Hotărâre nr.494 din 11.05.2011
privind înfiinţarea Centrului Naţional de Răspuns la Incidente de Securitate Cibernetică - CERT-RO

ACT EMIS DE: Guvernul Romaniei
ACT PUBLICAT ÎN MONITORUL OFICIAL NR. 388 din 02 iunie 2011

În temeiul art. 108 din Constituţia României, republicată, şi al art. 11 alin. (1) şi (2) din Ordonanţa Guvernului nr. 57/2002 privind cercetarea ştiinţifică şi dezvoltarea tehnologică, aprobată cu modificări şi completări prin Legea nr. 324/2003, cu modificările şi completările ulterioare,
Guvernul României adoptă prezenta hotărâre.

Articolul 1

(1) Se înfiinţează Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică - CERT-RO, ca structură independentă de expertiză şi cercetare-dezvoltare în domeniul protecţiei infrastructurilor cibernetice, denumit în continuare CERT-RO, cu sediul în bd. Mareşal Averescu nr. 8-10, sectorul 1, Bucureşti.

(2) CERT-RO este instituţie publică cu personalitate juridică, în coordonarea Ministerului Comunicaţiilor şi Societăţii Informaţionale, denumit în continuare MCSI, finanţată integral de la bugetul de stat prin bugetul MCSI.

(3) CERT-RO nu va prelua nicio parte din activitatea desfăşurată în prezent de Institutul Naţional de Cercetare-Dezvoltare în Informatică - ICI Bucureşti.

(4) CERT-RO nu are competenţe în domeniul infrastructurilor cibernetice destinate procesării, stocării sau transmiterii informaţiilor clasificate.

Articolul 2

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

a) CERT - centru de răspuns la incidente de securitate cibernetică - entitate organizaţională specializată care dispune de capacitatea necesară pentru prevenirea, analiza, identificarea şi reacţia la incidentele cibernetice;

b) Comunitatea CERT din România - ansamblul centrelor de tip CERT care funcţionează în cadrul autorităţilor şi instituţiilor publice ori al altor persoane juridice de drept public sau privat din România şi care relaţionează cu CERT-RO pe baza unor proceduri şi protocoale de cooperare;

c) infrastructuri cibernetice - infrastructuri de tehnologia informaţiei şi comunicaţii, constând în sisteme informatice, aplicaţii aferente, reţele şi servicii de comunicaţii electronice;

d) spaţiul cibernetic - mediul virtual, generat de infrastructurile cibernetice, incluzând conţinutul informaţional procesat, stocat sau transmis, precum şi acţiunile derulate de utilizatori în acesta;

e) securitate cibernetică - starea de normalitate rezultată în urma aplicării unui ansamblu de măsuri proactive şi reactive prin care se asigură confidenţialitatea, integritatea, disponibilitatea, autenticitatea şi nonrepudierea informaţiilor în format electronic, a resurselor şi serviciilor publice sau private din spaţiul cibernetic. Măsurile proactive şi reactive pot include: politici, concepte, standarde şi ghiduri de securitate, managementul riscului, activităţi de instruire şi conştientizare, implementarea de soluţii tehnice de protejare a infrastructurilor cibernetice, managementul identităţii, managementul consecinţelor;

f) atac cibernetic - orice acţiune ostilă desfăşurată în spaţiul cibernetic de natură să afecteze securitatea cibernetică;
g) incident cibernetic - orice eveniment survenit în spaţiul cibernetic de natură să afecteze securitatea cibernetică;
h) serviciile publice de tip preventiv:
1. anunţuri privind evenimente în domeniu;
2. anunţuri privind ameninţări nou-identificate pe plan naţional şi internaţional;
3. cercetare şi informare privind noutăţile tehnologice în domeniu;
4. realizarea, la cerere, de auditări şi evaluări de securitate sau teste de penetrare;
5. estimarea vulnerabilităţilor şi punerea la dispoziţie de situaţii actualizate privind încercările de intruziune şi servicii de localizare a surselor atacurilor, pe baza informaţiilor transmise de furnizorii de reţele şi servicii de comunicaţii electronice;
6. diseminarea informaţiilor de securitate cibernetică;
i) serviciile publice de tip reactiv:
1. alerte şi atenţionări privind apariţia unor activităţi premergătoare atacurilor;
2. gestiunea incidentelor la nivel naţional, în cooperare cu celelalte echipe CERT;
3. diseminarea rezultatelor investigaţiilor incidentelor de securitate cibernetică, cu respectarea prevederilor acordurilor de cooperare încheiate cu partenerii CERT-RO;
j) serviciile publice de consultanţă pentru managementul calităţii serviciilor de securitate cibernetică:
1. analize de risc aplicate la nivel local şi la nivel naţional privind infrastructurile cibernetice;
2. planificarea asigurării funcţionării continue şi a recuperării în caz de dezastre;
3. atestarea managementului securităţii cibernetice şi a incidentelor cibernetice;
4. pregătirea echipelor de tip CERT, a echipelor de audit în domeniul securităţii reţelelor, cu prioritate a celor incluse în infrastructura critică naţională;
k) 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.

Articolul 3
(1) CERT-RO îşi desfăşoară activitatea în conformitate cu legislaţia în vigoare şi cu regulamentul propriu de organizare şi funcţionare, în scopul realizării **prevenirii, analizei, identificării şi reacţiei la** incidente în cadrul infrastructurilor cibernetice ce asigură funcţionalităţi de utilitate publică ori asigură servicii ale societăţii informaţionale.
(2) Pentru infrastructurile cibernetice aflate în administrarea instituţiilor din domeniul apărării, ordinii publice şi siguranţei naţionale, CERT-RO îndeplineşte doar atribuţiile de cooperare, în baza unor acorduri dedicate, încheiate cu structurile de tip CERT ale acestora.
(3) CERT-RO reprezintă un punct naţional de contact cu structurile de tip CERT care funcţionează în cadrul instituţiilor sau autorităţilor publice ori al altor persoane juridice de drept public sau privat, naţionale ori internaţionale, cu respectarea competenţelor ce revin celorlalte autorităţi şi instituţii publice cu atribuţii în domeniu, potrivit legii.
(4) CERT-RO asigură elaborarea şi diseminarea politicilor publice de prevenire şi contracarare a incidentelor din cadrul infrastructurilor cibernetice, potrivit ariei de competenţă.
(5) CERT-RO analizează disfuncţionalităţile procedurale şi tehnice la nivelul infrastructurilor cibernetice, potrivit ariei de competenţă, şi transmite instituţiilor sau autorităţilor publice ori altor persoane juridice de drept public sau privat aspectele de interes.

Articolul 4

(1) În vederea îndeplinirii atribuţiilor ce îi revin, CERT-RO încheie protocoale de cooperare/colaborare cu instituţiile publice sau alte persoane juridice de drept public sau privat, naţionale sau internaţionale, respectând competenţele ce revin celorlalte autorităţi şi instituţii publice cu atribuţii în domeniu, putând dezvolta şi parteneriate publice-private.

(2) CERT-RO cooperează cu entităţile şi persoanele prevăzute la alin.(1) pentru asigurarea disponibilităţii, confidenţialităţii, integrităţii, autenticităţii şi nonrepudierii informaţiilor în format electronic, în scopul prevenirii, analizei, identificării şi reacţiei la incidente cibernetice.

(3) Criteriile şi cerinţele minime pe care trebuie să le îndeplinească un centru de tip CERT pentru a fi inclus în Comunitatea CERT din România, precum şi procedurile de colaborare se stabilesc şi se actualizează prin decizie a directorului general CERT-RO, cu avizul Comitetului de coordonare.

Articolul 5

CERT-RO realizează şi administrează un portal propriu, dedicat securităţii cibernetice, prin care sunt publicate noutăţi din domeniu, alerte privind ameninţările cele mai probabile, precum şi cele mai bune practici de protecţie recomandate.

Articolul 6

CERT-RO are următoarele atribuţii:

a) oferă servicii publice de tip preventiv, de tip reactiv şi de consultanţă;

b) organizează şi întreţine un sistem de baze de date privind ameninţările, vulnerabilităţile şi incidentele de securitate cibernetică identificate sau raportate, tehnici şi tehnologii folosite pentru atacuri, precum şi bune practici pentru protecţia infrastructurilor cibernetice;

c) asigură cadrul organizatoric şi suportul tehnic necesar schimbului de informaţii dintre diverse echipe de tip CERT, utilizatori, autorităţi, producători de echipamente şi soluţii de securitate cibernetică, precum şi furnizori de servicii în domeniu;

d) organizează, desfăşoară sau participă la activităţi de instruire în domeniul securităţii cibernetice;

e) organizează simpozioane, dezbateri pe teme de securitate cibernetică şi asigură diseminarea unor informaţii specifice prin mass-media;

f) desfăşoară activităţi de cercetare-dezvoltare în domeniu şi elaborează proceduri şi recomandări privind securitatea cibernetică, potrivit prevederilor legale privind cercetarea ştiinţifică şi dezvoltarea tehnologică;

g) asigură MCSI suportul tehnic şi de specialitate pentru elaborarea politicilor de securitate cibernetică necesar a fi respectate de furnizorii de reţele şi servicii de comunicaţii electronice publice pentru obţinerea autorizării de funcţionare a acestora, precum şi la evaluarea modului de implementare a acestora;

h) asigură consultanţă de specialitate autorităţilor publice responsabile, stabilite conform Ordonanţei de urgenţă a Guvernului nr. 98/2010 privind identificarea, desemnarea şi protecţia infrastructurilor critice, aprobată cu modificări prin Legea nr.18/2011, cu privire la produsele şi sistemele de securitate cibernetică care deservesc infrastructurile critice naţionale şi europene;

i) asigură puncte de contact pentru colectarea sesizărilor şi a informaţiilor despre incidente de securitate cibernetică atât automatizat, cât şi prin comunicare directă securizată, după caz;

j) identifică, analizează şi clasifică incidentele de securitate din cadrul infrastructurilor cibernetice, conform ariei de competenţă;

k) elaborează propuneri pe care le înaintează către MCSI sau Consiliului Suprem de Apărare a Ţării, denumit în continuare CSAT, privind modificarea cadrului legislativ în vederea stimulării dezvoltării securităţii infrastructurilor cibernetice ce asigură funcţionalităţi de utilitate publică ori asigură servicii ale societăţii informaţionale;

l) planifică şi programează în proiectul de buget propriu resursele financiare necesare în vederea realizării politicilor în domeniile sale de competenţă;
m) coordonează derularea proiectelor, ale căror beneficiari sunt MCSI şi/sau instituţiile din subordinea acestuia, cu finanţare naţională sau internaţională în domeniul securităţii infrastructurilor cibernetice ce asigură funcţionalităţi de utilitate publică, ori asigură servicii ale societăţii informaţionale, care vizează capacitatea instituţională operaţională a CERT-RO;
n) asigură MCSI suportul tehnic şi de specialitate pentru urmărirea şi controlul aplicării prevederilor cuprinse în actele normative în vigoare sau în acordurile internaţionale în domeniul de competenţă şi notifică organele competente pentru demararea procedurilor legale în vederea cercetării şi sancţionării, după caz.

Articolul 7
(1) În cadrul CERT-RO se constituie Sistemul de alertă timpurie şi informare în timp real privind incidentele cibernetice.
(2) Datele primite în Sistemul de alertă timpurie şi informare în timp real privind incidentele cibernetice vor fi centralizate şi prelucrate de către CERT-RO, în scopul:
a) avertizării în timp real şi emiterii de rapoarte cu privire la distribuţia şi natura incidentelor;
b) colaborării cu autorităţile naţionale responsabile în asigurarea securităţii cibernetice, în vederea prevenirii şi înlăturării efectelor incidentelor.

Articolul 8
Furnizorii de reţele şi servicii de comunicaţii electronice publice, precum şi alte persoane juridice de drept public sau privat, care deţin sau administrează infrastructuri cibernetice ce susţin funcţionalităţi de utilitate publică ori servicii ale societăţii informaţionale, asigură, în condiţiile legii, resursele tehnice şi funcţionale necesare dezvoltării componentei proprii de securitate în conformitate cu cerinţele şi specificaţiile furnizate de CERT-RO şi interconectării cu Sistemul de alertă timpurie şi informare în timp real cu privire la atacurile cibernetice.

Articolul 9
(1) CERT-RO cooperează cu institute de cercetare, instituţii de învăţământ superior şi persoane juridice de drept privat în realizarea unor proiecte de cercetare şi pregătirea unor specialişti în domeniu.
(2) CERT-RO formulează tematici şi proiecte de cercetare şi dezvoltare în domeniul securităţii cibernetice, independent sau în cooperare cu autorităţi naţionale ori cu alte persoane fizice sau juridice, la nivel naţional sau internaţional.

Articolul 10
CERT-RO participă cu specialişti la grupurile de lucru din ţară şi străinătate în domeniul de competenţă, pe bază de mandat aprobat de către directorul general.

Articolul 11
Pentru îndeplinirea atribuţiilor ce îi revin, CERT-RO gestionează şi utilizează următoarele categorii de informaţii:
a) informaţii publice;
b) informaţii nedestinate publicităţii, aparţinând entităţilor cu care are încheiate acorduri de cooperare;
c) informaţii clasificate.

Articolul 12

(1) CERT-RO este condus de un director general şi de un director general adjunct, sprijiniţi de Comitetul de coordonare.

(2) Directorul general este numit prin ordinul ministrului comunicaţiilor şi societăţii informaţionale şi îşi desfăşoară activitatea în baza unui contract de mandat pe o perioadă de 5 (cinci) ani, cu posibilitatea de prelungire a mandatului.

(3) Contractul de mandat este asimilat contractului individual de muncă şi conferă titularului vechime în muncă şi în specialitate.

(4) Pot ocupa funcţiile de director general şi director general adjunct persoanele care îndeplinesc cumulativ următoarele condiţii:

a) au cetăţenia română;

b) cunosc limba română, scris şi vorbit;

c) au capacitate deplină de exerciţiu;

d) au o stare de sănătate corespunzătoare, atestată pe bază de examen medical de specialitate;

e) au studii universitare de licenţă, respectiv studii superioare de lungă durată, absolvite cu diplomă;

f) nu au fost condamnate pentru săvârşirea unei infracţiuni săvârşite cu intenţie, cu excepţia situaţiei în care a intervenit reabilitarea;

g) nu se încadrează în dispoziţiile art. 2 lit. a) şi b) din Ordonanţa de urgenţă a Guvernului nr. 24/2008 privind accesul la propriul dosar şi deconspirarea Securităţii, aprobată cu modificări şi completări prin Legea nr. 293/2008.

(5) Directorul general este ordonator de credite, în condiţiile legii.

(6) Directorul general al CERT-RO este preşedintele Comitetului de coordonare, care are atribuţiile stabilite prin Regulamentul de organizare şi funcţionare al CERT-RO.

(7) Comitetul de coordonare este format din reprezentanţi ai:

a) MCSI;

b) Ministerului Apărării Naţionale;

c) Ministerului Administraţiei şi Internelor;

d) Serviciului Român de Informaţii;

e) Serviciului de Informaţii Externe;

f) Serviciului de Telecomunicaţii Speciale;

g) Serviciului de Protecţie şi Pază;

h) Oficiului Registrului Naţional al Informaţiilor Secrete de Stat;

i) Autorităţii Naţionale pentru Administrare şi Reglementare în Comunicaţii.

(8) În vederea îndeplinirii atribuţiilor ce revin CERT-RO, directorul general emite decizii şi instrucţiuni.

Articolul 13

(1) Activitatea CERT-RO este analizată semestrial în Comitetul de coordonare, pe baza raportului elaborat în acest sens de către directorul general.

(2) CERT-RO prezintă CSAT un raport anual privind activitatea sa.

Articolul 14

(1) Numărul maxim de posturi este de 41, iar salarizarea personalului CERT-RO se face potrivit legislaţiei aplicabile personalului bugetar plătit din fonduri publice, precum şi a prevederilor legale privind cercetarea ştiinţifică şi dezvoltarea tehnologică.

(2) Personalul CERT-RO este format din personal contractual sau detaşat de la alte instituţii sau alte autorităţi publice, în condiţiile legii.

(3) Organizarea şi desfăşurarea examenelor sau concursurilor vizând personalul contractual se realizează în condiţiile stabilite de directorul general al CERT-RO.

Articolul 15
Finanţarea cheltuielilor curente şi de capital ale CERT-RO se asigură integral de la bugetul de stat prin bugetul MCSI.

Articolul 16
(1) CERT-RO administrează, exploatează, dezvoltă, modernizează şi întreţine patrimoniul său.
(2) CERT-RO îşi desfăşoară activitatea într-un spaţiu din imobilul situat în bd. Mareşal Averescu nr. 8-10, sectorul 1, Bucureşti, în baza unui contract de comodat încheiat cu Institutul Naţional de Cercetare-Dezvoltare în Informatică - ICI Bucureşti, proprietarul imobilului.
(3) Bunurile mobile necesare desfăşurării obiectului de activitate vor fi preluate pe baza unui proces-verbal de predare-primire şi vor constitui patrimoniul CERT-RO, fiind înregistrate la valoarea de inventar din contabilitatea Institutului Naţional de Cercetare-Dezvoltare în Informatică - ICI Bucureşti.
(4) Patrimoniul Institutului Naţional de Cercetare-Dezvoltare în Informatică - ICI Bucureşti se va diminua, în mod corespunzător, cu valoarea bunurilor predate.
(5) Rezultatele cercetărilor concretizate în active corporale sau necorporale, obţinute în baza unor contracte finanţate din fonduri private, precum şi rezultatele obţinute din activităţi desfăşurate în asociere în participaţiune sau în entităţi cu personalitate juridică născute în urma unor alte forme de asociere rămân proprietatea Institutului Naţional de Cercetare-Dezvoltare în Informatică - ICI Bucureşti, CERT-RO având dreptul de a le utiliza şi/sau administra conform dispoziţiilor legale.

Articolul 17
Regulamentul de organizare şi funcţionare al CERT-RO se aprobă şi se revizuieşte de către CSAT la propunerea ministrului comunicaţiilor si societăţii informaţionale.

Articolul 18
(1) În termen de 90 de zile de la data intrării în vigoare a prezentei hotărâri, MCSI promovează normele de aplicare elaborate cu sprijinul CERT-RO prin ordin al ministrului comunicaţiilor şi societăţii informaţionale.
(2) Pentru instituţiile publice, termenul de implementare a obligaţiilor prevăzute de prezenta hotărâre va curge de la data identificării în bugetul propriu a sumelor necesare, iar achiziţia echipamentelor se va realiza cu respectarea dispoziţiilor Ordonanţei de urgenţă a Guvernului nr. 34/2006 privind atribuirea contractelor de achiziţie publică, a contractelor de concesiune de lucrări publice şi a contractelor de concesiune de servicii, aprobată cu modificări şi completări prin Legea nr. 337/2006, cu modificările şi completările ulterioare.

Articolul 19
Hotărârea Guvernului nr. 12/2009 privind organizarea şi funcţionarea Ministerului Comunicaţiilor şi Societăţii Informaţionale, publicată în Monitorul Oficial al României, Partea I, nr. 51 din 28 ianuarie 2009, cu modificările şi completările ulterioare, se modifică după cum urmează:
1. Articolul 15 va avea următorul cuprins:
Articolul 15
Ministerul Comunicaţiilor şi Societăţii Informaţionale are în subordine Centrul Naţional de Management pentru Societatea Informaţională, Centrul Naţional «România Digitală» şi Centrul Naţional de Supercomputing şi în coordonare directă Institutul Naţional de Cercetare-Dezvoltare în Informatică - ICI Bucureşti, Institutul Naţional de Studii şi Cercetări pentru Comunicaţii - I.N.S.C.C. Bucureşti şi Centrul Naţional de Răspuns la Incidente de Securitate Cibernetică - CERT-RO, instituţii prevăzute în anexele nr. 2 şi 3.

2. Anexa nr. 3 se modifică şi se înlocuieşte cu anexa la prezenta hotărâre.

PRIM-MINISTRU
EMIL BOC

Contrasemnează:

Ministrul comunicaţiilor şi societăţii informaţionale,
Valerian Vreme
Preşedintele Autorităţii Naţionale pentru Administrare şi Reglementare în Comunicaţii,
Cătălin Marinescu
Ministrul apărării naţionale,
Gabriel Oprea
p. Ministrul administraţiei şi internelor,
Gheorghe Emacu,
secretar de stat
Ministrul muncii, familiei şi protecţiei sociale, interimar,
Emil Boc
Ministrul educaţiei, cercetării, tineretului şi sportului,
Daniel Petru Funeriu
Directorul Serviciului Român de Informaţii,
George Cristian Maior
Directorul Serviciului de Telecomunicaţii Speciale,
Marcel Opriş
Directorul Serviciului de Informaţii Externe,
Mihai Răzvan Ungureanu
p. Directorul Oficiului Registrului Naţional al Informaţiilor Secrete de Stat,
Mihai Ion
Ministrul finanţelor publice,
Gheorghe Ialomiţianu
Bucureşti, 11 mai 2011.

ANEXĂ

(Anexa nr. 3 la Hotărârea Guvernului nr. 12/2009)
UNITĂŢI care funcţionează în coordonarea Ministerului Comunicaţiilor şi Societăţii Informaţionale

Nr. crt.	Denumirea unitatii
1.	Institutul National de Cercetare-Dezvoltare in Informatica - ICI Bucuresti
2.	Institutul National de Studii si Cercetari pentru Comunicatii - I.N.S.C.C. Bucuresti
3.	Centrul National de Raspuns la Incidente de Securitate Cibernetica - CERT-RO