ROMÂNIA
SERVICIUL ROMÂN DE INFORMAŢII
ACADEMIA NAŢIONALĂ DE INFORMAŢII
„MIHAI VITEAZUL"
Program postuniversitar de educație permanentă
dedicat formării ofițerilor de informații
Introducere în Analiza de Intelligence

PROBĂ SCRISĂ PENTRU EVALUAREA APTITUDINILOR NECESARE FORMĂRII OFIȚERILOR DE INFORMAȚII

VARIANTA 3

Citiţi informaţiile de mai jos:

Informația 1

În raportul anual „Digital Defence", Microsoft a analizat amenințările cibernetice din perioada iulie 2023 – iunie 2024 și modul în care infractorii și națiunile străine se folosesc de *hacking*, *spear phishing*, *malware* și alte tehnici pentru a obține acces și control asupra calculatoarelor victimelor. Microsoft a observat că anumite țări au început să folosească inteligența artificială pentru a-și desfășura atacurile.

Potrivit Microsoft, au loc peste 600 de milioane de atacuri cibernetice în fiecare zi, parțial alimentate de o tendință de creștere a grupurilor de hackeri afiliate Rusiei, Coreei de Nord sau Iranului. Utilizarea inteligenței artificiale în atacurile cibernetice a crescut și ea în anul 2024, infractorii cibernetici folosind conținut generat de inteligența artificială pentru a păcăli utilizatorii.

Microsoft arată că Rusia și-a concentrat o mare parte a operațiunilor cibernetice asupra Ucrainei, încercând să pătrundă în sistemele militare și guvernamentale și să răspândească dezinformare, pentru a submina sprijinul aliaților. Spre exemplu, în iunie 2024, un grup de hackeri a reușit să compromită cel puțin 50 de dispozitive militare ucrainene.

Pe de altă parte, în Coreea de Nord a fost dezvoltată o nouă tehnologie *ransomware* denumită *FakePenny*, pe care Microsoft afirmă că infractorii nord-coreeni au folosit-o împotriva organizațiilor din domeniul apărării. În ceea ce privește Iranul, Microsoft spune că acesta s-a concentrat în mod semnificativ asupra Israelului. Printre infracțiunile cibernetice înfăptuite de hackerii iranieni se numără piratarea anumitor site-uri și preluarea controlului unor baze de date pentru a obține sume de bani.

Toate cele trei țări au vizat inclusiv SUA, în contextul alegerilor prezidențiale care au avut loc în luna noiembrie 2024. S-au folosit de site-uri web și conturi de social media false pentru a răspândi informații false și înșelătoare cu privire la alegeri. Microsoft atrage atenția că hackerii au colaborat cu guverne pentru a obține finanțare – „Observăm în fiecare dintre aceste țări (Rusia, Coreea de Nord, Iran și

China) această tendință de a combina activitățile statului național cu cele ale infractorilor cibernetici", a declarat Tom Burt, vicepreședinte pentru securitate al Microsoft.

Informația 2

European Digital Media Observatory (EDMO) – program finanțat de Uniunea Europeană (UE) din care fac parte 34 de organizații – a publicat un newsletter referitor la acțiuni de dezinformare și narative false promovate de actori statali sau nonstatali pe teritoriul UE în cursul lunii mai 2024. Au fost analizate un total de 1.643 de articole de verificare a faptelor (*fack checking*). Dintre acestea, 250 (15%) s-au axat pe dezinformarea legată de UE – cel mai ridicat nivel, de când a început monitorizarea dedicată a EDMO, în mai 2023. Alte teme de dezinformare au fost: războiul din Ucraina (121 – 8 %), schimbările climatice (104 – 6%), confictul dintre Israel și Hamas (152 – 9%), pandemia COVID-19 (104 – 6%), imigrație (97 – 6%) și problemele LGBTQ+ și de gen (36 – 2%).

Ponderea dezinformărilor despre UE a fost cea mai ridicată pentru a doua lună consecutiv, mai arată newsletterul citat. Dezinformarea legată de schimbările climatice a scăzut semnificativ, aproape înjumătățindu-se. Poveștile false despre Ucraina au scăzut ușor în număr, la fel ca cele referitoare la conflictul din Orientul Mijlociu, în timp ce dezinformarea cu privire la alte subiecte monitorizate în mod constant a rămas stabilă.

Narativele false care au vizat UE au fost diverse, dar consecvente în a o prezenta ca fiind coruptă sau opusă diferitelor interese naționale. Unele narative false au atacat liderii UE. De exemplu, președinta Comisiei Europene, Ursula Von der Leyen, a fost vizată și descrisă ca fiind legată de nazism, având un conflict de interese în gestionarea pandemiei COVID-19 sau chiar arestată în Parlamentul European. De asemenea, în Franța, narativele false s-au axat pe ideea că Ursula Von der Leyen „nu a fost aleasă de nimeni", în urma unui efort mai larg de a descrie instituțiile UE ca fiind antidemocratice.

În unele țări au apărut narative false care sugerează manipulări și fraude înainte de alegerile europarlamentare. În Germania s-a afirmat că buletinele de vot cu găuri sau colțuri tăiate vor fi invalide „de la început", că votul pentru partidul de extremă dreapta AfD ar urma să fie manipulat sau chiar că acest partid va fi exclus din alegerile europene. Alte afirmații false care au circulat în Germania – similare altora identificate în Spania – păreau să aibă ca scop împingerea cetățenilor să își invalideze alegerile legitime, sugerând votul multiplu sau semnarea buletinelor de vot, practici care ar invalida alegerile legitime ale cetățenilor.

Cele mai circulate subiecte de dezinformare în România:

- soția celui care l-a împușcat pe premierul slovac Fico este un refugiat ucrainean;
- imagini, videoclipuri și alte conținuturi false care exagerează escaladarea conflictului din Ucraina cu implicarea directă a Occidentului/NATO în confict;

- sprijinul acordat de SUA pentru naziștii din Ucraina;
- estimări greșite ale ONU privind numărul de copii și femei uciși în Gaza.

Procentul de narative de dezinformare care utilizează conținut generat de inteligența artificială a scăzut ușor în luna mai, potrivid EDMO. Din cele 1.643 de articole de verificare a faptelor, 59 au folosit această tehnică de dezinformare, număr care corespunde unui procent de 4% din total.

Această situație este în concordanță cu previziunile EDMO privind circulația redusă a conținutului generat de inteligența artificială înainte de alegeri, din cauza limitărilor actuale ale tehnologiei disponibile. Cu toate acestea, este posibil ca un conținut generat de inteligența artificială deosebit de dăunător și cu potențial de impact, de exemplu deepfake audio, să circule în ultimele zile și ore înainte de vot, așa cum s-a întâmplat în Slovacia, înainte de alegerile naționale din septembrie 2023.

Informația 3

Un studiu realizat de Information Systems Audit and Control Association (ISACA) a arătat că 39% dintre cele aproape 6.000 de organizații globale intervievate recunosc că se confruntă cu mai multe atacuri cibernetice, iar 15% dintre acestea suferă de mai multe încălcări ale confidențialității, comparativ cu 2023. Mai mult de 60% dintre profesioniștii europeni din domeniul securității cibernetice afirmă că echipa de securitate cibernetică a organizației lor nu dispune de suficient personal, iar 52% consideră că bugetul de securitate cibernetică al organizației lor este subfinanțat.

Majoritatea atacurilor cibernetice sunt de tip *ransomware*. Acesta implică blocarea datelor sau a fișierelor unui utilizator până la plata unei răscumpărări. „Sofisticarea inteligenței artificiale face ca aceste atacuri să fie foarte, foarte greu de detectat", a declarat Chris Dimitriadis, Chief Global Strategy Officer la ISACA. El a explicat că inteligența artificială generativă (GenAI) poate analiza profilurile victimelor din cadrul organizațiilor și apoi poate genera conținut care simulează un om.

În februarie 2024, Microsoft și OpenAI au dezvăluit că hackerii folosesc modele lingvistice mari (LLM) pentru a perfecționa atacurile cibernetice. Companiile au detectat încercări din partea Rusiei, Coreei de Nord, Iranului și a grupurilor susținute de China. Acestea au utilizat *chatbot*-uri pentru cercetarea țintelor și îmbunătățirea scenariilor. Ambele companii au declarat că lucrează pentru a minimiza potențialul de utilizare abuzivă de către astfel de actori. Dar au recunoscut că nu pot opri toate cazurile.

Modul în care companiile se pot proteja este să se asigure că dispun de platforme tehnologice adaptate amenințărilor viitoare și să sprijine profesioniștii din domeniul securității cibernetice. ISACA a constatat că 71% dintre companii au raportat că organizația lor nu oferă personalului instruire de siguranță, iar jumătate din numărul echipelor de securitate cibernetică au declarat că sunt subfinanțate. „Cu mai puține fonduri, este foarte greu să pună în aplicare capacitățile de securitate cibernetică potrivite în cadrul organizațiilor lor", a declarat Dimitriades.

Informația 4

Înalți funcționari din domeniul securității cibernetice din statele membre ale UE și din cadrul Comisiei participă la exercițiul anual „Planul de acțiune la nivel operațional" (Blue OLEx) pentru a testa gradul de pregătire al UE în cazul unei crize cibernetice. Margrethe Vestager, vicepreședinta executivă în cadrul Comisiei Europenene, responsabilă pentru programul Europa pregătită pentru era digitală, a declarat: „acest exercițiu ne va ajuta să ne consolidăm mijloacele de apărare în materie de securitate cibernetică și să asigurăm un mediu digital mai sigur pentru cetățenii și întreprinderile noastre din toate statele membre".

Ediția din acest an este condusă de autoritățile italiene, cu sprijinul Agenției UE pentru Securitate Cibernetică (ENISA). În 2024, Blue OLEx se axează pe cooperarea la nivel executiv, în special prin intermediul Rețelei organizațiilor de legătură în caz de criză cibernetică (EU-CyCLONe), care a fost instituită atunci când a intrat în vigoare Directiva privind măsuri pentru un nivel comun ridicat de securitate cibernetică în Uniune (Directiva NIS2). Exercițiul îi va ajuta pe liderii în materie de securitate cibernetică să identifice domeniile în care se pot aduce îmbunătățiri în ceea ce privește modul standardizat de răspuns la incidente și crize.

Scopul EU CyCLONe este de a contribui la gestionarea incidentelor și crizelor cibernetice de mare amploare la nivel operațional. Acesta completează structurile de securitate cibernetică existente la nivelul UE prin corelarea cooperării la nivel tehnic, cum ar fi Centrul de răspuns la incidente de securitate informatică (CSIRT) și la nivel politic, cum ar fi mecanismul integrat pentru un răspuns politic la crize (IPCR). Rezultatele obținute în cursul exercițiului vor contribui la evaluarea Planului de acțiune pentru un răspuns coordonat la incidentele și crizele de securitate cibernetică de mare amploare, adoptat în 2017.

CERINȚE

Subiect I. Raportat strict la informațiile de mai sus (5,50p):

1. Formulați patru efecte negative (riscuri) generate de situațiile prezentate în cadrul textelor. (1,60p)
2. Alegeți un efect negativ (risc) identificat și menționați doi indicatori care vă pot ajuta să monitorizați evoluția acestuia. (0,80p)
3. În baza efectului negativ (risc) identificat la punctul 2, redactați un scenariu (realist, posibil, pertinent, plauzibil) referitor la evoluția securității cibernetice în spațiul european de cel mult 150 de cuvinte. Scenariul trebuie să releve factorii care ar putea conduce la materializarea riscului, modul concret în care s-ar materializa acesta și evoluția probabilă a problematicii. (1,20p)
4. Alegeți un efect negativ (risc) de la punctul 2. Precizați și motivați două măsuri/recomandări de reducere a acestuia. (1p)

5. Citiți următorul fragment de text și precizați două aspecte insuficient detaliate în acesta, care v-ar ajuta să înțelegeți mai bine situația. (0,90p)

> ***„Microsoft arată că Rusia și-a concentrat o mare parte a operațiunilor cibernetice asupra Ucrainei, încercând să pătrundă în sistemele militare și guvernamentale și să răspândească dezinformare, pentru a submina sprijinul aliaților. Spre exemplu, în iunie 2024, un grup de hackeri a reușit să compromită cel puțin 50 de dispozitive militare ucrainene."***

Subiect II. Sunteți jurnalist în cadrul unei publicații online care monitorizează evoluțiile înregistrate în domeniul securității cibernetice și redactorul v-a pus la dispoziție textele prezentate mai sus (3p):

1. Redactați un material de informare adresat publicului larg, de maximum 200 de cuvinte, care să contribuie la o mai bună înțelegere a riscurilor din informațiile prezentate. Stabiliți un titlu de maximum 10 cuvinte pentru materialul elaborat. (2,10p)
   Se acordă 1,20p pentru elaborarea unui material care include riscurile și oportunitățile identificate la subiectul I, punctul 1 și argumentează coerent impactul acestora, 0,60p pentru elaborarea unei sinteze care facilitează transmiterea eficientă a mesajului într-o manieră clară și concisă și 0,30p pentru stabilirea titlului.

2. Redactați un rezumat/abstract de maximum 80 de cuvinte în care să includeți trei idei principale surprinse în materialul realizat la Subiectul II, punctul 1. (0,90p)

***

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