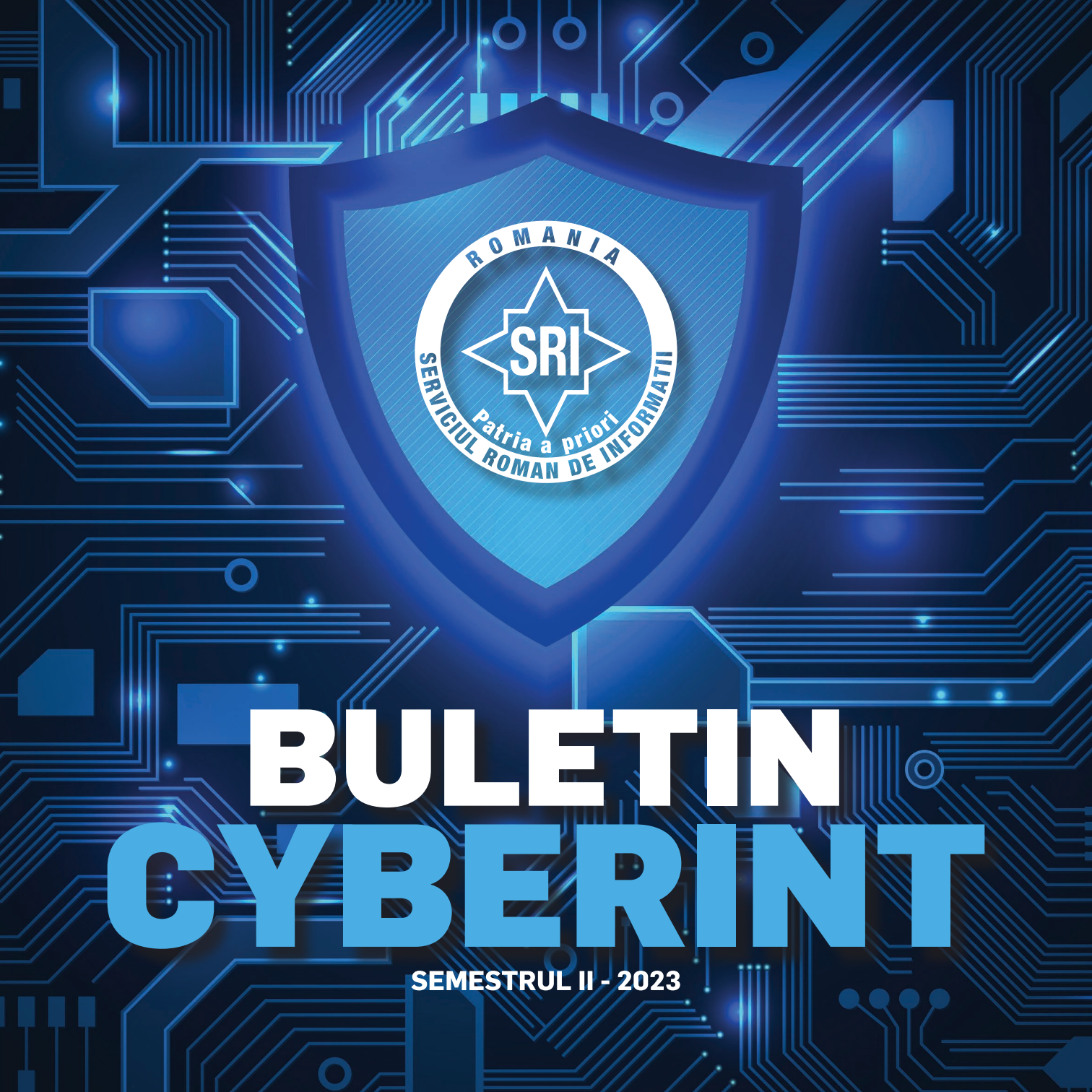


BULETIN CYBERINT

SEMESTRUL II - 2023

DOMENIUL DIPLOMATIC - ȚINTA PREFERATĂ A ATACURILOR DE SPEARPHISHING

Atacurile cibernetice de spearphishing derulate de actori statali vizează, în cea mai mare majoritate din cazuri, compromiterea și exfiltrarea de informații strategice de la nivelul unor entități guvernamentale de rang înalt.

Domeniul diplomatic reprezintă o țintă preferată de către actorii cibernetici statali, întrucât la nivelul acestui domeniu sunt vehiculate date referitoare la elemente de politică externă ale statelor. În acest sens, actori cibernetici asociați unor state precum Federația Rusă sau Republica Populară Chineză (RPC) sunt interesați în mod constant de obținerea unor astfel de date, care pot orienta deciziile strategice ale statelor pe care le susțin.

Atacurile de spearphishing la adresa domeniului diplomatic sunt facilitate inclusiv de abundența informațiilor existente cu privire la personalul diplomatic al statelor, care trebuie să existe în spațiul public pentru informarea propriilor cetățeni.

Suplimentar, evoluțiile din plan geopolitic (de ex. conflictul militar din Ucraina) oferă o multitudine de subiecte, pe care actorii cibernetici le pot folosi în construirea unor mesaje de spearphishing cât mai convingătoare, adaptate la temele de interes curente ale personalului ce activează în domeniul diplomatic.

Printre subiectele preferate de atacatori și incluse în mesajele de spearphishing se regăsesc invitații la diverse evenimente, programul de lucru al ambasadelor sau note de comunicare între entități guvernamentale. Utilizarea unor astfel de subiecte, coroborat cu alegerea unei ținte concrete care activează într-un departament ce are în atribuții aspectele semnalate în subiect (detalii regăsite, de cele mai multe ori, pe website-uri oficiale), crește rata de succes a atacatorilor.

În cazul în care persoana care a primit e-mailul de spearphishing accesează conținutul malware al atacatorului (link, fișier .rar, .pdf etc.), atacatorul declanșează un proces complex de compromitere treptată a victimelor, rezultatul fiind exfiltrarea de informații.

În acest context, menționăm că, la nivel mondial, acest tip de atacuri sunt derulate constant la adresa domeniului diplomatic, relevanți în acest sens fiind **APT 29/COZY BEAR** (atribuit SVR al Federației RUSE) sau **APT MUSTANG PANDA** (asociat RPC).

Pentru a scădea semnificativ șansele de succes ale atacurilor de spearphishing derulate, trebuie ca, pe lângă implementarea unor măsuri de securitate cibernetică eficiente, utilizatorii să conștientizeze faptul că există un risc ridicat de a fi vizați de astfel de atacuri și să acorde o atenție ridicată la e-mailurile primite, mai ales în cazul persoanelor ce activează în domeniul diplomatic.

DESTRUCTURAREA PLATFORMEI *GENESIS MARKET*

Începând cu anul 2022, SRI a cooperat cu instituții de aplicare a legii pentru investigarea și documentarea informativă a uneia dintre cele mai importante platforme de *cybercrime, Genesis Market*, specializată în vânzarea credențialelor de acces, utilizate atât în scop personal, cât și pentru acces în infrastructuri, obținute anterior prin atacuri cibernetice.

> În cadrul *Genesis Market* erau comercializate aproximativ 1,5 milioane de dispozitive infectate, care aveau asociate 2 milioane de credențiale, dintre care peste 31.000 de sisteme informatice compromise din România. Platforma era utilizată, în general, de actorii cibernetici care instrumentează atacuri de tip ransomware sau de afiliați ai acestora pentru achiziționarea de acces în cadrul unor infrastructuri.
>
> În urma cumpărării *botnet*-urilor, utilizatorii platformei aveau acces la toate datele colectate de acestea, cum ar fi amprentele digitale (*browser fingerprints*), *cookie*-urile, autentificările salvate și datele de completare automată a formularelor, toate colectate în timp real.

Mai mulți cetățeni români, care au fost semnalați activi la nivelul platformei *Genesis Market*, au achiziționat datele aferente unor sisteme informatice compromise anterior. Cetățenii români au achiziționat sisteme informatice compromise și credențialele asociate acestora, care aparțineau unui număr semnificativ de victime, inclusiv din România.

Investigațiile derulate la nivelul Centrului Național CYBERINT au condus la obținerea unor date care au fost valorificate în cooperarea cu partenerii, contribuind la activitatea acestora pentru destructurarea *marketplace*-ului.

La data de 4 aprilie 2023 a avut loc o operațiune internațională, coordonată de FBI-SUA și Poliția Națională din Țările de Jos, care a condus la eliminarea platformei *Genesis Market* și la confiscarea infrastructurii din Europa. În urma acestei operațiuni au fost puse în aplicare 208 mandate de percheziție, au fost efectuate 97 de verificări și au fost arestate 119 persoane. La nivel național, DIICOT și Poliția Română au efectuat 7 percheziții domiciliare, punând în executare 4 mandate de aducere emise pe numele a 4 cetățeni români.

ACTIVITATEA GRUPĂRILOR HACKTIVISTE PRO-RUSE

Pe fondul conflictului militar dintre Federația Rusă și Ucraina, actorii cibernetici hacktiviști pro-ruși s-au remarcat prin instrumentarea unor campanii cibernetice de amploare, ce au avut drept ținte rețele și sisteme informatice localizate atât în România, cât și în cadrul altor state membre NATO/UE. Ca efect, website-urile instituțiilor afectate au fost indisponibilizate temporar, ceea ce a blocat accesul populației la datele și serviciile conținute.

În ultima perioadă, s-a constatat că actorii hacktiviști pro-ruși și-au consolidat poziția de amenințare la adresa ecosistemului digital global, inclusiv prin actualizarea tacticilor, tehnicilor și procedurilor și utilizarea rețelelor de socializare pentru atragerea mai multor membri. Principalele grupări hacktiviste pro-ruse care au derulat atacuri cibernetice în contextul conflictului din Ucraina sunt:

- **KILLNET**

Pe parcursul anului 2023, gruparea a continuat seria de atacuri cibernetice în special asupra unor instituții din domeniul sănătății din Portugalia, Spania, Germania, Polonia, Finlanda, Norvegia, Țările de Jos și Regatul Unit ca răspuns pentru ajutorul oferit Ucrainei.

- **PHOENIX**

Gruparea este cunoscută încă din anul 2022 pentru atacurile cibernetice derulate asupra unor rețele și sisteme informatice aferente unor instituții din domeniul medical de la nivel internațional și asupra unor website-uri guvernamentale din Ucraina, Germania, Polonia, Japonia, Marea Britanie, SUA și Danemarca. În februarie 2023, PHOENIX a revendicat un atac cibernetic asupra Agenției Naționale a Funcționarilor Publici din România.

- **NoName057(16)**

Entitate de hackeri pro-rusă, cunoscută, începând cu martie 2022, pentru lansarea atacurilor cibernetice de tip *defacement* și *DDoS* împotriva unor rețele și sisteme informatice din Ucraina, precum și împotriva țărilor care condamnă invazia Federației Ruse în Ucraina. Principalele ținte ale grupării au fost: Letonia, Lituania, Polonia, Estonia, Danemarca, Cehia, Ucraina și Suedia.

- **XakNET**

Grup de hackeri ruși care a devenit activ începând cu februarie 2022, derulând atacuri de tip *DDoS* asupra mai multor instituții guvernamentale din Ucraina, inclusiv Administrația Prezidențială a Ucrainei, Departamentul de Securitate Cibernetică din Poliția Ucrainei, respectiv Ministerul de Externe Ucrainean.

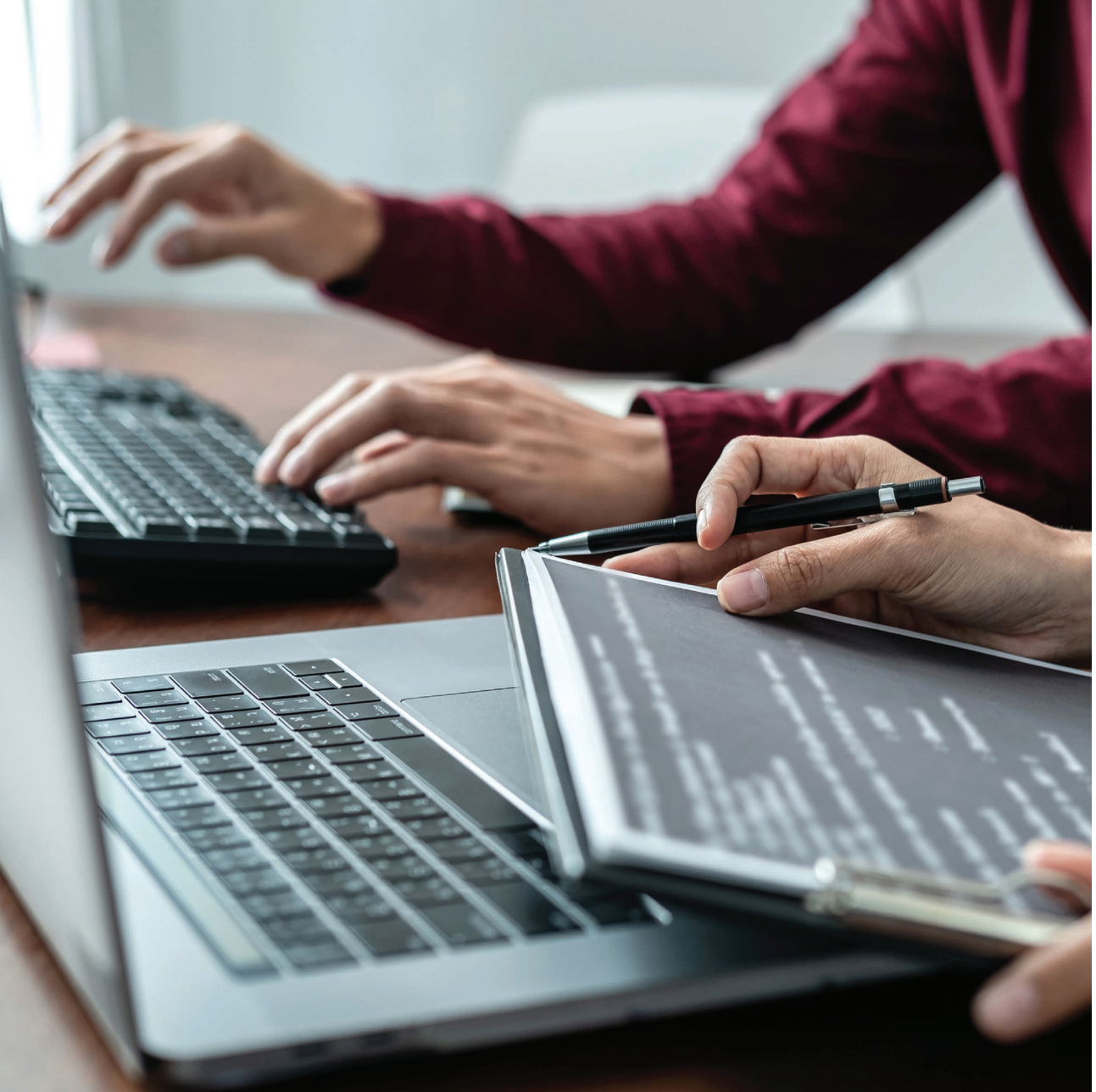
- **Anonymous Sudan**

Gruparea hacktivistă pro-rusă afiliată KILLNET a derulat o serie de atacuri cibernetice de tip DDoS asupra paginilor web ale unor instituții din Danemarca, Suedia și Franța.

ASIGURAREA SECURITĂȚII CIBERNETICE A SUMMITULUI COMUNITĂȚII POLITICE EUROPENE – REPUBLICA MOLDOVA, 1 IUNIE 2023

Summitul Comunității Politice Europene (CPE), aflat la a doua ediție, a avut loc la data de 01.06.2023, la Castelul MIMI (localitatea Bulboaca, raionul Anenii Noi) în Republica Moldova, cu participarea unor demnitari de nivel înalt din 45 de state și organisme europene.

În perioada conexă derulării Summitului, Serviciul Român de Informații (SRI) a contribuit la asigurarea securității cibernetice a evenimentului prin sprijinul acordat instituțiilor din Republica Moldova.



Astfel, au fost securizate infrastructuri cu importanță majoră în buna derulare a evenimentului și s-a contribuit la identificarea și contracararea unor incidente cibernetice, precum mitigarea unui atac DDoS inițiat din România asupra infrastructurii Aeroportului Internațional Chișinău.

ADOPTAREA UNOR ACTE NORMATIVE LA NIVELUL UE CU INCIDENȚĂ ASUPRA DOMENIULUI SECURITĂȚII CIBERNETICE

EU CYBERSECURITY ACT

Comisia Europeană a adoptat, la 18 aprilie 2023, modificarea Actului privind securitatea cibernetică (EU Cybersecurity Act). Amendamentul consolidează atribuțiile Agenției pentru Securitate Cibernetică a Uniunii Europene (ENISA) și îi acordă mandat permanent. Noile sale atribuții constau în adoptarea schemelor europene de certificare pentru servicii de securitate gestionate care acoperă domenii precum răspunsul la incidente, testarea de penetrare, auditurile de securitate cibernetică și consultanță. Certificarea serviciilor în domeniul securității cibernetice este esențială, întrucât vine în sprijinul companiilor și organizațiilor în ceea ce privește prevenirea, detecția, răspunsul și recuperarea ulterioară incidentelor de securitate.

EU CYBER SOLIDARITY ACT

La aceeași dată, Comisia Europeană a adoptat propunerea de Regulament privind Solidaritatea Cibernetică (CSA) pentru a consolida capacitățile de securitate cibernetică ale UE.

CSA stabilește capacitățile de care UE are nevoie pentru ca Europa să îmbunătățească reziliența și pregătirea modului de reacție la amenințările cibernetice.

Printre obiectivele CSA se regăsesc :

- **Crearea unui scut cibernetic european**. Acesta va fi compus din entități de tip Security Operation Center (SOC) de la nivelul tuturor statelor membre UE, reunite în

multiple platforme de operare comune, care vor fi construite cu sprijinul programului Europa digitală (DIGITAL). Scutul cibernetic are scopul de a îmbunătăți detectarea, analiza și răspunsul la amenințările cibernetice.

- **Dezvoltarea unui mecanism de urgență cibernetică**, care va presupune îmbunătățirea pregătirii și a răspunsului la incidentele de securitate cibernetică.
- **Crearea unei rezerve de securitate cibernetică a UE**, care constă în servicii de reacție prestate de furnizori de încredere contractați în prealabil, pregătiți să intervină în cazul unui incident de securitate cibernetică de mare amploare atunci când vor fi solicitați.

DECLARAȚIA COMUNĂ SUA – UE A CONSILIULUI PENTRU COMERȚ ȘI TEHNOLOGIE

În 31 mai 2023, la Lulea, Suedia, a avut loc cea de a patra întâlnire ministerială a Consiliului de Comerț și Tehnologie (TTC) SUA-UE, găzduită de Președinția suedeză a Consiliului UE. În cadrul întâlnirii au fost abordate subiecte de interes de pe agenda internațională cu privire la domeniul digital și cel al tehnologiilor emergente, cu implicații economice și asupra drepturilor omului. Aspectele principale ale întâlnirii au fost reprezentate de:

A. Cooperare transatlantică robustă privind tehnologiile emergente pentru leadership-ul comun SUA – UE, în privința:

» ***Inteligenței Artificiale*** cu accent pe reafirmarea angajamentului celor doi parteneri în direcția abordării bazate pe riscuri a IA, promovarea tehnologiilor IA într-o manieră responsabilă și consolidarea cooperării pentru a promova dezvoltarea responsabilă a acestor tehnologii.

A fost statuat faptul că SUA și UE au lansat trei grupuri de experți pentru elaborarea de contribuții privind:

- terminologia și taxonomia IA;
- cooperarea cu privire la standardele IA, instrumente IA de încredere și managementul riscurilor;
- monitorizarea și măsurarea riscurilor IA existente și emergente.

» **Demersuri de standardizare pentru tehnologiile critice și emergente**

Până la următoarea ședință ministerială a TTC, UE și SUA, în cooperare cu experți din domeniul guvernamental, societatea civilă și mediul academic, urmăresc maparea resurselor și inițiativelor de utilizare a identității digitale.

Până la finalul anului 2023, SUA și UE vizează elaborarea de recomandări de politici comune pentru accelerarea accesului și adoptarea instrumentelor digitale de către IMM-uri.

» **Standarde privind e-Mobilitatea și interoperabilitatea cu rețelele inteligente (smart grids)**

A fost apreciată publicarea recomandărilor tehnice comune SUA-UE pentru implementarea infrastructurii de încărcare a vehiculelor electrice, prin finanțări guvernamentale, în elaborarea cărora au fost consultate guverne și alte părți interesate.

» **Semiconductori**

A fost evidențiată necesitatea cooperării bilaterale în privința dezvoltării unor lanțuri de aprovizionare reziliente cu semiconductori. În acest context, SUA și UE au finalizat un mecanism de avertizare timpurie pentru întreruperile lanțului de aprovizionare cu semiconductori și un mecanism de transparență pentru schimbul reciproc de informații.

» **Tehnologii cuantice**

SUA și UE au înființat un grup de lucru comun (Task Force) pentru abordarea cooperării în domeniul tehnologiilor cuantice. Grupul de lucru va aborda aspecte privind participarea la programele publice de cercetare, drepturi de proprietate intelectuală, identificarea componentelor critice, standardizarea, definirea benchmarking-ului calculatoarelor cuantice și controlul exporturilor. De asemenea, sunt abordate aspecte cu privire la standardizarea criptografiei post-cuantice și căi de cooperare pentru consolidarea dialogului în materie de securitate cibernetică între SUA și UE.

B. Comerț, securitate și prosperitate economică

Au fost abordate aspecte cu privire la: cooperarea privind controlul exporturilor și aplicarea de sancțiuni; verificarea securității investițiilor; controlul asupra investițiilor străine; dezbaterea politicilor și practicilor comerciale neloiale; impunerea de constrângeri economice.

C. Conectivitate și infrastructură digitală

» **Ulterior 5G/6G**

SUA și UE au accelerat cooperarea pentru dezvoltarea unei viziuni comune și a unei foi de parcurs a industriei privind cercetarea și dezvoltarea sistemelor de comunicații wireless 6G. Până în anul 2030 este preconizată începerea înlocuirii standardului 5G.

» **Infrastructură și conectivitate digitale sigure și de încredere în țări terțe**

SUA și UE vizează consolidarea colaborării cu state terțe, în special economii emergente, în vederea promovării incluziunii digitale și a conectivității sigure și de încredere la nivel global.

D. Apărarea drepturilor și valorilor omului într-un mediu digital geopolitic în schimbare

» **Platforme online transparente și responsabile**

Conform viziunii comune SUA-UE, platformele online ar trebui să își asume o mai mare responsabilitate în privința asigurării faptului că serviciile furnizate contribuie la un mediu online în care sunt protejate, împuternicite și respectate interesele copiilor și ale tinerilor. Totodată, ar trebui adoptate măsuri responsabile pentru minimizarea impactului negativ al serviciilor de acest tip asupra dezvoltării acestora.

» **Interferențe și manipulări informaționale străine în țări terțe**

Reprezentanții SUA și UE manifestă preocupări solide cu privire la interferențele străine, manipulările informaționale și acțiunile de dezinformare care aduc atingere valorilor universale, fundamentelor democratice și bunăstării societăților de la nivel global.

În acest context, a fost subliniată activitatea Federației Ruse în pregătirea și derularea conflictului armat din Ucraina și a activităților derulate de RP China în amplificarea narativelor Rusiei de dezinformare cu privire la război.

PERSPECTIVA EUROPEANĂ ASUPRA CERTIFICĂRII DE SECURITATE A SERVICIILOR CLOUD

CE REPREZINTĂ?

Schema de certificarea de securitate a serviciilor cloud la nivelul UE (European Cybersecurity Certification Scheme for Cloud Services/ EUCS) constituie un cadru prin intermediul căruia se urmărește atingerea unui nivel ridicat de încredere în furnizorii de soluții de cloud, necesar utilizării în domenii esențiale și critice. Obiectivul principal al acestuia îl constituie protejarea eficientă a datelor guvernelor statelor membre și ale întreprinderilor.

EUCS va fi translatat într-un act european de punere în aplicare ce va cuprinde în mod clar cerințele ca o entitate să obțină un certificat recunoscut la nivelul statelor membre UE pentru a furniza servicii de Cloud.

CINE ESTE RESPONSABIL?

La solicitarea Comisiei Europene, elaborarea EUCS intră în responsabilitatea **Agenției Naționale de Securitate Cibernetică a Uniunii Europene** (European Union Agency for Cybersecurity/ ENISA). Agenția contribuie la politica cibernetică a UE și s-a înființat în anul 2004, având ca obiectiv atingerea unui nivel comun ridicat de securitate cibernetică la nivel european, prin cooperare cu țările și organismele UE.

DE CE ESTE NECESARĂ?

De câțiva ani, statele membre UE s-au angrenat într-un proces de transformare digitală marcat inclusiv de adoptarea și dezvoltarea tehnologiei și soluțiilor de *cloud computing*, factor-cheie în atingerea obiectivelor strategice din domeniul digitalizării. Acestea oferă acces la noi servicii pentru cetățeni și la instrumente utile în dezvoltarea afacerilor și presupun, în general, funcționalități de colectare și stocare de volume mari de date, inclusiv cu caracter personal, în centre de date. În acest sens, protecția datelor devine o cerință obligatorie, iar gestionarea deficitară a problemelor de confidențialitate poate determina eșecul acestor servicii.

Schemele și standardele de certificare internațională joacă un rol important în evoluția pieței serviciilor digitale prin furnizarea de cadre care ar trebui să garanteze siguranța utilizatorilor finali și o concurență loială.

EUCS prezintă interes la nivel național inclusiv din perspectiva desfășurării Proiectului de Cloud Guvernamental, obiectiv de interes strategic nominalizat inclusiv în numerele anterioare ale Buletinului CYBERINT (Semestrul II 2022 și Semestrul I 2023).

SECURITATEA CIBERNETICĂ ÎN DOMENIUL *AUTOMOTIVE*

În conformitate cu evoluțiile tehnologice recente, industria automotive s-a dezvoltat semnificativ în ultimii ani, aducând în prim-plan conceptul de autovehicule conectate și autonome. Aceste autovehicule sunt tot mai dependente de sisteme informatice și de comunicații, fiind conectate la internet și echipate cu o gamă largă de funcționalități digitale, motiv pentru care riscurile asociate atacurilor cibernetice în acest domeniu au crescut exponențial, existând posibilitatea punerii în pericol a vieții pasagerilor și siguranța traficului.

Începând cu anul 2022, atacurile cibernetice asupra API-urilor auto au crescut cu 380%. De asemenea, au fost observate atacuri cibernetice asupra:

- **infrastructurilor de încărcare:** pot fi afectate prin compromiterea procesului de încărcare și alterare a capacității vehiculului de a funcționa corect. Mai mult, rețelele de încărcare colectează și stochează date sensibile, precum informații de plată ale clienților, numere de identificare ale vehiculelor, date biometrice etc., motiv pentru care și acestea pot reprezenta o țintă atractivă pentru actorii *cybercrime*.
- **sistemelor informatice ale autovehiculelor:** sunt targetate prin atacuri de tip *brute-force*, prin comercializarea unor dispozitive *aftermarket* compromise anterior sau prin atacuri asupra sistemelor de *infotainment*.
- **sistemelor critice ale autovehiculelor:** există riscul ca actorii cibernetici să preia controlul asupra sistemului de frânare, accelerație sau direcție a vehiculului, acțiuni ce pot pune în pericol viețile persoanelor și afecta siguranța rutieră.

Pentru a stabili un standard pentru practicile de securitate cibernetică în domeniul automotive au fost dezvoltate norme adaptate special pentru această industrie. Un exemplu în acest sens este standardul ISO/SAE 21434, care oferă orientări privind securitatea cibernetică pentru vehiculele rutiere. Conformitatea cu aceste standarde asigură integrarea securității cibernetice pe tot parcursul ciclului de viață al vehiculului, promovând o abordare sistematică și cuprinzătoare a securității cibernetice.

Înțelegând importanța securității cibernetice în domeniul automotive, industria auto depune eforturi pentru a aborda în mod proactiv amenințările cibernetice cu care se confruntă. Astfel, prin adoptarea tehnologiilor emergente (ex. sisteme de detecție a intruziunilor), implementarea unor protocoale de comunicare sigure și adoptarea sistemului de actualizare a *software*-urilor *Over-the-Air*, industria automotive își poate consolida reziliența cibernetică. În plus, colaborarea și partajarea informațiilor între companiile din industrie sunt vitale pentru creșterea rezilienței colective – prin partajarea celor mai bune practici, a informațiilor despre amenințări și prin stabilirea standardelor la nivelul întregii industrii.

În perioada următoare, inteligența artificială și *machine learning*-ul vor avea un impact semnificativ în vederea îmbunătățirii capacităților de securitate cibernetică din domeniul automotive. Testarea vulnerabilităților, pentesting-ul și principiile *security-by-design* vor rămâne critice în identificarea și gestionarea vulnerabilităților, precum și în dezvoltarea și implementarea unor practici de dezvoltare *software* sigure.

TEHNOLOGIILE CUANTICE – PROVOCĂRI ȘI OPORTUNITĂȚI LA NIVEL NAȚIONAL

Tehnologia cuantică este un domeniu al științei și tehnologiei, respectiv o ramură a informaticii și a științei calculatoarelor, care se concentrează pe utilizarea principiilor mecanicii cuantice pentru a realiza calcule, respectiv pentru a dezvolta dispozitive și aplicații inovatoare. Unele dintre caracteristicile specifice mecanicii cuantice, care stau la baza tehnologiilor cuantice, sunt:

- **Superpoziția** – obiectele cuantice, cum ar fi particulele subatomice, pot exista în mai multe stări în același timp, în mod diferit de obiectele din lumea macroscopică, unde acestea ocupă o singură stare la un moment dat;
- **Interferența** – particulele cuantice pot interfera între ele în mod constructiv sau distructiv, ceea ce duce la modele complexe;
- **Entanglement** („încurcarea” cuantică) – particulele cuantice pot deveni interconectate într-un mod special, numit *entanglement*. Schimbările efectuate asupra unei particule în această stare vor afecta instantaneu starea celeilalte particule, indiferent de distanța dintre ele.

La nivel național, posibilitățile de finanțare a programelor de cercetare, inovare și dezvoltare în domeniul tehnologiilor cuantice sunt reduse, comparativ cu măsurile similare adoptate în state cu putere financiară mai mare. Acest fapt creează premisele unui decalaj tehnologic defavorabil României, încă din primele etape ale revoluției cuantice. Ținând cont de perspectivele actuale, România trebuie să împiedice crearea acestui decalaj tehnologic prin valorizarea unor atuuri naționale în domeniul IT, precum masa critică de specialiști IT existentă în țară, sistemul solid de educație și pregătire în domeniul IT și prezența în România a unor companii de top la nivel global.

PROVOCĂRI GENERATE DE TEHNOLOGIILE CUANTICE

- **Securitatea informațiilor și comunicațiilor:** tehnologiile cuantice amenință metodele de criptare utilizate în prezent, făcând inutilă criptarea datelor și a comunicațiilor prin utilizarea metodelor pre-cuantice.
- **Investiții și resurse:** dezvoltarea și implementarea tehnologiilor cuantice necesită investiții semnificative în cercetare și dezvoltare, infrastructură și resurse.
- **Reglementare și standarde:** este necesară dezvoltarea de politici și reglementări adecvate pentru a asigura securitatea și etica în utilizarea tehnologiilor cuantice. De asemenea, pot fi necesare standarde pentru interoperabilitate și compatibilitate între diferitele tehnologii și platforme cuantice.
- **Impactul asupra forței de muncă și educației:** tehnologiile cuantice implică abilități și cunoștințe specializate în mecanică și programare cuantică și, implicit, nevoia de dezvoltare a capacităților și competențelor forței de muncă, precum și de programe de educație și formare adaptate pentru a face față noilor cerințe tehnologice.

OPORTUNITĂȚI GENERATE DE TEHNOLOGIILE CUANTICE

- **Securitatea comunicațiilor:** calculul cuantic poate contribui la dezvoltarea de metode și sisteme mai sigure de comunicare, prin valorificarea principiului de înlănțuire, astfel încât datele să nu poată fi interceptate sau alterate fără ca acest lucru să fie detectat.

- **Simulări cuantice:** tehnologiile cuantice permit simularea și analiza sistemelor cuantice complexe. Aceste simulări pot fi utilizate în diverse domenii, cum ar fi dezvoltarea de noi materiale, cercetarea în domeniul chimiei și a biologiei sau optimizarea proceselor industriale.
- **Asigurarea avansului tehnologic la nivel național:** România poate beneficia masiv din dezvoltarea de aplicații pentru tehnologiile cuantice, prin implicarea masei critice de specialiști în domeniul IT (mediile academic și privat).
- **Inițierea de parteneriate public-private** cu marile companii din domeniul IT reprezintă o oportunitate majoră pentru statul român din perspectiva valorizării resursei umane înalt specializate și, mai ales, pentru accesarea tehnologiei, fără costurile semnificative specifice.

WORMGPT – PLATFORMA DE INTELIGENȚĂ ARTIFICIALĂ PENTRU HACKERI

WormGPT reprezintă un model de inteligență artificială sofisticat ce poate genera un limbaj natural pe baza unui input sau context din partea utilizatorilor. Programul este similar cu ChatGPT, ambele fiind modele de inteligență artificială cu acces la diferite baze de date. Cu toate acestea, între cele două există o serie de diferențe, una dintre acestea fiind faptul că WormGPT a fost realizat de un actor cibernetic, iar ChatGPT a fost realizat de organizația OpenAI.

WormGPT a fost creat cu scopul de a facilita derularea de atacuri cibernetice, fiind accesibil doar la nivelul DarkWeb, iar folosirea acestuia se face prin achitarea unei taxe prin intermediul criptomonedelor (Bitcoin sau Ethereum), ceea ce asigură anonimitate utilizatorilor. Suplimentar, WormGPT nu are limite sau bariere etice, spre deosebire de ChatGPT, care conține restricții în anumite domenii și încearcă să reducă cât mai mult utilizarea serviciilor în scopuri rău intenționate.

Funcția principală a WormGPT este de a automatiza atacurile cibernetice și, implicit, de a crește rata de succes a acestora. De asemenea, serviciile WormGPT au devenit o provocare în identificarea și mitigarea atacurilor cibernetice precum atacuri phishing, business e-mail compromise (BEC), furt de identitate, fraudă financiară, exfiltrare de date, ceea ce conduce la necesitatea implementării unor măsuri de securitate mai performante, pentru a nu fi afectată securitatea indivizilor, companiilor și a entităților guvernamentale.

Suplimentar, prin intermediul WormGPT, actorii cibernetici pot realiza acțiuni de dezinformare, de schimbare a opiniei publice și de influențare a campaniilor politice, precum și atacuri de tip Distributed Denial-of-Service (DDoS).

Caracteristicile cheie ale WormGPT sunt:

- **Suportul nelimitat de caractere:** WormGPT are abilitatea de a genera texte de orice mărime, ceea ce este important pentru crearea de e-mailuri de phishing cu un limbaj autentic, cât și a altor forme de atacuri ce folosesc ingineria socială;
- **Reținerea conversațiilor din chat:** întrucât WormGPT poate să păstreze conversațiile anterioare, programul poate crea răspunsuri adecvate necesităților utilizatorului, folosind informațiile din interacțiunile trecute;
- **Formatarea codului aplicațiilor malware:** WormGPT poate formata liniile de cod într-un mod care face dificilă identificarea aplicațiilor malware de către soluțiile de securitate cibernetică, crescând astfel șansele de succes ale unui atac cibernetic;

Utilizarea WormGPT-ului reprezintă un risc pentru securitatea organizațiilor și entităților guvernamentale întrucât prin automatizarea atacurilor cibernetice crește rata de succes a acestora. De asemenea, hackerii ce dețin cunoștințe reduse în domeniu pot realiza atacuri de succes de tip phishing folosind un limbaj autentic sau pot crea aplicații malware dificil de identificat de echipamentele de securitate cibernetică.

RISCURI ASOCIATE PLATFORMEI TIKTOK

De la începutul anului 2023, platforma chineză de social media TikTok (care aparține companiei ByteDance) a căpătat o atenție sporită la nivel internațional, pe fondul existenței mai multor probleme de securitate cibernetică pe care utilizarea platformei le generează.

Principalele probleme identificate la nivel internațional sunt următoarele:

- cadrul legislativ din Republica Populară Chineză (RPC) reglementează inclusiv activitatea societății ByteDance și a aplicației TikTok și permite ca instituțiile de stat ale RPC să aibă acces la datele înregistrate de aplicație;

- termenii de utilizare ai TikTok menționează explicit posibilitatea partajării datelor colectate, fără a fi stipulate restricții în acest sens;
- guvernul RPC poate determina ByteDance să deruleze activități propagandistice în beneficiul RPC.

Mai multe state și organizații internaționale occidentale au luat măsuri în ceea ce privește **limitarea utilizării aplicației TikTok** la nivelul dispozitivelor de serviciu (telefoane mobile sau laptopuri).

În luna februarie 2023, Administrația Prezidențială din SUA a solicitat agențiilor federale ca, în termen de 30 de zile, să dezinstaleze TikTok de pe toate dispozitivele guvernamentale. Măsura a fost adoptată ulterior unei evaluări demarate de Comisia de Investiții Străine (CFIUS) asupra implicațiilor de securitate națională ale utilizării TikTok.

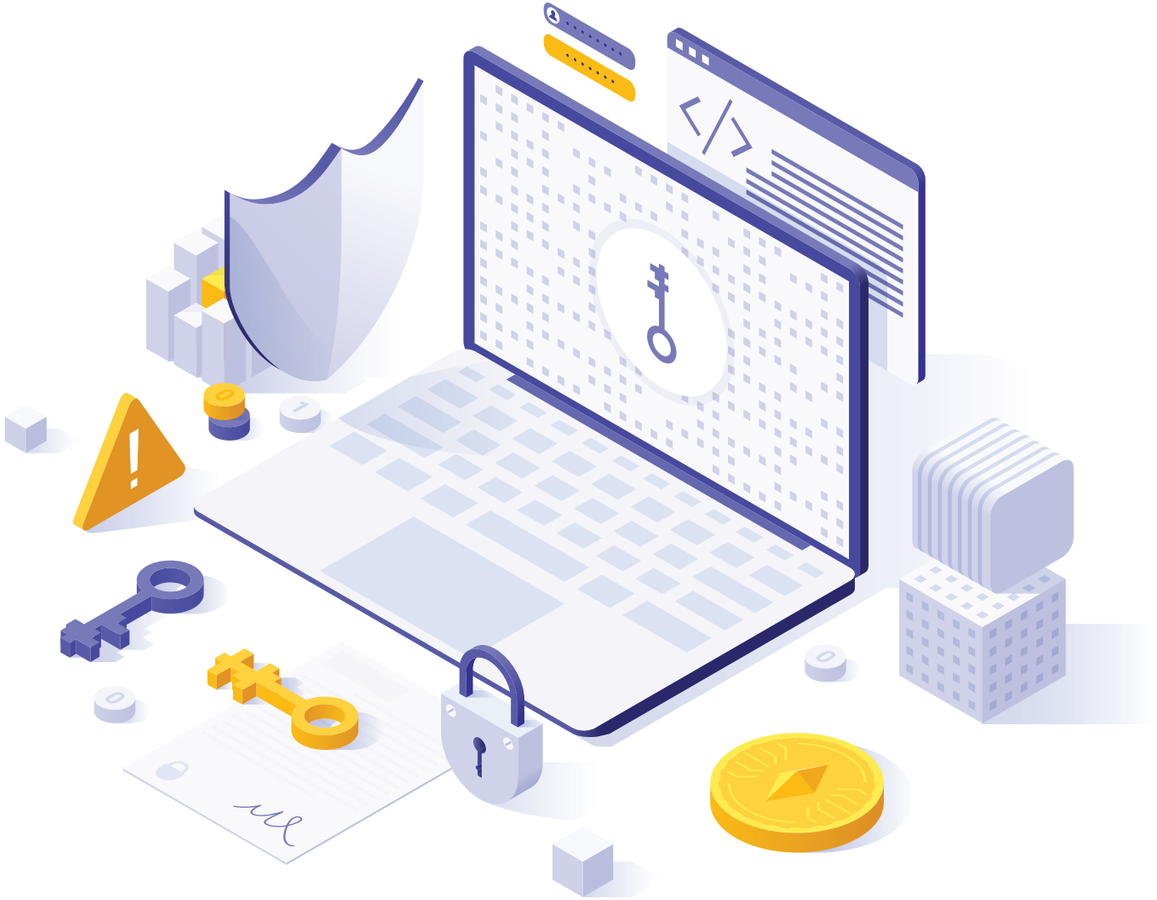
În mod similar, Comisia Europeană le-a transmis angajaților săi, în luna februarie 2023, o solicitare privind ștergerea aplicației TikTok de pe dispozitivele de serviciu sau personale (cele la nivelul cărora sunt utilizate aplicații CE corporate), până la data de 15.03.2023. Măsuri similare au fost adoptate la nivelul Parlamentului și Consiliului Uniunii Europene, precum și în NATO.

La nivelul Centrului Național CYBERINT a fost realizată o **evaluare tehnică proprie a TikTok**, fiind identificate multiple vulnerabilități de securitate cibernetică asociate aplicației, printre care:

- accesul la datele personale ale utilizatorilor și la conturarea unui profil al acestora;
- colectarea de multiple informații despre dispozitivul utilizatorilor, precum numărul de model al telefonului, seria cartelei SIM, număr de telefon, date de localizare, detalii cu privire la alte conturi conectate la dispozitiv, sistem de operare, adresă IP utilizată;
- posibilitatea de citire și stocare a mesajelor transmise direct prin intermediul aplicației, precum și metadatele asociate.

La nivel național, la începutul lunii martie 2023, ministrul Cercetării, Inovării și Digitalizării de la momentul respectiv, Sebastian BURDUJA, a transmis o serie de declarații publice conform cărora evalua posibilitatea interzicerii utilizării platformei TikTok pe dispozitivele utilizate în interes de serviciu, în acord cu măsurile adoptate la nivelul instituțiilor europene.

Suplimentar, la data de 18.05.2023, Directoratul Național de Securitate Cibernetică (DNSC) a emis o recomandare autorităților și instituțiilor publice din România privind interzicerea descărcării, instalării și utilizării TikTok pe dispozitivele de serviciu, măsuri necesare pentru limitarea riscurilor de securitate cibernetică cauzate de aplicația software.



WWW.SRI.RO/CYBERINT