BULETIN CYBERINT

SEMESTRUL II - 2022


TIMELINE
CYBERINT

➲ În data de 24 februarie 2022, FBI, Cybersecurity and Infrastructure Security Agency (CISA), US Cyber Command Cyber National Mission Force (CNMF) și National Cyber Security Centre United Kingdom (NCSC-UK) au atribuit public o serie de atacuri cibernetice derulate de către actorul cibernetic de origine iraniană, APT MUDDYWATER (asociat Ministerului de Intelligence și Securitate/ MOIS al Iranului). Atacurile au fost îndreptate împotriva unei game largi de organizații guvernamentale și private din domeniile telecomunicații, apărare, administrație publică locală, precum și petrol și gaze naturale din Asia, Africa, Europa și America de Nord.

➲ În contextul conflictului militar dintre Federația Rusă și Ucraina, între membrii de origine rusă și ucraineană ai grupării de criminalitate cibernetică CONTI au apărut divergențe care s-au soldat cu scurgeri de date în mediul online, cu privire la: resursele și serviciile utilizate, precum și recomandări generale pentru derularea cu succes a atacurilor cibernetice, instrumente și tehnici utilizate în procesul de injecție a *malware*-ului, tehnici defensive utilizate de instrumentele antivirus/ de detectare a intruziunilor și modalități de ocolire a acestora.

➲ Comisia Europeană a publicat în iunie 2020 raportul „*Twinning the green and digital transitions in the new geopolitical context*" în cadrul căruia punctează domeniile cheie de acțiune cu obiectivul de a maximiza coerența între climă și ambițiile noastre digitale.

AVÂND CA REPER ANUL 2050, UE ARE ÎN VEDERE:

- rezilienta intersectorială și autonomia strategică deschisă cu scopul de a face față noilor provocări globale;
- politici solide în materie de securitate cibernetică și de date;
- crearea cadrului de reglementare adaptat exigențelor viitorului și propice, inclusiv prin utilizarea inteligenței artificiale;
- investiții strategice suplimentare, în special în cercetare și inovare și tehnologii noi;
- intensificarea diplomației ecologice și a celei digitale prin valorificarea puterii de reglementare și de standardizare;
- sprijinirea tranziției pentru locuri de muncă noi prin adaptarea sistemelor de educație și formare;
- gestionarea strategică a aprovizionării cu bunuri critice pentru a spori diversificarea și de a reduce la minim riscul de dependențe noi;
- dezvoltarea de cadre pentru monitorizarea bunăstării;
- elaborarea de standarde pentru ecologizarea digitalizării;
- asigurarea coeziunii prin consolidarea protecției sociale și a statutului social.

➲ În data de 18 iulie 2022, guvernul belgian a realizat o atribuire publică a atacurilor cibernetice derulate pe parcursul anului 2021 de actori cibernetici de origine chineză APT 27, 30, 31 și GALLIUM/ UNSC 2814/ SOFTCELL asupra unor entități guvernamentale din Belgia (Ministerul de Interne și Ministerul de Apărare din Belgia).

➲ Cetățeanul român Mihai Păunescu, în vârstă de 37 de ani, arestat anul trecut în Columbia, a fost extrădat în iulie 2022 în Statele Unite ale Americii, fiind acuzat că a administrat un serviciu de găzduire online care a fost utilizat în distribuirea de *malware* Gozi.

➲ Mai multe *website*-uri guvernamentale din Taiwan au fost vizate de atacuri cibernetice de tip DDoS în timpul vizitei la Taipei din perioada 2-3 august 2022 a președintelui Camerei Reprezentanților SUA, Nancy Pelosi. Printre victimele atacurilor s-au numărat: versiunea în limba engleză a portalului guvernamental și *website*-urile Biroului Prezidențial, Ministerului de Externe și Ministerului Apărării. Experții în securitate cibernetică din Taiwan apreciază că în spatele atacurilor se află o entitate care susține interesele Republicii Populare Chineze.

ELIMINAREA AMENINȚĂRII CIBERNETICE GENERATĂ DE **APT SANDWORM**

În prima jumătate a anului 2022, a fost identificată o campanie cibernetică derulată de actorul de origine rusă APT SANDWORM (atribuit Serviciului Militar de Informații al Federației Ruse/ GRU) și denumită CYCLOPS BLINK. Campania viza infectarea de dispozitive *firewall* produse de compania americană WatchGuard și routere de internet produse de compania ASUS, localizate cu precădere pe teritoriul Europei și Americii de Nord.

APT SANDWORM a vizat compromiterea cât mai multor dispozitive pentru includerea acestora într-un *botnet*. Există 2 ipoteze cu privire la scopul în care APT SANDWORM urma să utilizeze acest *botnet*: (1) pentru derularea de atacuri cibernetice (cel mai probabil în contextul conflictului militar actual) sau (2) drept elemente de infrastructură pentru alte tipuri de activități cibernetice.

Pe plan național, SRI a acționat pentru prevenirea și eliminarea amenințării cibernetice generată de APT SANDWORM prin derularea demersurilor necesare sanitizării dispozitivelor infectate de actorul cibernetic rus.

Pe plan internațional, conform comunicatului FBI, autoritățile americane au indisponibilizat serverele de Comandă și Control/ C2 utilizate în rețea (*botmaster*). Astfel, în prezent, APT SANDWORM nu mai poate utiliza *botnet*-ul creat anterior pentru derularea de atacuri cibernetice, dar se menține riscul ca atacatorul să compromită alte dispozitive de același tip, care în prezent nu mai beneficiază de actualizări de software din partea producătorilor.

ATRIBUIREA PUBLICĂ A **ATACULUI CIBERNETIC** ASUPRA INFRASTRUCTURII SATELITARE ÎN BANDĂ KA-SAT

Ulterior începerii conflictului militar dintre Federația Rusă și Ucraina, la nivel european, zeci de mii de terminale care funcționează pe baza infrastructurii satelitare în bandă KA-SAT (deținută de compania VIASAT) au încetat brusc să mai funcționeze în mai multe țări europene, printre care Marea Britanie, Germania, Ucraina, Polonia, Grecia, Franța, Ungaria și România.

Nefuncționarea acestor terminale a fost cauzată de un atac cibernetic și a avut impact ridicat asupra telecomunicațiilor, fiind afectați mai mulți furnizori de servicii în bandă largă prin satelit (ex. EUTELSAT Franța și ORANGE) și companii care au contractat servicii de la furnizorii afectați. Spre exemplu, compania germană ENERCON a anunțat că aproximativ 5.800 dintre turbinele sale eoliene (cel mai probabil, operate de la distanță printr-o legătură SATCOM) au pierdut contactul cu serverul SCADA.

În acest context, la 10 mai 2022, România printr-un comunicat public emis de Ministerul Afacerilor Externe, s-a alăturat demersurilor internaționale de atribuire către Federația Rusă a acestui atac cibernetic. De asemenea, MAE a condamnat atacurile cibernetice derulate de Federația Rusă asupra Ucrainei în contextul conflictului actual.

RANSOMWARE
CAMPANIA HIVE

În ultimul an, amenințările cibernetice generate de atacurile *ransomware* au continuat să se mențină la un nivel ridicat, vizând nu doar utilizatori individuali, ci și entități private sau chiar instituții publice. Atacurile *ransomware* continuă să reprezinte o variantă preferată de actorii cibernetici motivați financiar, aceștia utilizând inclusiv noi tactici (*triple extortion*) pentru a-și maximiza profiturile.

Triple extortion presupune obținerea de beneficii financiare atât de la victimele atacurilor *ransomware*, cât și de la clienții/partenerii acestora, prin șantajarea celor din urmă cu publicarea unor date confidențiale. În unele situații, atacatorii amenință victimele că, în cazul în care nu va fi achitată recompensa solicitată, un atac cibernetic de tip DDoS va fi derulat împotriva rețelelor și sistemelor informatice de la nivelul entității victimă. Această tactică este cunoscută inclusiv sub denumirea de *ransom-DDoS*.

La nivel național, principala aplicație *malware* utilizată de actorii cibernetici motivați financiar a fost *ransomware*-ul HIVE, utilizat atât pentru criptarea datelor victimei, cât și pentru indisponibilizarea unor resurse informatice.

HIVE este o aplicație *malware* de tip *ransomware*, comercializată în regim *Ransomware-as-a-Service*. Aceasta a fost observată pentru prima dată în iulie 2021, fiind utilizată în atacurile cibernetice derulate împotriva mai multor platforme *software* – Windows, Linux, ESXI Hypervisor.

Dintre atacurile cibernetice de tip *ransomware* derulate cu aplicația *malware* HIVE atrage atenția cel asupra unei companii de carburanți din România, în cadrul căruia atacatorii au criptat elemente de infrastructură IT&C, solicitând suma de 2 milioane de dolari drept răscumpărare. Pentru limitarea pagubelor, compania și-a suspendat temporar serviciile online, inclusiv serviciul de alimentare rapidă din benzinării. Cu toate acestea, benzinăriile și-au continuat activitatea, fiind disponibilă posibilitatea de a achita atât numerar, cât și prin card bancar.

INFO BOX

TACTICI, TEHNICI & PROCEDURI ASOCIATE HIVE

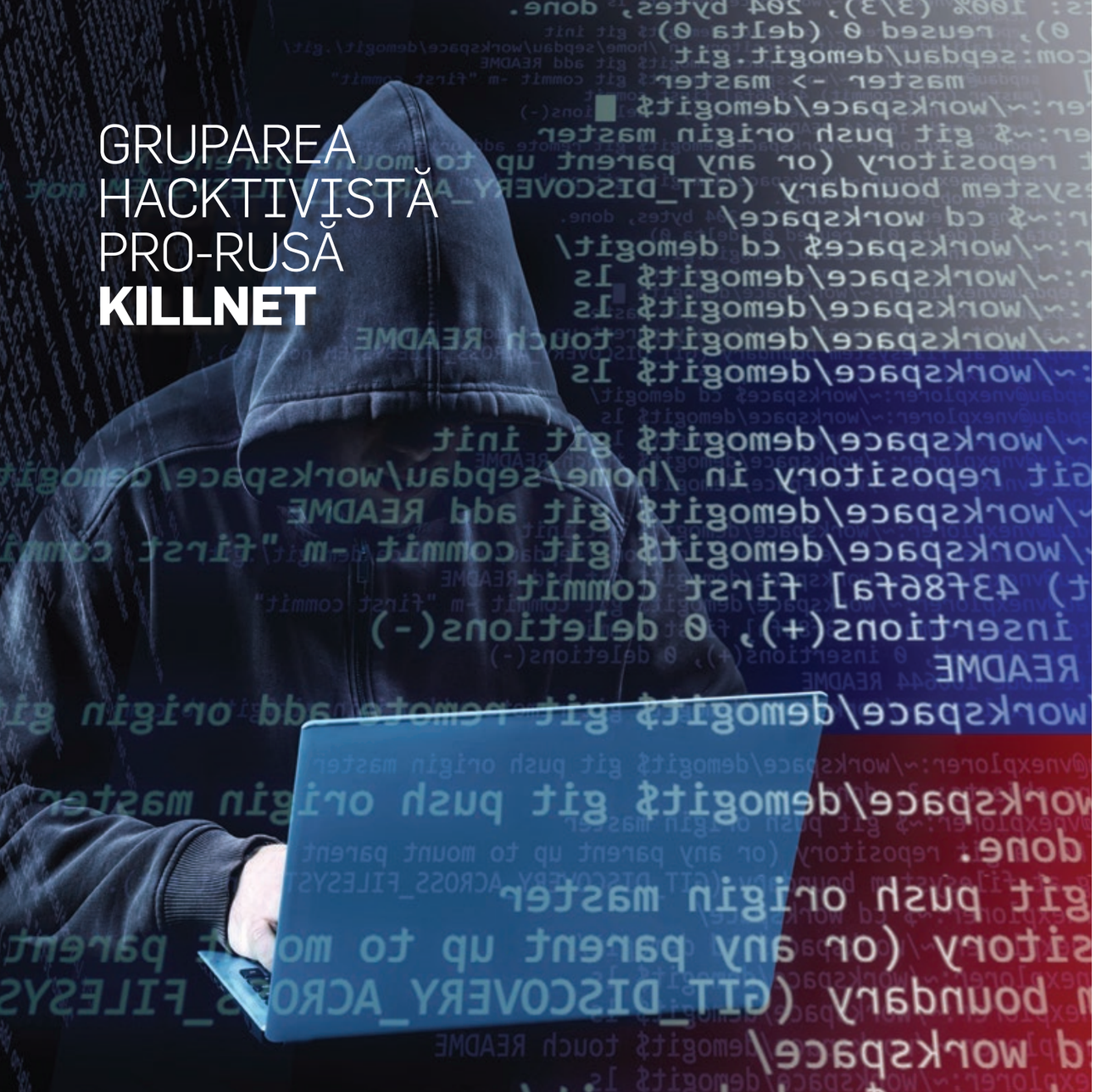
Ransomware-ul **HIVE** reprezintă o provocare majoră pentru companiile și infrastructurile cu valențe critice la nivel mondial, întrucât operatorii acestui *ransomware* vizează compromiterea și extorcarea entităților din domenii esențiale. Concret, în prima parte a anului 2022, la nivel mondial au fost identificate 186 de atacuri cibernetice cu *malware*-ul **HIVE** asupra sectorului energetic, 125 asupra celui medical și 102 asupra domeniului financiar.

De la prima operaționalizare a acestui *malware* și până în prezent au fost observate o serie de modificări tehnice la nivelul **HIVE**, care au influențat inclusiv tacticile, tehnicile și procedurile utilizate de atacatori.

În vederea asigurării accesului inițial, operatorii **HIVE** utilizează atât e-mailuri de tip *phishing*, dar și exploatarea **RDP**-ului (Remote Desktop Protocol). *Malware*-ul deține capabilitatea de a opri serviciile de securitate existente la nivelul sistemului informatic infectat și de a șterge eventuale *back-up*-uri, care să prevină recuperarea datelor.

Pentru a asigura reziliența cibernetică a instituțiilor în fața atacurilor de tip ransomware se recomandă implementarea unor politici și măsuri de securitate precum:

- Utilizarea unei soluții de antivirus actualizate;
- Dezactivarea serviciului RDP de pe toate stațiile și serverele de lucru;
- Actualizarea sistemelor de operare și a tuturor aplicațiilor din rețea;
- Schimbarea frecventă a parolelor tuturor utilizatorilor, respectând recomandările de complexitate;
- Verificarea periodică a tuturor utilizatorilor înregistrați, pentru a identifica utilizatorii noi, adăugați în mod nelegitim;
- Realizarea unor copii de siguranță pentru datele critice pe suporți de date offline;
- Păstrarea datelor criptate în eventualitatea în care ar putea apărea o aplicație de decriptare în mediul online.



GRUPAREA HACKTIVISTĂ PRO-RUSĂ **KILLNET**

Declanșarea conflictului ruso-ucrainean a generat intensificarea activităților derulate de entitățile hacktiviste în mediul virtual, acestea venind în sprijinul intereselor Federației Ruse sau Ucrainei, sub forma unui război cibernetic.

Una dintre cele mai active și vizibile entități, care s-a remarcat prin susținerea discursului de propagandă rusească, a fost gruparea hacktivistă KILLNET.

Aceasta s-a evidențiat la nivelul României începând cu data de 29 aprilie 2022, la scurt timp după vizita unor oficiali români în Ucraina, printr-o amplă campanie de atacuri cibernetice de tip DDoS, care au vizat rețelele și sistemele informatice localizate pe teritoriul național, din domenii precum: guvernamental, apărare, transporturi, bancar, energetic, mass-media etc.

Deși efectele atacurilor cibernetice nu au generat un impact semnificativ, acestea au fost în măsură să creeze prejudicii de imagine la adresa statului și să blocheze accesul utilizatorilor la servicii și resurse informatice.

Exponenții KILLNET și-au motivat atacurile cibernetice derulate pe fondul sprijinului oferit de România Ucrainei în contextul conflictului militar.

Printre alte ținte ale atacurilor cibernetice derulate de gruparea hacktivistă pro-rusă se numără Germania, Lituania, Republica Moldova, Republica Cehă, Italia și Statele Unite ale Americii.

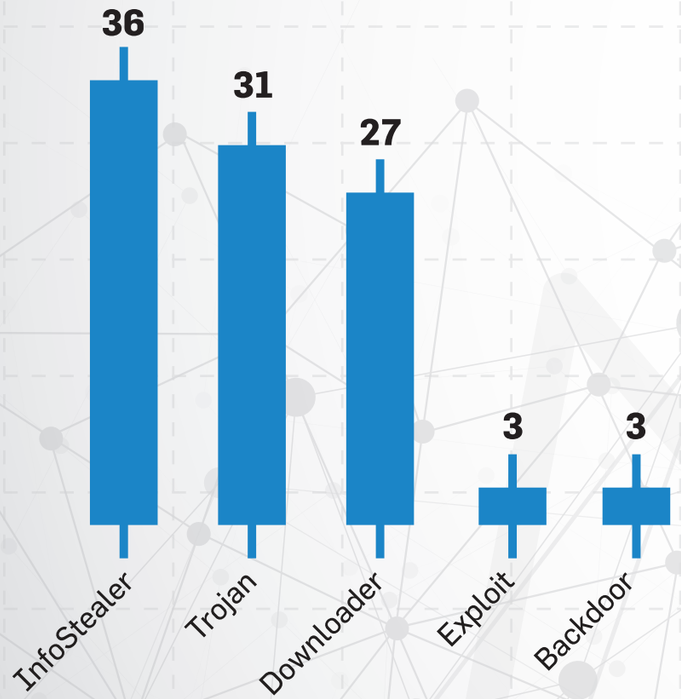
Aceste inițiative au fost rapid preluate și promovate de alți utilizatori din mediul virtual, care s-au raliat demersurilor exponenților KILLNET, o parte dintre aceștia coagulându-se sub forma unor grupuri de hackeri cu obiective similare.

Apreciem faptul că, atâta vreme cât va dura conflictul militar dintre Federația Rusă și Ucraina, actorii cibernetici motivați ideologic își vor continua activitățile ostile în mediul virtual sub aceleași argumente.

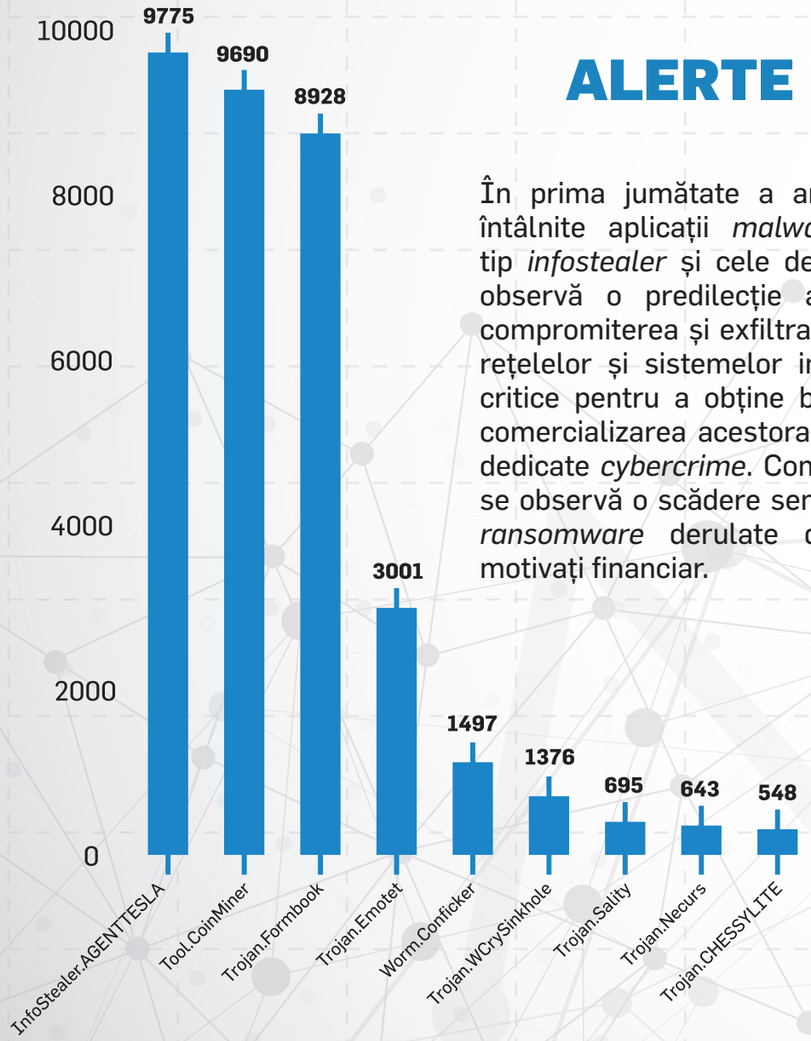
STATISTICI

În perioada ianuarie-iunie 2022 au fost înregistrate un număr total de 64.308 de alerte de securitate provenite de la *Sistemul național de protecție a infrastructurilor IT&C de interes național împotriva amenințărilor provenite din spațiul cibernetic (Țițeica)* au rezultat următoarele informații:

CELE MAI UTILIZATE TIPURI DE APLICAȚII MALWARE

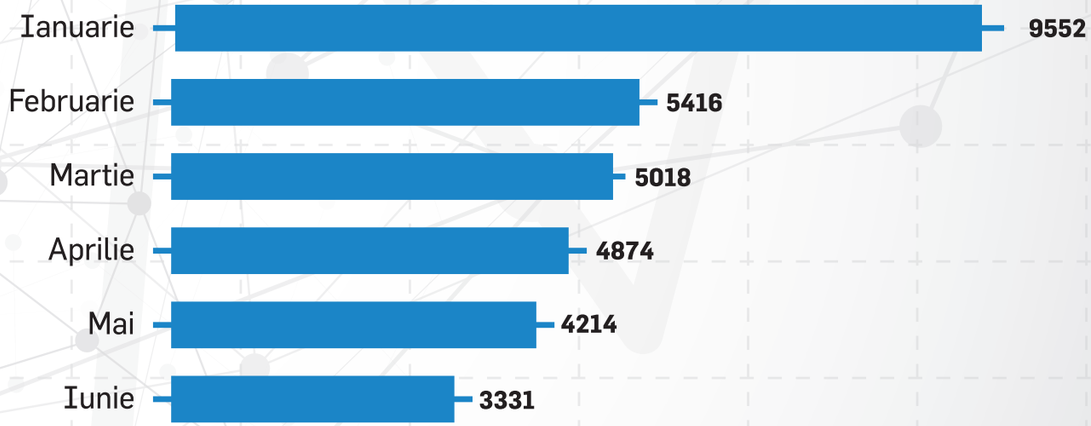


TOP 10 ALERTE MALWARE



În prima jumătate a anului 2022, cele mai întâlnite aplicații *malware* au fost cele de tip *infostealer* și cele de tip *troian*. Astfel, se observă o predilecție a atacatorilor pentru compromiterea și exfiltrarea de date din cadrul rețelelor și sistemelor informatice cu valențe critice pentru a obține beneficii financiare din comercializarea acestora la nivelul forumurilor dedicate *cybercrime*. Comparativ cu anul 2021, se observă o scădere semnificativă a atacurilor *ransomware* derulate de actorii cibernetici motivați financiar.

FRECVENȚA LUNARĂ A ACTIVITĂȚILOR DE PHISHING



CONFERINȚA PLENIPOTENȚIARILOR **UNIUNII INTERNAȚIONALE A COMUNICAȚIILOR**

În perioada 26 septembrie – 14 octombrie a.c., la Palatul Parlamentului din București va avea loc cea de-a 21-a ediție a Conferinței Plenipotențiarilor Uniunii Internaționale a Comunicațiilor organizată de Autoritatea Națională pentru Administrare și Reglementare în Comunicații (ANCOM).

Conferința Plenipotențiarilor reprezintă organismul suprem al Uniunii Internaționale a Comunicațiilor (ITU), care se reunește o dată la 4 ani și are rolul de a adopta politica generală a ITU, planurile strategice și financiare ale organizației și de a alege conducerea acesteia.

Din punct de vedere al numărului de participanți și al duratei de desfășurare, Conferința Plenipotențiarilor ITU de la București reprezintă cea mai mare reuniune organizată în România, de la admiterea țării noastre ca stat membru al ONU, în anul 1955, fiind așteptați 2.000 de oficiali din 191 de state ale lumii.

În cadrul Conferinței Plenipotențiarilor din acest an (PP-22) se va decide rolul organizației în ansamblu, capacitatea de a influența direcții specifice legate de domeniul IT&C, precum convergența tehnologiilor, dezvoltarea Internetului și serviciul universal.

Având în vedere că mandatul actualului secretar general al ITU, Houlin Zhao, este la final (acesta fiind deja la al doilea mandat), în cadrul Conferinței PP-22 de la București vor avea loc alegeri pentru șefia ITU. De asemenea, se vor organiza alegeri și pentru secretarul general adjunct și directorii birourilor din sectorul radiocomunicațiilor, sectorul de standardizare a telecomunicațiilor și sectorul de dezvoltare a telecomunicațiilor, precum și pentru membrii Comitetului pentru reglementări radiofonice. În cadrul PP-22 vor fi alese statele membre care vor constitui următorul Consiliu al ITU, care va acționa ca organ de conducere, în intervalul dintre conferitele plenipotențiarilor (PP).

Lucrările Conferinței PP-22 vor avea la bază propunerile de dezbateri și discuții avansate de statele membre ITU, care se vor regăsi în Agenda de organizare a evenimentului, în conformitate cu prevederile din art.8 din Constituția ITU.

CONCURSURI ȘI EXERCIȚII
DE SECURITATE CIBERNETICĂ LA NIVEL NAȚIONAL ȘI INTERNAȚIONAL

ROCSC și ECSC

Cea de-a treia ediție a Campionatului Național de Securitate Cibernetică (ROCSC22) a fost organizată în perioada 22 iulie – 6 august 2022 de către Serviciul Român de Informații, împreună cu Directoratul Național de Securitate Cibernetică (DNSC) și Asociația Națională pentru Securitatea Sistemelor Informatice.

Formatul competiției ROCSC22 a constat în două etape:

- Prima etapă de calificare, desfășurată online în perioada 22-23 iulie 2022, la care s-au înscris inițial peste 200 de tineri;

- Etapa finală a concursului, desfășurată la Palatul Parlamentului în data de 6 august 2022, unde 28 de concurenți au rezolvat, timp de 8 ore, probe de securitate web și exerciții din domeniul criptografiei, analizei traficului de rețea, ingineriei inverse și investigațiilor.

Competiția a fost organizată pe două categorii de vârstă: juniori (până la 20 de ani) și seniori (21-25 ani), iar primii 10 clasați din fiecare categorie au primit premii în bani sau echipamente din partea sponsorilor.

INFO BOX

România a debutat la ECSC acum 7 ani, perioadă în care a adăugat în palmares titlul de campioană în 2019 și două titluri de vicecampioană în 2016 și 2017.

Ulterior, finaliștii au participat la un bootcamp de pregătire, organizat la Bran, în perioada 17-21 august. În cadrul bootcamp-ului au fost selectați cei 10 concurenți care au reprezentat România la concursul „European Cyber Security Championship" (ECSC22). Anul acesta, ECSC22 a avut loc la Viena, în perioada 13-16 septembrie, echipa României clasându-se pe locul 8.

Participanții la ROCSC au oportunitatea de a-și testa și îmbunătăți abilitățile tehnice de profil și pot beneficia de recunoaștere națională și promovare, mentorat cu specialiști în domeniu, stagii specializate de pregătire tehnică și soft skills sau oportunități de angajare.

Locked Shields

Centrul de Excelență NATO pentru Apărare Cibernetică din Tallinn a planificat și organizat în perioada 19-21 aprilie exercițiul internațional de apărare cibernetică Locked Shields 2022, care a reunit în mediul online peste 2000 de specialiști militari și civili din 32 de state aliate și partenere.

România a participat, pentru al doilea an consecutiv, cu o echipă interinstituțională formată din 110 specialiști din cadrul instituțiilor din sistemul național de apărare, ordine publică și securitate națională (SRI, MApN, MAI, STS, SPP și SIE), Directoratului Național de Securitate Cibernetică și principalelor companii private din domeniu.

Scopul exercițiului a fost de a perfecționa pregătirea specialiștilor și capacitatea acestora de a acționa în echipe interinstituționale și multidisciplinare în vederea protejării în timp real a rețelelor informatice guvernamentale și infrastructurilor critice naționale împotriva unei game largi de atacuri cibernetice.

CyDex2022

În perioada 4-6 octombrie, Serviciul Român de Informații organizează a șasea ediție a celui mai mare exercițiu național de securitate cibernetică axat pe componenta practică. Anul acesta se preconizează că vor participa peste 100 de instituții publice, entități private și academice, care își vor exersa capacitățile de apărare cibernetică live în poligonul cibernetic al Centrului Național CYBERINT.
Similar cu ediția precedentă, participanții vor lua parte la 6 scenarii practice sau teoretice, cu nivele de complexitate diferite.

#CloudGuvernamental

INFO BOX

Cloudul Privat Guvernamental reprezintă o infrastructură formată dintr-un ansamblu de resurse și servicii utilizate în comun de către autorități și instituții publice, precum și de către structurile aflate în coordonarea și subordonarea acestora.

Implementarea și operaționalizarea platformei de Cloud Privat Guvernamental este un proiect asumat în Planul Național de Redresare și Reziliență (PNRR) al României, Componenta C7 – TRANSFORMARE DIGITALĂ. Proiectul urmărește, în principal, optimizarea activităților și fluxurilor instituționale, în vederea diminuării birocrației și facilitării interacțiunii cu cetățenii.

În context, la data de 27 iunie 2022, a fost adoptată OUG 89/2022 privind înființarea, administrarea și dezvoltarea infrastructurilor și serviciilor informatice de tip cloud utilizate de autoritățile și instituțiile publice.

Conform acestui act normativ, Platforma de Cloud Privat Guvernamental va fi reprezentată de o infrastructură de tip cloud hibrid, prin integrarea caracteristicilor de cloud privat și public, în vederea asigurării unui echilibru între măsurile de securitate cibernetică adoptate și necesitățile impuse de principiile de *flexibilitate, scalabilitate* și *accesibilitate*.

Principalele beneficii care derivă din implementarea și operaționalizarea platformei de Cloud Privat Guvernamental sunt: crearea unei infrastructuri securizate și scalabile, asigurarea unei performanțe ridicate cu eficientizarea costurilor și consolidarea unei poziții superioare în cadrul clasamentului Indicelui Economiei și Societății Digitale (DESI), România ocupând ultimul loc în anii 2021 și 2022.

SECURITATEA CIBERNETICĂ A CLOUDULUI PRIVAT GUVERNAMENTAL

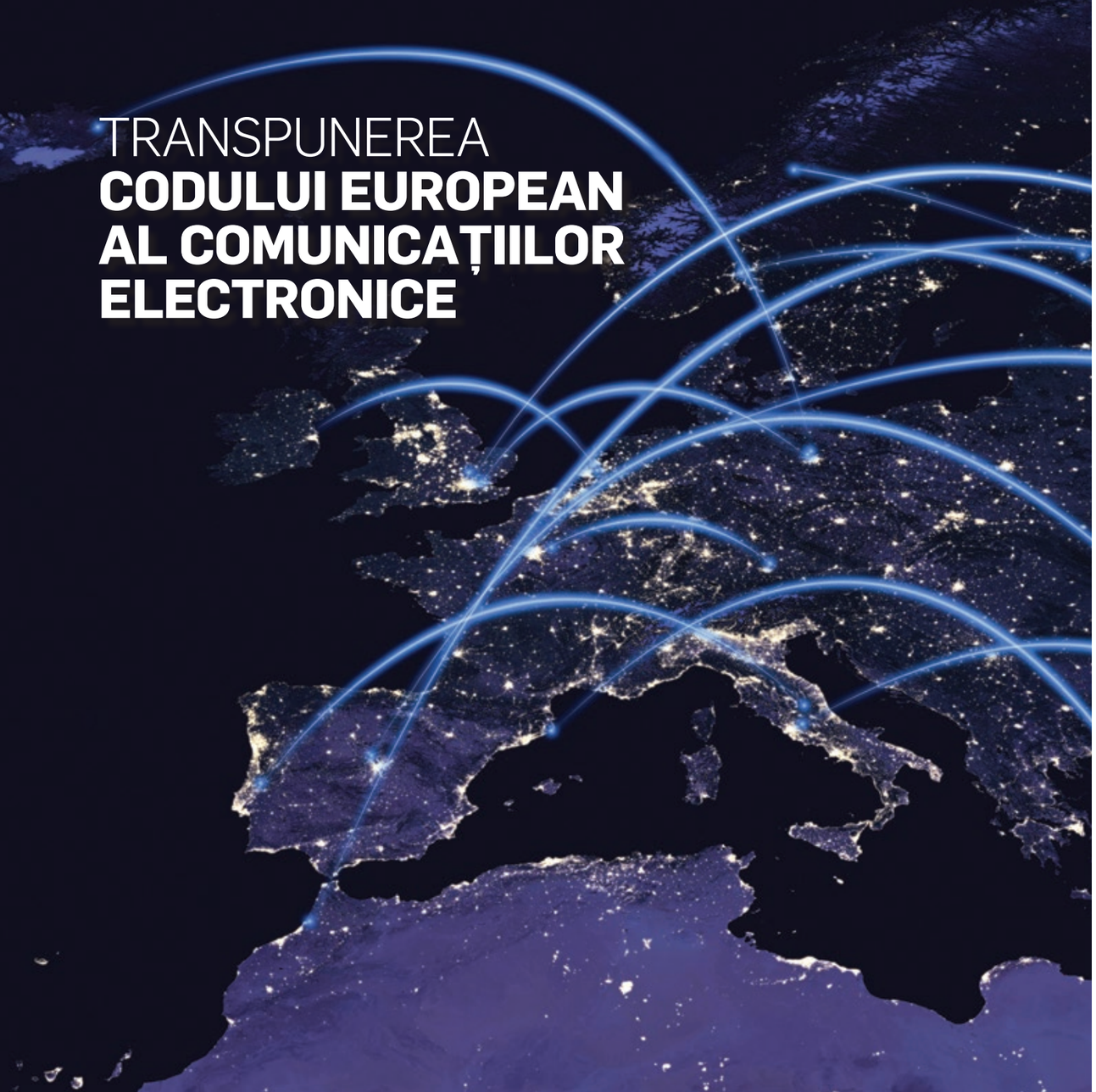
În ultimii ani, actorii cibernetici s-au orientat inclusiv spre exploatarea vulnerabilităților de securitate cibernetică prezente în cadrul platformelor Cloud, care au devenit în scurt timp unele dintre cele mai vizate medii.

Din această perspectivă, componenta de securitate cibernetică reprezintă un pilon important, prin prisma nevoii de protejare a confidențialității, integrității și disponibilității unui volum mare de date vehiculate în cadrul acestei infrastructuri.

În cadrul proiectului se are în vedere aplicarea conceptului de security-by-design, urmând a fi implementate și aplicate servicii și măsuri pentru asigurarea securității cibernetice pentru fiecare componentă a Cloudului Privat Guvernamental, încă din etapa de dezvoltare.

Astfel, prin OUG 89/2022 sunt stabilite responsabilități și atribuții concrete privind asigurarea securității cibernetice a Cloudului Privat Guvernamental care revin Serviciului Român de Informații și Serviciului de Telecomunicații Speciale.

Conform OUG 89/2022, securitatea cibernetică a Cloudului Privat Guvernamental reprezintă starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive și reactive, prin care se asigură confidențialitatea, integritatea, disponibilitatea, autenticitatea și nonrepudierea informațiilor în format electronic aferente resurselor și serviciilor publice sau private din spațiul cibernetic al Cloudului Privat Guvernamental.



TRANSPUNEREA **CODULUI EUROPEAN AL COMUNICAȚIILOR ELECTRONICE**

Codul european al comunicațiilor electronice, reprezintă unul din actele esențiale pentru tranziția digitală a Uniunii Europene, facilitând accesul consumatorilor, persoanelor private și întreprinderilor, la:

- norme clare privind drepturile utilizatorilor și elemente de protecție a consumatorului;
- o mai bună calitate a serviciilor, în special în ceea ce privește acoperirea cu internet și vitezele de conectare;
- corectitudinea pieței, în privința tratamentului pe care actorii din sectorul serviciilor de telecomunicații îl primesc, indiferent dacă aceștia sunt tradiționali sau folosesc servicii bazate pe aplicații.

Astfel, a fost aprobată Legea nr. 198 din 6 iulie 2022 pentru modificarea și completarea unor acte normative în domeniul comunicațiilor electronice și pentru stabilirea unor măsuri de facilitare a dezvoltării rețelelor de comunicații electronice, care a abordat explicit transpunerea în legislația națională a Codului european al comunicațiilor electronice.

Conform președintelui Autorității Naționale pentru Administrare și Reglementare în Comunicații, Vlad Stoica, pe lângă protejarea drepturilor consumatorilor, „actul normativ urmărește stimularea concurenței și a creșterii investițiilor în rețelele 5G, reglementări previzibile pentru spectrul radio, promovarea conectivității, precum și asigurarea unei calități superioare a serviciilor de comunicații electronice. În acest context, Autoritatea are pârghiile necesare pentru a demara organizarea licitației de spectru”.

PRINCIPIUL „ONCE-ONLY”

Referitor la principiul „o singură dată” (*once-only*), acesta se regăsește printre prioritățile Comisiei Europene pentru perioada 2019-2024, precum și în prevederile articolului 14, din cadrul *Regulamentului (UE) nr. 2018/1724 Privind înființarea unui portal digital unic (gateway) pentru a oferi acces la informații, la proceduri și la servicii de asistență și de soluționare a problemelor și de modificare a Regulamentului (UE) nr. 1024/2012.*

INFO BOX

Conform principiului, persoanele fizice și juridice vor furniza informații și documente administrației publice o singură dată, fără obligația de a le prezenta unei alte entități odată furnizate anterior. Implementarea și aplicarea acestui principiu presupune ca instituțiile administrației publice să asigure partajarea și reutilizarea datelor despre cetățeni ori companii, inclusiv la nivel transfrontalier, cu respectarea reglementărilor privind protecția datelor cu caracter personal.

Conform Anexei II din Regulamentul (UE) nr. 2018/1724, principiul „o singură dată” este aplicabil pentru 21 de proceduri administrative aferente a șapte evenimente de viață. Cu privire la acestea, fiecare Stat Membru (SM) al UE va asigura faptul că, până la finalul anului 2023, utilizatorii le vor putea accesa și finaliza, în întregime online, dacă procedura relevantă a fost stabilită în statul membru în cauză. Cele șapte evenimente de viață sunt: nașterea, reședința, studiile, munca, mutarea, pensionarea și demararea, desfășurarea și închiderea unei activități comerciale.

Conform *Regulamentului* indicat, SM UE pot solicita utilizatorilor să se prezinte personal în fața autorităților competente, în situații excepționale justificate de motive imperative de interes public în domeniile securității și sănătății publice sau combaterii fraudelor.

O EUROPĂ PREGĂTITĂ PENTRU **ERA DIGITALĂ**

"*O Europă pregătită pentru era digitală*" este una dintre cele șase priorități stabilite de Comisia Europeană (COM EU) pentru perioada 2019-2024. Aceasta cuprinde o serie de acțiuni precum: securitate cibernetică, inteligență artificială, strategia europeană privind datele, strategia industrială pentru Europa, competențe digitale, calcul de înaltă performanță, conectivitatea, actul legislativ privind piețele digitale și identitatea digitală europeană.

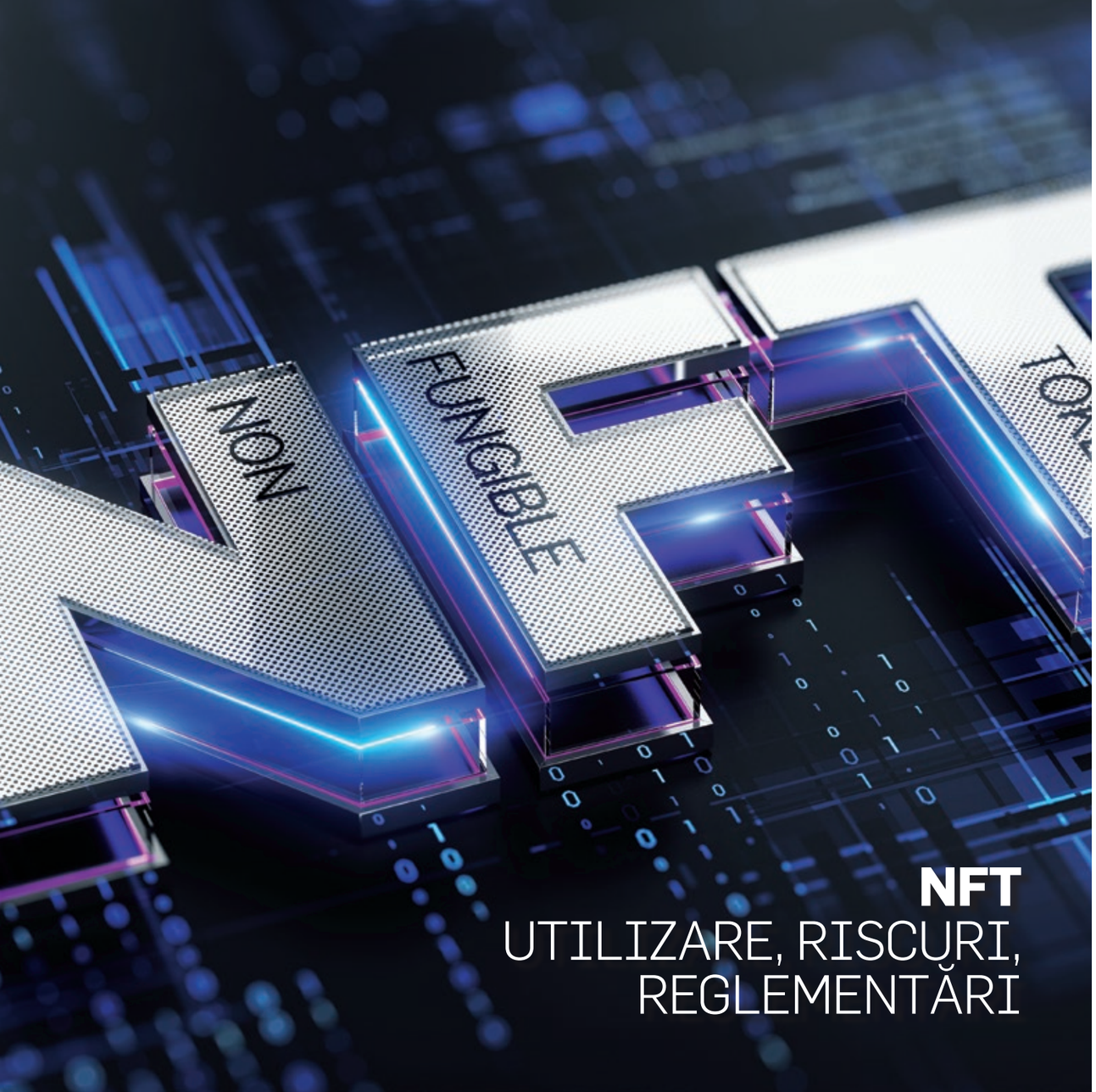
Subsumat acestei priorități, COM EU a stabilit două direcții de acțiune:

1. *Deceniul digital al Europei* (Comunicarea COM EU privind „*Busola pentru dimensiunea digitală 2030: modelul european pentru deceniul digital*"/ COM/2021/118 final), în care viziunea COM este articulată în jurul a patru puncte:

- o populație cu competențe digitale și profesioniști înalt calificați în domeniul digital: specialiști IT&C și competențe digitale de bază;
- infrastructuri durabile sigure și performante: conectivitate, semiconductori de ultimă generație, date – servicii *edge* și cloud, informatică;
- transformarea digitală a întreprinderilor: adoptarea tehnologiei, inovatori, inovatori tardivi;
- digitalizarea serviciilor publice: servicii publice-cheie, servicii de e-sănătate, identitate digitală.

2. Conturarea viitorului digital al Europei, axat în jurul a trei piloni:

- tehnologie în beneficiul oamenilor, cu accent pe dezvoltarea cunoștințelor, asigurării securității, utilizării noilor tehnologii, creșterea gradului de inter-conectivitate, susținerea inovației digitale în medicină, transporturi și mediu;
- o economie digitală corectă și competitivă, care să susțină finanțarea *start-up*-urilor și micilor afaceri, responsabilizarea platformelor și reglementarea serviciilor online, adaptarea reglementărilor la realitățile economiei digitale, asigurarea unui cadru concurențial corect și asigurarea accesului la date de calitate cu garantarea protejării acestora;
- o societate deschisă, democratică și durabilă, în care tehnologia să asigure o Europă neutră-climatic până în 2050, amprenta de carbon să fie redusă, cetățenii să dobândească control asupra datelor proprii, să fie creat un spațiu european al datelor medicale, să fie combătută dezinformarea online și promovat conținutul media de calitate și de încredere.



NFT
UTILIZARE, RISCURI, REGLEMENTĂRI

NFT-urile (*token*-uri non-fungibile) sunt active digitale care certifică și garantează dreptul de proprietate, unicitatea și autenticitatea unui bun digital sau fizic. Caracterul non-fungibil al acestor *token*-uri presupune deținerea unor proprietăți unice, care nu pot fi replicate sau înlocuite.

Token-urile pot fi asociate criptografic cu anumite bunuri digitale sau fizice. Bunurile digitale pot fi imagini, fișiere video și audio, texte sau obiecte de colecție din lumea virtuală; iar bunurile fizice pot fi bilete la evenimente sau documente oficiale (permis de conducere, acte de identitate etc.). Crearea de *token*-uri („tokenizarea") se realizează printr-un proces numit *minting*.

Minting-ul reprezintă un proces de validare a informațiilor, urmat de crearea unui bloc nou și înregistrarea informațiilor într-un *blockchain*. Noul *token* are încorporată o licență de utilizare a bunului respectiv. Acest proces de tranzacție criptografică asigură autentificarea fiecărui fișier digital printr-o semnătură digitală, utilizată pentru a urmări drepturile de proprietate a *token*-ului respectiv.

Trăsăturile definitorii ale NFT-urilor sunt:

- **Unicitatea** – NFT-urile nu pot fi copiate sau reproduse în niciun fel;
- **Indivizibilitatea** –NFT-urile nu pot fi divizate;
- **Nefungibilitatea** – NFT-urile nu sunt interschimbabile.

Un NFT conține: (1) informații cronologice despre tranzacțiile anterioare și informații despre creatorul acestuia; (2) un număr unic de identificare (*token ID*); (3) un contract *smart.*

Contractele *smart* implementează și pun în aplicare clauze, termeni și condiții asupra oricăror operațiuni juridice care vor avea loc asupra unui NFT, fiind înscris definitiv în elementul criptografic al *token*-ului. Mai simplu, contractele *smart* reprezintă codificarea termenilor și condițiilor agreate de părți cu privire la operațiunile care implică NFT-ul respectiv.

Deși aflate într-o strânsă legătură, NFT-urile nu trebuie confundate cu criptomonedele, întrucât cele din urmă sunt caracterizate prin fungibilitate (interschimbabilitate). Cele două active se diferențiază inclusiv prin termenii utilizați: criptoactive (aferent criptomonedelor și al unei categorii restrânse de NFT-uri), respectiv active digitale (aferent majorității NFT-urilor). Similar criptomonedelor, NFT-urile sunt comercializate

la nivelul unor platforme dedicate în mediul online. Cele mai utilizate platforme în acest moment sunt: OpenSea, Nifty, SuperRare, Myth Market, Enjin etc.

NFT-urile sunt utilizate astăzi sub următoarele forme:

- Activ virtual – în contextul în care dezvoltatorii rețelelor sociale, *metaverse*-urilor, jocurilor sau producătorii de articole vestimentare construiesc infrastructuri virtuale complexe pentru a facilita accesul la produsele și serviciile furnizate, NFT-urile sunt folosite drept mijloc de tranzitare a mediilor virtuale de către utilizatori, oferindu-le acestora posibilitatea creării unei personalități virtuale unice;

- Cheie de acces – o serie de spații virtuale și reale își fundamentează exclusivitatea prin permiterea accesului doar posesorilor unui NFT dintr-o anumită colecție.

În acest context, NFT-urile pot prezenta următoarele **riscuri**:

- Valoarea NFT-urilor – având în vedere caracterul volatil al criptomonedelor și comercializarea NFT-urilor prin intermediul acestora, valoarea *token*-urilor non-fungibile nu poate fi garantată.

- Siguranța NFT-urilor – NFT-urile sunt stocate inclusiv la nivelul unor portofele digitale, existând riscul ca acestea să fie compromise, iar *token*-urile să fie furate de către actori cibernetici, cu scopul de a obține beneficii financiare;

- Monetizarea activităților ilegale – NFT-urile pot susține monetizarea activităților ilegale prin achiziționarea acestora din fonduri obținute în mod fraudulos. De asemenea, NFT-urile pot fi utilizate ca modalitate de plată pentru servicii nelegitime, similar criptomonedelor;

- Impactul asupra mediului înconjurător – *blockchain*-ul ca tehnologie consumă o cantitate mare de energie, în fiecare zi, întrucât are nevoie de o putere de procesare considerabilă pentru a sprijini înregistrările NFT-urilor în *blockchain* și tranzacțiile ulterioare. În afară de consumul de energie, NFT-urile și criptomonedele contribuie semnificativ la creșterea emisiilor de CO2.

Cu toate că NFT-urile au evoluat proporțional cu criptomonedele și cu tehnologia *blockchain*, emiterea, utilizarea și comercializarea *token*-urilor non-fungibile nu sunt în prezent reglementate de niciun act legislativ dedicat la nivel internațional.

Deși în martie 2022, Parlamentul European a adoptat versiunea finală a „Propunerii de regulament al Parlamentului European și al Consiliului privind piețele criptoactivelor și de modificare a Directivei (UE) 2019/1937" (MiCA), care are rolul de a reglementa emiterea, utilizarea și tranzacționarea de criptoactive, actul normativ nu vizează activele digitale (inclusiv o mare parte din NFT-urile existente).

Concret, MiCA reglementează exclusiv activele digitale care au caracter fungibil și oferă deținătorilor beneficii de ordin financiar (de ex. o parte din profiturile obținute de dezvoltatori să fie redistribuită către deținători; procese de *staking* care recompensează deținătorii activelor etc.). În acest caz, singurele NFT-uri care sunt reglementate sunt cele care se încadrează în categoria de criptoactive.

În următoarele 18 luni, Comisia Europeană urmează să evalueze și să înainteze o propunere legislativă pentru a reglementa piața NFT-urilor și pentru a aborda riscurile emergente aduse de această tehnologie.

WWW.SRI.RO/CYBERINT