționalități tehnice, pe fondul unui atac cibernetic de tip DDoS, care a afectat acccesul extern pe platforma companiei Rompetrol Downstream. Toate sistemele vizate de atac au fost restaurate în cursul serii și s-au luat măsuri suplimentare pentru securizarea și protejarea accesului din partea clienților pe platforma Fill & Go, precizează compania într-un comunicat. Rompetrol nu a menționat de unde provine atacul, deși grupul de hackeri ruși Killnet l-a revendicat încă de ieri.

Rompetrol susține că nu s-au înregistrat pierderi de informații și nu au fost afectate datele privind conturile clienților (informații confidențiale, limite de alimentare, plăți etc.). Firma dorește să precizeze că, în urma primului atac cibernetic din 7 martie, care a fost unul complex de tip malware – ransomware, a decis, pentru protejarea datelor, sistarea temporară a site-urilor și inclusiv, pentru o scurtă perioadă de timp, a serviciului Fill & Go, atât pentru flote, cât și pentru persoanele fizice.

În linie cu prioritățile de business, Rompetrol și-a restaurat treptat prezența în mediul online, prioritare fiind platformele digitale utilizate de clienți, site-urile corporative urmând a fi făcute publice în cursul acestei săptămâni. În cadrul unui interviu acordat postului PRO TV, Ioan Corpoș, director al Rompetrol, a declarat oficial că, „în momentul atacului cibernetic de ieri al grupării Killnet, aceste site-uri nu erau publice și nu puteau fi accesate/afectate".

Rompetrol le mulțumește clienților pentru încrederea și înțelegerea din această perioadă, îi asigură că remedierea serviciilor în condiții de maximă siguranță pentru activitățile clienților și a partenerilor comerciali a fost și este o prioritate pentru companie. Anumite activități operaționale ale Rompetrol nu au fost afectate de aceste atacuri cibernetice. Activitățile de producție din rafinăriile Petromidia Năvodari și Vega Ploiești au fost temporar oprite pentru desfășurarea lucrărilor de revizie, iar depozitele și benzinăriile Rompetrol din România, Bulgaria, Georgia și Republica Moldova și-au continuat activitățile de bază: transportul și distribuția de produse petroliere.

Informația 3

Serverele care gestionează website-urile Companiei Naţionale Aeroporturi Bucureşti (CNAB) au fost supuse la atacuri cibernetice repetate în ultimele zile, dar nu au fost înregistrate pierderi de informaţii, a anunţat CNAB. „În cursul ultimelor zile, serverele care gestionează website-urile CNAB au fost supuse la atacuri cibernetice repetate. Atacurile au fost de tip DDoS, ultimul dintre acestea afectând, în primele ore ale zilei de 2 mai 2022, funcţionarea website-ului bucharestairports.ro. Pentru câteva ore, acest site a fost inaccesibil publicului dar, începând cu dimineaţa aceleiaşi zile, funcţionarea normală a fost restabilită prin colaborarea între specialiştii CNAB şi cei ai firmei care asigură găzduirea şi mentenanţa lui", informează compania. Potrivit sursei citate, nu s-au înregistrat pierderi de informaţii şi nu a fost afectat serverul de e-mail.

Directoratul Naţional de Securitate Cibernetică (DNSC) a avertizat că vor continua atacurile cibernetice de tip DDoS (phishing şi spear-phishing propagate pe email sau platforme de mesagerie) asupra unor site-uri web din România, acestea fiind auto-asumate de gruparea pro-rusă Killnet. „Se observă o diversificare a atacurilor prin utilizarea unor noi metode care vizează infectarea cu aplicaţii malware de tip ransomware a sistemelor informatice ale organizaţiilor deja atacate prin DDoS, ce au ca efect compromiterea datelor utilizatorilor. Atacatorii cibernetici transmit mesaje pe email, WhatsApp, Signal, Telegram, Messenger, Slack etc., pretinzând că sunt o sursă/persoană de încredere, pentru a convinge potenţialele victime să divulge informaţii confidenţiale, date personale sau să efectueze acţiuni care permit preluarea controlului unor infrastructuri sau dispozitive informatice de către atacatori. „Pentru a încerca să inducă în eroare potenţialele victime şi pentru o rată de succes mai ridicată, atacatorii intenţionează să utilizeze inclusiv adrese de email sau conturi de utilizator falsificate ca aparţinând unor instituţii publice sau organizaţii cunoscute din România", a declarat DNSC.

Specialiştii DNSC recomandă prudenţă în cazul în care se recepţionează mesaje ce au următoarele caracteristici: sunt prezentate ca fiind solicitări urgente, inclusiv din partea autorităţilor; sunt ciudat formulate şi apar ca provenind de la o sursă sau persoană „de încredere"; includ linkuri sau ataşamente care nu au fost solicitate; cer furnizarea unor date cu caracter personal sau tehnice (parole, PIN, IP etc.). Pentru a limita riscul infectării cu ransomware şi a evita criptarea sau distrugerea datelor, este obligatorie şi realizarea de copii de siguranţă (backup) pentru site-uri, baze de date sau orice alt tip de date expuse în mediul internet, precum şi stocarea acestor copii în locaţii separate.

Informația 4

Peste 200 de români au fost victime ale unei fraude online cu un site care a copiat vechea identitate vizuală a HotNews.ro pentru a extrage date personale sau financiare, a precizat recent pentru HotNews.ro Dan Cîmpean, directorul Directoratului Național de Securitate Cibernetică (DNSC).

Site-ul a fost blocat după ce a fost adăugat în lista cu site-uri fake-news și fraude pentru care autoritatea recomandă blocarea traficului de internet. DNSC a avertizat sâmbătă, 26 februarie 2022, asupra unui site care copiază fosta identitate vizuală a HotNews.ro și promovează false oportunități de investiții online, cu scopul de a frauda utilizatorii și de a le extrage date personale sau financiare. Site-ul a fost adăugat imediat pe lista cu site-uri care ar propaga fake-news și fraude precum și IP-uri care ar fi folosite pentru atacuri malware. Amintim că după ce un astfel de site este adăugat pe lista DNSC, directoratul recomandă mai departe către Autoritatea Națională pentru Administrare și Reglementare în Comunicații (ANCOM) ori furnizorilor de internet blocarea traficului de internet către aceste surse, demers care reduce semnificativ rata fraudelor în mediul online.

Directorul DNSC a precizat într-un interviu acordat HotNews.ro care au fost efectele listării acestui site și blocării de către furnizorii de internet. Declarațiile au fost făcute în data de 7 martie 2022, în ziua atacului cibernetic de la Rompetrol. „În urma listării acestui site și a blocării lui de către furnizorii de internet a scăzut numărul de notificări din partea unor cetățeni care s-au conectat la site-ul respectiv. Astfel, folosind abuziv imaginea, brandul și credibilitatea HotNews.ro, site-ul trimite utilizatorii către tranzacționări de monedă virtuală, către anunțuri de job-uri pentru care, pentru a primi detalii suplimentare, oamenii trebuie să-și dea datele personale de pe cardul de credit. Prin apăsarea unor butoane și dat click pe anumite elemente de pe site se instalează malware pe laptopul, tableta, telefonul ori dispozitivul utilizatorului, malware care este folosit pentru a derula alte activități infracționale. Deci utilizatorul se infectează cu malware, iar dacă merge mai departe prin meniu, utilizatorul este invitat, într-un mod tendențios, să-și dea date de pe cardul de credit, să facă niște plăți pentru a beneficia de niște servicii care nu vor veni niciodată", a declarat Dan Cîmpinean.

Directorul DNSC a spus că sunt în jur de 200 de români care au căzut victime acestei fraude și că blocarea accesului nu rezolvă în totalitate problema. „Nu am cifra exactă, dar sunt mulți, în jur de 200 de victime. Sunt foarte mulți care probabil au reclamat direct la Poliție. În cazuri de genul acesta, preocuparea principală este să blocăm accesul. În momentul în care am blocat accesul, atacatorii nu mai au posibilitatea să fraudeze cetățenii români. Să nu uităm – blocarea nu o facem noi, ci doar solicităm altor autorități competente. Site-ul în sine, dacă nu este găzduit pe infrastructură românească, pe teritoriul României, funcționează mai departe, nu este închis, ci doar nu mai este accesibil de pe teritoriul României, dar poate fi accesat din alte țări", a mai declarat Dan Cîmpean.

Amintim că această autoritate a început de ceva timp să publice o listă cu site-uri fake-news și fraude, precum și IP-uri care ar fi utilizate la atacuri malware. Dan Cîmpean susține că DNSC nu este implicat și nici nu desfășoară activități de analiză de conținut redacțional sau de altă natură, ale unor publicații online sau ale unor site-uri active în România. Potrivit acestuia, DNSC are atribuții pe domeniul de securitate cibernetică în domeniul civil, gestionând un volum imens de notificări și alerte de risc informatic pe care trebuie să le verifice. După aceste analize, DNSC emite alerte ori recomandări către furnizori ori ANCOM pentru luarea măsurilor legale de blocare a

traficului către și înspre aceste surse. Așa cum HotNews.ro a semnalat anterior în cazul altor site-uri blocate, DNSC a trimis o notificare către ANCOM cu listele de site-uri fake-news și IP-uri cu malware, cu rugămintea de a dispune măsurile tehnice pentru blocarea accesului la internet către acestea. La rândul său, ANCOM a trimis adresa către furnizori cu solicitarea de a efectua de îndată operațiunile tehnice cerute de DNSC, fără a fi menționată nici baza legală pentru această solicitare și nici motivele precise. Este de notorietate scandalul iscat după blocarea accesului la site-ul Aktual24.ro, după ce acest site a fost adăugat de DNSC pe lista site-urilor de publicitate și fraude online.

După ce HotNews.ro a semnalat aceste lucruri, DNSC a spus că acestea ar fi fost implicate în activități frauduloase în mediul online și au fost identificate ca fiind asociate cu atacuri cibernetice de tip DDoS asupra unor instituții guvernamentale din UE. DNSC susține că a adăugat aceste site-uri pe lista propusă a fi blocată de furnizorii de internet după ce a fost informat prin intermediul mecanismului de cooperare CSIRT Network (rețeaua structurilor de tip CSIRT din fiecare stat membru UE) cu privire la 679 site-uri web din spațiul UE – dintre care trei cu domeniul „.ro" care ar fi fost implicate în activități frauduloase. HotNews.ro a stat de vorbă cu proprietarul Bookblog.ro, Dan Călugăreanu, care a mărturisit că site-ul îi fusese spart cu câteva zile în urmă, după care nu a mai putut fi accesat din anumite rețele. Dan Călugăreanu a spus că încerca să pună site-ul pe picioare și nu înțelegea de ce nu mai poate fi accesat. Potrivit acestuia, nimeni de la DNSC, despre care nici nu auzise, sau altă autoritate nu l-a sunat să-i spună că site-ul său ar fi fost adăugat pe o listă neagră cu site-uri. De altfel, în răspunsul dat în urmă cu o zi ca reacție la articolul HotNews.ro, DNSC cere proprietarilor de domenii ori site-uri web a căror activitate este suspendată să contacteze autoritatea pentru detalii. Cu alte cuvinte, DNSC nu identifică proprietarii site-urilor pentru care cere blocarea accesului în scopul rezolvării problemelor.

CERINȚE

Subiect I. Raportat strict la informaţiile de mai sus (4,50p):

1. Identificați și menționați, prin citare, patru neconcordanţe (nepotriviri, date contradictorii) din textele date. (0,60p)
2. Formulați cinci efecte negative (riscuri) generate de situațiile prezentate în cadrul textelor. Detaliați în cel mult 50 de cuvinte, pentru fiecare risc identificat, impactul pe care îl are acesta asupra climatului de securitate. (2p)
3. Alegeți un efect negativ (risc) identificat și redactați un scenariu (realist, posibil, pertinent, corect formulat, plauzibil) referitor la evoluția fenomenului criminalității cibernetice, de cel mult 100 de cuvinte. (0,90p)
4. Alegeți un efect negativ (risc) de la punctul 2. Precizați și motivați două măsuri/recomandări de reducere a acestuia. (1p)

Subiect II. Sunteți jurnalist în cadrul unei publicații online care monitorizează evoluțiile în domeniul securității cibernetice și redactorul v-a pus la dispoziție textele prezentate mai sus (4p):

1. Redactați un material de informare adresat publicului larg, de maximum 150 de cuvinte, în care să sintetizați aspectele din texte și să includeți trei idei principale, relevante pentru securitatea cibernetică. Stabiliți un titlu de maximum 10 cuvinte pentru materialul elaborat.
   Se acordă 0,75p pentru elaborarea unui material care include trei idei principale, 0,50p pentru elaborarea unei sinteze pertinente, corect formulată, care să includă aspectele menționate în cerință și 0,25p pentru stabilirea titlului.
   Total: 1,50p

2. Pe baza unuia dintre riscurile identificate la cerința I.2, propuneți o persoană cu expertiză, dintr-un mediu relevant, cu care ați realiza un interviu pentru a obține date suplimentare față de cele cuprinse în texte. Motivați alegerea în maximum 100 de cuvinte. (1,30p)
   Nu se punctează alegerea unor persoane care ocupă funcții înalte în stat sau în cadrul organizațiilor suprastatale.

3. Scrieți 6 întrebări pe care le-ați adresa persoanei alese la cerința II.2, utile pentru a obține date suplimentare față de cele cuprinse în texte. (1,20p)

***

NOTĂ
Se acordă:
- **0,50 p** *pentru corectitudine gramaticală (0,30p) şi respectarea cerinţelor referitoare la numărul maxim de cuvinte (0,20p)*
- **1 punct** din oficiu

ROMÂNIA
SERVICIUL ROMÂN DE INFORMAŢII
ACADEMIA NAŢIONALĂ DE INFORMAŢII
„MIHAI VITEAZUL"
Program studii universitare de masterat
profesional dedicat formării ofițerilor de informații
Analiză de Intelligence

BAREM

PROBĂ SCRISĂ PENTRU EVALUAREA APTITUDINILOR NECESARE FORMĂRII OFIȚERILOR DE INFORMAȚII

VARIANTA 2

Subiect I (4,50 puncte)

Răspunsuri

1. Identificați și menționați, prin citare, patru neconcordanţe (nepotriviri, date contradictorii) din textele date. (0,60p)

Criterii de punctare:
0,15p – pentru fiecare menționare exclusivă a aspectelor definite mai jos.

Se punctează următoarele neconcordanţe (nepotriviri):

1. „gruparea de hackeri Killnet" vs. „gruparea de racheți ruși Killnet";
2. „Rompetrol nu a menționat de unde provine atacul, deși grupul de hackeri ruși Killnet l-a revendicat încă de ieri." vs. „Ioan Corpoș, director al Rompetrol, a declarat oficial că, „în momentul atacului cibernetic de ieri al grupării Killnet, aceste site-uri nu erau publice și nu puteau fi accesate/afectate".
3. „Dan Cîmpean" vs. „Dan Cîmpinean";
4. „listele de site-uri fake-news" vs. „lista site-urilor de publicitate și fraude online".

2. Formulați cinci efecte negative (riscuri) generate de situațiile prezentate în cadrul textelor. Detaliați în cel mult 50 de cuvinte, pentru fiecare risc identificat, impactul pe care îl are acesta asupra climatului de securitate. (2p)

Criterii de punctare:
0,40p – pentru fiecare risc identificat și detaliere a impactului.

Punctaje parțiale:
0,10p – pentru formularea riscului, <u>fără detalierea impactului</u>;
0,30p – pentru detalierea impactului, <u>fără precizarea explicită a riscului.</u>

<u>Exemple riscuri:</u>

1. creșterea gradului de dificultate în identificarea sursei atacului, din cauza utilizării unor adrese IP identice;

2. generarea de disfuncționalități ale site-urilor web aparținând unor instituții oficiale și companii;
3. provocarea de pierderi financiare pentru clienți/instituții;
4. accesul facil la resurse pentru desfășurarea atacurilor cibernetice;
5. afectarea intereselor clienților/beneficiarilor;
6. afectarea activităților economice ale companiilor;
7. compromiterea datelor utilizatorilor prin diversificarea metodelor utilizate de atacatori;
8. decredibilizarea unor site-uri cu notorietate prin clonarea identității vizuale.

Exemple detaliere impact:

- creșterea numărului de atacatori și diversificarea metodelor utilizate;
- incapacitatea autorităților competente de a face față numărului de posibile atacuri cibernetice;
- acces limitat la serviciile/platformele instituțiilor publice;
- incapacitatea instituțiilor/utilizatorilor de a recupera prejudiciul creat, posibila dispariție de pe piață a acestora;
- scăderea încrederii clienților/beneficiarilor în instituțiile/companiile afectate, cât și în autoritățile competente;
- exploatarea bazelor de date compromise în derularea unor campanii de *phishing*;
- renunțarea clienților la serviciile prestate de companiile/instituțiile afectate.

3. Alegeți un efect negativ (risc) identificat și redactați un scenariu (realist, posibil, pertinent, corect formulat, plauzibil) referitor la evoluția fenomenului criminalității cibernetice, de cel mult 100 de cuvinte. (0,90p)

Criterii de punctare:
0,20p – pentru includerea riscului în scenariul elaborat;
0,20p – pentru elaborarea unui scenariu;
0,50p – pentru îndeplinirea criteriilor definite în cerință pentru elaborarea scenariului - realist, posibil, pertinent, corect formulat, plauzibil.

Exemple de idei pentru elaborarea scenariilor:

- multiplicarea atacurilor realizate în baza adreselor de IP identice;
- apariția unor noi grupări de criminalitate cibernetică;
- dezvoltarea metodelor și tehnologiilor de realizare a atacurilor cibernetice/de combatere și protecție împotriva atacurilor cibernetice;
- solicitarea unor recompense financiare pentru recuperarea datelor compromise;
- generarea unei potențiale crize privind alimentarea cu combustibil;
- actualizarea procedurilor de intervenție în gestionarea atacurilor cibernetice (reducerea timpilor de reacție).

4. Alegeți un efect negativ (risc) de la punctul 2. Precizați și motivați două măsuri/recomandări de reducere a acestuia. (1p)

Criterii de punctare:
0,25p – pentru fiecare măsură/recomandare precizată
0,25p – pentru motivarea logică a fiecărei măsuri/recomandări

Risc	Măsuri/recomandări	Motivarea logică
1. generarea de disfuncționalități ale site-urilor web aparținând unor instituții oficiale și companii	1. dezvoltarea metodelor și tehnologiilor de combatere/prevenire a atacurilor cibernetice	1. protecția eficientă a datelor, identificarea în timp util și sancționarea atacatorilor, evitarea pierderilor financiare, evitarea afectării imaginii instituției/companiei
	2. informarea cetățenilor cu privire la metodele de protecție împotriva unor atacuri cibernetice	2. protejarea datelor cu caracter personal, conștientizarea asupra riscurilor, sesizarea în timp util a situațiilor de risc

<u>Subiect II</u> Sunteți jurnalist în cadrul unei publicații online care monitorizează evoluțiile în domeniul securității cibernetice și redactorul v-a pus la dispoziție textele prezentate mai sus (4 p):

1. Redactați un material de informare adresat publicului larg, de maximum 150 de cuvinte, în care să sintetizați aspectele din texte și să includeți trei idei principale, relevante pentru situația menționată. Stabiliți un titlu de maximum 10 cuvinte pentru materialul elaborat.

Se acordă 0,75p pentru elaborarea unui material care include trei idei principale, 0,50p pentru elaborarea unei sinteze pertinente, corect formulată, care să includă aspectele menționate în cerință și 0,25p pentru stabilirea titlului.
Total: 1,50p

Criterii de punctare:
0,25p – pentru fiecare idee principală inclusă în material;
0,50p – pentru elaborarea unei sinteze pertinente, corect formulată, care să includă aspectele menționate în cerință;
0,25p – pentru alegerea unui titlu relevant.

<u>Exemplu de idei principale:</u>

- intensificarea și diversificarea atacurilor cibernetice la nivel național;
- creșterea numărului de atacuri revendicate de gruparea Killnet;
- sistarea temporară a site-urilor și serviciilor online oferite de diferite instituții și companii;
- diversificare a atacurilor prin utilizarea unor noi metode care vizează infectarea cu aplicaţii malware de tip ransomware a sistemelor informatice ale organizaţiilor deja atacate prin DDoS, ce au ca efect compromiterea datelor utilizatorilor;
- implicarea activă a ANCOM și DNSC în combaterea/prevenirea atacurilor cibernetice.

<u>Exemple titlu</u>:

- Intensificarea atacurilor cibernetice la nivelul României;
- Rolul DNSC și ANCOM în combaterea atacurilor cibernetice;
- Impactul atacurilor cibernetice asupra funcționării instituțiilor și companiilor în România.

2. Pe baza unuia dintre riscurile identificate la cerința I.2, propuneți o persoană cu expertiză, dintr-un mediu relevant, cu care ați realiza un interviu pentru a obține <u>date</u>

suplimentare față de cele cuprinse în texte. Motivați alegerea în maximum 100 de cuvinte. (1,30p)

Nu se punctează alegerea unor persoane care ocupă funcții înalte în stat sau în cadrul organizațiilor suprastatale.

Criterii de punctare:
0,30p – pentru precizarea persoanei;
1p – pentru motivare și corelare cu persoana/riscul identificat (posibilitatea reală de a contacta persoana, accesul direct al persoanei la informații, competențele persoanei, studiile/pregătirea persoanei etc.).

Exemplu persoană:

- un specialist recunoscut/expert în domeniul securității cibernetice;
- un specialist ANCOM;
- un specialist DNSC;
- un specialist din mediul universitar (ex. Universitatea Politehnică);
- un specialist în domeniul IT;
- un jurist.

3. Scrieți 6 întrebări pe care le-ați adresa persoanei alese la cerința II.2, utile pentru a obține date suplimentare față de cele cuprinse în texte. (1,20p)

Criterii de punctare:
0,20p – pentru fiecare întrebare corelată cu persoana identificată la cerința II.2.

Exemple:

- Care este profilul atacatorilor?
- Care este frecvența atacurilor?
- Ce alte riscuri sunt asociate?
- Care a fost *modus operandi* al grupării Killnet în alte cazuri?
- Care sunt sancțiunile în cazul atacurilor cibernetice?
- Care sunt principalele metode de finanțare ale grupării?
- Care sunt recomandările DNSC/ANCOM pentru protejarea datelor?
- Unde a mai operat gruparea Killnet și care au fost prejudiciile create?
- Care ar fi cele mai bune metode de protecție?
- Care este rolul universității în educarea studenților cu privire la securitatea datelor?

NOTĂ
Se acordă:

- **0,50 p** *pentru corectitudine gramaticală (0,30p) şi respectarea cerinţelor referitoare la numărul maxim de cuvinte (0,20p)*
- **1 punct** din oficiu