Proiect

GUVERNUL REPUBLICII MOLDOVA

HOTĂRÎRE nr._____
din _____2019
mun. Chișinău

privind aprobarea unor măsuri necesare pentru asigurarea securității cibernetice la nivel guvernamental

În temeiul obiectivului 1, acțiunii 2) din Planul de acţiuni pentru implementarea Strategiei securităţii informaţionale a Republicii Moldova pentru anii 2019–2024, aprobat prin Hotărârea Parlamentului nr.257/2018 (Monitorul Oficial al Republicii Moldova, 2019, nr. 13-21, art.80), Guvernul,

HOTĂRĂȘTE:

1. Instituția Publică „Serviciul Tehnologia Informației și Securitate Cibernetică”, se desemnează în calitate de Centru guvernamental de reacţie la incidente de securitate cibernetică (*în continuare CERT Gov*).

2. CERT Gov, va constitui punctul unic de contact și de raportare a incidentelor de securitate cibernetică a Guvernului, pentru structurile de tip CERT departamentale, care funcționează în cadrul instituțiilor sau entităților publice guvernamentale, și va asigura implementarea măsurilor necesare pentru asigurarea securității cibernetice la nivel guvernamental.

3. I.P. „Serviciul Tehnologia Informației și Securitate Cibernetică” în termen de 9 luni, va crea și va pune în aplicarea Registrul de Stat al incidentelor de securitate cibernetică.

4. Se aprobă măsurile necesare pentru asigurarea securității cibernetice la nivel guvernamental (se anexează).

5. Ministerele, alte entități administrative centrale subordonate Guvernului, Cancelariei de Stat şi structurile organizaționale din sfera lor de competenţă (autorităţilor administrative din subordine, serviciilor publice desconcentrate şi celor aflate în subordine, precum şi instituţiilor publice şi întreprinderilor de stat în care ministerul, Cancelaria de Stat sau altă autoritate administrativă centrală are calitatea de fondator), entitățile publice şi organizațiile de stat autonome subordonate sau înfiinţate de Guvern, numite în continuare entități publice vor asigura implementarea prevederilor prezentei hotărâri.

6. Altor autorităţi şi instituţii publice decât cele menţionate la pct.5 din prezenta hotărâre, inclusiv autorităţile administraţiei publice locale, precum şi

persoanele de drept privat se recomandă asigurarea implementării prevederilor prezentei hotărâri.

7. Punctul 8 al anexei nr. 1 la Hotărîrea Guvernului nr. 414/2018 cu privire la măsurile de consolidare a centrelor de date în sectorul public și de raționalizare a administrării sistemelor informaționale de stat, (Monitorul Oficial, 2018, nr.157-166, art.474) cu modificările ulterioare, se completează cu subpunctul 34) cu următorul conținut: „exercitarea rolului de Centru guvernamental de reacție la incidente de securitate cibernetică”.

8.Controlul asupra executării prezentei hotărâri se pune în sarcina Cancelariei de Stat.

PRIM-MINISTRU **Ion CHICU**

Anexa
la Hotărîrea Guvernului nr.
din 2019

MĂSURILE NECESARE PENTRU ASIGURAREA SECURITĂȚII CIBERNETICE LA NIVEL GUVERNAMENTAL

I. DISPOZIȚII GENERALE

1. Măsurile necesare pentru asigurarea securităţii cibernetice la nivel guvernamental (*în continuare Măsuri*) , se aplică în cadrul ministerelor, altor autorităţi administrative centrale subordonate Guvernului, Cancelariei de Stat şi structurilor organizaţionale din sfera lor de competenţă (autorităţilor administrative din subordine, serviciilor publice desconcentrate şi celor aflate în subordine, precum şi instituţiilor publice şi întreprinderilor de stat în care ministerul, Cancelaria de Stat sau altă autoritate administrativă centrală are calitatea de fondator), autorităţilor/instituţiilor publice şi organizaţiilor de stat autonome subordonate sau înfiinţate de Guvern, denumite în continuare entităţi publice.

2. CERT Gov reprezintă un punct unic de contact cu structurile de tip CERT Departamentale, care funcționează în cadrul instituțiilor sau entităților publice ori al altor persoane juridice de drept public, cu respectarea competențelor ce revin celorlalte entități şi instituții publice cu atribuții în domeniu.

3. În înţelesul prezentei hotărâri, termenii şi expresiile de mai jos au următoarea semnificaţie:

a) *CERT Gov* - Centru guvernamental de reacţie la incidente de securitate cibernetică, entitate care constituie punctul unic de contact și de raportare a incidentelor de securitate cibernetică a Guvernului și dispune de capacitatea necesară pentru prevenirea, analiza, identificarea şi reacţia la incidentele cibernetice, la nivel guvernamental;

b) *CERT Departamental* – subdiviziune sau persoană responsabilă desemnată în cadrul entităților publice ce dețin sisteme informaționale de stat și care dispun de capacitatea necesară pentru a duce evidența operativă obligatorie și raporta incidentele de securitate cibernetică;

c) *Securitatea rețelelor* - capacitatea unei rețele și a unui sistem informatic de a rezista, la un nivel de încredere dat, oricărei acțiuni care compromite disponibilitatea, autenticitatea, integritatea sau confidențialitatea datelor stocate sau transmise sau prelucrate ori a serviciilor conexe oferite de rețeaua sau de sistemele informatice respective sau accesibile prin intermediul acestora;

d) *Criminalitatea informatică* – totalitatea faptelor prevăzute de legea penală care reprezintă pericol social şi sunt săvârşite cu vinovăţie, prin intermediul sau asupra infrastructurilor cibernetice;

e) Sistem de alertă timpurie şi informare în timp real privind incidentele cibernetice - ansamblul de proceduri şi sisteme tehnice care au rolul de a identifica premisele de apariţie a incidentelor cibernetice şi de a avertiza în cazul producerii acestora. Sistemul include şi conexiuni de date ce vor transporta informaţii referitoare la incidentele cibernetice identificate de senzori dedicaţi, precum şi informaţii statistice referitoare la valorile de trafic înregistrate în nodurile de reţea ale infrastructurilor cibernetice ce asigură funcţionalităţi de utilitate publică ori asigură servicii ale societăţii informaţionale.

II. DREPTURI și ATRIBUȚII

4. În vederea realizării atribuțiilor sale CERT Gov, are dreptul:

1) Să prezinte propuneri privind elaborarea cadrului normativ pentru asigurarea unui nivel înalt de securitate a sistemelor informatice de stat;
2) Să elaboreze mecanisme și metode de prevenire a pericolelor în spațiul cibernetic, care pot afecta securitatea cibernetică la nivel guvernamental;
3) Să solicite informații de la structurile de tip CERT departamentale, create în cadrul entităților publice privind incidentele de securitate cibernetică identificate în cadrul acestora, precum și informații aferente acestora;
4) Să încheie protocoale de cooperare/colaborare cu entitățile publice sau alte persoane juridice de drept public sau privat, naţionale sau internaţionale în domeniul securității cibernetice;
5) Să colaboreze cu persoanele prevăzute la pct. 5 din prezenta hotărâre pentru asigurarea disponibilităţii, confidenţialităţii, integrităţii, autenticităţii şi nonrepudierii informaţiilor în format electronic, în scopul prevenirii, analizei, identificării şi reacției la incidente cibernetice;
6) Să presteze servicii precum audit şi evaluări de securitate sau teste de penetrare în bază contractuală;
7) Să dezvolte parteneriate şi să creeze echipe mixte compuse din specialişti proprii şi specialişti proveniţi de la alte instituţii ori entităţi din mediul privat, cu respectarea legii şi asigurarea condiţiilor privind confidenţialitatea şi accesul la informaţii în limitele legii şi cu acordul părţilor implicate în incident în vederea administrării adecvate a incidentelor majore la nivel guvernamental ori pentru administrarea

unor incidente care necesită înaltă specializare şi pregătire tehnică de specialitate;

8) Să coopereze cu instituții de cercetare, învățământ superior şi persoane juridice de drept privat în realizarea unor proiecte de cercetare şi pregătire a specialiștilor calificați în domeniu.

5. CERT Gov are următoarele atribuții:

1) Asigură implementarea politicilor de prevenire şi contracarare a incidentelor din cadrul infrastructurilor cibernetice, potrivit ariei de competență;
2) Asigură cadrul organizatoric şi suportul tehnic necesar schimbului de informații dintre diverse echipe de tip CERT, utilizatori, entități publice;
3) Asigură interacțiunea cu structurile de tip CERT Departamental din cadrul entităților publice, privind modalitatea de raportare, stocare și prelucrare a informațiilor aferente incidentelor și amenințărilor la adresa securității informaționale;
4) Identifică, înregistrează, clasifică şi analizează incidente de securitate cibernetică;
5) Oferă consultanță și elaborează recomandări de soluționare și prevenire a incidentelor de securitate;
6) Întocmește date statistice şi elaborează rapoarte anuale cu privire la incidentele de securitate înregistrate, precum și dinamica acestora;
7) Organizează şi întreține un sistem de baze de date privind amenințările, vulnerabilitățile şi incidentele de securitate cibernetică identificate sau raportate, tehnici şi tehnologii folosite pentru atacuri, precum şi bune practici pentru protecția infrastructurilor cibernetice;
8) Oferă o platformă informațională de comunicare strategică, prin intermediul paginii sale oficiale, care conține informații despre incidente de securitate informațională și ghiduri de securitate;
9) Desfășoară acțiuni de sensibilizare şi informare privind amenințările, vulnerabilitățile, riscurile la adresa securității cibernetice şi măsurile de protecție întreprinse;
10) Desfășoară exerciții şi antrenamente comune de consolidare a capacităților de reacție la atacuri cibernetice, inclusiv de blocare a atacurilor cibernetice simulate;
11) Organizează și desfășoară ateliere de lucru în domeniul securității cibernetice;
12) Asigură diseminarea informațiilor prin mass-media.
13) Emite avertizări timpurii, alerte și anunțuri și diseminează informațiile privind riscurile și incidentele către entitățile publice stabilite în

punctul 6 din prezenta hotărîre, precum și orice entitate publică căreia îi poate fi afectată securitatea sistemelor informaționale și a rețelelor;

14) Primește raportări privind incidentele care afectează sistemele informaționale și rețelele entităților publice și stabilește impactul acestora;
15) Furnizează entităților publice care au făcut raportarea, în măsura posibilităților, informații relevante în ceea ce privește acțiunile ulterioare raportării;"
16) Asigură răspunsul la incidente de securitate cibernetică
17) Cooperează cu CERT-urile Departamentale și entitățile publice stabilite în punctul 6 din prezenta hotărâre, în cadrul unei platforme de management a incidentelor și schimbului de informații."

6. În vederea exercitării rolului de CERT Departamental, entitățile publice au următoarele drepturi:

1) Să solicite consultanță și recomandări de soluționare și prevenire a incidentelor de securitate cibernetică;
2) Să participe la atelierele de lucru în domeniul securității cibernetice;
3) Să solicite informații cu privire la statutul incidentelor de securitate cibernetică raportate către CERT Gov;
4) Să elaboreze mecanisme și metode de prevenire a pericolelor în spațiul cibernetic, care pot afecta securitatea cibernetică la nivel de entitate;
5) Să coopereze cu institute de cercetare, instituții de învățământ superior şi persoane juridice de drept privat în realizarea unor proiecte de cercetare şi pregătire de specialiști calificați în domeniu;
6) Să participe la exerciții și antrenamente de consolidare a capacităților de reacție la incidentele și atacurile cibernetice.

7. În vederea exercitării rolului de CERT Departamental, entitățile publice au următoarele atribuții:

1) Desemnează, prin act administrativ, persoana (subdiviziunea) responsabilă de punerea în aplicare în cadrul entității a măsurilor necesare pentru asigurarea securității cibernetice;
2) Interacționează cu CERT Gov privind modalitatea de raportare, de stocare și de prelucrare a informațiilor aferente incidentelor și amenințărilor la adresa securității cibernetice;
3) Raportează și duc evidență operativă obligatorie a incidentelor de securitate cibernetică în cadrul entității;
4) Elaborează și aplică metode de prevenire a incidentelor de securitate cibernetică;

5) Asigură implementarea Cerințelor minime obligatorii de securitate cibernetică;
6) Întreprinde acțiunile necesare pentru efectuarea anuală a auditului;
7) Desfășoară exerciții și antrenamente de consolidare a capacităților de reacție la incidentele și atacurile cibernetice;
8) Planifică şi programează în proiectul de buget propriu resursele financiare necesare în vederea implementării prezentelor Măsuri.

III. MODUL DE INTERACȚIUNE

8. CERT Gov va crea și asigura funcționarea unei platforme de management a incidentelor și schimbului de informații.

9. Interacțiunea privind incidentele de securitate cibernetică și alte informații aferente, se va realiza prin:

1) corespondență scrisă;
2) corespondență electronică, prin email;
3) portal electronic, pus la dispoziție de către CERT Gov;
4) apeluri telefonice.

10. CERT-urile departamentale se conectează și realizează schimbul de informații cu CERT Gov prin intermediul platformei create în acest sens.

11. Securitatea cibernetică la nivel guvernamental, se realizează prin următoarele măsuri, întreprinse de către CERT Gov:

1) Măsuri de prevenire:

a) publicarea alertelor şi atenționărilor privind apariţia unor activităţi premergătoare atacurilor;

b) analiza incidentelor și anticiparea riscurilor de securitate cibernetică;

c) estimarea vulnerabilităților şi punerea la dispoziţie a informațiilor actualizate privind încercările de intruziune;

d) diseminarea informațiilor de securitate cibernetică;

e) formularea recomandărilor de prevenire a incidentelor de securiate cibernetică, inclusiv remiterea avertizărilor operative către entitățile publice supuse riscurilor și organele competente;

f) ridicarea nivelului de instruire și conștientizare a populației asupra riscurilor derivate din utilizarea spațiului cibernetic;

g) asigurarea confidențialității, integrității, disponibilității, autenticității și nonrepudierii informațiilor din spațiul cibernetic;

h) dezvoltarea mecanismelor pentru creșterea nivelului de cultură de securitate.

2) Măsuri de reacție:

a) tratarea incidentelor de securitate cibernetică şiboferirea recomandărilor de soluționare a acestora;

b) investigarea incidentelor de securitate cibernetică și identificarea cauzei producerii acestora, inclusiv măsurile de prevenire, care vor asigura depistarea la timp a unor incidente similare.

3) Măsuri de contracarare:

a) notificarea imediată a CERT-urilor departamentale cu privire la depistarea unor încălcări de securitate cibernetică;

b) identificarea la timp a amenințărilor sau atacurilor cibernetice și blocarea manifestării acestora;

c) cooperarea eficientă și permanentă între CERT Gov, CERT-urile departamentale şi organizaţiile competente sau cu capabilităţi în domeniu;

d) aplicarea unui plan de măsuri cu privire la asigurarea funcționalității sistemelor în condiții de securitate a serviciilor publice sau private;

e) diseminarea rezultatelor analizei incidentelor de securitate cibernetică, cu respectarea prevederilor acordurilor de cooperare încheiate cu partenerii CERT Gov.

IV. SECURITATEA INFORMAŢIEI ŞI PROTECŢIA DATELOR CU CARACTER PERSONAL

12. În scopul implementării prezentelor Măsuri, CERT Gov și entitățile publice prelucrează date cu caracter personal, în conformitate cu legislația în domeniul protecției datelor cu caracter personal.

13. Prelucrarea de date în cadrul implementării prezentelor Măsuri, trebuie să garanteze respectarea următoarelor principii privind protecţia datelor cu caracter personal:

1) specificarea şi limitarea scopului;
2) adoptarea de măsuri tehnice şi organizaţionale în scopul asigurării unui nivel adecvat de protecţie a datelor cu caracter personal, în conformitate cu prevederile legislaţiei.

14. Informaţia comunicată (sub orice formă) reciproc între entitățile publice și CERT Gov, va fi considerată drept confidenţială şi nu va fi divulgată în nici un mod, total sau parţial, decât în scopuri de efectuare a analizelor, investigațiilor, statisticilor, sau alte cazuri prevăzute de legislație.