MINISTERUL CERCETĂRII, INOVĂRII ȘI DIGITALIZĂRII

ORDIN

privind aprobarea criteriilor de stabilire şi lista nominală privind produsele, serviciile şi entităţile producătoare şi/sau furnizoare interzise, provenind direct sau indirect din Federaţia Rusă

Având în vedere necesitatea prevenirii şi contracarării ameninţărilor cibernetice derulate de Federația Rusă, precum și de actori statali şi nonstatali aflați sub controlul Federației Ruse asupra infrastructurilor de comunicaţii şi tehnologia informaţiei cu valenţe critice pentru securitatea naţională;

Ținând cont de faptul că Ministerul Cercetării, Inovării și Digitalizării este organ de specialitate al administrației publice centrale, cu rol de elaborare și implementare, la nivel național, a politicii, strategiei și reglementărilor specifice de dezvoltare și de armonizare ale activităților în cadrul politicii generale a Guvernului, precum și a faptului că îndeplinește rolul de autoritate de stat în domeniul securității cibernetice, conform prevederilor art. 1 alin. (3) și art. 4 alin. (1) din Hotărârea Guvernului nr. 371/2021 privind organizarea şi funcţionarea Ministerului Cercetării, Inovării şi Digitalizării, cu modificările şi completările ulterioare;

În conformitate cu prevederile art. 2 alin. (2) din Legea nr. 354/2022 privind protecţia sistemelor informatice ale autorităţilor şi instituţiilor publice în contextul invaziei declanşate de Federaţia Rusă împotriva Ucrainei, publicat în Monitorul Oficial, Partea I nr. 1200 din 14 decembrie 2022;

În temeiul art. 12 alin. (3) din Hotărârea Guvernului nr. 371/2021 privind organizarea şi funcţionarea Ministerului Cercetării, Inovării şi Digitalizării, cu modificările şi completările ulterioare;

ministrul cercetării, inovării şi digitalizării emite prezentul ordin.

Art. 1. -

Se aprobă criteriile de stabilire a produselor şi serviciilor software de tip antivirus provenind direct sau indirect din Federaţia Rusă sau de la un operator economic aflat sub controlul direct sau indirect al unei persoane fizice sau juridice din Federaţia Rusă sau al cărei capital este constituit cu participaţie provenind în mod direct sau prin firme interpuse din Federaţia Rusă ori din ale cărui organe de administrare fac parte persoane din Federaţia Rusă, prevăzute în Anexa 1 care face parte integrantă din prezentul ordin.

Art. 2. -

Se aprobă lista nominală privind produsele, serviciile şi entităţile producătoare şi/sau furnizoare interzise în temeiul Legii nr. 354/2022 privind protecţia sistemelor informatice ale autorităţilor şi instituţiilor publice în contextul invaziei declanşate de Federaţia Rusă împotriva

Ucrainei, denumită în continuare Legea, prevăzută în Anexa 2 care face parte integrantă din prezentul ordin.

Art. 3. -

Se aprobă procedura metodologică privind întocmirea listei de produse și servicii software care îndeplinesc criteriile prevăzute la art. 1 și art. 2 din Lege, prevăzută în Anexa 3 care face parte integrantă din prezentul ordin.

Art. 4. -

Direcțiile de specialitate din cadrul Ministerului Cercetării, Inovării și Digitalizării împreună cu autoritățile și instituțiile prevăzute la art. 2 alin. (3) și (4) din Lege duc la îndeplinire prezentul ordin.

Art. 5. -

(1) Prezentul ordin se aplică tuturor autorităților și instituțiile publice de la nivel central și local, precum și persoanele fizice și juridice care dețin reţele şi sisteme informatice prin care se gestionează informaţii clasificate.

(2) Prezentul ordin nu este obligatoriu pentru autorităţile şi instituţiile publice cu atribuţii proprii în domeniul securităţii naţionale, în domeniul securităţii cibernetice, apărării naţionale şi ordinii publice, cu excepția situației în care conducătorul autorității sau instituției respective decide aplicarea lui.

Art. 6. -

Prezentul ordin se publică în Monitorul Oficial al României, Partea I.

MINISTRU
SEBASTIAN-IOAN BURDUJA

București
Nr:
Data:

Anexa 1

Criteriile de stabilire a produselor şi serviciilor software de tip antivirus provenind direct sau indirect din Federaţia Rusă sau de la un operator economic aflat sub controlul direct sau indirect al unei persoane fizice sau juridice din Federaţia Rusă sau al cărei capital este constituit cu participaţie provenind în mod direct sau prin firme interpuse din Federaţia Rusă ori din ale cărui organe de administrare fac parte persoane din Federaţia Rusă

Art. 1. -

(1) Ministerul Cercetării, Inovării și Digitalizării, denumit în continuare MCID, analizează semestrial sau ori de câte ori este nevoie produsele și/sau serviciile software care se încadrează în una din categoriile de produse și servicii software prevăzute la art. 2 al Legii nr. 354/2022 privind protecţia sistemelor informatice ale autorităţilor şi instituţiilor publice în contextul invaziei declanşate de Federaţia Rusă împotriva Ucrainei, denumită în continuare Legea.

(2) În sensul prezentului ordin, categoriile de produse și servicii software prevăzute la art. 2 din Legea nr. 354/2022 au următoarele semnificații:

a) produse privind securitatea dispozitivului, securitatea punctului final - produse software care funcționează direct la nivelul dispozitivelor finale din cadrul unei rețele (precum computere, laptopuri, telefoane mobile, tablete etc.) și care asigură măsuri de securitate cibernetică pentru acestea.

b) aplicaţii şi programe software de detecție antivirus - produse software care furnizează măsuri de securitate cibernetică precum prevenirea, scanarea, detectarea şi eliminarea fişierelor infectate sau suspecte ce pot duce la compromiterea sistemului informatic și/sau a întregii rețele informatice din care acesta face parte;

c) aplicații și programe software antimalware, firewall pentru aplicații web, Firewall-as-a-Service - componente ale unor aplicații și programe software de detecție antivirus, specializate în prevenirea, detectarea şi eliminarea fişierelor malware, precum și implementarea de măsuri de securitate cibernetică pentru filtrarea traficului web în vederea prevenirii infectării unui dispozitiv informatic conectat la Internet;

d) reţele virtuale private - modalitate care asigură, prin utilizarea de servicii, aplicații ori programe software, anonimizarea și confidențialitatea activităţilor derulate în mediul Internet prin ascunderea adresei IP a utilizatorului și înlocuirea acesteia cu o altă adresă IP. Acest mecanism permite crearea unui tunel criptat şi securizat pentru conectarea de la distanță la o rețea internă de lucru existentă la nivelul unei organizații.

e) sisteme de detecție și răspuns pentru Endpointuri - soluţii integrate de securitate cibernetică cu capabilități de analiză și răspuns automat la incidente de securitate cibernetică.

Art. 2. -

(1) Produsele și serviciile prevăzute la art. 2 alin. (1) din Lege se identifică pe baza interogării bazelor de date publice și private ale autorităților și instituțiilor publice centrale și locale, pe baza codurilor CAEN specifice producerii, furnizării și comercializării unor astfel de produse și servicii.

(2) Operatorii economici de la care provin produsele și serviciile prevăzute la art. 2 alin. (1) din Lege sunt identificați pe baza criteriilor prevăzute la art. 1 alin. (1) și (3) din Lege.

Art. 3. -

(1) Datele prevăzute la art. 2 sunt utilizate pentru interogarea bazei de date de la Ministerul Justiției, respectiv Registrul Comerțului, cu aplicarea filtrelor specifice privind sediul social, sedii secundare, acționariat, ponderea acționariatului, rezultând o listă preliminară cu persoanele fizice și juridice care se încadrează în prevederile art. 1, alin. (3) din Lege.

(2) Datele prevăzute la art. 2 și cele rezultate din activitatea prevăzută la alin. (1) sunt utilizate pentru interogarea bazelor de date existente la nivelul Platformei SEAP administrată de Autoritatea pentru Digitalizarea României, denumită în continuare ADR, în scopul identificării operatorilor economici care furnizează produse și servicii software prevăzute la art. 2, alin. (1) din Lege, precum și a utilizatorilor acestora, inclusiv pe baza codurilor CPV și / sau CAEN relevante.

Art. 4. -

(1) Datele rezultate din activitățile prevăzute la art. 2 și 3 se vor completa cu date specifice relevante obținute de la Ministerul Finanțelor Publice, Ministerul Economiei, Serviciului Român de Informaţii, Serviciului de Informaţii Externe și de la alte autorități și instituții publice competente, inclusiv a autorităților publice prevăzute la art. 2 alin. (4) din Lege.

(2) Datele rezultate din activitățile prevăzute la art. 2 și 3 se vor completa cu date specifice relevante obținute și de la alte autorități și instituții publice, altele decât cele prevăzute la alin. (1), pe baza solicitării formulate de MCID.

(3) Autoritățile și instituțiile publice prevăzute la alin. (1) sunt obligate să răspundă în maximum 5 zile calendaristice de la trimiterea solicitării formulate de MCID. În cazuri temeinic motivate, acestea pot solicita prelungirea termenului la 10 zile calendaristice care se calculează de la data trimiterii solicitării formulate de MCID.

Art. 5. -

(1) Operatorii economici identificați în urma procedurii prevăzute la art. 2-4 pot fi notificați de către MCID pentru furnizarea unor informații suplimentare privind tipul de produse și servicii software pe care aceștia le produc sau comercializează, terțele părți cu care colaborează precum și beneficiarii finali.

(2) Operatorii economici prevăzuți la alin. (1) sunt obligați să răspundă la notificare în termen de maximum 5 zile calendaristice de la data comunicării acesteia de către MCID.

Art. 6. -

Produsele și serviciile software identificate, potrivit criteriilor prevăzute în prezenta anexă, rămân incluse în lista nominală privind produsele, serviciile și entitățile producătoare și/sau furnizoare interzise, conform prevederilor art. 2, alin. (2) din Legea nr. 354/2022, indiferent de categoria de licențiere ulterioară (e.g. open source, freeware) sau de modificare a denumirii.

Anexa 2

Lista nominală privind produsele, serviciile şi entităţile producătoare şi/sau furnizoare interzise în temeiul Legii nr. 354/2022 privind protecţia sistemelor informatice ale autorităţilor şi instituţiilor publice în contextul invaziei declanşate de Federaţia Rusă împotriva Ucrainei

	Categorie cf. art. 1 alin. (3) L nr. 354/2022	Categorie cf. Art.2 alin. (1) L nr.354/2022	Denumirea persoanei juridice și/sau a produselor și serviciilor software	Elemente de identificare	URL / site
1.	**AB**	**A**	XSIGNAL • Serviciu	19801, US, Delaware, 919, Wilmington, North Market Street, 950	https://xsignal.io/
2.	**A,B,C,D, E**	**A**	Metascan • Serviciu	Krasnohorsk Street, Egorova 5 Moscow, Russia TIN 5024179758 KPP 502401001 PSRN 1175024028772	https://metascan.ru/
3.	**A,B,C,D, E**	**B**	Dr. Web • Dr.Web Control Center • Dr.Web Desktop Security Suite • Dr.Web Server Security Suite • Dr.Web Mail Security Suite • Dr.Web Gateway Security Suite • Dr.Web Mobile Security Suite • Dr.Web KATANA • Dr.Web Security Space (for Windows) • Dr.Web Security Space (for Linux) • Dr.Web Security Space (for macOS) • Dr.Web Security Space (for MS-DOS, OS/2) • Dr.Web Security Space (for Android)	Global HQ, 125124, 3rd street Yamskogo polya 2-12A, Moscow Russia	https://www.drweb.com/
4.	**A,B,C,D, E**	**A, B, C, D, E**	Kaspersky Security • Kaspersky Anti-Virus • Kaspersky Internet Security	Leningradskoye Hwy, 39A строение 2, Moskva, Rusia, 125212	https://www.kaspersky.com/about/team

	Categorie cf. art. 1 alin. (3) L nr. 354/2022	Categorie cf. Art.2 alin. (1) L nr.354/2022	Denumirea persoanei juridice și/sau a produselor și serviciilor software	Elemente de identificare	URL / site
			• Kaspersky Total Security • Kaspersky Security Cloud Personal • Kaspersky VPN Secure Connection • Kaspersky Password Manager • Kaspersky Safe Kids • Kaspersky Internet Security for Mac • Kaspersky Internet Security for Android • Kaspersky Virus Removal Tool • Kaspersky Rescue Disk		
5.	**A,B,C,D, E**	**A**	RPA RusBITech JSC RusBITech Astra • ПТК Каркас-С - PTK Karkas-S • КП СГП Комплекс программ «Специальный генератор паролей» - KP SGP Complex de programe „Generator de parole speciale”	117105, Moscow, Varshavskoye shosse, 26, building 11	https://rusbitech.ru/
6.	**A,B,C,D, E**	**A, B, C, D, E**	Infotecs • ViPNet Coordinator HW • ViPNet xFirewall • ViPNet EndPoint Protection • ViPNet Coordinator IG • ViPNet SIES • ViPNet OSSL • ViPNet TIAS • ViPNet Client for mobile platforms • ViPNet Client for workstations • ViPNet Coordinator IG • ViPNet Coordinator HW • ViPNet Coordinator KB • ViPNet Coordinator VA • ViPNet CSP 4	127273, Moscow, st . Otradnaya, 2B str. 1	https://infotecs.ru/

	Categorie cf. art. 1 alin. (3) L nr. 354/2022	Categorie cf. Art.2 alin. (1) L nr.354/2022	Denumirea persoanei juridice și/sau a produselor și serviciilor software	Elemente de identificare	URL / site
			• ViPNet EndPoint Protection • ViPNet IDS HS • ViPNet IDS MC (Management Center) • ViPNet IDS NS • ViPNet Password Generator • ViPNet Personal Firewall 4 • ViPNet PKI Client • ViPNet PKI Service • ViPNet Policy Manager • ViPNet Quantum Trusted System (ViPNet QTS) • ViPNet QTS Lite • ViPNet Quandor 2 • ViPNet SafeBoot • ViPNet SafePoint • ViPNet SIES • ViPNet Statewatcher • ViPNet Terminal • ViPNet TIAS ViPNet TLS Gateway		
7.	**A,B,C,D, E**	**a,b,c, d, e,**	Era Technopolis	Adresa sediului principal: Federația Rusă, Krasnodar, Bulevardul Pionerskiy, 41	https://mil.ru/era.htm
8.	**A,B,C,D, E**	**a,b,c, d, e,**	Pasit Ao	Adresa sediului principal: Federația Rusă, Moscova, Bulevardul Lenin, 30	https://pasit.ru/
9.	**A,B,C,D, E**	**a,b,c, d, e,**	Neobit, 000	Adresa sediului principal: Federația Rusă, Saint Petersburg, strada Gzhatskaya, 21	https://neobit.ru/
10.	**A,B,C,D, E**	**a,b,c, d, e,**	Advanced System Technology, Ao	Adresa sediului principal: Federația Rusă, Moscova, Autostrada Kashirskoye, 3k2	https://acti.ru/
11.	**A,B,C,D, E**	**a,b,c, d, e,**	Positive Technologies, Ao	Adresa sediului principal: Federația Rusă, Moscova, Autostrada Shchelkovskoe, 30	https://www.ptsecurity.com/

Legendă:

1. **Pentru Coloana ”Categorie cf. art. 1 alin. (3) L nr. 354/2022”, literele au următoarele semnificații:**

A. **una sau mai multe persoane fizice sau juridice din Federația Rusă dețin, individual sau împreună, în mod direct sau indirect, o participație calificată de cel puțin 25% din drepturile de vot ale respectivului operator;**

B. **una sau mai multe persoane fizice sau juridice din Federația Rusă dețin, în mod direct sau indirect, majoritatea drepturilor de vot în adunarea generală a operatorului respectiv;**

C. **în calitate de asociat sau acționar al respectivului operator, o persoană fizică sau juridică din Federația Rusă dispune de puterea de a numi sau de a revoca majoritatea membrilor organelor de administrație, conducere sau supraveghere;**

D. **una sau mai multe persoane fizice sau juridice din Federația Rusă îl finanțează, prin orice mod, direct sau indirect, pe operator;**

E. **una sau mai multe persoane fizice sau juridice din Federația Rusă promite, oferă sau dă bani sau alte foloase operatorului.**

2. **Pentru Coloana ”Categorie cf. Art.2 alin. (1) L nr.354/2022”, literele au următoarele semnificații:**

a) **Produse privind securitatea dispozitivului, securitatea punctului final / device security, endpoint security products;**

b) **Aplicații și programe software de detecție antivirus / antivirus software;**

c) **Aplicații și programe software antimalware, firewall pentru aplicații web, firewall as a service / antimalware software applications, web application firewall (WAD), firewall as a service;**

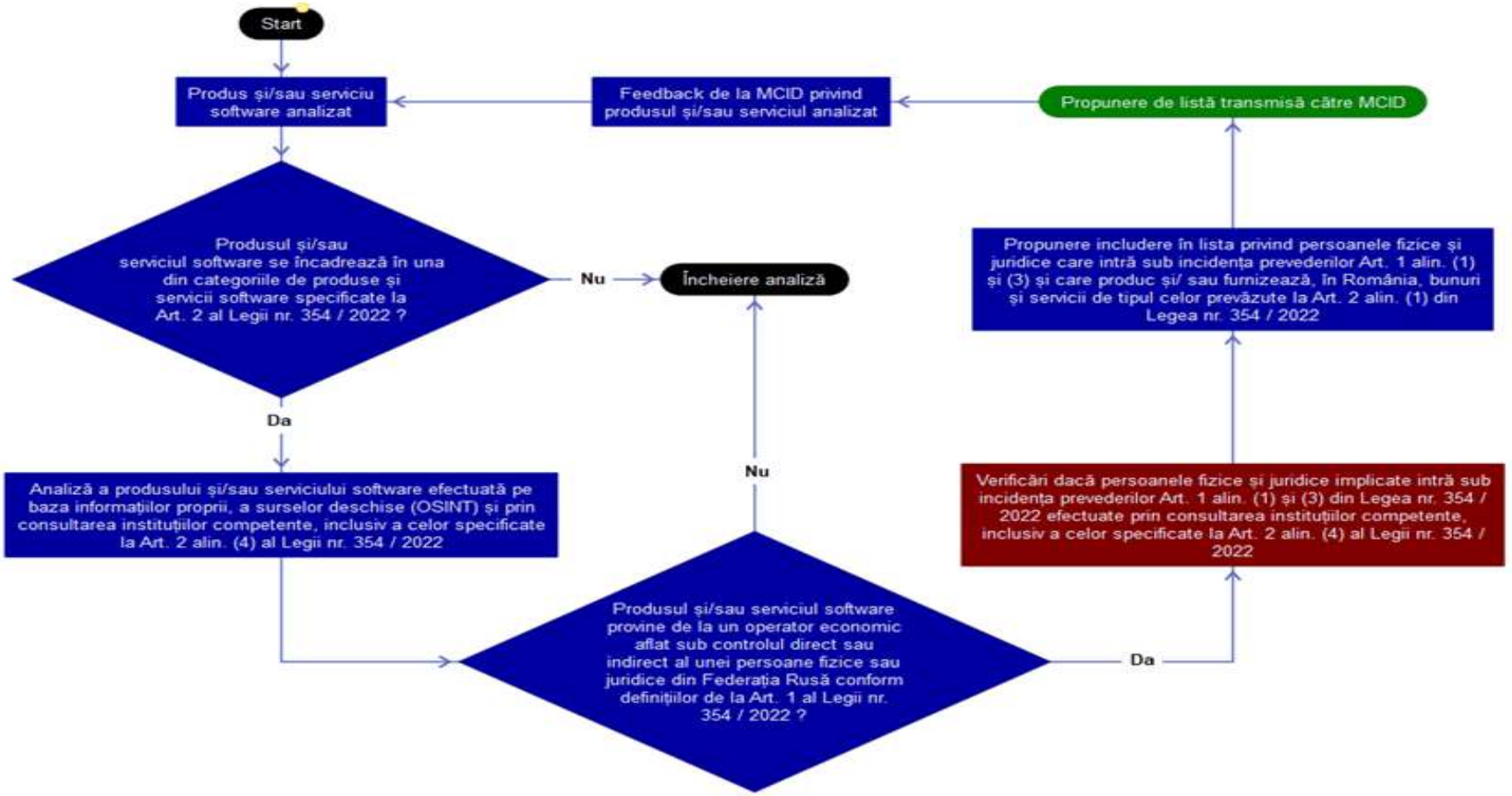
d) **Rețele virtuale private / virtual private networks (VPN);**

e) **Sisteme de detecție și răspuns pentru endpointuri / endpoint detection and response systems (EDR).**

MINISTERUL CERCETĂRII, INOVĂRII ȘI DIGITALIZĂRII

Anexa 3

Procedura metodologică privind întocmirea listei de produse și servicii software care îndeplinesc criteriile prevăzute la art. 1 și art. 2 din Legea nr. 354/2022



MINISTERUL CERCETĂRII, INOVĂRII ȘI DIGITALIZĂRII

REFERAT DE APROBARE

În contextul războiului de agresiune asupra Ucrainei, tot mai multe state membre ale Uniunii Europene au emis recomandări sau acte normative cu caracter imperativ prin care au impus propriilor lor autorități și instituții publice să schimbe soluțiile antivirus dacă le folosesc pe cele de la Kaspersky Lab, deoarece există riscul ca Rusia să exploateze aceste soft-uri într-un atac cibernetic.

Spre exemplu, Autoritatea germană BSI (Federal Office for Information Security) avertizează că riscul poate fi mai mare pentru companiile din domeniul infrastructurilor esențiale. BSI susține că ar fi bine ca toate companiile germane care folosesc soluții AV sau alte tipuri de softuri de la Kaspersky să renunțe la ele și să folosească programe de la alte companii. BSI explică faptul că soluțiile antivirus mențin o legătură permanentă, criptată și imposibil de verificat cu serverele vendorului, pentru o actualizare permanentă a definițiilor virușilor. Teama este că fișiere sensibile ar putea fi extrase de pe computerele care folosesc soluțiile companiei, pentru a fi trimise pe serverele Kaspersky și ale altor companii rusești[1].

În Italia, Franco Gabrielli, secretar de stat la preşedinţia Consiliului de miniştri, a declarat în Senat că Guvernul de la Roma lucrează la un set de reguli care ar permite entităţilor de stat să înlăture programele software dezvoltate de firma rusă Kaspersky[2]. Între timp, reglementările au fost adoptate astfel cum sunt descrise la secțiunea 5, pct. VI din prezenta expunere.

Potrivit unor informații publice apărute în presă[3], Primăria municipiului București a organizat o licitație pentru achiziționarea unui antivirus Kaspersky Endpoint Security For Business-Select pentru 1.200 de echipamente, cu mentenanță inclusă 12 luni. Biroul de Presă al instituției primarului general a transmis că Primăria Capitalei folosește antivirusul Kaspersky din anul 2012.

[1]Disponibil la:https://economie.hotnews.ro/stiri-it-25436103-germania-avertizeaza-software-kaspersky-lab-putea-exploatat-federatia-rusa-recomanda-companiilor-renunte.htm; accesat la data de 10.01.2023.

[2]Disponibil la: https://spotmedia.ro/stiri/it/italia-va-limita-utilizarea-antivirusului-kaspersky-in-sectorul-public-de-teama-ca-rusia-l-ar-folosi-pentru-atacuri-cibernetice; accesat la data de 10.01.2023.

[3]Disponibil la: https://stiripesurse.directorylib.com/primaria-capitalei-vrea-antivirus-rusesc-declarat-amenintare-de-securitate-988775.html; accesat la 10.01.2023.

Foarte multe instituții publice și autorități ale administrației publice locale achiziționează programe software de antivirus rusești din cauza prețurilor mici și care au prevalență prin Sistemul informatic colaborativ pentru mediu performant de desfășurare al achizițiilor publice (SICAP).

Prezența software-urilor rusești de tip antivirus reprezintă o vulnerabilitate la adresa securității cibernetice a autorităților și instituțiilor românești, din cauză că aceste programe acaparează funcții importante ale rețelelor și sistemelor informatice, creând relații de interdependență. În contextul în care Federația Rusă utilizează inclusiv atacuri de tip cibernetic la adresa statelor occidentale și își folosește companiile naționale și cetățenii ruși, prin diverse metode, în războiul asupra Ucrainei, încălcând toate normele de drept internațional în materie, România nu poate să-și asume prezența unor produse și servicii IT rusești în infrastructura cibernetică națională.

Potrivit **Hotărârii Parlamentului României nr. nr. 22 din 30 iunie 2020 privind aprobarea Strategiei Naționale de Apărare a Țării pentru perioada 2020-2024**, **obiectivele naționale de securitate vizează și ”***asigurarea securității și protecției infrastructurilor de comunicații și tehnologia informațiilor cu valențe critice pentru securitatea națională, precum și cunoașterea, prevenirea și contracararea amenințărilor cibernetice derulate asupra acestora de către actori cu motivație strategică, de ideologie extremist-teroristă sau financiară. Redimensionarea și reconstrucția sistemului de comunicații, la nivel național, conform cerințelor de calitate internaționale, astfel încât zonele de eșec ale pieței (acolo unde operatorii consideră că nu este oportun să investească) să fie compensate prin infrastructuri de comunicații finanțate din fonduri publice*”.

În aceeași strategie, la **pct. 161**, se reliefează ca **vulnerabilitate** ”*nivelul redus de securitate cibernetică a infrastructurilor de comunicații și tehnologia informației din domenii strategice (inclusiv ca efect al vulnerabilităților tehnologice și procedurale ale infrastructurilor deținute de operatorii de comunicații) facilitează derularea de atacuri cibernetice de către actori statali sau non-statali*”.

Din perspectiva **dimensiunii de informații, contrainformații și de securitate**, la pct. 179, Strategia își propune următoarele obiective:

”– ***Prevenirea și contracararea amenințărilor cibernetice*** *- derulate de entități ostile, statale și nonstatale - asupra infrastructurilor de comunicații și tehnologia informației cu valențe critice pentru securitatea națională;*

Creșterea capacității instituțiilor publice*, companiilor private și a organizațiilor neguvernamentale* ***de a implementa norme de securitate cibernetică*** *și de a-și forma personalul în vederea protecției datelor cu caracter personal, a datelor privind activitatea și rezultatele cercetării științifice și a altor date ce nu sunt de interes public;*

– Prevenirea și contracararea amenințărilor hibride, *concretizate în acțiuni conjugate ostile, derulate de actori statali sau nonstatali, în plan politico-administrativ, economic, militar, social, informațional,* ***cibernetic*** *sau al crimei organizate.*"

În **Hotărârea Guvernului României nr. 1.321 din 30 decembrie 2021** privind aprobarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027, precum și a Planului de acțiune pentru implementarea Strategiei de securitate cibernetică a României, pentru perioada 2022-2027 se prevede, printre cele 5 obiective strategice, acela de a avea "*Rețele și sisteme informatice sigure și reziliente*".

Strategia prezintă o sinteză a tipurilor de atacuri cibernetice care au guvernat aparatul de stat în ultima perioadă, astfel:

„Atacurile cibernetice derulate de actori statali sunt de regulă de tip Advanced Persistent Threat (APT). Au un nivel tehnologic ridicat, atât în ceea ce privește modul de operare, cât și din punct de vedere al aplicațiilor malware folosite, actualizate permanent în vederea eludării mecanismelor de detecție și menținerii persistenței pentru o perioadă îndelungată de timp. Instrumentarul cibernetic folosit de atacatori este divers, adaptat scopurilor operaționale ale acestora.

Peisajul autohton a fost dominat în ultimii ani de atacuri cibernetice cu aplicații malware de tip ransomware, infostealer sau cryptojacking, care au vizat rețele și sisteme informatice aparținând unor autorități și instituții ale administrației publice sau entități private. De asemenea, se remarcă intensificarea atacurilor cibernetice din ce în ce mai complexe, inclusiv de tip APT, dedicate exploatării sistemelor informatice din domeniul financiar-bancar."

Cu privire la obiectiv strategic de "*Rețele și sisteme informatice sigure și reziliente*" acesta prevede o serie de măsuri, astfel:

"*Pentru România este prioritară securitatea cibernetică a rețelelor și sistemelor informatice, îndeosebi a celor din domenii aferente serviciilor esențiale, precum și a celor cu valențe critice pentru securitatea națională. Menținerea în parametri optimi a disponibilității, continuității și integrității și asigurarea rezilienței acestora contribuie la susținerea în condiții optime a tuturor domeniilor vieții economice și sociale.*

Autoritățile și instituțiile administrației publice și entitățile private trebuie să implementeze și să opereționalizeze politici de securitate cibernetică adecvate. Acest deziderat presupune *inclusiv realizarea de investiții în domeniul tehnologic și alocarea de resursă umană cu pregătire de specialitate. Totodată este necesară impunerea și respectarea unui set de standarde calitative pentru produsele și serviciile utilizate în cadrul acestor rețele și sisteme.*

Măsuri:

4.1.1. Implementarea de politici și măsuri de securitate cibernetică

Pentru a putea avea rețele și sisteme informatice sigure este dezirabilă crearea și implementarea corectă, de către întregul personal al unei entități, a unui set minim de politici și măsuri de securitate cibernetică. Acestea trebuie să fie adaptabile, permanent corelate cu nivelul amenințării cibernetice și cu trendul rapid de dezvoltare al tehnologiilor.

De asemenea, aceste politici trebuie să fie însoțite de implementarea unor planuri de recuperare în caz de atac cibernetic și de măsuri tehnice și organizaționale, menite să contribuie la creșterea atât a capacității de reacție la atacuri și incidente de securitate cibernetică, cât și a rezilienței infrastructurilor.

În plus, este necesar ca fiecare operator de rețele și sisteme cu impact la adresa securității naționale, inclusiv cei desemnați prin legislația de transpunere a Directivelor NIS, să elaboreze proceduri de testare și auditare periodică a nivelului de securitate cibernetică, ca parte integrantă a procesului de evaluare a riscurilor, și să actualizeze permanent tehnologiile hardware și software folosite în cadrul infrastructurilor.

În același timp, autoritățile și instituțiile administrației publice cu responsabilități în asigurarea securității cibernetice trebuie să încurajeze și să susțină implementarea de politici și măsuri de securitate cibernetică prin crearea unui cadru de lucru unitar, oferirea pregătirii necesare și coagularea unei comunități de experți în domeniu.

4.1.2. Dezvoltarea capabilităților naționale de detectare, investigare și contracarare a atacurilor cibernetice

Pentru a avea rețele și sisteme informatice sigure și reziliente este necesară dezvoltarea și adaptarea permanentă a capabilităților de detecție și investigare. Acest lucru trebuie să fie făcut în concordanță atât cu evoluțiile tehnologice, cât și cu schimbările mediului de securitate *cibernetică, printr-o cooperare între autorități și instituții ale administrației publice și entități private.*

Cunoașterea obținută ca urmare a investigațiilor derulate reprezintă un element important în contracararea și, ulterior, în atribuirea atacurilor cibernetice.

4.1.3. Alocarea eficientă a resurselor financiare, tehnologice și umane

Având în vedere diversitatea domeniilor în care se regăsesc rețele și sisteme informatice și interconectarea dintre acestea, este importantă promovarea și conștientizarea în rândul operatorilor, autorități și instituții ale administrației publice sau entități private, a necesității realizării de investiții în tehnologii.

Aceste investiții trebuie să fie susținute prin demersuri de specializare a personalului din domeniu, care să fie pregătit pentru a:

- *înțelege amenințarea provenită din spațiul cibernetic;*
- *cunoaște evoluțiile din domeniul tehnologic;*
- *dobândi cunoștințele necesare pentru o reacție adecvată în cazul unui atac cibernetic sau a unui incident de securitate cibernetică.*

O cooperare permanentă între autoritățile și instituțiile administrației publice cu responsabilități în domeniul securității cibernetice, precum și între acestea și mediul de afaceri și industrie este dezirabilă în sensul partajării cunoașterii, de exemplu prin elaborarea de ghiduri de bune practici, recomandări pe domenii de activitate, identificării celor mai bune soluții de asigurare a protecției rețelelor și sistemelor informatice, precum și alocării eficiente și complementare a resurselor.

4.1.4. Consolidarea mecanismului de raportare a incidentelor de securitate cibernetică

Un sistem de management centralizat al incidentelor de securitate cibernetică oferă imaginea de ansamblu asupra amenințării cibernetice la adresa unei infrastructuri, a unui domeniu de activitate și chiar a securității naționale. Totodată, un mecanism de raportare eficient contribuie la asigurarea unui răspuns concret la amenințările provenite din spațiul cibernetic. Este necesară elaborarea unui set de măsuri și mecanisme de raportare a incidentelor, îndeosebi la nivelul entităților care operează rețele și sisteme informatice din domenii aferente serviciilor esențiale sau cu valențe critice pentru securitatea națională. Operatorii trebuie să înțeleagă și să își asume rolul de facto și atribuțiile care le revin și să optimizeze fluxul subsumat mecanismului de raportare a incidentelor de securitate cibernetică, în conformitate cu recomandările și reglementările UE și cu legislația națională.

4.1.5. Crearea unor mecanisme de certificare, conformitate și standardizare în domeniul securității cibernetice

Calitatea și nivelul de securitate cibernetică al produselor hardware și software folosite sunt deosebit de importante pentru menținerea unor rețele și sisteme informatice sigure și reziliente în fața amenințărilor cibernetice și trebuie să prevaleze aspectelor restrictive de ordin bugetar. în acest sens, este necesară crearea unor mecanisme la nivel național de certificare, conformitate și standardizare în domeniul securității cibernetice, care să aibă în vedere un set strict de criterii (tehnice, non-tehnice, inclusiv prin raportare la aspecte ce țin de securitate națională) și care să permită identificarea riscurilor și vulnerabilităților de securitate cibernetică existente la nivelul produselor hardware și software.

De asemenea, este necesară crearea cadrului normativ și a mecanismelor necesare astfel încât în cadrul programelor și proiectelor să fie respectat principiul "securizare din etapa de proiectare", având în vedere că, produsele și capabilitățile sunt proiectate pentru a corespunde standardelor din domeniul securității cibernetice

4.1.6. Securizarea lanțului de aprovizionare

Trebuie menținută în atenție securizarea lanțului de aprovizionare, prin impunerea implementării unor mecanisme de securitate cibernetică la toate componentele acestui ecosistem. Este necesară definirea criteriilor de încredere pentru furnizorii de echipamente hardware, software și servicii, în special pentru sistemele ce țin de securitatea națională."

Având în vedere agresiunea armată a Federației Ruse împotriva Ucrainei, la nivelul statului român s-a constatat o multiplicare a atacurilor cibernetice, dar și a altor operațiuni clandestine efectuate în spațiul cibernetic și având proveniență în Federația Rusă. Conform datelor și informațiilor obținute de la autoritățile naționale în domeniul securității naționale există suspiciuni că Federația Rusă utilizează produse și servicii de tip antivirus cu proveniență din Federația Rusă pentru a intra neautorizat în sisteme informatice, în scopul furtului, alterării sau supravegherii neautorizate de date și informații. Prin intermediul acestui sistem există indicii că actori statali și nonstatali apropiați Federației Ruse sunt apți să efectueze activități de spionaj cibernetic asupra rețelelor și sistemelor informatice ale autorităților și instituțiilor publice din România. Astfel, interzicerea unor produse și servicii software de tip antivirus, cu proveniență din Federația Rusă sau având legături cu Federația Rusă, reprezintă o măsură necesară și proporțională prevenirii și combaterii amenințărilor la adresa securității naționale a României.

Prezentul proiect de ordin prevede, potrivit art. 2 alin. (2) din Legea nr. 354/2021, următoarele:

- criteriile de stabilire a produselor şi serviciilor software de tip antivirus provenind direct sau indirect din Federaţia Rusă sau de la un operator economic aflat sub controlul direct sau indirect al unei persoane fizice sau juridice din Federaţia Rusă sau al cărei capital este constituit cu participaţie provenind în mod direct sau prin firme interpuse din Federaţia Rusă ori din ale cărui organe de administrare fac parte persoane din Federaţia Rusă;
- lista nominală privind produsele, serviciile şi entităţile producătoare şi/sau furnizoare interzise în temeiul Legii nr. 354/2022 privind protecţia sistemelor informatice ale autorităţilor şi instituţiilor publice în contextul invaziei declanşate de Federaţia Rusă împotriva Ucrainei;
- procedura metodologică privind întocmirea listei de produse și servicii software care îndeplinesc criteriile prevăzute la art. 1 și art. 2 din Legea nr. 354/2022.

Datele și informațiile care au stat la baza elaborării listei nominale privind produsele, serviciile şi entităţile producătoare şi/sau furnizoare interzise au fost colectate de la autoritățile și instituțiile publice prevăzute la art. 2, alin. (3) și (4) din Legea nr. 354/2022. Autoritățile și instituțiile cu atribuții în domeniul securității naționale au desfășurat activități specifice culegerii de informații și au analizat riscurile, vulnerabilitățile și amenințările la adresa securității naționale a României în acord cu prevederile Legii nr. 51/1991 și ale legilor de organizare și funcționare ale acestora, rezultatul activității concretizându-se în propunerile formulate către Ministerul Cercetării, Inovării și Digitalizării, în vederea emiterii ordinului.

Având în vedere necesitatea prevenirii şi contracarării ameninţărilor cibernetice derulate de Federația Rusă, precum și de actori statali şi nonstatali aflați sub controlul Federației Ruse asupra infrastructurilor de comunicaţii şi tehnologia informaţiei cu valenţe critice pentru securitatea naţională, MCID a prelucrat și interpretat cu celeritate datele și informațiile obținute, a consultat autoritățile cu atribuții în domeniul ordinii publice, apărării naționale și securității naționale și a elaborat prezentul proiect de ordin.

Ministerul Cercetării, Inovării și Digitalizării este organ de specialitate al administrației publice centrale, cu rol de elaborare și implementare, la nivel național, a politicii, strategiei și reglementărilor specifice de dezvoltare și de armonizare ale activităților în cadrul politicii generale a Guvernului, precum și a faptului că îndeplinește rolul de autoritate de stat în domeniul securității cibernetice, conform prevederilor art. 1 alin. (3) și art. 4 alin. (1) din

Hotărârea Guvernului nr. 371/2021 privind organizarea şi funcţionarea Ministerului Cercetării, Inovării şi Digitalizării, cu modificările şi completările ulterioare;

Prezentul proiect de ordin a fost elaborat în conformitate cu prevederile art. 2 alin. (2) din Legea nr. 354/2022 privind protecţia sistemelor informatice ale autorităţilor şi instituţiilor publice în contextul invaziei declanşate de Federaţia Rusă împotriva Ucrainei, publicat în Monitorul Oficial, Partea I nr. 1200 din 14 decembrie 2022;

Având în vedere caracterul normativ al proiectului de act administrativ, precum și urgența reglementării generată de amplificarea atacurilor cibernetice la adresa autorităților și instituțiilor publice și de numărul mare de softuri de tip antivirus rusești încărcate pe sistemele informatice ale autorităților publice, în temeiul art. 7 alin. (13) din Legea nr. 52/2003, propunem ca supunerea spre cunoștință publică a anunțului referitor la intenția de adoptare a proiectului de act normativ să fie făcută pe o perioadă de 10 zile lucrătoare.

În temeiul art. 12 alin. (3) din Hotărârea Guvernului nr. 371/2021 privind organizarea şi funcţionarea Ministerului Cercetării, Inovării şi Digitalizării, cu modificările şi completările ulterioare, propunem aprobarea prezentului referat și emiterea prezentului proiect de ordin.