BULETIN CYBERINT

SEMESTRUL II - 2024

UTILIZAREA INTELIGENȚEI ARTIFICIALE ÎN ATACURI DE TIP APT

Grupările *Advanced Persistant Threat* (APT) investesc resurse majore în dezvoltarea de noi TTP-uri (Tactici, Tehnici și Proceduri) pentru a-și atinge scopurile în raport cu entitățile pe care le vizează. Pentru eficientizarea activităților, atenția acestor grupări este îndreptată și asupra tool-urilor ce utilizează *Inteligența Artificială* (IA), capabile să faciliteze generarea și implementarea de coduri *malware*.

Cu titlu de exemplu, Federația Rusă nu a ezitat să exploateze acest aspect în contextul războiului din Ucraina, astfel că grupări APT rusești au utilizat tehnologii de IA pentru a obține date cu privire la diverse tehnologii militare.

Grație eficienței pe care o asigură, dar și potențialului remarcabil pe care îl prezintă, domeniul IA a fost deja exploatat de către grupările APT, care au procedat la realizarea de aplicații similare ChatGPT, al căror obiectiv este susținerea activităților ilicite din apanajul acestora.

Încă din anul 2023, actorii APT au realizat patru aplicații de IA, denumite WolfGPT, FraudGPT, WormGPT și DarkBARD. Aceste aplicații au fost distribuite pe forumuri și rețele de comunicații (precum Telegram) pentru ca alți actori cibernetici să aibă acces la ele nerestricționat. Funcționalitățile aplicațiilor IA dezvoltate de grupările APT sunt diverse, FraudGPT și WormGPT fiind utilizate în campaniile de *phishing* și inginerie socială, pe când WolfGPT este folosit pentru scrierea de coduri sau *exploit*-uri.

De asemenea, sistemele de IA sunt exploatate de actorii APT ruși pentru identificarea istoricului de căutări al unor angajați din cadrul unor entități de interes. În acest sens, în perioada ianuarie – octombrie 2023, au fost vândute pe *dark web* circa 225.000 de credențiale compromise ale unor conturi de ChatGPT, fiind cunoscut de către actorii cibernetici că acest serviciu de IA este folosit de angajați ai instituțiilor publice pentru a rezolva sarcini profesionale.

Suplimentar scrierii de coduri *malware*, creării *exploit*-urilor sau exfiltrării de credențiale, IA poate sprijini actorii cibernetici inclusiv în acțiunile tipice pe care aceștia le derulează în procesul de compromitere și exploatare a unui sistem informatic. Concret, IA poate facilita etapele clasice de *reconnaissance*, acces inițial, execuție a codului *malware*, asigurare a persistenței în sistemul compromis și chiar de exfiltrare a datelor de interes.

De exemplu, în cadrul procesului de *reconnaissance*, IA facilitează grupărilor de tip APT identificarea și documentarea potențialelor ținte, prin analiza automată de date din surse diverse, precum baze de date online și platforme de social media, dar și prin colectarea informațiilor cu privire la sistemele și aplicațiile utilizate preponderent într-o anumită companie.

Pentru obținerea accesului inițial în sistem, IA poate crea mesaje de *phishing* utilizând concepte de inginerie socială și bazate pe analiza automată a țintei realizată în procesul de *reconnaissance*. Totodată, inteligența artificială poate facilita procesul de *brute-force*, prin generarea de parole raportate la datele de cunoaștere obținute anterior.

În procesul propriu-zis de exploatare a sistemului informatic accesat, IA are abilitatea de a adapta comportamentul aplicației *malware*-ului, astfel încât să nu fie detectat. De asemenea, acesta poate analiza mediul accesat, cu scopul de a-l înțelege și a identifica opțiunea potrivită pentru rularea aplicației *malware*.

Pentru a asigura persistența în sistem, inteligența artificială poate crea cel mai potrivit *script* pentru executarea *malware*-ului, bazându-se pe analizarea comportamentului utilizatorului. Actorii cibernetici pot realiza un motor IA *malware* care să adapteze mecanismele de asigurare a persistenței în raport cu schimbările din mediul accesat.

Subsumat procesului de exfiltrare de date, IA poate analiza *pattern*-urile traficului de rețea, cu scopul de a obține mai multe detalii care să-i permită identificarea modului optim de comunicare dintre țintă și atacator. Totodată, poate realiza criptarea datelor sustrase pentru a evita procesele de detecție a traficului neobișnuit.

În contextul în care *software*-urile bazate pe inteligența artificială vor pătrunde accelerat în toate domeniile vieții cotidiene, iar decelarea conținutului veridic de cel generat artificial va fi din ce în ce mai dificilă, derularea unor campanii de conștientizare a acestor pericole va fi dezirabilă. Odată dobândită această cultură a securității cibernetice, șansele de succes ale grupărilor de tip APT se vor putea diminua.

OPERAȚIUNI INTERNAȚIONALE DE DESTRUCTURARE A UNOR INFRASTRUCTURI INFORMATICE CONEXE CRIMINALITĂȚII CIBERNETICE

În perioada ianuarie – august 2024, dinamica ecosistemului *cybercrime* a fost influențată semnificativ de operațiunile internaționale ale organelor de aplicare a legii, care au urmărit destructurarea și preluarea sub control a platformelor specializate de criminalitate cibernetică sau a elementelor de infrastructură informatică utilizate de grupările cibernetice motivate financiar. Operațiunile au vizat în special indisponibilizarea rețelelor de tip *botnet* (Operațiunea „Endgame"), platformelor *cybercrime (BreachForums, Nemesis Market)* sau destructurarea infrastructurilor informatice utilizate în cadrul unor campanii cibernetice cu *malware*-uri de tip *ransomware* (Operațiunea „Cronos" – Lockbit, Radar/Dispossessor *ransomware*) sau *Remote Access Trojan* (Warzone RAT).

RADAR/DISPOSSESSOR RANSOMWARE

La 12 august 2024 a avut loc o operațiune internațională condusă de FBI, care a vizat destructurarea infrastructurii informatice asociate *ransomware*-ului Radar/Dispossessor. În urma acestei operațiuni au fost preluate sub control mai multe servere și domenii asociate unor activități specifice criminalității cibernetice, localizate în SUA, UK și Germania.

INFO BOX

Gruparea Radar/ Dispossessor, condusă de utilizatorul alias-ului Brain, a avut un impact semnificativ la nivel internațional, vizând entități publice și private din sectoarele financiar-bancar, logistic, educație și sănătate. Gruparea Radar utilizează tactica *double-extortion*, respectiv criptează și exfiltrează datele gestionate de sistemele informatice compromise, amenințând victimele că le vor publica dacă nu plătesc răscumpărările.

Operațiunea condusă de FBI a fost realizată în colaborare cu National Crime Agency (NCA-UK), Procuratura din Bamberg, Germania, Bavarian State Criminal Police Office (BLKA-DE) și Procuratura din Ohio, SUA. Au fost identificați 12 suspecți, membri ai grupării Radar/ Dispossessor, localizați în Federația Rusă, Ucraina, Germania, Kenya, Serbia, Lituania și Emiratele Arabe Unite.

OPERAȚIUNEA „ENDGAME”

Între 27-29 mai 2024, EUROPOL a coordonat operațiunea „Endgame”, care a vizat elementele de infrastructură informatică asociate aplicațiilor *malware* de tip *dropper* IcedID, Bumblebee, Trickbot, Smokeloader, Pikabot și SystemBC. Acțiunea a avut un impact semnificativ asupra activității specifice ecosistemului *cybercrime*, întrucât aceste aplicații joacă un rol principal în distribuirea altor programe *malware*.

INFO BOX

Aplicațiile de tip *dropper* sunt *malware*-uri care au ca scop descărcarea și instalarea altor programe malware, de cele mai multe ori de tip *ransomware* sau *infostealer*, la nivelul sistemelor informatice vizate. Acestea sunt utilizate în prima etapă a *killchain*-ului unui atac cibernetic, fiind esențiale pentru distribuirea aplicațiilor *malware* fără a fi detectate de soluțiile antivirus.

„Endgame” a fost, de asemenea, cea mai importantă operațiune internațională care a vizat rețelele de tip *botnet*, fiind indisponibilizate peste 100 de servere din România, Bulgaria, Canada, Germania, Lituania, Țările de Jos, Elveția, UK, SUA și Ucraina. Operațiunea a condus la arestarea a 4 suspecți în Armenia și Ucraina, fiind preluate sub control și peste 2.000 de domenii asociate unor activități specifice *cybercrime*. Operațiunea „Endgame”, coordonată de organele de aplicare a legii din Franța, Germania și Țările de Jos, a fost sprijinită inclusiv de organele de aplicare a legii din România și o serie de companii private din domeniul securității cibernetice, inclusiv compania autohtonă Bitdefender.

BREACHFORUMS

În prima jumătate a anului 2023, administratorul platformei BreachForums, Conor Brian Fitzpatrik (pompompurin), a fost arestat. La 3 luni după arestare, infrastructura informatică a platformei a fost indisponibilizată. Cu toate acestea, o clonă a forumului a fost publicată la scurt timp, fiind dezvoltată și administrată de utilizatorul Baphomet și gruparea *cybercrime* ShinyHunters.

INFO BOX

Prin intermediul BreachForums au fost comercializate peste 11 miliarde de date exfiltrate din cadrul unor sisteme informatice compromise, aparținând unor entități publice sau private din majoritatea domeniilor de activitate, fiind considerată una dintre cele mai importante platforme specializate de criminalitate cibernetică la nivel global. În cadrul acesteia erau promovate inclusiv aplicații *malware* și alte servicii specifice ecosistemului *cybercrime*.

La 15 mai 2024, FBI și mai multe agenții internaționale de aplicare a legii din Marea Britanie, Ucraina, Australia, Noua Zeelandă și Islanda au preluat sub control a doua versiune a platformei BreachForums și canalul de Telegram asociat acesteia. La doar o lună după această operațiune, gruparea ShinyHunters a restabilit domeniul inițial al BreachForums, acesta fiind activ în continuare sub administrarea utilizatorului alias-ului Anastasia.

NEMESIS MARKET

La 20 martie 2024, autoritățile din Germania (Bundeskriminalamt – BKA), în colaborare cu organele de aplicare a legii din SUA și Lituania, au preluat sub control mai multe servere asociate platformei Nemesis Market, confiscând bunuri în valoare de aproximativ 94.000 euro și închizând mai multe operațiuni ilegale.

INFO BOX

Platforma *underground* Nemesis Market a fost înființată în anul 2021, având peste 150.000 de utilizatori și peste 1.100 de vânzători activi la nivel internațional, dintre care aproximativ 20% erau localizați în Germania. Membrii Nemesis utilizau platforma pentru a comercializa substanțe interzise și pentru a oferi o serie de servicii asociate criminalității cibernetice, respectiv infrastructura și aplicațiile *malware* necesare pentru derularea de atacuri de tip *ransomware*, DDoS sau *phishing*.

OPERAȚIUNEA „CRONOS”

Infrastructura celui mai prolific proiect Ransomware-as-a-Service – Lockbit – a fost destructurată la data de 20 februarie 2024, în urma unei operațiuni internaționale coordonate de NCA-UK.

INFO BOX

Gruparea care a dezvoltat și operează *ransomware*-ul Lockbit a fost responsabilă, la nivelul anului 2023, pentru 25% din atacurile cibernetice cu *ransomware* la nivel global.

În urma operațiunii „Cronos” au fost preluate sub control peste 200 de portofele virtuale, 34 de servere și 14.000 de conturi, fiind arestați 3 afiliați ai Lockbit în Ucraina și Polonia. Site-ul Lockbit a fost utilizat de organele de aplicare a legii inclusiv pentru publicarea unor comunicate de presă, știri despre arestările membrilor, precum și a unor chei de decriptare obținute în urma operațiunii. În luna mai, administratorul Lockbit, respectiv utilizatorul alias-ului LockbitSupp, a fost identificat în persoana cetățeanului rus Dimitry Yuryevich Khoroshev. În ciuda acestor acțiuni, în perioada martie – august 2024, gruparea Lockbit a revendicat un număr semnificativ de atacuri cibernetice cu *ransomware*, rămânând cea mai prolifică amenințare din ecosistemul *cybercrime*.

INFO BOX

Cu titlu de exemplu, în prima jumătate a anului 2024, gruparea Lockbit a publicat 325 de victime pe *Dedicated Leak Site*-ul asociat, fiind cea mai activă grupare *cybercrime*, urmată de gruparea Play ransomware, care a revendicat 155 de atacuri cu *ransomware* în aceeași perioadă.

WARZONE RAT

O acțiune comună internațională, condusă de FBI și sprijinită de Europol și J-CAT (*Joint Cybercrime Action Taskforce*), a condus la preluarea sub control a infrastructurii informatice asociate *malware*-ului Warzone RAT.

INFO BOX

Warzone RAT este o aplicație *malware* de tip *Remote Access Trojan*, care are capabilități avansate de exfiltrare de date, realizare de capturi de ecran, captare a șirurilor de caractere introduse de la tastatură (*keylogger*), accesare a camerei web sau microfoanelor, exfiltrare credențialelor și datelor bancare etc.

Operațiunea, care a avut loc la data de 7 februarie 2024, a culminat cu arestarea a doi dintre membrii grupării, localizați în Malta și Nigeria. Operațiunea a fost susținută de organe de aplicare a legii din mai multe țări, inclusiv din România, care au jucat un rol esențial în preluarea sub control a elementelor de infrastructură de comandă și control asociate aplicației *malware*.

Concluzionând, pe parcursul anului 2024 au fost înregistrate mai multe operațiuni de succes împotriva exponenților ecosistemului *cybercrime*, fiind destructurate mai multe platforme *cybercrime*, rețele *botnet* sau infrastructuri informatice conexate unor grupări cibernetice care derulează atacuri cibernetice cu aplicații *malware* de notorietate. Aceste acțiuni au condus inclusiv la arestarea unor membri ai acestor grupări, concretizându-se într-un factor cu un grad ridicat de importanță în descurajarea acestor activități ilegale.

Pe de altă parte, în aceeași perioadă au fost observate evoluții în tacticile, tehnicile și procedurile utilizate de aceștia, îmbunătățiri considerabile ale capabilităților aplicațiilor *malware* utilizate și, nu în ultimul rând, capacitatea de adaptare și repliere a exponenților ecosistemului *cybercrime*, prin reapariția unor grupări/*malware*-uri de notorietate după perioade semnificative de absență sau după ce au fost vizate de operațiuni internaționale similare. Aceste aspecte susțin ipoteza conform căreia riscurile generate de grupările cibernetice motivate financiar vor rămâne de actualitate în continuare pentru toate entitățile publice și private la nivel internațional și național.

CAMPANII DE ATACURI CIBERNETICE DE TIP DDOS DERULATE DE ENTITĂȚI HACKTIVISTE PRORUSE

Campaniile de atacuri cibernetice inițiate la adresa statelor membre NATO/UE care și-au exprimat susținerea față de Ucraina, inclusiv România, ilustrează că acțiunile și deciziile politice cu implicații în planul relațiilor internaționale pot crea premisele manifestării unor amenințări cibernetice motivate ideologic.

Până în prezent, atacurile cibernetice de tip *DDoS* îndreptate asupra unor infrastructuri informatice și de comunicații de interes național au fost realizate, în principal, de către aceleași grupări hacktiviste identificate anterior, asociate Federației Ruse (NoName057(16), Cyber Army of Russia, Cyber Dragon, Phoenix, Server Killers etc.).

INFO BOX

S-a constatat creșterea frecvenței atacurilor cibernetice derulate de actorii mediului hacktivist și diversificarea țintelor vizate, prin includerea unor entități care prezintă relevanță din prisma susținerii eforturilor de război ale Ucrainei. Acest aspect poate slăbi capacitatea instituțiilor statului de a răspunde eficient, determinând concentrarea eforturilor instituționale pentru contracararea atacurilor în detrimentul altor activități cu relevanță strategică.

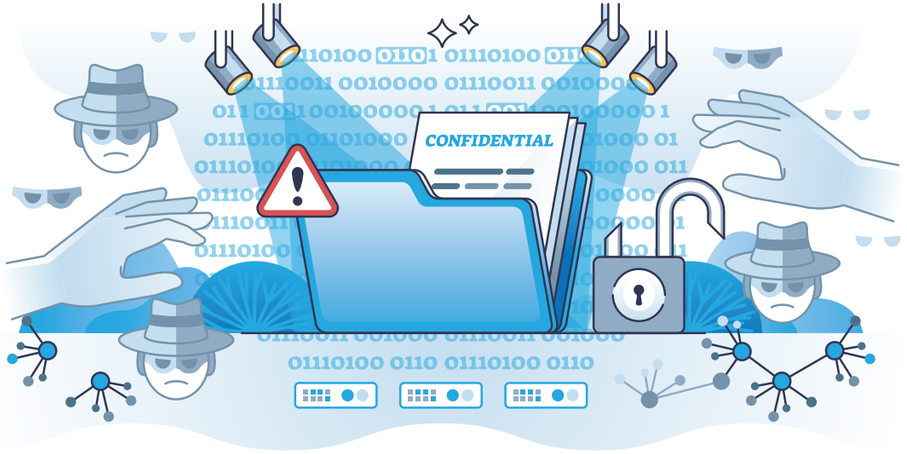
Concret, inclusiv pe parcursul anului 2024, pe fondul unor acțiuni de susținere a Ucrainei, România s-a numărat printre țintele grupărilor hacktiviste care și-au îndreptat atacurile cibernetice de tip DDoS asupra site-urilor unor instituții guvernamentale (Guvernul României), instituții publice (Banca Națională a României și Bursa de Valori București), precum și unor entități private din sectorul financiar-bancar (BCR, Banca Transilvania și Alpha Bank).

INFO BOX

Atacurile cibernetice orchestrate de actori hacktiviști proruși asupra instituțiilor publice din România sunt de natură a afecta disponibilitatea resurselor vizate și a genera prejudicii de imagine acestora. Până în prezent, efectele unor astfel de atacuri au fost în mare parte limitate, blocarea accesului populației la datele și serviciile de la nivelul website-urilor afectate fiind doar temporară.

Deși nu au fost identificate până în prezent legături concrete între grupări hacktiviste și entități statale, se conturează ipoteza existenței unei relații de coordonare sau, cel puțin, a aplicării unui regim permisiv de către autoritățile statale în raport cu activitățile întreprinse de grupările hacktiviste. Acestea ar putea utiliza instrumentele specifice grupărilor de tip APT pentru a derula atacuri cibernetice din ce în ce mai sofisticate, care să vizeze inclusiv exfiltrare de date, obținerea de beneficii materiale și indisponibilizarea unor infrastructuri critice. Totodată, pentru a disimula interesul unor actori cibernetici statali, grupările APT pot derula activități ostile în mediul cibernetic sub aparența unei motivații ideologice.

În perioada premergătoare alegerilor există probabilitatea ca numărul atacurilor cibernetice derulate în state membre NATO/UE să crească, actorii hacktiviști proruși alegând să se coaguleze în noi alianțe pentru a crește atât numărul atacurilor, cât și cel al țintelor vizate.



VULNERABILITĂȚI DE SECURITATE CIBERNETICĂ

CRITICE DE MARE IMPACT DESCOPERITE ÎN ANUL 2024 ȘI MIJLOACE DE REMEDIERE

În prezent, securitatea cibernetică este un punct de interes vital pe agenda dezvoltatorilor de tehnologie, fiind aplicate standarde, norme și proceduri prin care se vizează asigurarea confidențialității, integrității și disponibilității datelor. Cu toate acestea, există numeroase cazuri în care sunt identificate vulnerabilități de securitate cibernetică ulterior lansării tehnologiilor în mediile operaționale.

O parte dintre aceste vulnerabilități sunt cele de tip *zero-day (0-day)*, care reprezintă breșe de securitate la nivelul unor soluții *software* sau echipamente *hardware*, necunoscute dezvoltatorilor. Gradul ridicat de risc generat de vulnerabilitățile *0-day* este determinat de faptul că acestea nu dispun de actualizări de securitate, fiind facil de exploatat în cadrul unor campanii cibernetice.

În primul trimestru al anului 2024 au fost identificate o serie de vulnerabilități *0-day* la nivelul mai multor soluții și echipamente, enumerate în figura următoare, în care sunt prezentate clasificările atribuite în Glosarul CVE (*Common Vulnerabilities and Exposures*), perioada de timp cât au fost exploatate anterior divulgării publice și numărul de dispozitive compromise la nivel global.

IVANTI

CVE-2024-21877 este o vulnerabilitate de tip *path traversal*, a cărei exploatare permite unui atacator să realizeze acțiuni arbitrare, în mod neautentificat, de citire și ștergere a fișierelor de pe sistemul compromis.

CVE-2024-21888 este o vulnerabilitate care permite unui atacator escaladarea de privilegii și obținerea de drepturi de administrator la nivelul soluției compromise.

CVE-2024-21893 este o vulnerabilitate de tip *server-side request forgery*, prezentă la nivelul unor soluții VPN și de control al accesului. Exploatarea acesteia poate permite unui atacator eludarea mecanismului de autentificare și obținerea accesului la resurse restricționate din cadrul sistemului compromis.

FORTINET

CVE-2024-21762 este o vulnerabilitate de tip *out-of-bound write* prezentă în componenta *SSL VPN daemon* a instanței *firmware*-ului FortiOS, a cărei exploatare permite unui atacator să obțină acces neautorizat de la distanță, să execute comenzi și să preia controlul asupra echipamentelor compromise.

CISCO

CVE-2024-20353 și CVE-2024-20359 sunt vulnerabilități prezente la nivelul componentei VPN a soluției *Cisco Adaptive Security Appliance*. Exploatarea CVE-2024-20353 permite unui atacator neautentificat să execute comenzi de la distanță la nivelul soluției compromise (precum repornirea dispozitivului), generând astfel o condiție de *denial of service*.

CVE-2024-20359 permite unui atacator neautentificat să execute cod arbitrar cu privilegii root prin care poate să-și asigure persistența la nivelul soluțiilor compromise.

PALO ALTO

CVE-2024-3400 este o vulnerabilitate prezentă la nivelul unei soluții *firewall* a cărei exploatare poate permite unui atacator neautentificat să execute cod arbitrar cu privilegii *root*. În acest fel, atacatorul poate instala *backdoor*-uri, iar ulterior poate executa tehnici specifice de mișcare laterală prin care poate compromite alte resurse din cadrul organizației, de la nivelul cărora poate exfiltra fișiere și credențiale de acces.

În vederea remedierii acestor vulnerabilități și a eliminării riscului de a fi exploatate, este recomandată implementarea unor măsuri minime de securitate, precum:

- actualizarea soluțiilor vulnerabile la ultima versiune disponibilă, folosind instrumentele sau recomandările emise de producători;
- dezactivarea componentelor vulnerabile, în cazul în care actualizările nu pot fi implementate;
- monitorizarea soluțiilor vulnerabile în vederea identificării eventualelor comportamente neobișnuite ori nelegitime;
- realizarea unor acțiuni de conștientizare adresate angajaților și utilizatorilor sistemelor informatice de la nivelul organizației;
- menținerea unei abordări proactive prin elaborarea și implementarea unor planuri și măsuri de securitate cibernetică la nivelul întregii organizații.

- monitorizarea soluțiilor vulnerabile în vederea identificării eventualelor comportamente neobișnuite ori nelegitime;
- realizarea unor acțiuni de conștientizare adresate angajaților și utilizatorilor sistemelor informatice de la nivelul organizației;
- menținerea unei abordări proactive prin elaborarea și implementarea unor planuri și măsuri de securitate cibernetică la nivelul întregii organizații.

VULNERABILITĂȚI DE TIP ZERO-CLICK

Exploatarea de vulnerabilități reprezintă una din modalitățile preferate ale actorilor cibernetici pentru a obține accesul în cadrul dispozitivelor vizate. Vulnerabilitățile de securitate cibernetică pot fi de ordin uman și tehnologic, dintre care se remarcă cele de tip *zero-click*.

Prin acest tip de vulnerabilitate atacatorii încearcă să realizeze atacuri cibernetice fără ca victima să știe că a fost ținta unui astfel de atac și, totodată, fără a putea împiedica infectarea sistemului. Concret, vulnerabilitatea *zero-click* este exploatată de un atacator într-un atac cibernetic pentru a compromite un dispozitiv mobil sau un sistem informatic, fără ca victima să fie nevoită să acceseze un link, să deschidă un fișier sau să instaleze o aplicație *malware*. Exploatarea efectivă a unei vulnerabilități *zero-click* necesită transmiterea de către atacator a unui e-mail, mesaj sau apel audio prin intermediul unei aplicații instalate pe dispozitive mobile sau pe sisteme informatice.

Aceste vulnerabilități prezintă un risc ridicat pentru entitățile-țintă, deoarece utilizatorii nu pot evita materializarea atacului cibernetic prin utilizarea de sisteme de securitate cibernetică sau prin neaccesarea unor e-mailuri suspecte/ a unor fișiere din surse necunoscute. Odată ce exploatarea vulnerabilităților *zero-click* se materializează, actorii cibernetici pot exfiltra date sau instala aplicații *malware* pentru asigurarea persistenței.

În anul 2019 a fost derulată o campanie cibernetică în care a fost exploatată o vulnerabilitate *zero-click* asupra aplicației de mesagerie instantă WhatsApp. Atacatorii au compromis aplicația fără a fi necesară o interacțiune cu utilizatorul, expunând mesajele private și conținutul multimedia ale victimei.

O altă aplicație afectată de astfel de vulnerabilități o reprezintă Microsoft Outlook. Actorul statal rus APT28 a exploatat vulnerabilitatea *zero-click* Microsoft Outlook CVE-2023-23397 în trei campanii de atac: martie-decembrie 2022, martie 2023 și septembrie-octombrie 2023. Pe data de 14 martie 2023, compania americană a publicat o actualizare de securitate cibernetică pentru Microsoft Outlook prin care a remediat vulnerabilitatea. Suplimentar, în anul 2024, a fost identificată o nouă vulnerabilitate de tip *zero-click* în cadrul Microsoft Outlook (CVE-2024-30103), remediată de compania Microsoft.

Actorii statali exploatează astfel de vulnerabilități pentru a derula activități de spionaj cibernetic asupra unor ținte de interes din domeniul guvernamental, diplomatic, militar sau neguvernamental.

Protejarea împotriva exploatării vulnerabilităților *zero-click* este dificil de realizat, însă există câteva măsuri prin care se poate reduce riscul, precum actualizări de *software*, dezactivarea/ dezinstalarea/ limitarea accesului aplicațiilor și serviciilor ce nu sunt folosite frecvent, utilizarea soluțiilor *anti-spyware* și *anti-malware* (pentru detectarea comportamentului anormal sau pentru oprirea atacurilor) sau utilizarea de dispozitive distincte pentru activități de serviciu sau uz personal.

ANALIZĂ DE RISC
PE SEGMENTUL SECURITĂȚII CIBERNETICE ÎN DOMENIILE TELECOMUNICAȚII ȘI ENERGIE LA NIVELUL UE

În iulie 2024, Statele Membre (SM) ale Uniunii Europene (UE), cu sprijinul Comisiei Europene (COM) și al Agenției UE pentru Securitate Cibernetică (ENISA), au publicat primul raport privind securitatea și reziliența cibernetică în sectoarele telecomunicații și energie.

Raportul evidențiază o serie de riscuri cibernetice conexe lanțului de aprovizionare, lipsei resursei umane specializate și activității generate de actori motivați financiar și strategic.

O preocupare permanentă pentru ambele sectoare o reprezintă amenințările determinate de *ransomware*, *data wipers* și exploatarea vulnerabilităților *zero-day (0-day)*, acestea generând provocări, în special pe segmentul tehnologiei operaționale.

Pentru sectorul energetic, cel mai ridicat grad de risc este reprezentat de amenințările de tip *insider threats*, amplificate de lipsa unor proceduri adecvate de *vetting* a personalului nou angajat și dublate de dificultatea atragerii de specialiști în domeniul securității cibernetice.

Pentru sectorul telecomunicațiilor, principalele amenințări cibernetice sunt generate de atacuri cibernetice derulate prin intermediul infrastructurii de roaming și cele lansate de rețele de boți. Suplimentar, sabotajul fizic al infrastructurii de cabluri maritime de comunicații și bruiajul semnalelor satelitare au fost identificate ca riscuri specifice sectorului telecomunicațiilor care sunt deosebit de dificil de atenuat.

Din perspectiva asigurării unui răspuns optim cu privire la riscurile evidențiate, în cadrul raportului au fost punctate o serie de recomandări defalcate pe patru arii de acțiune, după cum urmează:

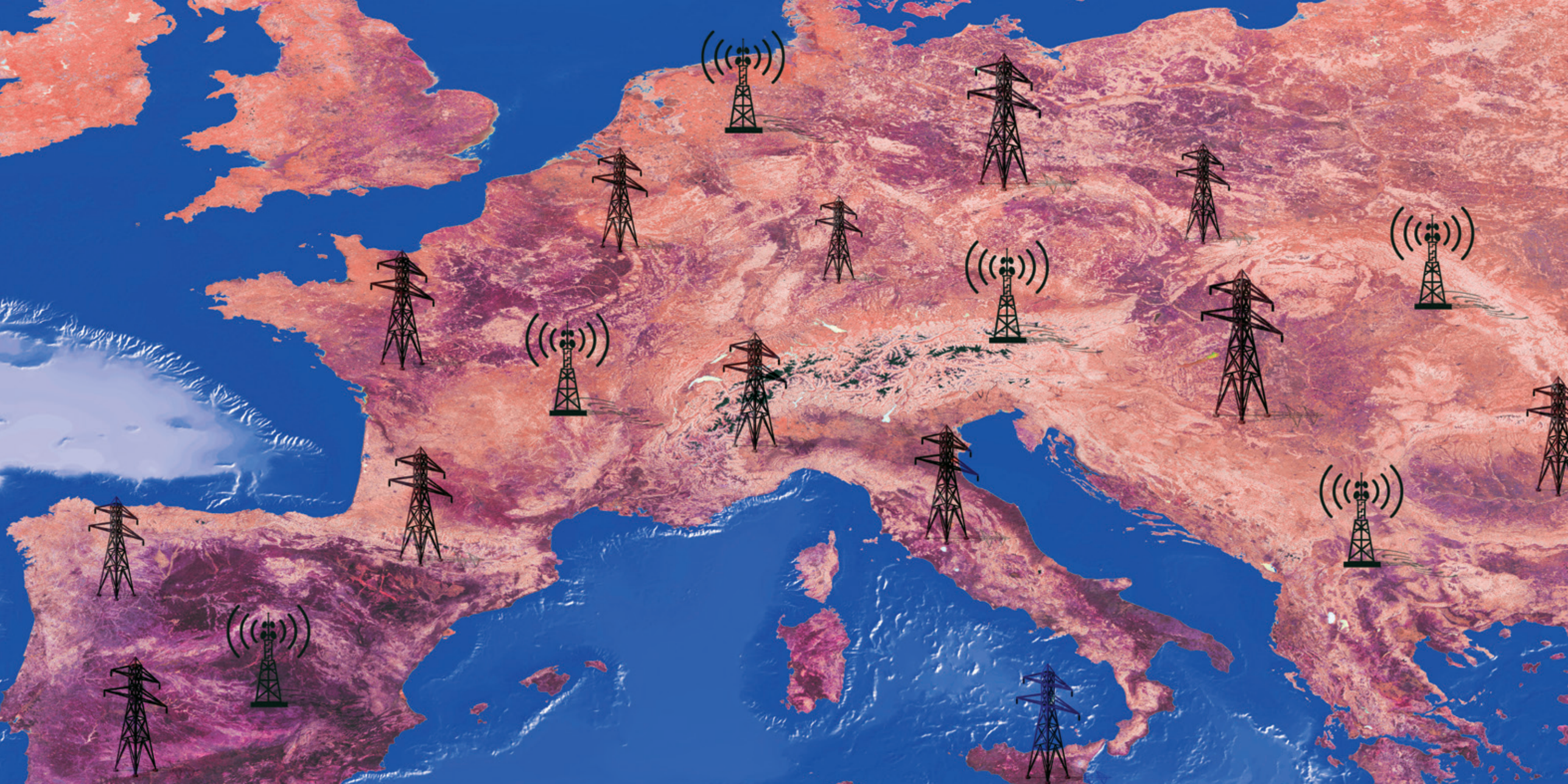
1. Reziliența și capacitatea de răspuns la incidente cibernetice pot fi îmbunătățite prin intermediul unor măsuri precum:
   - ➡ schimbul de bune practici cu privire la atacurile *ransomware*;
   - ➡ monitorizarea vulnerabilităților de securitate cibernetică;
   - ➡ implementarea unor politici de securitatea a personalului;
   - ➡ gestionarea eficientă a activelor organizațiilor;
   - ➡ intensificarea cooperării pe segmentul securității cibernetice la nivel comunitar, cu entitățile CSIRT, instituțiile de aplicare a legii și partenerii internaționali.

De asemenea, SM UE trebuie să realizeze evaluări de securitate cibernetică în conformitate cu prevederile Directivei NIS 2 pentru sectoarele cuprinse în cadrul acesteia (Directiva 2555/2022).

2. Activitățile de *awareness* și schimbul de informații trebuie să fie consolidate prin includerea în cadrul acestora a unor aspecte cu privire la contextul geopolitic, potențiale pericole la adresa integrității fizice a echipamentelor și dezinformarea.

3. Consolidarea planurilor de contingență, management al crizelor și colaborare operațională, în materie de proceduri, prin scurtarea liniilor de comunicare dintre sectoarele implicate și autoritățile responsabile în domeniul securității cibernetice.

4. Securitatea lanțurilor de aprovizionare ar trebui abordată prin realizarea de evaluări care să vizeze identificarea dependențelor față de furnizori din țări terțe care prezintă grad ridicat de risc.



CyDEx24

CyDEx este un exercițiu național de securitate cibernetică, ajuns anul acesta la cea de-a opta sa ediție. Evenimentul este organizat de SRI, prin intermediul Centrului Național Cyberint, în parteneriat cu structurile membre ale Consiliului Operativ de Securitate Cibernetică (COSC), fiind cel mai important eveniment din domeniul securității cibernetice la nivel național.

Principalul obiectiv al exercițiului este exersarea capacităților defensive în domeniul securității cibernetice împotriva amenințărilor la adresa infrastructurilor informatice și de comunicații de interes național.

CyDEx24 este singurul exercițiu național de tip *hands-on*, axat cu precădere pe componenta practică, care oferă în același timp un grad avansat de complexitate, realism, precum și un nivel ridicat de expunere.

Evenimentul reunește experți în domeniu care, pe perioada celor trei zile de exercițiu, se vor confrunta cu simulări de amenințări cibernetice cu mai multe niveluri de dificultate, simulate în poligonul Centrului Cyberint.

La exercițiu vor fi invitate să desemneze participanți instituțiile publice cu atribuții în domeniul securității cibernetice, instituții care dețin infrastructuri informatice și de comunicații de interes național, entități din mediul academic și companii care dețin capital public sau privat.

BENEFICIILE REZULTATE DIN PARTICIPAREA ACTIVĂ LA EXERCIȚIU:

- alinierea la prevederile Planului de acțiune la nivel național privind implementarea Sistemului Național de Securitate Cibernetică;
- verificarea și stimularea mecanismelor de cooperare între instituțiile publice cu responsabilități în domeniul securității naționale;
- verificarea și stimularea mecanismelor de cooperare între instituțiile publice, mediul privat și cel academic;
- dezvoltarea unui mecanism eficient de avertizare, alertă și reacție la incidente/atacuri cibernetice;
- verificarea nivelului de expertiză tehnică a specialiștilor din cadrul entităților participante în cazul unui incident cibernetic major la nivel național;
- creșterea nivelului de conștientizare atât la nivelul instituțiilor publice, cât și al entităților private cu privire la amenințările provenite din spațiul cibernetic, precum și la efectele cauzate de un incident cibernetic major la nivel național.

CyDEx24

STRATEGII NAȚIONALE
ÎN DOMENIUL INTELIGENȚEI ARTIFICIALE ȘI TEHNOLOGIILOR CUANTICE

La data de 11 iulie 2024, Guvernul României a adoptat Hotărârea nr. 832 privind aprobarea Cadrului strategic național în domeniul inteligenței artificiale 2024-2027 (CSN-IA), intrată în vigoare din 25 iulie 2024.

CSN-IA contribuie semnificativ la strategia României privind adoptarea tehnologiilor digitale în economie și societate în condiții de respectare a drepturilor omului și de promovare a excelenței și încrederii în tehnologia IA. Strategia susține eforturile de standardizare, operaționalizare și reglementare a dezvoltării IA și de potențare a efectelor pozitive asociate cu această tehnologie, promovând potențialul inovativ național în domeniul IA, contribuind și la gestionarea riscurilor pe care le prezintă evoluția acestor tehnologii.

CSN-IA asigură, de asemenea, o aliniere a demersurilor României cu direcțiile strategice la nivel european privind regulile comune aplicate serviciilor digitale, susținând eforturile de stabilire a standardelor europene și internaționale în domeniul gestionării tehnologiilor care au la bază inteligență artificială.

Cadrul strategic național în domeniul Inteligenței Artificiale urmărește susținerea educației și formarea de competențe specifice IA, dezvoltarea și utilizarea eficientă a infrastructurii *hardware* specifice IA, dezvoltarea sistemului național de Cercetare – Dezvoltare – Inovare în domeniul IA și facilitatea adoptării IA în întreaga societate, în special în cadrul sectoarelor socio-economice prioritare și, nu în ultimul rând, dezvoltarea unui sistem de guvernanță și de reglementare a IA.

La data de 21 august 2024, Guvernul României a adoptat Hotărârea nr. 1028 privind aprobarea Strategiei naționale în domeniul tehnologiilor cuantice pentru perioada 2024-2029 (SN-TC), intrată în vigoare din 04.09.2024, care propune crearea unui cadru național privind dezvoltarea tehnologiilor cuantice în vederea valorificării oportunităților oferite de acestea.

Întrucât domeniul tehnologiilor cuantice poate reprezenta un potențial semnificativ de dezvoltare economică și de creștere a cunoștințelor tehnice, România urmărește să devină un centru regional de excelență în acest domeniu și să fie unul dintre liderii la nivel global în cercetare, dezvoltare și scriere de aplicații care au la bază tehnologii cuantice.

Printre avantajele și oportunitățile oferite de tehnologiile cuantice se numără:

- dezvoltarea și valorificarea expertizei în acest domeniu;
- dezvoltarea unui avantaj strategic pentru progresele viitoare;
- susținerea economiei și îmbunătățirea productivității;
- poziționarea României ca destinație regională și internațională pentru talente și investiții, cu un ecosistem local puternic.

Pe lângă oportunitățile economice semnificative generate de acest domeniu, adoptarea tehnologiilor cuantice trebuie realizată în condiții de siguranță, securitate și cu asigurarea principiilor și valorilor democratice, întocmai cu atitudinea abordată în gestionarea implementării tehnologiilor de IA. SN-TC creează premisele unor evoluții notabile în domeniul securității cibernetice, tehnologiile cuantice având capabilitatea de a contribui decisiv la creșterea rezilienței infrastructurilor informatice și de comunicații de interes național și a furnizorilor de servicii esențiale din România, respectiv la contracararea amenințărilor provenite din spațiul cibernetic.

Astfel, SN-TC vizează: **(1)** asigurarea resurselor necesare pentru dezvoltarea tehnologiilor cuantice, **(2)** dezvoltarea industriei naționale în domeniul cuantic și **(3)** consolidarea poziției României în arhitectura internațională a domeniului cuantic, prin dezvoltarea unui ecosistem cuantic, care poate să faciliteze colaborarea între domeniile IT, academic și guvernamental. Aceste obiective au în vedere:

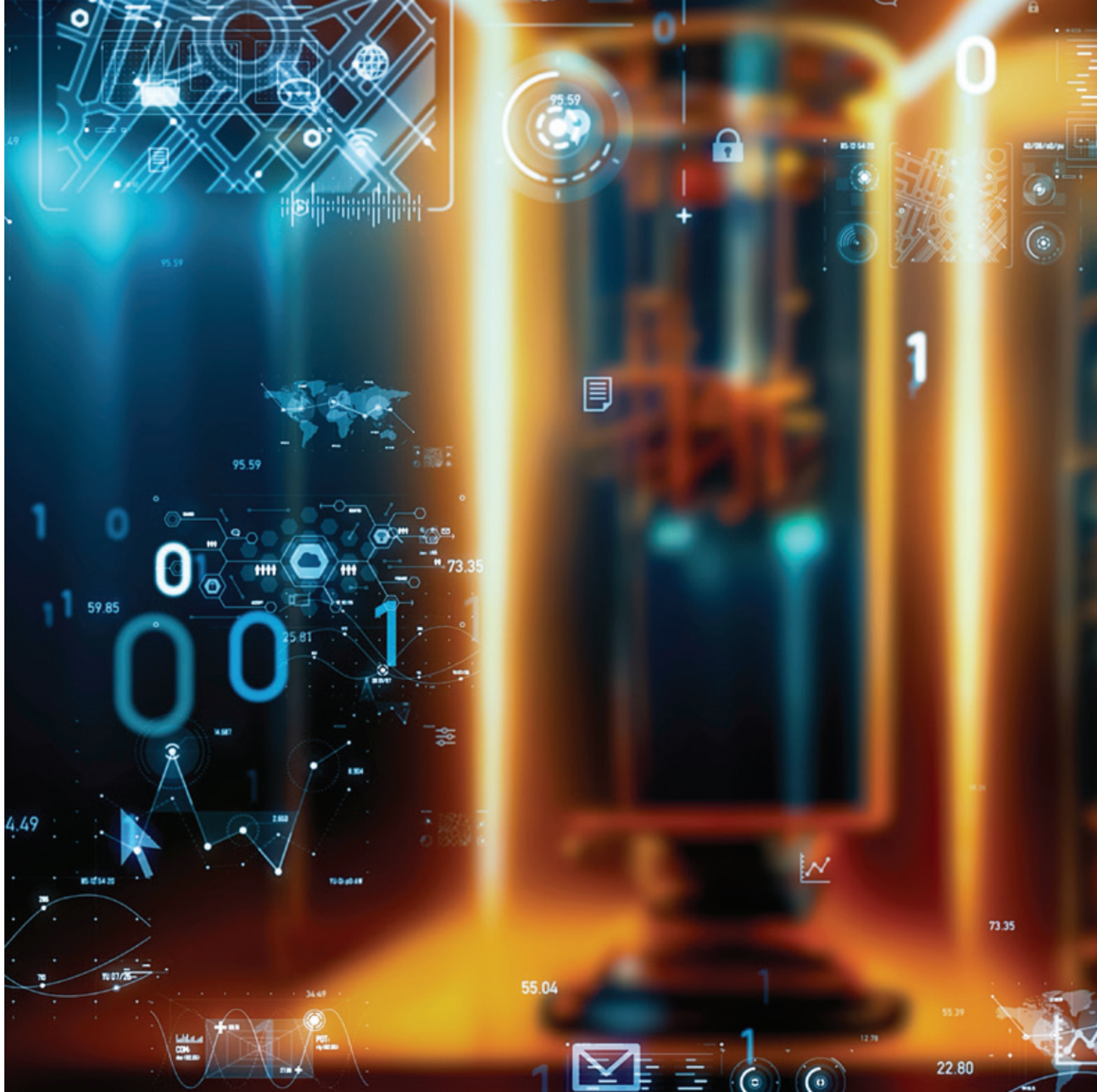
- dezvoltarea infrastructurii de comunicații cuantice autohtone și conectarea la infrastructura de comunicații cuantice europene;
- dezvoltarea unor centre de cercetare și platforme de testare și validare, necesare pentru susținerea cercetării și inovației în domeniul cuantic;
- dezvoltarea de aplicații software care să generalizeze utilizarea tehnologiilor cuantice în societate;
- creșterea investițiilor în formarea de specialiști în domeniul tehnologiilor cuantice;
- încurajarea cooperării internaționale și cercetarea și dezvoltarea tehnologiilor cuantice, prin participarea la inițiative și proiecte globale.

SN-TC susține cooperarea internațională în domeniul dezvoltării tehnologiilor cuantice, prin: (1) participarea activă în cadrul proiectelor și inițiativelor UE și NATO și (2) cooperarea cu liderii din domeniul cuantic (SUA, UK, Israel, Canada și Coreea de Sud), activitate care poate reprezenta fundamentul asigurării intereselor naționale ale României, precum și principalul instrument de evaluare a riscurilor generate în domeniul tehnologiilor cuantice.

INFO BOX

Adoptarea strategiilor naționale în domeniile inteligenței artificiale și tehnologiilor cuantice reprezintă un pas esențial în demersurile naționale de valorificare a capabilităților specifice acestor tehnologii și pentru a preîntâmpina eventualele provocări generate de acestea, în special în domeniul securității cibernetice.

Ambele tehnologii pot contribui la eficientizarea măsurilor de securitate cibernetică la nivel național, însă pot genera și potențiale provocări (spre exemplu, soluțiile criptografice actuale vor putea fi compromise cu ușurință prin utilizarea tehnologiilor cuantice).



REGULAMENTUL PRIVIND SERVICIILE DIGITALE
(DIGITAL SERVICE ACT - DSA)

La data de 19 octombrie 2022 a fost semnat de către Consiliul Uniunii Europene și Parlamentul European actul legislativ privind serviciile digitale, iar începând cu 17 februarie 2024 prevederile actului se referă la platformele online, precum serviciile intermediare, piețele online, rețelele sociale sau platformele de partajare de conținut și se adresează furnizorilor de servicii digitale care acționează drept intermediari între consumatori și bunuri, servicii și conținut.

INFO BOX

Regulamentul are la bază un principiu simplu, conform căruia ce este ilegal în mediul offline trebuie să fie ilegal și în mediul online.

În legislația națională actul a fost transpus prin Legea nr. 50/2024 din 18 martie 2024 *privind stabilirea unor măsuri pentru aplicarea Regulamentului UE 2022/2065 privind o piață unică pentru serviciile digitale.*

Obiectivele regulamentului privind serviciile digitale vizează trei categorii principale:

CETĂȚENI:

- Îmbunătățirea protecției drepturilor fundamentale;
- Sporirea controlului și extinderea opțiunilor de care pot beneficia utilizatorii;
- Creșterea protecției copiilor în mediul online;
- Diminuarea șanselor de expunere la conținut ilegal.

FURNIZORII DE SERVICII DIGITALE:

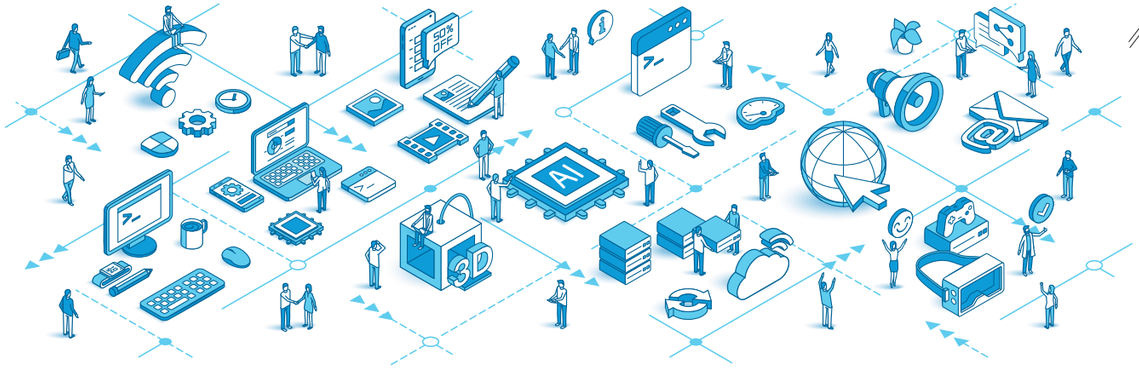
- Augmentarea nivelului de certitudine juridică;
- Stabilirea unui set unic de norme la nivelul întregii Uniuni Europene;
- Facilitarea accesului și dezvoltării pe piața din Europa.

UTILIZATORI COMERCIALI DE SERVICII DIGITALE:

- Facilitarea accesului la piețele din întreaga UE prin intermediul platformelor dedicate;
- Asigurarea unor condiții de concurență echitabile, care descurajează furnizorii de conținut ilegal.

EXEMPLE DE PLATFORME ONLINE ȘI MOTOARE DE CĂUTARE FOARTE MARI PE CARE DSA ÎȘI PROPUNE SĂ LE REGLEMENTEZE:

- Bing, Google Search;
- AliExpress, Amazon Store, Apple AppStore, Google Play, Google Shopping;
- Facebook, Instagram, TikTok, X, Snapchat, YouTube, LinkedIn etc.



REGULAMENTUL PRIVIND REZILIENȚA OPERAȚIONALĂ DIGITALĂ A SECTORULUI FINANCIAR DIN UNIUNEA EUROPEANĂ (DORA)

Regulamentul (UE) 2022/2554 privind reziliența operațională digitală a sectorului financiar, numit și Regulamentul DORA (*Digital Operational Resilience Act*), stabilește norme uniforme privind securitatea rețelelor și sistemelor informatice aparținând entităților financiare din Uniunea Europeană. Regulamentul vizează instituțiile bancare, societățile de asigurări, companiile de investiții, platformele crypto de tranzacționare și furnizorii de servicii de tip IT&C contractați.

INFO BOX

Regulamentul DORA a fost publicat în Jurnalul Oficial al Uniunii Europene la 27.12.2022, intrând în vigoare la 17.01.2023, și urmează să fie aplicat începând cu data de 17.01.2025.

Acest regulament face parte din pachetul legislativ care include și Directiva (UE) 2022/2556 a Parlamentului european și a Consiliului privind reziliența operațională digitală pentru sectorul financiar. Directiva stabilește norme generale de guvernanță internă și dispoziții privind riscurile operaționale. Acestea conțin cerințe referitoare la planurile de intervenție și de continuare a activității, care servesc drept bază pentru abordarea riscurilor din domeniul IT&C. Cu toate acestea, pentru a aborda riscurile IT&C în mod explicit, cerințele privind planurile de intervenție și de continuitate a activității trebuie să fie modificate în conformitate cu cerințele Regulamentului DORA.

Regulamentul DORA urmărește sporirea nivelului de armonizare în ceea ce privește diferitele componente ale rezilienței digitale, prin introducerea unor cerințe privind gestionarea riscurilor cibernetice și raportarea acestor incidente.

Concret, instituțiile financiare și furnizorii de servicii de tip IT&C vor trebui să raporteze breșele de securitate/ incidentele cibernetice care au avut loc la nivelul acestora. Datele despre astfel de incidente (inclusiv informații despre tipul de incident identificat, motivația atacului cibernetic, măsurile de securitate implementate etc.) vor fi colectate de o nouă autoritate desemnată, care va asigura implementarea regulamentului DORA pe 5 direcții principale de acțiune: (1) gestionarea riscurilor, (2) raportarea incidentelor, (3) reziliența operațională, (4) părți terțe și (5) agregarea datelor.

INFO BOX

La nivelul UE, instituțiile care asigură supravegherea și controlul instituțiilor financiare și crypto-exchange-urilor din perspectiva respectării regulamentelor DORA și MiCA (*Markets in Crypto-Assets*) sunt *The European Banking Authority* (EBA) și *The European Securities and Markets Authority* (ESMA).

Regulamentul DORA stabilește un set de cerințe uniforme privind securitatea rețelelor și sistemelor informatice care sprijină procesele operaționale ale entităților financiare din UE, respectiv:

1. Cerințe aplicabile entităților financiare în legătură cu:

➡ gestionarea riscurilor legate de tehnologia informației și comunicațiilor (IT&C);

➡ raportarea incidentelor majore legate de tehnologia informației și comunicațiilor și notificarea, în mod voluntar, a autorităților competente desemnate despre amenințările cibernetice semnificative;

➡ raportarea de către entitățile financiare către autoritățile desemnate a incidentelor operaționale sau de securitate majore legate de plăți;

➡ testarea rezilienței operaționale digitale;

➡ schimbul de informații și de date operative cu privire la amenințările cibernetice și vulnerabilități;

➡ măsuri pentru buna gestionare a riscurilor IT&C generate de părți terțe.

DIGITAL OPERATIONAL RESILIENCE ACT

2. Cerințe aplicabile în legătură cu acordurile contractuale încheiate între furnizorii de servicii IT&C și entitățile financiare.

3. Reguli privind instituirea și desfășurarea cadrului de supraveghere pentru furnizorii terți esențiali de servicii IT&C, atunci când furnizează servicii entităților financiare.

4. Reguli privind cooperarea între autoritățile competente și norme privind supravegherea și asigurarea conformității de către autoritățile competente în legătură cu toate aspectele vizate de regulament.

De asemenea, potrivit regulamentului DORA, entitățile financiare au obligația utilizării de strategii, politici, proceduri și protocoale și instrumente IT&C pentru a proteja împotriva riscurilor și amenințărilor cibernetice toate activele informaționale și IT&C (aplicații *software, hardware*, servere etc.), precum și toate componentele și infrastructurile fizice relevante (sediile, centrele de date și zonele desemnate sensibile). Concret, entitățile financiare trebuie:

➡ să definească, să instituie și să pună în aplicare măsuri pentru a detecta, a gestiona și a notifica incidentele cibernetice;

➡ să clasifice incidentele cibernetice și să determine impactul acestora pe baza unor criterii, precum numărul de clienți și contrapărți afectate, durata și pierderile de date;

➡ să prezinte un raport referitor la incidentele majore legate de tehnologia informației și comunicațiilor autorității competente desemnate, care le transmite unui organism superior;

➡ să instituie proceduri și procese adecvate pentru a garanta monitorizarea, tratarea și urmărirea consecventă și integrată a incidentelor cibernetice, pentru a asigura identificarea, documentarea și abordarea cauzelor lor principale, astfel încât să se prevină apariția unor astfel de incidente cibernetice.

Entitățile financiare pot notifica, în mod voluntar, amenințările cibernetice semnificative către autoritatea competentă desemnată conform DORA, atunci când consideră că amenințarea este relevantă pentru sistemul financiar, pentru utilizatorii serviciilor sau pentru clienții entității respective.

În plus, în cazul în care are loc un incident cibernetic major, care are impact asupra intereselor financiare ale clienților, entitățile bancare îi informează pe aceștia cu celeritate, inclusiv cu privire la măsurile care au fost implementate pentru a atenua efectele negative ale incidentului respectiv.

REGULAMENTUL DORA VIZEAZĂ URMĂTOARELE DOMENII DE APLICARE:

➡ Instituții de credit, instituții de plată, instituții emitente de monedă electronică și instituții de pensii ocupaționale;

➡ Prestatori de servicii de informare cu privire la conturi, de criptoactive, de raportare a datelor, de finanțare participativă și terțe părți IT&C;

➡ Firme de investiții, fonduri de investiții alternative, societăți de administrare, agenții de rating de credit și administratori de indici de referință critici;

➡ Societăți de asigurare, intermediari de asigurări și societăți de reasigurare.

În contextul gradului ridicat de digitalizare a entităților din sectorul financiar și al intensificării nivelului de interconectivitate între acestea, care amplifică riscurile și amenințările cibernetice la adresa acestor entități, regulamentul DORA va avea un impact profund asupra domeniului financiar din Uniunea Europeană. DORA reprezintă atât o completare semnificativă a cadrului de reglementare actual, cât și un pas important în eforturile UE de a-și proteja sectorul financiar de amenințările cibernetice. Concret, prin impunerea unor practici standardizate de gestionare a riscurilor cibernetice, de raportare a incidentelor cibernetice, de testare a rezilienței și de gestionare a riscurilor de către terți, regulamentul DORA urmărește asigurarea rezilienței cibernetice a sistemului financiar din statele membre UE în fața unui peisaj digital în continuă evoluție.

Nu în ultimul rând, promovarea de către regulamentul DORA a standardizării raportării incidentelor și a schimbului de informații/ bune practici poate contribui la sporirea capacității sectorului de a anticipa, a răspunde și a se recupera mai eficient în urma unor incidente cibernetice semnificative.

WWW.SRI.RO/CYBERINT