

ORDIN nr. 1062 din 19 octombrie 2011 privind desemnarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO ca autoritate de avizare, verificare și control, organism de analiză, evaluare și intervenție în domeniul securității cibernetice

În temeiul prevederilor art. 4 alin. (1) pct. 54-59 și art. 6 alin. (6) din Hotărârea Guvernului nr. [12/2009](#) privind organizarea și funcționarea Ministerului Comunicațiilor și Societății Informaționale, cu modificările și completările ulterioare, și ale art. 6 lit. g) și n) din Hotărârea Guvernului nr. [494/2011](#) privind înființarea Centrului Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO,

ministrul comunicațiilor și societății informaționale emite prezentul ordin.

Art. 1

La data intrării în vigoare a prezentului ordin, Ministerul Comunicațiilor și Societății Informaționale, în calitate de autoritate de reglementare în domeniu, desemnează Centrul Național de Răspuns la Incidente de Securitate Cibernetică - CERT-RO ca autoritate de avizare, verificare și control, organism de analiză, evaluare și intervenție în domeniul securității cibernetice, pentru furnizorii de servicii electronice, pentru Registrul Național RoTLD, pentru furnizorii de servicii de înregistrare de resurse internet, de tip registru local internet, precum și pentru operatorii sistemelor prin care se prestează servicii e-guvernare și servicii de informare în cadrul portalului e-Romania din subordinea Ministerului Comunicațiilor și Societății Informaționale.

Art. 2

În înțelesul prezentului ordin, următorii termeni se definesc astfel:

- a)** MCSI - Ministerul Comunicațiilor și Societății Informaționale;
- b)** CERT-RO - Centrul Național de Răspuns la Incidente de Securitate Cibernetică;
- c)** furnizor de servicii - orice persoană, fizică sau juridică, ce oferă servicii electronice (comerț electronic, semnătură electronică, marcă temporală, activitate electronică notarială, arhivarea documentelor în formă electronică, emiterea facturilor în formă electronică sau instrumente de plată cu acces la distanță);
- d)** CNMSI - Centrul Național de Management pentru Societatea Informațională;
- e)** CNRD - Centrul Național "România Digitală";
- f)** verificare - activitate în baza căreia se emite/nu se emite avizul de specialitate;
- g)** control - activități desfășurate de personal anume desemnat în vederea constatării modului de îndeplinire a obligațiilor stabilite.

Art. 3

Pentru îndeplinirea prevederilor art. 1, directorul general CERT-RO, la solicitarea ministrului comunicațiilor și societății informaționale, emite ordinul cu privire la persoanele care au dreptul de a participa la misiunile de control.

Art. 4

- (1)** Activitatea de control se desfășoară numai la solicitarea MCSI, pe baza unui mandat clar.
- (2)** Controlul se realizează la solicitarea ministrului comunicațiilor și societății informaționale, pe baza ordinului de control emis de directorul general CERT-RO, aprobat de ministrul comunicațiilor și societății informaționale.
- (3)** Controlul tematic se realizează pe baza Planului de control anual elaborat de CERT-RO și

aprobat de ministrul comunicațiilor și societății informaționale.

(4) Concluziile controalelor, precum și măsurile stabilite vor fi prezentate ministrului comunicațiilor și societății informaționale.

(5) În situația în care în urma controlului sunt identificate fapte care depășesc sfera contravențională, raportul de control va fi prezentat ministrului comunicațiilor și societății informaționale pentru luarea măsurilor legale.

Art. 5

În vederea exercitării atribuțiilor de control, personalul împuternicit în acest scop este autorizat în limitele legii:

a) să aibă acces liber, permanent, în orice loc în care se află echipamentele necesare furnizării serviciilor;

b) să solicite orice document sau informație necesară în vederea verificării respectării obligațiilor ce incumbă furnizorul de servicii;

c) să verifice punerea în aplicare a oricăror proceduri utilizate de către furnizorul de servicii supus controlului;

d) să sigileze orice echipamente necesare furnizării de servicii sau să rețină orice document care are legătură cu această activitate, pe o perioadă care nu poate depăși 15 zile, dacă aceste măsuri se impun;

e) să propună ministerului comunicațiilor și societății informaționale, în calitate de autoritate de reglementare în domeniu, aplicarea sancțiunilor contravenționale prevăzute în legislația specifică acestora;

f) să propună MCSI suspendarea activității furnizorului de servicii până la încetarea cauzelor care au determinat luarea măsurii;

g) să propună măsuri de îmbunătățire a activității furnizorului de servicii.

Art. 6

(1) În baza prevederilor prezentului ordin, CERT-RO este împuternicit să efectueze toate activitățile de verificare a operatorilor care solicită MCSI aviz de funcționare în oricare dintre domeniile la care face referire acest ordin.

(2) Avizul CERT-RO este obligatoriu pentru primirea dreptului de operare în domeniu, solicitat MCSI, cu excepția semnăturii digitale.

Art. 7

(1) CERT-RO are obligația de a păstra confidențialitatea tuturor informațiilor primite de la furnizorul de servicii sau operatorii de servicii, cu excepția celor prevăzute de legislația aplicabilă fiecărui domeniu menționat în art. 1 și de prezentul ordin ca fiind publice.

(2) CERT-RO poate încheia acorduri de confidențialitate asupra informațiilor primite de la furnizorul de servicii sau operatorii de servicii, la cererea acestora.

(3) Personalul cu atribuții de control din cadrul CERT-RO este obligat să păstreze confidențialitatea datelor de care a luat cunoștință cu ocazia exercitării atribuțiilor de analiză, evaluare și constatare.

Art. 8

(1) În termen de 10 zile de la intrarea în vigoare a prezentului ordin, operatorii de sisteme prin care se prestează servicii e-guvernare și servicii de informare din cadrul portalului e-Romania, aflate în subordinea MCSI, sunt obligați să prezinte la cabinetul ministrului comunicațiilor și societății informaționale un set de parole și chei de acces la sistemele pe care le operează, informațiile respective fiind păstrate în condiții de maximă securitate.

(2) În caz de incident cibernetic, care duce la întreruperea activităților de operare sau de risc iminent legat de activitatea de operare, ministrul comunicațiilor și societății informaționale poate asigura accesul CERT-RO la parole și la chei în vederea remedierii situației și asigurării continuității funcționării sistemelor, în raport cu procedura de intervenție stabilită.

Art. 9

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

Ministrul comunicațiilor și societății informaționale,

Valerian Vreme

Publicat în Monitorul Oficial cu numărul 34 din data de 16 ianuarie 2012