



ORDIN

privind procedura, metodele și instrumentele încetării utilizării produselor și serviciilor provenind direct sau indirect din Federația Rusă sau de la un operator economic aflat sub controlul direct sau indirect al unei persoane fizice sau juridice din Federația Rusă sau al cărei capital este constituit cu participație provenind în mod direct sau prin firme interpuse din Federația Rusă ori din ale cărui organe de administrare fac parte persoane din Federația Rusă

Având în vedere necesitatea prevenirii și contracarării amenințărilor cibernetice derulate de Federația Rusă, precum și de actori statali și nonstatali aflați sub controlul Federației Ruse asupra infrastructurilor de comunicații și tehnologia informației cu valențe critice pentru securitatea națională;

Având în vedere faptul că autoritățile și instituțiile publice trebuie să beneficieze de proceduri unitare, clare, previzibile, transparente și calitative privind deconectarea, respectiv dezinstalarea produselor și serviciilor provenind direct sau indirect din Federația Rusă sau de la un operator economic aflat sub controlul direct sau indirect al unei persoane fizice sau juridice din Federația Rusă sau al cărei capital este constituit cu participație provenind în mod direct sau prin firme interpuse din Federația Rusă ori din ale cărui organe de administrare fac parte persoane din Federația Rusă;

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 prevederile art. 1 alin. (3) și art. 4 alin. (1) din Hotărârea Guvernului nr. 371/2021 privind organizarea și funcționarea Ministerului Cercetării, Inovării și Digitalizării, cu modificările și completările ulterioare;

În vederea aplicării prevederile art. 5 alin. (1) din Legea nr. 354/2022 privind protecția sistemelor informatice ale autorităților și instituțiilor publice în contextul invaziei declanșate de Federația 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 și funcționarea Ministerului Cercetării, Inovării și Digitalizării, cu modificările și completările ulterioare;

ministrul cercetării, inovării și digitalizării emite prezentul ordin:



Art. 1. -

- (1) Se aprobă procedura, metodele și instrumentele încetării utilizării produselor și serviciilor provenind direct sau indirect din Federația Rusă sau de la un operator economic aflat sub controlul direct sau indirect al unei persoane fizice sau juridice din Federația Rusă sau al cărei capital este constituit cu participație provenind în mod direct sau prin firme interpuse din Federația Rusă ori din ale cărui organe de administrare fac parte persoane din Federația Rusă prevăzute în Anexa 1 care face parte integrantă din prezentul ordin.
- (2) Se aprobă chestionarul privind produsele și serviciile software care îndeplinesc criteriile Legii nr. 354 / 2022 prevăzută în Anexa 2 care face parte integrantă din prezentul ordin.

Art. 2. -

- (1) Prezentul ordin se aplică tuturor autorităților și instituțiilor publice de la nivel central și local, precum și persoanele fizice și juridice care dețin rețele și sisteme informatice prin care se gestionează informații clasificate.
- (2) Prezentul ordin nu este obligatoriu pentru autoritățile și instituțiile publice cu atribuții proprii în domeniul securității naționale, în domeniul securității cibernetice, apărării naționale și ordinii publice, cu excepția situației în care conducătorul autorității sau instituției respective decide aplicarea lui.

Art. 3. -

Direcțiile de specialitate din cadrul Ministerului Cercetării, Inovării și Digitalizării împreună cu autoritățile și instituțiile prevăzute la art. 2 alin. (3) și (4) din Legea nr. 354/2022 privind protecția sistemelor informatice ale autorităților și instituțiilor publice în contextul invaziei declanșate de Federația Rusă împotriva Ucrainei, duc la îndeplinire prezentul ordin.

Art. 4. -

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

**MINISTRU
SEBASTIAN-IOAN BURDUJA**

București

Nr:

Data:



Anexa 1 la Ordinul nr.

Procedura, metodele și instrumentele încetării utilizării produselor și serviciilor provenind direct sau indirect din Federația Rusă sau de la un operator economic aflat sub controlul direct sau indirect al unei persoane fizice sau juridice din Federația Rusă sau al cărui capital este constituit cu participație provenind în mod direct sau prin firme interpuse din Federația Rusă ori din ale cărui organe de administrare fac parte persoane din Federația Rusă

Art. 1.

- (1) Prezenta procedură se aplică tuturor autorităților și instituțiile publice de la nivel central și local, precum și persoanele fizice și juridice care dețin rețele și sisteme informatice prin care se gestionează informații clasificate, denumite în continuare entități.
- (2) Prezenta procedura nu este obligatorie autorităților și instituțiilor publice cu atribuții proprii în domeniul securității naționale, în domeniul securității cibernetice, apărării naționale și ordinii publice, cu excepția situației în care conducătorul autorității sau instituției respective decide altfel.
- (3) În vederea aplicării prezentei proceduri, autoritățile și instituțiile publice prevăzute la alin. (2) au în vedere să nu le fie afectate următoarele:
 - a) activitatea de cercetare-dezvoltare și inovare;
 - b) activitatea de informații și contrainformații;
 - c) misiunile operative și tactice;
 - d) personalul, metodele, mijloace sau procedurile specifice exercitării atribuțiilor;
 - e) respectarea regimului juridic al informațiilor clasificate;
 - f) crearea unei amenințări, vulnerabilități sau risc la adresa securității naționale a României.



Art. 2.

- (1) Entitățile analizează și constată dacă produsele și serviciile software aflate în proprietatea, administrarea sau folosința acestora sunt de tipul celor prevăzute la art. 2 alin. (1) din Lege și dacă acestea provin de la persoanele prevăzute la art. 1 alin. (1) și (3) din Lege.
- (2) Entitățile stabilesc necesitățile de înlocuire a produselor și serviciilor software de tipul celor prevăzute la art. 2 alin. 1 din Legea nr. 354/2022 și pe care le au în proprietate, administrare sau folosință.

Art. 3.

Entitățile constată încetarea contractelor încheiate cu operatorii economici, produsele și serviciile software interzise de Lege și îi notifică pe aceștia în condițiile prevăzute de Legea nr. 287/2009 privind Codul civil, cu modificările și completările ulterioare.

Art. 4.

- (1) Entitățile își elaborează o procedură internă de încetare a utilizării, respectiv de deconectare/ deinstalare a produselor și serviciilor software interzise de Lege și o pun în aplicare în termen de 60 de zile de la intrarea în vigoare a prezentului ordin.
- (2) Entitățile elaborează un plan propriu de înlocuire a produselor și serviciilor software interzise de Lege cu unele legale și compatibile din punct de vedere tehnic și operațional, în acord cu necesitățile fiecărei entități.
- (3) În vederea implementării prevederilor alin. (2), entitățile sunt obligate să respecte cumulativ cel puțin următoarele obligații:
 - a) perioada de tranziție între produsele și serviciile software interzise și cele legale și compatibile să fie cât mai scurtă posibil, astfel încât să nu se compromită buna funcționare a rețelelor și sistemelor informatice;
 - b) produsele și serviciile software achiziționate să fie instalate în mediul de test, înainte de deinstalarea/decuplarea celor interzise de Lege;
 - c) să se asigure prevenirea și combaterea atacurilor cibernetice pe perioada de tranziție, luând în calcul toate posibilitățile disponibile în piață;

Art. 5.

Instalarea produselor și serviciilor software legale și compatibile se realizează cu respectarea următorilor pași tehnici:

1. Se copiază local, pe sistemul informatic, fișierele necesare pentru instalarea produsului antivirus substituent, în funcție de tipul sistemului de operare. Fișierele de instalare se vor descărca de pe pagina oficială a producătorului, împreună cu manualul de instalare și utilizare a produsului.
2. Se izolează sistemul informatic de la orice sursă de Internet (atât conexiune fizică, prin cablu, cât și wireless), inclusiv de la rețeaua internă/locală din care face parte sistemul



informatic pentru a nu interacționa cu alte dispozitive în timpul procesului de deinstalare/instalare a produsului antivirus.

3. Pe toată durata activității de deinstalare și instalare a produsului antivirus nu se vor efectua alte operațiuni la nivelul sistemului informatic, precum conectarea altor dispozitive de stocare, instalarea altor programe, deschiderea fișierelor stocate pe sistem sau instalarea și pornirea altor aplicații.
4. Se urmează procedura standard de deinstalare a antivirusului existent la nivelul sistemului informatic, în funcție de sistemul de operare și tipul produsului antivirus.
5. La finalizarea procesului de deinstalare, se repornește sistemul informatic.
6. După repornire, se instalează produsul antivirus substituent conform pașilor recomandați de către producător și se va efectua o primă scanare rapidă a sistemului informatic pentru validarea funcționării corespunzătoare a noului antivirus și pentru identificarea posibilelor fișiere infectate la nivelul sistemului.
7. În cazul în care nu sunt detectate fișiere infectate, se continuă procesul cu pasul 9.
8. În situația în care au fost identificate fișiere suspecte sau infectate, acestea se transmit personalului specializat pentru analiză suplimentară. Până la stabilirea unui verdict, sistemul informatic nu va fi reconectat la rețeaua din care face parte și nu se va continua procesul. În funcție de tipul de malware și capacitățile acestuia, se procedează la ștergerea fișierelor infectate sau după caz, la reinstalarea sistemului de operare, și se revine la pasul 6.
9. Se reconectează sistemul informatic la rețeaua din care face parte sau la o sursă cu conexiune la Internet, protejată, de preferat, cel puțin cu o soluție de tip firewall.
10. Se actualizează semnăturile din baza de date a produsului antivirus și se scanează complet sistemul informatic pentru detecția eventualelor fișiere infectate.

Art. 6.

(1) În termen de 30 de zile de la data intrării în vigoare a prezentului ordin, entitățile demarează procedura de achiziție a produselor și serviciilor software compatibile și legale, cu respectarea legislației privind achizițiile publice, pentru asigurarea continuității activității, cu încadrarea în bugetul autorităților și instituțiilor publice.

(2) Documentația de atribuire trebuie să cuprindă elemente suficiente și necesare care să excludă posibilitatea achiziționării produselor și serviciilor software interzise de Lege.

(3) În cadrul documentației de atribuire pentru achiziția de produse și servicii de tipul celor prevăzute la art. 2 alin. (1) din Lege, entitățile sunt obligate să prevadă excluderea de la procedura de achiziție a persoanelor prevăzute de art. 1 alin. (1) și (3) din Lege, respectiv:

- a) operatorilor economici aflați sub controlul direct sau indirect al unei persoane fizice sau juridice din Federația Rusă;
- b) operatorilor al căror capital este constituit cu participație provenind în mod direct sau prin firme interpușe din Federația Rusă;
- c) operatorilor economici din ale căror cărui organe de administrare fac parte persoane din Federația Rusă.



Art. 7.

(1) Entitățile care identifică că au în proprietate, administrare sau folosință produse și servicii interzise de Lege comunică Ministerului Cercetării, Inovării și Digitalizării, Autorității pentru Digitalizarea României și Directoratului Național de Securitate Cibernetică cel puțin următoarele:

- a) tipul de produs sau serviciu software interzis de Lege și aflat în proprietate, administrare sau folosință;
- b) operatorul economic de la care a achiziționat produsul sau serviciul software;
- c) operatorul economic care a fabricat produsul sau serviciul software;
- d) data efectivă a dezinstalării/deconectării produselor și serviciilor software interzise prin Lege;
- e) procedura internă prevăzută la art. 4 alin. (1);
- f) planul de înlocuire prevăzut la art. 4 alin. (2);
- g) solicitare expresă, dacă este cazul, pentru suport tehnic în ceea ce privește asigurarea securității cibernetice a rețelelor și sistemelor informatice conectate cu produsele și serviciile software interzise de Lege;

(2) Notificarea prevăzută la alin. (1) se transmite prin completarea unui formular online administrat de ADR prin Sistemul informatic colaborativ pentru mediu performant de desfășurare a achizițiilor publice, denumit SICAP, având drept conținut întrebările prevăzute în Anexa 2.



Chestionar privind produse și servicii software care îndeplinesc criteriile Legii nr. 354 / 2022

Legea nr. 354/2022 privind protecția sistemelor informatice ale autorităților și instituțiilor publice în contextul invaziei declanșate de Federația Rusă împotriva Ucrainei stabilește cadrul juridic și instituțional general și necesar în vederea interzicerii achiziționării și utilizării de către autoritățile și instituțiile publice, de la nivel central și local, a produselor și serviciilor software de tip antivirus provenind direct sau indirect din Federația Rusă sau de la un operator economic aflat sub controlul direct sau indirect al unei persoane fizice sau juridice din Federația Rusă sau al cărei capital este constituit cu participație provenind în mod direct sau prin firme interpuse din Federația Rusă ori din ale cărui organe de administrare fac parte persoane din Federația Rusă.

Se interzic achiziționarea, instalarea și utilizarea de către autoritățile și instituțiile publice a următoarelor produse și servicii software, care îndeplinesc criteriile prevăzute la art. 1 al Legii nr. 354 / 2022:

- 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)

Chestionar online pentru identificarea situației la nivel național privind utilizarea de produse și servicii software care îndeplinesc criteriile Legii nr. 354 / 2022

A. Secțiunea - date de identificare ale organizației



Completați datele de identificare ale organizației dvs.

- Numele organizației
- Oraș
- Strada
- Județ / sector
- Nume persoana de contact
- Telefon persoana de contact
- Email persoana de contact

B. Secțiunea - profilul organizației (număr de utilizatori)

Care este numărul aproximativ de utilizatori IT&C din organizația dvs.

- Selectați o valoare
 - o 1-10 utilizatori
 - o 10-50 utilizatori
 - o 50-100 utilizatori
 - o 100-500 utilizatori
 - o 500-1000 utilizatori
 - o Peste 1000 utilizatori
 - o N/A

C. Secțiunea - informații privind categoriile produse și servicii software

Care din următoarele categorii de produse și servicii software sunt utilizate în organizația dvs. ?

- Produse privind securitatea dispozitivului, securitatea punctului final / device security, endpoint security products
- Aplicații și programe software de detecție antivirus / antivirus software
- Aplicații și programe software antimalware, firewall pentru aplicații web, firewall as a service / antimalware software applications, web application firewall (WAD), firewall as a service
- Rețele virtuale private / virtual private networks (VPN)
- Sisteme de detecție și răspuns pentru endpointuri / endpoint detection and response systems (EDR)



D. Secțiunea - informații privind produse și servicii software specifice

Care din următoarele produse și servicii software specifice sunt instalate în infrastructura dvs. ?

- Kaspersky Security
 - o MULTI-SELECT sau CHECKBOX
 - § Kaspersky Anti-Virus
 - § Kaspersky Internet Security
 - § 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
 - o Altele
- Infotecs
 - o MULTI-SELECT sau CHECKBOX
 - § ViPNet Coordinator HW
 - § ViPNet xFirewall
 - § ViPNet EndPoint Protection
 - § ViPNet EndPoint Protection
 - § ViPNet Client for mobile platforms
 - § ViPNet Client for workstations
 - § ViPNet Coordinator IG/HW/KB/VA
 - § ViPNet Personal Firewall
 - § ViPNet SIES/OSSL/TIAS

o FREE-TEXT Altele

- XSIGNAL



MINISTERUL CERCETĂRII,
INOVĂRII ȘI DIGITALIZĂRII

- Metascan
- Dr. Web

o MULTI-SELECT sau CHECKBOX

- § 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)

o Altele

- RPA RusBITech JSC
- RusBITech Astra
- Era Technopolis
- Pasit Ao
- Neobit, 000
- Advanced System Technology, Ao
- Positive Technologies, Ao

- Altele, care nu se regasesc in lista de mai sus

- Confirm ca am parcurs lista de mai sus



D1. Dacă la întrebarea de la secțiunea D. lit. e ați selectat Dr. Web, vă rugăm să selectați una sau mai multe din opțiunile de ma jos, potrivit celor deținute de entitatea dumneavoastră?

- **MULTI-SELECT** sau **CHECKBOX**
 - § Kaspersky Anti-Virus
 - § Kaspersky Internet Security
 - § 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
- **FREE-TEXT** Altele

D2. Dacă la întrebarea de la secțiunea D. lit. e ați selectat Infotecs, vă rugăm să selectați una sau mai multe din opțiunile de ma jos, potrivit celor deținute de entitatea dumneavoastră?

- **MULTI-SELECT** sau **CHECKBOX**
 - § ViPNet Coordinator HW
 - § ViPNet xFirewall
 - § ViPNet EndPoint Protection
 - § ViPNet EndPoint Protection
 - § ViPNet Client for mobile platforms
 - § ViPNet Client for workstations
 - § ViPNet Coordinator IG/HW/KB/VA
 - § ViPNet Personal Firewall
 - § ViPNet SIES/OSSL/TIAS
- **FREE-TEXT** Altele



D3. Dacă la întrebarea de la secțiunea D. lit. a ați selectat Kaspersky Security, vă rugăm să selectați una sau mai multe din opțiunile de mai jos, potrivit celor deținute de entitatea dumneavoastră?

o MULTI-SELECT sau CHECKBOX

- § 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)

o FREE-TEXT Altele

E. Secțiunea - date privind suportul/mentenanța produselor și serviciilor software specifice

În prezent, există suport/mentenanță pentru produsele sau serviciile identificate anterior ?

· DROP LIST Selectați o valoare

- o Da
- o Nu
- o Nu știu

F. Secțiunea - date privind inventarul de produse și servicii software

Aveți întocmit, la acest moment, în organizația dvs. un inventar al produselor și serviciilor software utilizate sau achiziționate ?

· DROP LIST Selectați o valoare



- Da
- Nu
- Nu știu

G. Secțiunea - date privind modul de achiziție al produselor și serviciilor software

Cum achiziționați, în organizația dvs. produsele și serviciilor software?

- Ca licențe software achiziționate direct de organizație
- Ca licențe software achiziționate în numele organizației de o alta instituție, for superior, autoritate contractantă etc.
- Ca parte a unor contracte de prestări servicii
- Ca parte a implementării de proiecte
- Alte situații

H. Secțiunea - date privind operatorii economici ce furnizează produse și servicii software

Organizația dvs. utilizează, după informațiile disponibile la acest moment, furnizori de produse și servicii software cu sediul în Federația Rusă, sau care se cunosc a fi sub controlul direct sau indirect al unei persoane fizice sau juridice din Federația Rusă conform definițiilor de la Art. 1 al Legii nr. 354 / 2022 ?

- Selectați o valoare
 - Da
 - Nu
 - Nu știu
- Dacă DA, completați numele furnizorului utilizat

I. Secțiunea - alte informații relevante

- Alte informații relevante



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 rusești¹.

În Italia, Franco Gabrielli, secretar de stat la președinția Consiliului de miniștri, a declarat în Senat că Guvernul de la Roma lucrează la un set de reguli care ar permite entităților de stat să înlăture programele software dezvoltate de firma rusă Kaspersky². Între timp, reglementările au fost adoptate astfel cum sunt descrise la secțiunea 5, pct. VI din prezenta expunere.

Potrivit unor informații publice apărute în presă³, 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.

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

¹Disponibil 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.

²Disponibil 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.

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



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-terroristă 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, **cibernetice** 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 cibernetică care au guvernat aparatul de stat în ultima perioadă, astfel:

„Atacurile cibernetică 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 cibernetică 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 cibernetică din ce în ce mai complexe, inclusiv de tip APT, dedicate exploatarea sistemelor informatice din domeniul financiar-bancar.”

Cu privire la obiectivul 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 operaționalizeze 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 cibernetică 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 cibernetică 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 cibernetică

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 cibernetică.

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 cibernetică, 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 cibernetică 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 cibernetică

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 cibernetică 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 capacitățile 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 apti 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. 5 alin. (1) din Legea nr. 354/2021, procedura, metodele și instrumentele încetării utilizării produselor și serviciilor provenind direct sau indirect din Federația Rusă sau de la un operator economic aflat sub controlul direct sau indirect al unei persoane fizice sau juridice din Federația Rusă sau al cărei capital este constituit cu participație provenind în mod direct sau prin firme interpușe din Federația Rusă



ori din ale cărui organe de administrare fac parte persoane din Federația Rusă prevăzută în Anexa care face parte integrantă din prezentul ordin.

Având în vedere necesitatea prevenirii și contracarării amenințărilor cibernetice derulate de Federația Rusă, precum și de actori statali și nonstatali aflați sub controlul Federației Ruse asupra infrastructurilor de comunicații și tehnologia informației cu valențe critice pentru securitatea națională, 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 și funcționarea Ministerului Cercetării, Inovării și Digitalizării, cu modificările și completările ulterioare;

Prezentul proiect de ordin a fost elaborat în conformitate cu prevederile art. 5 alin. (1) din Legea nr. 354/2022 privind protecția sistemelor informatice ale autorităților și instituțiilor publice în contextul invaziei declanșate de Federația Rusă împotriva Ucrainei, publicat în Monitorul Oficial, Partea I nr. 1200 din 14 decembrie 2022;

Autoritățile cu atribuții în domeniul securității cibernetice și a securității naționale au contribuit cu procedura de deconectare/dezinstalare a produselor și serviciilor neconforme, astfel încât să se asigure o activitate unitară și coordonată la nivelul autorităților și instituțiilor publice din România.

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 și funcționarea Ministerului Cercetării, Inovării și Digitalizării, cu modificările și completările ulterioare, propunem aprobarea prezentului referat și emiterea prezentului proiect de ordin.

Întocmit,