DISPOZIȚIE

Nr. I.18 / 01.04.2013

COMITETUL DIRECTOR AL SOCIETĂȚII ROMÂNE DE RADIODIFUZIUNE

În temeiul prevederilor Legii nr. 41/1994 privind organizarea şi funcționarea Societății Române de Radiodifuziune şi Societății Române de Televiziune, republicată, cu modificările şi completările ulterioare;

În conformitate cu art. 5 alin. (1) lit. g), h) şi alin. (4) şi art. 22 alin. (3) din Regulamentul de organizare şi funcționare a Comitetului Director al Societății Române de Radiodifuziune şi a Comitetelor Directoare Teritoriale ale Unităților Funcționale Autonome, aprobat prin Hotărârea Consiliului de Administrație nr. 16/2011, republicat;

Potrivit art. 2 alin. (2) lit. c), art. 12 alin. (1), alin. (2) lit. e) şi alin. (4) din Procedura de Elaborare, Avizare şi Aprobare a Proiectelor de Hotărâri, Decizii şi Dispoziții, aprobată prin Ordinul Preşedintelui Director General nr. 123/2012;

Având în vedere prevederile HCA nr.105/2012 privind aprobarea limitelor de competență ale structurilor organizatorice din SRR privind angajarea patrimonială;

Având în vedere Nota de fundamentare nr. 77042/25.03.2013, elaborată de către Serviciul Tehnologia Informației şi Comunicații Departamentul Tehnic;

În urma analizei, dezbaterii şi realizării consensului cu privire la documentele prezentate la pct ..I.4.... de pe ordinea de zi a şedinței din data de..01.04...2013,

adoptă prezenta

DISPOZIȚIE:

Art.1. – (1) Se aprobă inițierea procedurii de achiziție a unor **"Servicii de siguranță informatică"**, conform OUG nr.34/2006, privind achizițiile publice, cu modificările şi completările ulterioare.

(2) Valoarea contractului se estimează la suma de **430 000 lei,** (exclusiv TVA), echivalentul a **95 556 euro**, (exclusiv TVA), la cursul de **4,5 lei/euro**.

Art. 2 – Departamentul Economic, în considerarea competențelor specifice, va face demersurile necesare ducerii la îndeplinire a activităților prevăzute la art.1, cu respectarea legislației incidente şi vor informa Comitetul Director, în legătură cu lansarea şi finalizarea procedurii de achiziție publică.

Pentru conformitate,
Ovidiu MICULESCU
Preşedinte Director General

AVIZATORI

Compartiment	**Nume reprezentant**	**Mențiuni**
Departamentul Tehnic	Constantin Burloiu	
Departamentul Economic	Constantin Puşcaş	
Serviciul Juridic	Mariana Milan	

Radio România
DEPARTAMENTUL TEHNIC
SERVICIUL TEHNOLOGIA
INFORMATIEI SI COMUNICATII

Str. General Berthelot, Nr. 60-64,
RO-010165, Bucureşti, România
tel: + 4021-303 17 52
fax: + 4021-312 10 56

Nr. 77042 /25.03.2013

Notă de fundamentare

1. Denumirea achiziţiei: - Servicii de siguranţă informatică

2. Cod CPV: 72910000-2 Servicii de siguranţă informatică

3. Cantitatea: 1 buc.

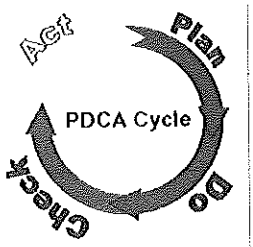
4. Poziţia în PAAP :
Serviciile solicitate sunt cuprinse în PAAP-2013, Anexa 2-Servicii - poz 92.

5. Valoarea estimata (lei / euro, fără TVA):
Suma previzionată este de 430000 lei echivalentul a 95 556 euro.

6. Procedura de achiziţie şi criteriul de atribuire:
Procedura de achiziţie este *„Cerere de oferte".*
Criteriul de atribuire este *"Preţul cel mai scazut".*

7. Termen necesar / estimat de finalizare a procedurii:
Termenul estimat de finalizare a procedurii este 30.Iunie.2013

8. Tip achiziţie: periodică
In conformitate cu *Strategia de protecţie a informaţiei în SRR* aprobată de către Consiliul de Administraţie din 16 ianuarie 2008, întreţinerea stării de protecţie a informaţiei este o activitate interdepartamentală **permanentă** şi se realizează pe baza unui sistem de tip „Plan Do Check ACT"



Astfel, achiziţia de „Servicii de siguranţă informatică" este periodică.

9. Descrierea serviciilor

Serviciile de siguranţă informatică cuprind următoarele elemente:
1. Protecţie antivirus pentru servere şi staţii de lucru, mail şi web
    a. Protecţia antivirus se realizează printr-o soluţie antimalware de mare complexitate instalată şi optimizată de către furnizor dar administrată de către specialiştii din SRR in conformitate cu evoluţia ameninţărilor din internet
        i. Sistemul asigură următoarele funcţionalităţi

1. Funcționalități anti-virus, anti-spyware, anti-ppm (Ppm - programe potențial malițioase)
2. Funcționalități de prevenire a intruziunilor şi firewall, controlul accesului in rețea, blocarea aplicațiilor neautorizate
3. Funcționalități de control al dispozitivelor externe care se pot conecta la calculatoare

b. Protecția la nivel de mail se realizează printr-un sistem specializat, care preia tot traficul de mail şi pune in carantină mesajele care conțin viruşi sau spam. Sistemul protejează toate serverele de mail din SRR pe domeniile:
   i. @radioromania.ro,
   ii. @rornet.ro,
   iii. @srr.ro
   iv. @jurnalist.srr.ro
   v. @rri.ro
   vi. @rador.ro
   vii. @gaudeamus.ro
   viii. @romania-muzical.ro
   ix. @politicaromaneasca.ro
   x. @radioromaniajunior.ro

   Soluția va fi instalată şi optimizată de către furnizor dar administrată de către specialiştii din SRR in conformitate cu evoluția amenințărilor din internet

c. Protecția la nivel de web se realizează printr-un sistem specializat, care preia tot traficul de web şi opreşte codurile răuvoitoare. De asemenea sistemul opreşte accesul utilizatorilor la site-uri web periculoase şi la cele care incalcă politicile şi regulamentele din SRR, de exemplu site-uri cu conținut pornografic.

   Soluția va fi instalată şi optimizată de către furnizor dar administrată de către specialiştii din SRR in conformitate cu evoluția amenințărilor din internet şi a necesităților proceselor de producție ale instituției.

2. Servicii de actualizare şi suport pentru Firewall-ul deținut de către SRR, care indeplineşte următoarele funcții:
   a. Firewall intre rețeaua internet şi rețelele interne ale SRR
      i. Permite doar trafic autorizat intre internet şi serverele din zona demilitarizată
      ii. Realizează translația intre rețele astfel incât utilizatorii din SRR să aibă accces la internet folosind adrese proprii private
   b. Sistem de prevenire a intruziunilor cu funcția de a opri trafic specific unei game largi de exploituri. Exploit-urile sunt programe sau metode prin care pe calculatoarele victimă se obțin drepturi de acces, scriere, execuție, ce contravin modului in care a fost proiectat, configurat respectivul calculator.
   c. Sistem de control al aplicațiilor care comunică in internet cu rolul de a opri comunicația aplicațiilor neautorizate sau periculoase.
   d. Sistem de acces securizat de tip VPN din exterior in rețeaua SRR.
   e. Sistem de management a componentelor de mai sus.

10. Necesitatea si oportunitatea achizitiei:

(rezumat semnificativ al referatelor de necesitate si oportunitate, locul de utilizare, operatiuni efectuate, beneficii aduse)

Necesitatea achiziției se regăseşte în *„Strategia de protecție a informației în SRR"* aprobată de Consiliul de Administrație în data de 16 ianuarie 2008.
Prin achiziția serviciilor de protecție se urmăreşte:

- Apărarea instituției față de situația ilegală in care din sistemul informatic al SRR s-ar efectua atacuri informatice in internet cum ar fi atacurile deny of service, răspândirea de viruşi sau de mesaje nesolicitate,
- Implementarea *Politicilor de protecție a informației din sistemul informatic al SRR,*
- Apărarea sistemului informatic impotriva viruşilor, a spyware-ului, blocarea programelor potențial periculoase cum ar fi cele de tip password crackers, key loggers precum si apărarea împotriva atacurilor din rețea,
- Apărarea utilizatorilor sistemului informatic.

Facem mențiunea că informația şi sistemul informatic ca suport al informației sunt supuse următoarelor amenințări:

- *interne, generate de*:
  - utilizatorii sistemului (angajați, colaboratori şi furnizori de servicii)
  - coduri ostile (viruşi, viermi, troieni, boți, etc.)
- *externe, generate de*:
  - penetrări neautorizate ale sistemului informatic;
  - coduri ostile (viruşi, viermi, troieni, boți, etc.).

Infectarea cu coduri ostile poate produce o multitudine de efecte cu impact semnificativ asupra activităților şi proceselor din Societatea Română de Radiodifuziune.
Enumerăm câteva dintre riscurile asociate acestor infecții:

1. *riscuri directe*:
   a. blocarea sistemului informatic respectiv a sistemelor de emisie radio;
   b. implicarea instituției in rețelele de criminalitate informatică;
2. *riscuri indirecte*:
   a. pierderea de date şi crearea de avantaje competitive pentru alte companii media;
   b. inlocuirea materialelor audio ce urmează a fi difuzate cu mesaje ce pot afecta ordinea şi siguranța publică.

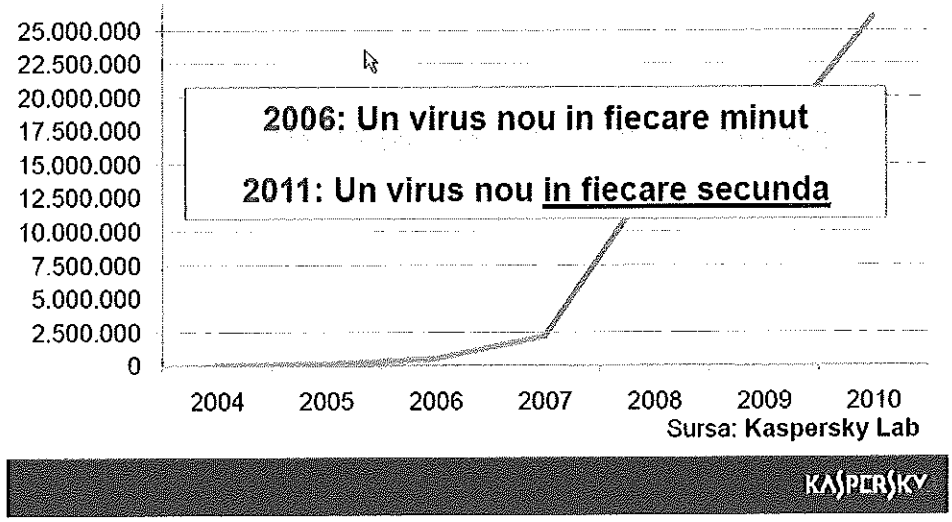
Achiziția de Servicii de siguranță informatică are următoarele componente:

a. protecție antivirus pentru servere şi stații de lucru
b. protecție antimalware mail şi antispam pentru mail
c. protecție antimalware WEB cu URL filtering
d. servicii de actualizare şi suport pentru Firewall

Sistemul de protecție antivirus

Pentru a evidenția gravitatea amenințărilor virale in mediul informatic, prezentăm anunțul companiei Kaspersky, care in 2011 in cadrul conferinței IDC Security Roadshow, arăta că la fiecare secundă se descoperă un virus nou.

▸ Kaspersky Lab proceseaza mai mult de 70.000 de programe periculoase (virusi, troieni, viermi, adware, etc) in fiecare zi



Toate calculatoarele conectate in rețea sau la internet sunt supuse amenințării de a se infecta cu programe periculoase.

Riscul de infecție creşte cu mai mult de 3600 de viruşi noi in fiecare oră.

Sistemul de protecție antivirus pentru servere şi stații de lucru este necesar pentru minimizarea riscurilor legate de infectarea serverelor şi calculatoarelor din SRR cu codurile ostile. De asemenea sistemul implementează politica **E.18. Apărare împotriva virușilor şi a intruziunilor în calculatoare** din *„Politicile de protecție a informației din sistemul informatic al SRR"*, politici aflate in vigoare din 01 martie 2008.

Internetul este, in primul rând, cea mai mare comunitate de oameni. Din păcate, această comunitate inocentă, este o adevărată mină de aur pentru o intreagă industrie a fraudei electronice. Se disting următoarele categorii de activități caracteristice acestei industrii:

1. activități comerciale
    a. SPAM-ul reprezintă o industrie in care se vehiculează sute de milioane de euro.
    b. SPAM-ul are ca vectori de transport calculatoarele controlate de catre industria fraudei electronice, prin coduri malițioase.
2. atacuri asupra persoanelor
    a. Phishing-ul reprezintă o formă de activitate criminală care constă in obținerea unor date confidențiale cu scopul principal de a fura din conturile bancare ale victimelor.
3. atacuri cu intindere limitată asupra unor companii
    a. spionaj informatic
    b. alterarea sau distrugerea informațiilor
    c. blocarea activității prin blocarea sistemelor informatice
4. acțiuni teroriste cu efecte majore
    a. la nivelul companiilor media, se pot insera in fişierele audio ce urmează să fie emise, mesaje care pot incita la violențe stradale, pot genera panică etc.
    b. tot prin intermediul sistemelor informatice pot fi afectate grav centrale electrice, sisteme de ditribuție, sau orice sistem informatizat care este vital pentru desfăşurarea activităților cotidiene.

O foarte mare parte a infracţiunilor informatice se bazează pe mediul de transport e-mail.

Sistemul de protecţie antimalware mail şi antispam

Statisticile companiei CISCO estimează că circa 85% din traficul de global de mesaje e-mail este SPAM.

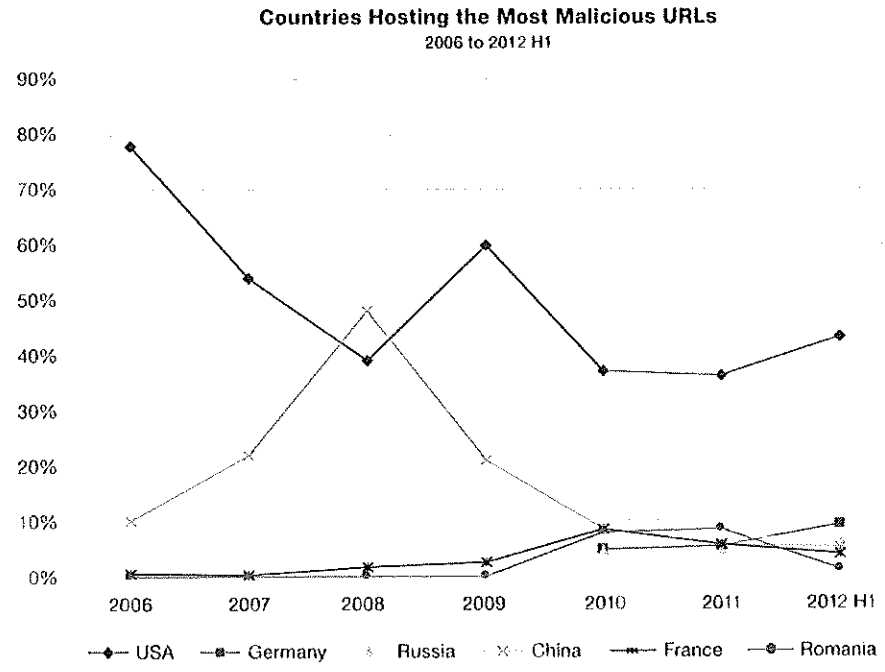
Month	Average Daily Volume (Billions)	% of Global Email Volume	Spam Volume Change
2013 January	77.3	85.5%	-10% ↓
2012 December	86.6	85.5%	-5% ↓
2012 November	91.5	85.3%	15% ↑
2012 October	79.5	85.2%	1% ↑
2012 September	78.5	85.4%	-10% ↓
2012 August	87.8	85.2%	-14% ↓

Sursa:
http://www.senderbase.org/home/detail_spam_volume?displayed=last18months&action=&screen=&order=

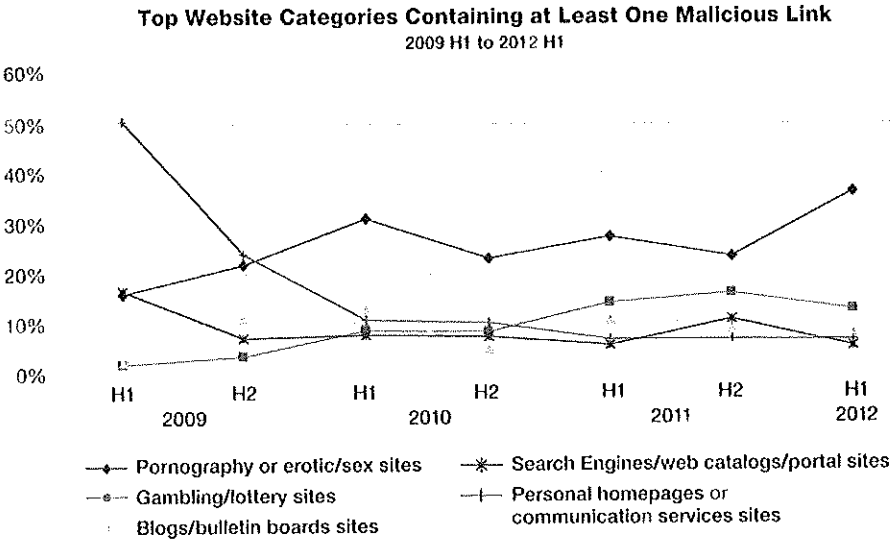
Sistemul de protecţie antimalware mail şi antispam pentru mail are ca scop protejarea sistemului informatic şi a utilizatorilor faţă de ameninţările informatice asociate poştei electronice, respectiv coduri ostile, mesaje nesolicitate, diverse excrocherii (social engineering). De asemenea sistemul implementează politica **E.14. Folosirea sistemelor de poştă electronică (E-mail) .**

Sistemul de protecţie antimalware WEB

O foarte mare parte a infracţiunilor informatice se bazează pe coduri malitioase plasate pe site-uri web. De cele mai multe ori victima se infectează cu asemenea coduri, fără să vrea şi fără să fie conştientă de pericol. Aceste probleme globalizate din punct de vedere geografic, se regăsesc pe toate categoriile de site-uri.



Source: IBM X-Force® Research and Development



Source: IBM X-Force® Research and Development

Sistemul de protecţie antimalware WEB cu URL filtering are ca scop minimizarea riscurilor legate de infectarea serverelor şi calculatoarelor din SRR cu codurile ostile. De asemenea sistemul implementează politica de securitate **E.12. Folosirea acceptabilă a internetului şi restricţii.**

Servicii de actualizare şi suport pentru Firewall

Pentru a se asigura o protecţie de înalt nivel este necesar să se folosească tehnologii care au la bază cea mai bună expertiză din domeniu.
Soluţia Firewall deţinută de către SRR fiind produsă de către CheckPoint, compania care a produs primul firewall funcţional, este una dintre cele mai performante soluţii la nivel mondial cu numeroase aprecieri intrenaţionale. http://www.darkreading.com/security/news/208803808/who-invented-the-firewall.html
In cei trei ani de la achiziţia iniţială soluţia a funcţionat conform aşteptărilor, foarte bine.
De asemenea, soluţia a evoluat continuu de la versiunea R70 la R75.30. Această evoluţie este necesară pentru a ţine pasul cu evoluţia ameninţărilor din mediul informatic, şi a constat atât in dezvoltarea motoarelor de protecţie cât şi a semnăturilor necesare componentei de prevenire a intruziunilor.

Soluţia este necesară pentru indeplinirea următoarelor funcţii:

1. Firewall intre reţeaua internet şi reţelele interne ale SRR
   a. Permite doar trafic autorizat intre internet şi serverele din zona demilitarizată
   b. Realizează translaţia intre reţele astfel incât utilizatorii din SRR să aibă accces la internet folosind adrese proprii private
2. Sistem de prevenire a intruziunilor cu funcţia de a opri trafic specific unei game largi de exploituri. Exploit-urile sunt programe sau metode prin care pe calculatoarele victimă se obţin drepturi de acces, scriere, execuţie, ce contravin modului in care a fost proiectat, configurat respectivul calculator.
3. Sistem de control al aplicaţiilor care comunică in internet cu rolul de a opri comunicaţia aplicaţiilor neautorizate sau periculoase.
4. Sistem de acces securizat de tip VPN din exterior in reţeaua SRR.
5. Contribuie la implementarea tehnică a următoarelor politici din *„Politicile de protecţie a informaţiei din sistemul informatic al SRR"*, aflate in vigoare din 01 martie 2008.:
   a. E.2. Securizare reţea
   b. E.8. Jocuri pe calculatoarele companiei
   c. E.9. Aplicaţiile de tip peer-to-peer (p2p) „file sharing" pe computerele SRR
   d. E.10. Aplicaţii de tip „Instant Messenger" pe computerele SRR
   e. E.12. Folosirea acceptabilă a internetului şi restricţii
   f. E.15. Apărarea împotriva acţiunilor ostile
   g. E.17. Apărarea împotriva hackerilor şi a codurilor ostile
   h. F.3. Securitate în reţea
   i. F.7. Accesul în reţea de la distanţă
   j. F.12. Monitorizarea accesului şi folosirii computerelor

Menţionăm faptul că în 1 iulie 2013 expiră contractul de suport din partea producătorului. Pentru ca SRR să beneficieze in continuare de toate actualizările de produs necesare din cauza evoluţiei pericolelor din internet, este necesar să se achiziţioneze aceste servicii de actualizare şi suport.

Inlocuirea soluţiei nu este eficientă deoarece serviciile de suport pentru firewall-ul existent sunt mai ieftine decât o soluţie nouă cu aceleaşi caracteristici de funcţionalitate şi performanţă.

Prin această achiziţie se vor proteja un numar de 1800 de echipamente ale SRR, circa 2500 de conturi de mail şi circa 1300 de utilizatori de web.

11. Acțiuni de prospectare a pieței, consultări:

Costul total al achiziției pe 1 an in valoare de 430000 lei fără TVA reprezentand circa 6 lei pe lună pentru fiecare utilizator, este compus din 2 elemente:

- Costul pentru protecția antivirus pentru calculatoare, mail şi web, estimat prin consultarea prețurilor publicate pe site-uri internet.
- Costul pentru actualizările necesare firewall-ului, estimat cu ajutorul instrumentului de cotații personalizate pentru clienți din portalul de suport de la producătorul Checkpoint.

12. Achiziții similare anterioare în SRR

Soluție anti-malware McAfee pentru stații servere şi gateway (mail şi web) – contract nr. 579/14.07.2008 in valoare de 69954 euro plus TVA pe o perioadă de 12 luni pentru protejarea a 1300 calculatoare şi a traficului de mail şi web

Soluție de protecție a informației – firewall – contract nr. 649/02.06.2010 in valoare de 239040.02 lei plus TVA pe o perioadă de 36 de luni

Servicii de protecție anti-malware pentru servere, stații de lucru, e-mail şi web – contract A0990/05.09.2011 (SRR 901/30.08.2011) in valoare de 233000 lei plus TVA pe o perioadă de 12 luni pentru protejarea a 1800 calculatoare şi a traficului de mail şi web

13. Servicii similare în SRR:

- Pentru protectia antivirus servere, stații de lucru, mail şi web in SRR
  - SRR are un contract de servicii similare care expira in 2 aprilie 2013.
  - Serviciile au fost efectuate dar au ridicat o multitudine de probleme:
    a. Echipamentul folosit pentru protecția web funcționează in mod aleatoriu după cum rezultă din imaginile din anexa 1.
    b. Echipamentul folosit pentru protecția email greşeşte destul de mult in identificarea mesajelor nesolicitate lăsând să treacă spam. După notificarea emisă furnizorului pentru remedierea situației, acesta a activat o setare care creează intârzieri aleatoare la primirea mesajelor de către utilizatorii din SRR.
    c. Ca soluție antivirus pentru stații si servere a fost instalat un produs de la Kaspersky. Aceasta are următoarele deficiențe:
       a. Blocheaza aleatoriu diverse programe sau functii din windows.
          i. Ex. a blocat word, excel, powerpoint, sap, prezența, remote desktop connection.
       b. Nu respectă configurarile efectuate de către administrator.
          i. Ex. sterge constant vnc server desi este setat sa il lase sa ruleze.
       c. Nu respecta excluderile de scanare
       d. Comunicarea dintre serverul de administrare si clienti este defectuoasa.
          i. Ex. trebuie sa fortezi de 3 ori sincronizarea intre server si o statie ca sa vada starea reala buna a unei statii pe care initial o arata in stare critica

e. Nu este in stare sa isi indeplineasca sarcinile programate decat pe calculatoare noi.
    i. De ex. se blocheaza daca incerci sa-l instalezi de pe serverul de administrare dar pe statii gaseste in registry urme de bitdefender desi acesta nu mai este prezent pe statiile respective.
d. Ultima versiune incarcă foarte mult stațiile de lucru ingerunând funcționarea acestora.
e. **In data de 4.02.2013 din cauza unei erori a producătorului, a fost blocată funcționarea agenției de presă RADOR timp de 3 ore.**

- Sistemul firewall CheckPoint existent in SRR funcționează foarte bine dar contractul de suport expiră la 1 iulie 2013

14. Alte informații / documente considerate relevante.

- Documentele relevante sunt :
    a. Strategia de protecție a informației în SRR
    b. Politici de protecție a informației din sistemul informatic al SRR

Întocmit,
ing. Dan Nistor, MSc InfoSec, CISM, CRISC

Şef serviciu Tehnologia Informației şi Comunicații,
ing.Şapcaliu Gheorghe