SERVICIUL ROMÂN DE INFORMAŢII

CENTRUL NAŢIONAL CYBERINT

13

Nr. 355 172 din 29.04.2016

MINISTERUL AFACERILOR INTERNE

DEPARTAMENTUL DE INFORMAŢII

ŞI PROTECŢIE INTERNĂ

Nr. 13 din 09.05.2016

MULTIPLICAT D.G.P.I.
RM. nr. 9326 Niv. clasificare NESECRET
Nr. ex. rezultat 1x Data 27.09.2019

ACORD DE COOPERARE

ÎNTRE SERVICIUL ROMÂN DE INFORMAŢII ŞI MINISTERUL AFACERILOR INTERNE ÎN DOMENIUL SECURITĂŢII CIBERNETICE

PREAMBUL

Având în vedere:

- Legea nr.14/1992 privind organizarea şi funcţionarea Serviciului Român de Informaţii, cu modificările şi completările ulterioare;
- Legea nr. 15/2008 pentru aporbarea Ordonanței de Urgență a Guvernului nr. 30/2007 privind organizarea și funcționarea Ministerului Afacerilor Interne, cu modificările şi completările ulterioare;
- Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenţei în exercitarea demnităţilor publice, a funcţiilor publice şi în mediul de afaceri, prevenirea şi sancţionarea corupţiei, cu modificările şi completările ulterioare, Titlul III – Prevenirea şi combaterea criminalităţii informatice;
- Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal şi protecţia vieţii private în sectorul comunicaţiilor electronice, cu modificările şi completările ulterioare;
- Legea nr. 365/2002 privind comerţul electronic, republicată;
- Hotărârea de Guvern nr. 271 din 15 mai 2013 pentru aprobarea Strategiei de securitate cibernetică a României și a Planului de Acțiune la nivel național privind implementarea Sistemului Național de Securitate Cibernetică.

MINISTERUL AFACERILOR INTERNE prin **DEPARTAMENTUL DE INFORMAŢII ŞI PROTECŢIE INTERNĂ (DIPI),** cu sediul în București, strada Răzoare nr.5, sector 6, reprezentat prin domnul secretar de stat, **comisar-șef de poliție** [redacted]

și

SERVICIUL ROMAN DE INFORMATII (S.R.I.) prin **Centrul National CYBERINT** [redacted] diul în Bucuresti, strada Splaiul Independenţei nr.323A, sector 6, reprezentat prin [redacted] ctor **colonel** [redacted]

denumite în continuare Părţi, au decis încheierea prezentului *Acord de cooperare în domeniul securităţii cibernetice*, denumit în continuare Acord şi convin prin prezentul următoarele:

[redacted]

CAPITOLUL I – Dispoziţii Generale

Art.1 – Obiectul Acordului îl reprezintă stabilirea:

a) condiţiilor în care se face schimbul de informaţii între Părţi;

b) modalităţilor prin care acestea sunt transmise între Părţi;

c) cadrului general de cooperare între Părţi, în scopul identificării, alertării şi prevenirii consecinţelor incidentelor de securitate în care pot fi implicate serviciile informatice ale cele doua instituţii.

Art. 2 – Termenii utilizaţi în prezentul Acord au semnificaţia conform art.2 din HG 494/2011 privind infiinţarea CERT-RO, iar înţelesul termenilor tehnici este cel specificat în Anexa 1.

CAPITOLUL II – Categoriile de informaţii transmise

Art.3 – *DIPI* transmite către *CNC* informaţii ce sunt relevante din punct de vedere al securităţii cibernetice naţionale. Aceste informaţii sunt furnizate de sistemele proprii de supraveghere a reţelei de date şi sunt referitoare la atacuri cibernetice sau reflectă incidente de securitate cibernetică.

Art.4 – *La solicitarea DIPI,* structurile MAI vor pune la dispoziţia *CNC*, pentru a fi utilizate în cadrul unui honeynet dezvoltat *în parteneriat cu MAI*, adrese IP relevante specifice diferitelor categorii de locaţii geografice, care fac parte din clasele de adrese IP alocate ministerului.

Art.5 – *CNC* transmite către *DIPI:*

(1) Informaţii actualizate privind vulnerabilităţile sistemelor informatice şi de comunicaţii, alerte şi buletine de securitate, bune practici privind sporirea securităţii spaţiului cibernetic, modul de gestionare a incidentelor de securitate, precum şi alte informaţii care pot fi utilizate în prevenirea şi reducerea numărului incidentelor de securitate.

(2) Rapoarte periodice cu privire la starea de securitate a reţelelor instituţiei bazate pe informaţiile puse la dispoziţie de *DIPI.*

(3) Informaţii cu privire la ameninţările cibernetice constatate sau cu privire la incidentele de securitate existente în cadrul reţelelor şi serviciilor de comunicaţii electronice administrate sau aflate în proprietatea instituţiei, rezultate ca urmare a evaluării securităţii informatice a reţelelor administrate sau aflate în proprietatea instituţiei, realizate de către *CNC* la solicitarea *DIPI.*

Art.6 – Informaţiile transmise între *DIPI* şi *CNC* nu reprezintă conţinut (total sau parţial) al conexiunilor TCP/IP.

Art.7 – Transmiterea între părţi a informaţiilor clasificate se va realiza cu respectarea prevederilor legislaţiei naţionale în domeniul protecţiei informaţiilor clasificate.

CAPITOLUL III – Metode şi mijloace de transmitere a informaţiilor

Art.8 –Transmiterea informaţiilor între DIPI şi CNC se realizează prin linii de comunicaţii dedicate, stabilite de comun acord de cele două părţi.

Art. 9 – Transmiterea informaţiilor de la DIPI către CNC se poate face prin una din metodele:

a) periodic, prin transmiterea de fişiere folosind conexiuni, tunele sau programe de transfer fişiere ce oferă un grad sporit de siguranţă (ssh, sftp, ftps) către un server din reţeaua CNC;

b) periodic, prin transmiterea de fişiere către una sau mai multe adrese de e-mail aparţinând CNC; transmiterea informaţiilor prin e-mail se realizează de preferinţă criptat, folosind tehnologie PGP sau certificate digitale x509 v3 cu profil de criptare emise de o infrastructură de tip PKI;

c) online, folosind protocoale securizate (de exemplu, dar nu limitat la https) şi autentificare.

Art.10 – Transmiterea informaţiilor de la CNC către DIPI se face:

a) periodic, prin transmiterea de informaţii şi/sau fişiere către adresele de e-mail de contact specificate în Anexa 2 a prezentului Acord; transmiterea informaţiilor prin e-mail se realizează de preferinţă criptat, folosind tehnologie PGP sau certificate digitale x509 v3 cu profil de criptare emise de o o infrastructură de tip PKI;
b) atunci când este cazul, prin transmiterea de fişiere folosind conexiuni sau programe de transfer de fişiere ce oferă un grad sporit de siguranţă;
c) prin intermediul portalului www.cyberint.ro.

CAPITOLUL IV – Obligaţiile Părţilor

Art.11 – (1) Părţile au următoarele obligaţii generale:

a) să desemneze structurile din interiorul instituției ce pot pune în practică solicitările Părţilor şi prin intermediul cărora se va face schimbul de informaţii;

b) să anunţe în cel mai scurt timp cealaltă Parte, prin canale sigure de comunicare, orice modificare a listei de contact menţionate la lit.a);

(2) Lista datelor de contact menţionate la alin.(1) este prevăzută în Anexa 2 la prezentul Acord.

Art.12 – *CNC* are următoarele obligaţii:

a) să realizeze, la solicitarea *DIPI*, evaluarea securității informatice a rețelelor administrate sau aflate în proprietatea MAI și să informeze cu privire la vulnerabilitățile/amenințările cibernetice constatate;

b) să informeze DIPI cu privire la incidentele de securitate identificate în cadrul rețelelor și serviciilor de comunicații electronice administrate sau aflate în proprietatea *MAI*;

c) să ofere suport, la solicitarea *DIPI*, pentru definirea și actualizarea politicilor de securitate în cadrul rețelelor de interes pentru *MAI*;

d) să ofere suport, la solicitarea *DIPI*, pentru întocmirea și actualizarea procedurilor de intervenție în caz de incident sau atac cibernetic în cadrul *MAI*;

e) să ofere sprijin, la solicitarea *DIPI*, în situații de criză generate de atacuri cibernetice pentru investigarea cauzelor care au condus la criză, pentru determinarea efectelor atacului și a daunelor provocate, precum și pentru restaurarea situației de normalitate;

f) să asigure respectarea prevederilor legale în cadrul operațiunilor privind colectarea datelor transmise de *DIPI*, precum și legalitatea măsurilor adoptate în cadrul acțiunilor solicitate de la *DIPI;*

g) să asigure păstrarea confidențialității privind datele tehnice ale MAI referitoare la arhitectura actuală și evoluția rețelei de comunicații de date pe care o gestionează sau o va gestiona în viitor, date de care a luat la cunoștință în baza prezentului Acord;

h) să nu întreprindă acțiuni care vizează împiedicarea proiectării, dezvoltării sau funcționării sistemelor IT sau de comunicații ale *MAI.*

i) să anonimizeze toate datele primite din partea DIPI dacă acestea vor fi disponibilizate către terți.

Art.13 – *DIPI* are următoarele obligaţii:

a) de a transmite către CNC informaţiile relevante din punct de vedere al securității cibernetice naționale, informații stabilite de comun acord pentru detectarea, prevenirea şi contracararea atacurilor cibernetice ce pot periclita securitatea națională;

b) de a pune la dispoziția CNC datele și informațiile relevante pentru derularea unor investigații în spațiul cibernetic sau derulării activităților de evaluare a securității cibernetice realizate la solicitarea ministerului.

CAPITOLUL V – Caracterul confidenţial al Acordului

Art.14 – O Parte semnatară a Acordului nu are dreptul, fără acordul prealabil scris al celeilalte Părţi:

a) de a face cunoscut Acordul sau orice prevedere a acestuia unei terţe părţi, în afara acelor persoane implicate în îndeplinirea Acordului;
b) de a utiliza informaţiile şi documentele obţinute sau la care are acces în perioada de derulare a Acordului, în alt scop decât acela de a-şi îndeplini obligaţiile prevăzute în Acord;
c) de a transmite datele şi informaţiile obţinute în baza Acordului, către terţi.

Art.15 – Dezvăluirea oricărei informaţii faţă de persoanele implicate în îndeplinirea Acordului se realizează numai în măsura în care este necesar în vederea îndeplinirii Acordului.

Art.16 – Partea semnatară a Acordului, care dezvăluie informaţii referitoare la acesta, este exonerată de răspundere în cazul în care:
a) informaţia era cunoscută Părţii înainte ca ea să fi fost primită de la cealaltă Parte sau,
b) informaţia a fost dezvăluită după ce a fost obţinut acordul scris al celeilalte Părţi pentru asemenea dezvăluire sau,
c) partea semnatară avea obligaţia, potrivit legii, să comunice informaţia.

CAPITOLUL VI – Dispoziţii finale

Art.17 – **(1)** În scopul cooperării în baza prezentului Acord, Părțile vor folosi următoarele date de contact:

1. **DEPARTAMENTUL DE INFORMAŢII ŞI PROTECŢIE INTERNĂ din cadrul MINISTERULUI AFACERILOR INTERNE**

CENTRUL DE RĂSPUNS AL MAI LA INCIDENTE DE SECURITATE IT (CERT-INT)

Adresa: Strada Răzoare nr.5, sector 6, Bucureşti;

Telefon: 021.311.22.40;

Fax: 021.311.13.53;

E-mail: cert-int@dipi.ro

2. **CENTRUL NAŢIONAL CYBERINT (CNC) din cadrul SERVICIUL ROMAN DE INFORMATII**

Adresa: Strada Splaiul Independenţei nr. 323A, sector 6, Bucureşti

Telefon/Fax: 0377.724.902

E-mail: cnc@cyberint.ro

(2) Acordul va fi interpretat conform legilor din România.

Art.18 – Părţile vor depune toate eforturile pentru a soluţiona pe cale amiabilă, prin tratative directe, orice neînţelegere sau dispută care poate apărea în cadrul sau în legătură cu prezentul Acord.

Art.19 – Prezentul Acord intră în vigoare la data semnării de către ambele Părţi.

Art.20 – **(1)** Oricare dintre Părţile semnatare poate suspenda, motivat, aplicarea prezentului Acord, prin notificare scrisă adresată celeilalte părţi.

(2) Suspendarea va produce efecte începând cu data indicată în respectiva notificare.

Art.21 – Părţile vor conveni asupra eventualelor modificări sau completări ale prezentului Acord, prin încheierea de acte adiţionale.

Art.22 – **(1)** Oricare dintre Părţile semnatare poate denunţa prezentul Acord prin notificare scrisă adresată celeilalte Părţi.

(2) Denunţarea va produce efecte în termen de 30 de zile de la data primirii unei astfel de notificări.

Art.23 – Anexele 1 şi 2 fac parte integrantă din prezentul Acord.

Art.24 – Prezentul Acord a fost încheiat în 2 (două) exemplare originale, câte unul pentru fiecare Parte.

DIN PARTEA
CENTRULUI NAŢIONAL CYBERINT

DIRECTOR

[redacted]

DIN PARTEA
DEPARTAMENTULUI DE INFORMAŢII ȘI PROTECŢIE INTERNĂ

[redacted]

AVIZAT [redacted] ALITATE

[redacted]

[redacted] NTRU LEGALITATE

[redacted]

GLOSAR DE TERMENI TEHNICI

- *informaţii de tip log* – informaţii privind funcţionarea unor sisteme, echipamente sau aplicaţii IT;
- *informaţii de tip log referitoare la atacuri cibernetice* – informaţii privind acţiuni nelegitime efectuate asupra unor sisteme, echipamente sau aplicaţii IT;
- *spam* – mesaje electronice nesolicitate;
- *filtre anti-spam* - sisteme ce realizează procesarea automată a mesajelor electronice, având ca scop identificarea şi înlăturarea mesajelor de tip spam;
- *NetFlow* – protocol dezvoltat de Cisco Systems pentru colectarea informaţiilor despre traficul IP;
- *servere de tip syslog* – servere folosite pentru colectarea informaţiilor de tip log obţinute de la mai multe tipuri de sisteme, într-un format standardizat;
- *ssh* – protocol de reţea ce permite schimbul de date între două echipamente de reţea folosind un canal securizat; criptarea folosită de protocolul ssh asigură confidenţialitatea şi integritatea datelor;
- *sftp, ftps* – protocoale de reţea ce permit transferul fişierelor între echipamente de reţea folosind un canal securizat;
- *infrastructură de tip PKI* – sistem informatic ce asigură integritatea, autenticitatea, confidenţialitatea şi nerepudierea informaţiilor utilizând standarde de criptare şi semnare a datelor în format electronic utilizând chei publice;
- *https* – protocol de transfer securizat al datelor .

1. Persoane responsabile din partea **CNC**

Nr. crt.	Nume şi Prenume	Funcţia	Adresă email	Telefon
1.	[redacted]	Director	[redacted]	[redacted]
2.		Director adjunct		
3.		Responsabil departament securitate IT		
4.		Responsabil departament securitate IT		
5.		Responsabil departament securitate IT		

2. Persoane responsabile din partea **DIPI**

Nr. crt.	Nume şi Prenume	Funcţia	Adresă email	Telefon
1.	[redacted]	Director general adjunct	[redacted]	[redacted]
2.		Şef Birou CERT-INT		
3.		Şef Sector		

MULTIPLICAT
D.I.P.I.
RM 290 10
Data 29.04.2016 Ex. Nr. ....