Consiliul Superior al Magistraturii „garantul independenței justiției"	Centrul Național Cyberint
Nr. înregistrare I/27933/2014	Nr. înregistrare 443509/22.12.2014

Protocol

privind

COOPERAREA ÎNTRE CONSILIUL SUPERIOR AL MAGISTRATURII ȘI CENTRUL NAȚIONAL CYBERINT ÎN DOMENIUL SECURITĂȚII SISTEMELOR INFORMATICE ȘI DE COMUNICAȚII

încheiat azi, 18.12.2014

Preambul

Având în vedere:

Legea nr. 14/1992 privind organizarea și funcționarea Serviciului Român de Informații, cu modificările și completările ulterioare;

Legea nr. 161/2003 privind unele măsuri pentru asigurarea transparenței în exercitarea demnităților publice, a funcțiilor publice și în mediul de afaceri, prevenirea și sancționarea corupției, cu modificările și completările ulterioare – Titlu III – Prevenirea și combaterea criminalității informatice;

Legea nr. 677/2001 pentru protecția persoanelor cu privire la prelucrarea datelor cu caracter personal și libera circulație a acestor date;

Legea nr. 506/2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice, cu modificările și completările ulterioare;

Legea nr. 365/2002 privind comerțul electronic, cu modificările și completările ulterioare;

Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României și a Planului de acțiune la nivel național privind implementarea Sistemului național de securitate cibernetică;

Consiliul Superior al Magistraturii (CSM) și Centrul Național Cyberint (CNC), denumite, în continuare Părți, au decis încheierea prezentului Protocol de cooperare în domeniul securității sistemelor informatice și de comunicații, denumit în continuare Protocol.

CAPITOLUL I - Dispoziții generale

Art. 1 – Obiectul Protocolului îl reprezintă stabilirea:

a) condițiilor în care se face schimbul de informații între părți;

b) modalităților prin care acestea sunt transmise între părți;

c) cadrului general de cooperare între cele două părți în scopul identificării, alertării și prevenirii consecințelor incidentelor de securitate în care pot fi implicate serviciile informatice administrate de către Consiliul Superior al Magistraturii;

d) obligațiile pe care cele două părți și le asumă prin încheierea protocolului.

CAPITOLUL II - Categoriile de informații transmise

Art. 2 – (1) Consiliul Superior al Magistraturii transmite către Centrul Național Cyberint:

a) informații referitoare la atacurile cibernetice sau care reflectă incidente de securitate importante stabilite ca având acest caracter de comun acord de către părți, furnizate de sistemele proprii de supraveghere a rețelei și serviciilor de comunicații electronice, cum ar fi sisteme de detectare/prevenire a accesului neautorizat, filtre anti-spam, sisteme de auditare a stării de securitate etc;

b) mesajele de email tip spam stocate de serverele de poștă electronică stabilite ca având acest caracter de administratorii de rețea și care nu reprezintă trafic al utilizatorilor din rețeaua instituției;

c) la solicitare, mesajele de tip NetFlow provenite de la serverele conectate în rețelele furnizorilor de servicii de telecomunicații (upstream).

Art. 3 - Consiliul Superior al Magistraturii pune la dispoziția Centrului Național Cyberint, pentru a fi utilizate în cadrul unui honeypot dezvoltat de CNC conectat la rețeaua CSM, adrese IP relevante specifice diferitelor categorii de locații geografice, ce fac parte din clasele de adrese Ip alocate instituției.

Art. 4 – Centrul Național Cyberint transmite către Consiliul Superior al Magistraturii:

a) informații actualizate privind vulnerabilitățile sistemelor informatice și de comunicații, alerte și buletine de securitate, bune practici privind sporirea securității spațiului cybernetic, modul de gestionare a incidentelor de securitate, precum și alte informații care pot fi utilizate în prevenirea și reducerea numărului incidentelor de securitate;

b) rapoarte periodice cu privire la starea de securitate a rețelelor instituției bazate pe informațiile puse la dispoziție de Consiliul Superior al Magistraturii;

c) informații cu privire la amenințările cibernetice constatate sau cu privire la incidentele de securitate existente în cadrul rețelelor și serviciilor de comunicații electronice administrate sau aflate în proprietatea instituției, rezultate ca urmare evaluării securității informatice a rețelelor administrate sau aflate în proprietatea instituției, realizate de către CNC la solicitarea Consiliul Superior al Magistraturii.

Art. 5 – (1) Informațiile transmise între Consiliul Superior al Magistraturii și Centrul Național Cyberint nu reprezintă conținut al comunicărilor transmise de utilizatorii rețelei sau între aceștia.

(2) Centrul Național Cyberint nu are acces la conținutul documentelor Consiliului Superior al Magistraturii.

Art. 6 - Înțelesul termenilor tehnici utilizați în prezentul Protocol este specificat în Anexa 1.

CAPITOLUL III – Metode și mijloace de transmitere a informațiilor

Art. 7 – Conectarea între Consiliul Superior al Magistraturii și Centrul Național Cyberint se realizează prin linii de comunicații dedicate, ce urmează a fi definite în detaliu, de comun acord, prin eforturile ambelor părți, ulterior semnării prezentului protocol.

Art. 8 – (1) Liniile de comunicații sunt protejate prin criptare în urma acordului între Părți.

(2) Pentru realizarea criptării informației pe liniile de comunicații, Centrul Național Cyberint asigură echipamentul de criptare pentru ambele capete ale conexiunii.

(3) Prin excepție de la dispozițiile alin. (2), criptarea se poate realiza și prin echipamente care aparțin Consiliului Superior al Magistraturii, dacă acesta asigură mijloacele de criptare pentru ambele capete ale conexiunii.

Art. 9 – (1) Transmiterea informațiilor de la Consiliul Superior al Magistraturii către Centrul Național Cyberint se face atât în timp real, către unul sau mai multe servere de tip syslog din rețeaua CNC, cât și periodic prin transmiterea de fișiere folosind conexiuni, tunele sau programe de transfer de fișiere ce oferă un grad sporit de siguranță (ssh, sftp, ftps) către un server din rețeaua CNC sau prin email către una sau mai multe adrese de e-mail aparținând CNC.

(2) Transmiterea informațiilor prin e-mail se realizează de preferință criptat, folosind o infrastructură de tip PKI.

(3) Transmiterea informațiilor se poate face și *on line*, folosind protocoale securizate (de exemplu, dar nu limitat la https).

Art. 10 - Transmiterea informațiilor de la Centrul Național Cyberint către Consiliul Superior al Magistraturii se face:

a) periodic, prin transmiterea de informații și/sau fișiere către adresele de e-mail de contact specificate în Anexa 2 a prezentului Protocol; transmiterea informațiilor prin e-mail se realizează de preferință criptat, folosind o infrastructură de tip PKI;

b) atunci când este cazul, prin transmiterea de fișiere folosind conexiuni sau programe de transfer de fișiere ce oferă un grad sporit de siguranță;

c) prin intermediul portalului www.cyberint.ro.

Capitolul IV – Obligațiile Părților

Art. 11 – (1) Părțile au următoarele obligații comune:

a) să desemneze persoanele de contact, ce pot pune în practică solicitările Părților și prin intermediul cărora se va face schimbul de informații;

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

(2) Lista persoanelor menționate la alin. (1) este prevăzută în Anexa 2 la prezentul Protocol.

Art. 12 – CNC are următoarele obligații:

a) să realizeze, la solicitarea Consiliului Superior al Magistraturii, evaluarea securității informatice a rețelelor administrate sau aflate în proprietatea acestuia și să informeze Consiliu cu privire la amenințările cibernetice constatate sau cu privire la incidentele de securitate existente în cadrul rețelelor și serviciilor de comunicații electronice administrate sau aflate în proprietatea instituției;

b) să ofere suport pentru definirea și actualizarea politicilor de securitate în cadrul rețelelor de interes pentru Consiliului Superior al Magistraturii;

c) să ofere suport pentru întocmirea și actualizarea procedurilor de intervenție în caz de incident sau atac cibernetic în cadrul Consiliului Superior al Magistraturii;

d) să ofere sprijin în situații de criză generală 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;

e) să asigure respectarea prevederilor legale în cadrul operațiunilor privind colectarea datelor transmise de Consiliul Superior al Magistraturii, precum și legalitatea în cadrul acțiunilor solicitate de Consiliu;

f) să asigure păstrarea confidențialității privind datele tehnice relevante referitoare la arhitectura actuală și evoluția rețelei de comunicații de date pe care Consiliul Superior al Magistraturii o gestionează sau o va gestiona în viitor, date de care a luat la cunoștință în baza prezentului Protocol;

g) să nu întreprindă acțiuni care vizează împiedicarea dezvoltării sau funcționării rețelei de comunicații de date a Consiliului Superior al Magistraturii.

Art. 13 – Consiliul Superior al Magistraturii are următoarele obligații:

a) să nu blocheze sau să filtreze transmiterea către Centrul Național Cyberint a informațiilor relevante stabilite de comun acord pentru detectarea, prevenirea și contracararea atacurilor cibernetice;

b) să nu alterneze informațiile transmise către Centrul Național Cyberint. Acestea vor fi în formatul original, furnizat de sistemele/aplicațiile de securitate IT ale instituției. Excepție fac datele a căror transmitere ar afecta caracterul privat al comunicațiilor;

c) să trateze informațiile furnizate de Centrul Național Cyberint în funcție de indicațiile acestuia pentru operarea serviciului de securitate;

d) să întreprindă măsurile legale pentru a preveni și limita activitățile ce constituie incidente de securitate cibernetică;

e) să pună la dispoziția Centrului Național Cyberint datele și informațiile disponibile în cadrul rețelelor proprii, necesare derulării unor investigații în spațiul cibernetic;

f) să pună la dispoziția Centrului Național Cyberint datele și informațiile disponibile în cadrul rețelelor proprii, necesare derulării activităților de evaluare a securității cibernetice realizate la solicitarea Consiliului Superior al Magistraturii.

Capitolul V – Caracterul confidențial al unor prevederi ale Protocolului

Art. 14 – (1) Orice parte semnatară a protocolului nu are dreptul să dezvăluie terților, fără acordul prealabil scris al celeilalte părți:

a) prevederile din cuprinsul Protocolului care se referă la măsuri/specificații de ordin tehnic sau la informațiile care rezultă din aplicarea dispozițiilor protocolului;

b) de a utiliza informațiile și documentele obținute sau la care are acces în perioada de derulare a protocolului, în alt scop decât acela de a-și îndeplini obligațiile prevăzute în protocol.

(2) Partea semnatară a Protocolului, care dezvăluie informațiile prevăzute la alin. (1) este exonerată de răspundere dacă avea obligația, potrivit legii, să comunice informația.

CAPITOLUL VI – Dispoziții finale

Art. 15 – Protocolul va fi interpretat conform legilor din România.

Art. 16 – Părțile vor depune toate eforturile pentru a soluționa pe cale amiabilă, prin tratative directe, orice neînțelegere sau dispută care poate apărea în cadrul sau în legătură cu prezentul protocol.

Art. 17 – Prezentul protocol intră în vigoare odată cu semnarea lui și este încheiat pe o perioadă nedeterminată.

Art. 18 – (1) Fiecare parte semnatară poate suspenda, din motive temeinice, aplicarea prezentului protocol, prin notificare scrisă adresată celeilalte părți.

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

Art. 19 – Părțile vor conveni asupra eventualelor modificări sau completări ale prezentului protocol prin încheierea unor acte adiționale.

Art. 20 – (1) Oricare dintre părțile semnatare poate denunța prezentul protocol prin notificare scrisă adresată celeilalte părți.

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

Art. 21 – Anexele 1 și 2 fac parte integrantă din prezentul protocol.

Art. 22 – Prezentul protocol a fost încheiat în 2 (două) exemplare originale, câte unul pentru fiecare parte.

Președintele
Consiliului Superior al Magistraturii
Judecător dr. Adrian BORDEA

Directorul
Serviciului Român de Informații
George – Cristian MAIOR

ANEXA 1

GLOSAR DE TERMENI TEHNICI

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

ANEXA 2

1. Persoane responsabile din partea Centrului Național Cyberint

Nr. crt.	Nume și prenume	Funcția	Adresă email	Telefon
1.				
2.				
3.				
4.				
5.				

2. Persoane responsabile din partea Consiliului Superior al Magistraturii

Nr. crt.	Nume și prenume	Funcția	Adresă email	Telefon
1.				
2.				
3.				

ANEXA 3

Cursuri de pregătire pentru administrarea tehnologiilor şi aplicaţiilor implementate prin proiect, care urmează a fi organizate pentru persoanele cu pregătire tehnică de specialitate din cadrul Consiliului Superior al Magistraturii

Nr. Crt.	Perioadă	Denumire curs[1]
1.	24.11 – 28.11.2014	• Curs pentru administrarea soluţiei WEB Gateway • Curs pentru administrarea soluţiei Router
2.	01.12 – 5.12.2014	• Curs pentru administrarea soluţiei Email Gateway • Curs pentru administrarea soluţiei de monitorizare a traficului de reţea
3.	8.12 – 12.12.2014	• Curs pentru administrarea soluţiei Firewall • Curs pentru administrarea soluţiei Switch
4.	15.12 – 19.12.2014	• Curs pentru administrarea soluţiei IDS/IPS • Curs pentru administrarea soluţiei UTM
5.	05.01 – 09.01.2015	• Curs pentru administrarea soluţiei Web Application Firewall • Curs pentru administrarea soluţiei Network Vulnerability Management
6.	12.01 – 16.01.2015	• Curs pentru administrarea soluţiei Web Application Vulnerability Management • Curs pentru instalarea şi administrarea serverului, a mediului virtualizat open source şi a sistemului de transfer unidirecţional al datelor
7.	19.01 – 23.01.2015	• Curs pentru administrarea soluţiei EndPoint Security • Curs pentru administrarea soluţiei Unified Security Management
8.	26.01 – 30.01.2015	• Curs pentru administrarea soluţiei Device Control şi EndPoint Protection Suite • Curs pentru administrarea soluţiei System Information and Event Management

1 Fiecare tehnologie/aplicaţie de securitate informatică este prezentată într-o clasă de cursuri separată. Astfel, în fiecare săptămână, se desfăşoară cursuri în două clase paralele.