

Raport privind crearea unei unități guvernamentale CERT (Computer Emergency Response Team) în România *10-Feb-2005*

Mulțumiri:

Liviu Nicolescu – MCTI

Iulia Bumbac – MCTI

Gheorghe Șerban –ANISP

Pentru aportul lor la acest document

Având în vedere situația actuală din domeniul securității IT atât la nivel global, cât și la nivel național unde tot mai multe sisteme informatice sunt implementate în diverse instituții ale statului, considerăm că o unitate de tip CERT (Computer Emergency Response Team) dedicată sectorului guvernamental românesc devine o necesitate.

Prezentul raport, inițiat de proiectul RITI dot-Gov, prezintă principalele aspecte ce trebuie avute în vedere pentru o acțiune în acest sens.

Despre unitățile CERT (Computer Emergency Response Team)

La 2 noiembrie 1988 cinci la sută din aproximativ 85,000 de utilizatori ai Internet-ului au avut de a face cu prăbușiri fatale ale sistemelor. Primul incident internațional major pe Internet a devenit cunoscut ca viermele Internet sau Morris, după numele programatorului care a scris și lansat incidentul. Departamentul Apărării SUA a hotărât că un astfel de eveniment nu trebuie să se mai întâmple vreodată și, în 1989, a creat prima unitate CERT (Computer Emergency Response Team) cunoscută acum ca CERT CC (Centrul de coordonare CERT - CERT Co-Ordination Centre) www.cert.org.

Activitățile CERT au în vedere prevenirea și detectarea incidentelor de securitate IT, dar și informarea în legătură cu acestea. CERT este abrevierea cuvintelor Computer Emergency Response Team (Echipă de Răspuns pentru Incidente de securitate din domeniul IT). Centrele de tip CERT cooperează prin asigurarea de informații legate de incidente de securitate pentru utilizatorii sistemelor informaționale prin intermediul Internet-ului. Scopul activităților CERT este prevenirea amenințărilor de securitate la adresa sistemelor informaționale și răspunsul la amenințări, pe cât de obiectiv și eficient posibil.

Incidente de securitate legate de computer înseamnă situații în care sunt schimbate ilicit disponibilitatea, integritatea sau confidențialitatea informațiilor gestionate de sistemele informaționale ale unei organizații, companii, asociații sau persoane private. Aceste incidente pot include, de exemplu, împiedicarea voită a funcționării sistemului informațional al unei alte persoane sau organizații. Un alt incident de securitate legat de

computer poate fi utilizarea fără permisiune a sistemelor informaționale ale unei organizații, companii, asociații sau utilizator.

În prezent, există în lume diferite tipuri de unități CERT în diverse tipuri de organizații. Acestea s-au format în sectorul privat, în sectorul public și uneori într-un parteneriat între sectorul privat și cel public.

Se pot identifica 3 tipuri majore de organizații CERT:

- private, care se ocupă doar de incidentele de securitate IT în cadrul unei companii sau a clienților acesteia (vezi BT CERT - <http://www.btcert.bt.com/>)
- CERT din rețelele academice și de cercetare (vezi SURFnet-CERT - <http://cert.surfnet.nl>)
- publice, care se ocupă de incidente de securitate IT în cadrul instituțiilor guvernamentale și, uneori, primesc plângeri și din partea publicului. Un rol important îl joacă serviciile pro-active. (vezi BSI – Bund - <http://www.bsi.bund.de/certbund/>)

Tendențe Internaționale

Cooperarea internațională dintre diversele tipuri de unități CERT din diverse țări și continente devine esențială în activitatea de securitate informatică. De obicei, există relații strânse între actualele unități CERT. Dar și cele noi sunt binevenite în această familie și pot beneficia de experiența și expertiza deja obținute.

Iată de ce este important să prezentăm structurile de cooperare internaționale majore:

FIRST

În 1990, unsprezece unități CERT (Computer Emergency Response Teams) în principal din armată, au format primii membrii fondatori ai FIRST (Forum al Echipelor de Răspuns la Incidente de Securitate). Astăzi, FIRST are 170 membri care formează o comunitate închisă și de încredere, de echipe care împărtășesc resurse tehnice dar și informații vitale în prevenirea și combaterea incidentelor de securitate prin Internet și rețele de calculatoare. În cadrul FIRST, organizațiile se consideră colaboratori mai degrabă decât competitori. În cadrul FIRST, unitățile CERT (Computer Emergency Response Teams) își unesc eforturile în protejarea propriilor nume, a reputației și datelor organizațiilor lor individuale.

TF-CSIRT

TF-CSIRT este un Task Force stabilit sub auspiciile TERENA, un program tehnic de promovare a colaborării între unitățile CSIRT (Computer Security Incident Response Teams) din Europa. Scopul acestui Task Force este de:

- a asigura un forum pentru schimb de experiență și cunoștințe
- a stabili servicii pilot pentru comunitățile europene CSIRT
- a promova standarde și proceduri comune de răspuns la incidentele de securitate

- a ajuta la stabilirea de noi unități CSIRT și la instruirea personalului acestora.

Activitățile TF-CSIRT se concentrează în Europa, în concordanță cu Specificațiile aprobate de Comitetul Tehnic TERENA la 15 Septembrie 2004.

TF-CSIRT are de asemenea disponibilă o listă extinsă a tuturor unităților CSIRT europene. Toate datele sunt prezentate fără nici un fel de garanție și sunt păstrate în mod pasiv de TERENA, cu excepția acelor date ale CSIRT-urilor „acreditate”.

Grupul European de unități CERT guvernamentale (EGC) - European Government CERTs (EGC) group

Grupul European de unități CERT guvernamentale (EGC) este un grup ne-formal de unități CERT guvernamentale care dezvoltă cooperarea între membrii săi pentru răspunsul la incidente, bazându-se pe similitudinile de componență și probleme stabilite între unitățile CERT guvernamentale din Europa.

Pentru a-și realiza scopurile, membrii grupului ECG:

- Dezvoltă în comun măsuri de răspuns la incidente de securitate la scară largă sau regională
- Facilitează schimbul de informații și tehnologie legate de incidente de securitate IT și posibile amenințări și vulnerabilități
- Identifică domeniile de cunoștințe și expertiză specializate care pot fi împărtășite în cadrul grupului
- Identifică domeniile de cercetare și dezvoltare, în colaborare, pe subiecte de interes comun
- Încurajează formarea de unități CSIRT guvernamentale în țările europene
- Comunică puncte de vedere comune cu alte inițiative și organizații.

Membrii actuali ai grupului de unități CSIRT europene guvernamentale sunt:

CERTA - Franța

CERT-Bund - Germania

CERT-FI - Finlanda

GOVCERT.NL - Olanda

SITIC - Suedia

UNIRAS – Marea Britanie

ENISA

Agenția Europeană de Securitate a Rețelelor și Informațiilor, ENISA, este o nouă agenție a Uniunii Europene care s-a înființat la 15 martie 2004.

Activitățile agenției sunt în primul rând îndreptate către atingerea unui grad ridicat de securitate IT în cadrul comunității europene. Agenția caută de asemenea să dezvolte o cultură a securității IT de care să beneficieze cetățenii, consumatorii, mediul de afaceri și organizațiile din sectorul public din Uniunea Europeană. Aceasta va contribui și la o bună funcționare a pieței interne.

Pe măsură ce va crește nivelul de expertiză din cadrul său, ENISA va susține Comisia, Statele membre și, prin urmare, comunitatea de afaceri în a răspunde la probleme de securitate IT și mai ales în a le preveni.

Agenția va ajuta de asemenea Comisia în activitățile pregătitoare pentru aducerea la zi și dezvoltarea legislației în domeniul securității IT.

Propunere RITI dot-Gov

Problematika securității sistemelor informaționale ale sectorului public în general și ale celui guvernamental în special a devenit o prioritate de nivel național.

MCTI a întreprins multe activități în crearea unui centru de răspuns la incidente de securitate IT, în cadrul oferit de Minister. În același timp, personalul din cadrul MCTI care se ocupă de incidente de securitate IT este angajat într-o mulțime de alte sarcini importante. Structura actuală ar putea probabil beneficia de o stabilitate organizatorică și o securitate financiară mai bună.

Pentru a identifica problemele majore ce trebuie luate în considerare, dar și pentru a învăța din experiența altor țări, RITI dot-Gov împreună cu reprezentanți ai MCTI și ai sectorului privat au făcut o vizită de studiu la SITIC, unitatea CERT din Suedia. **Anexa 1** a prezentului document conține un raport al acestei vizite care rezumă cadrul suedez de securitate IT și lecțiile ce pot fi învățate din experiența suedeză.

Prezentul document arată principalele concluzii privind dezvoltarea capacității de răspuns la incidente de securitate IT în România. Studiul se concentrează pe considerațiile principale care stau la baza propunerii RITI dot-Gov de a crea o unitate CERT românească guvernamentală independentă. S-a încercat identificarea problemelor majore care s-ar putea pune la crearea unei astfel de instituții și găsirea unor propuneri de soluționare a acestor probleme.

1) Politica românească de securitate IT

Contextul actual ne arată că interconectarea rețelelor publice cu cele private, convergența domeniilor media, IT și comunicații și folosirea comună a resurselor au crescut considerabil dificultatea de a obține un control adecvat asupra acestora. Mai mult, în unele cazuri proiectarea sistemelor informatice și de comunicații a fost făcută neglijându-se securizarea acestora.

Protejarea sistemelor informatice este esențială pentru fiecare sector al economiei. Obiectivele urmărite în acest sens sunt:

- prevenirea acțiunilor îndreptate împotriva sistemelor informatice și rețelelor de comunicații,
- reducerea vulnerabilității la aceste atacuri,
- minimizarea pagubelor și a timpului de recuperare în urma atacurilor;

Deși pe termen scurt securitatea presupune îndeplinirea atributelor de integritate, disponibilitate și confidențialitate, pe termen lung, pentru protecția valorilor organizațiilor și asigurarea continuității serviciilor sunt necesare măsuri:

- **Preventive:**
 - implementarea de controale în cadrul organizațiilor,
 - informarea și conștientizarea publicului,
 - crearea unei culturi naționale privind securitatea, pentru o mai ușoară identificare și conștientizare a riscurilor și amenințărilor,
 - coduri de conduită,
 - instruirea utilizatorilor,

- **Protective:**
 - măsuri tehnice de protecție, utilizarea de echipamente și dispozitive securizate;
 - reglementări,
 - planuri de recuperare în caz de dezastru,

- **De reacție / combatere:**
 - crearea și specializarea organismelor abilitate de lege,
 - răspuns prompt și coerent al autorităților la incidente
 - cooperare între sectorul public și cel privat,
 - cooperare internațională,

- **De revizuire și perfecționare continuă:**
 - controale periodice,
 - urmărirea progreselor tehnologice,
 - adaptarea la noile tehnologii;

Conform strategiei MCTI pentru anul 2025, ținând cont de tehnologiile prezente, dar și de practicile consacrate în ultimii 20 de ani în țările avansate, pot fi urmărite următoarele acțiuni:

- Construcție instituțională
- Implementarea infrastructurii PKI naționale
- Respectarea standardelor europene și internaționale
- Securitatea tranzacțiilor financiare dematerializate
- Controlul asupra produselor cu utilizare dublă
- Rețele și servicii sigure
- Monitorizarea evoluției și combaterea criminalității informatice

2) **Activități în sectorul privat în România**

În cadrul sectorului privat din România există semne vizibile că problematica “securității informatice” trebuie tratată cu multă seriozitate. În mai multe companii (în special mari)

și organizații din diverse sectoare de activitate au început să fie implementate sisteme și aplicații de securitate. Nu există un forum organizat de dezbatere a problematicii « securității IT », acest lucru făcându-se cu prilejul diverselor alte manifestări (a se vedea ROCS- Romanian Open Computer Show). De asemenea, nu există un mecanism de semnalare și analiză a incidentelor de securitate informatică la nivelul comunităților din diverse sectoare de activitate.

Considerăm ca ar trebui lăsat la latitudinea comunității de afaceri să decidă modalitățile prin care se poate crește securitatea IT pentru propriile soluții informatice.

În cele ce urmează ne vom referi la securitatea IT în ceea ce îi privește pe operatorii de comunicații electronice, ISP-iști în particular.

Există dezvoltate unele canale specifice de semnalare a unor incidente de securitate, dar fără să fie o uniformitate specifică – bazată pe un set de reguli. Considerăm că există de asemenea anumite legături și colaborări între operatorii acestor canale de comunicare, fiind însă puțin formalizate, dintr-o serie de motive :

- teama de înmulțire a atacurilor împotriva unei companii sau a alteia
- lipsa de investiții și de colaborare pentru crearea unor contacte regulate
- teama de o anumită reclamă negativă care s-ar putea face companiei care ar recunoaște că a suferit din pricina unor incidente de securitate.

Există canale de comunicare cu autoritățile competente ale statului. Dar sunt destul de multe situațiile în care incidentele de securitate, chiar dacă îmbracă forma unor infracțiuni sau contravenții, nu sunt raportate organelor competente pentru a acționa în acest sens.

Asociația Națională a Internet Service Providerilor din România, ANISP, are constituit un Grup de lucru pentru discutarea diverselor chestiuni legate de problematica securității comunicațiilor electronice. A existat o încercare la nivelul ANISP de creare a unui grup de lucru ne-formal mai larg (în sensul de atragere și a altor specialiști din afara listei membrilor asociației), care să încerce să adreseze problema securității informatice și care să dezvolte în timp mijloace de comunicare și de informare adecvate: recomandări în domeniul securității IT, un site specific etc.

Nu există la nivelul operatorilor de comunicații electronice, a ISP-iștilor în particular, ofițeri de securitate IT, persoane dedicate pe domeniul securității IT. De obicei aceste atribuții intră în sarcina unor administratori de rețea. ANISP crede însă că ar trebui să fie persoane dedicate, cu un profil profesional bine definit, cu responsabilități și resurse specifice, care să se ocupe de aceste aspecte privind prevenirea și combaterea incidentelor de securitate. Mai mult, aceștia trebuie să colaboreze într-un cadru organizat la nivelul comunității.

Există interes la nivelul ANISP de a iniția un grup de lucru pentru începerea discuțiilor în vederea creării unui organism de tip CERT la nivelul comunității furnizorilor de servicii electronice, în special a ISP-iștilor. Se speră să fie atrase și companii care oferă tehnologii și servicii de securitate.

S-au dezvoltat în sectorul privat și o serie de companii¹ care acordă diverse servicii legate de securitatea IT, unele dintre ele de tipuri asemănătoare cu cele pe care le poate oferi un CERT.

În domeniul bancar cele mai multe bănci au făcut public faptul că au implementat sisteme și aplicații de securitate. De asemenea, în mai multe organizații din diverse sectoare de activitate sunt implementate sisteme și aplicații de securitate. Nu există însă un mecanism de semnalare și analiză a incidentelor de securitate informatică la nivelul comunității sectoarelor de activitate.

3) Nevoia unui CERT la nivel guvernamental

În ultimii ani numărul sistemelor informatice instalate în diversele instituții aparținând administrației publice locale și centrale din România a cunoscut o creștere exponențială. Existența unui sistem informatic în cadrul unei primării sau a unui minister reprezintă, cu siguranță, o necesitate în ziua de azi.

Un astfel de sistem trebuie să aibă o componentă importantă legată de securitate, atâta vreme cât date personale și documente confidențiale sunt stocate și utilizate în cadrul sistemului informatic. În același timp, diversele proiecte de e-government implementate, ca și necesitatea de transparență în sectorului public, fac ca aceste sisteme informatice ale administrației publice să permită accesul public, în limita impusă de proiectele dezvoltate.

Ținând cont de aspectele prezentate mai sus, dar și de atacurile informatice tot mai diverse și mai sofisticate, componenta de securitate IT din cadrul sistemelor informatice implementate în sectorul guvernamental devine un punct critic în realizarea și menținerea unor sisteme IT sigure și funcționale. La acest nivel, de obicei, componenta de securitate este fie subapreciată, fie ne-acoperită. Astfel, un antivirus actualizat și un firewall activat nu mai reprezintă metode suficiente de protecție. Cu cât sistemele implementate sunt mai complexe, cu atât cresc și nevoile de securitate.

Statul are o responsabilitate globală în problemele de securitate, inclusiv în domeniul IT. În unele sectoare ale societății resursele private sunt utilizate pentru a îmbunătăți securitatea statală, fără a diminua responsabilitatea acestuia. Dar o posibilă participare privată nu micșorează în nici un fel responsabilitatea statului.

Experiența internațională, cum ar fi exemplul suedez, demonstrează că o cooperare constructivă poate fi stabilită printr-un parteneriat public-privat în ceea ce privește securitatea IT, iar responsabilitățile publice pot fi realizate prin intermediul unui CERT guvernamental.

În România, sectorul public nu își permite la ora actuală să plătească experți în securitate informatică care să supravegheze fiecare rețea în parte. În practică, lipsește uneori chiar un administrator de rețea al unui astfel de sistem. Pe de altă parte, nici serviciile oferite de sectorul privat în domeniul securității IT nu sunt accesibile sectorului public din punct de vedere financiar. Acest fapt întărește necesitatea unui CERT guvernamental. Acesta ar strânge informații și cunoștințe în problemele de securitate la

¹ Vezi Softwin, Gecad, Provision, Business Information Systems, UTI, Omnilogic etc

nivelul întregului spectru guvernamental utilizându-le pentru a preveni atacuri și incidente de securitate ulterioare. Prin prevenirea atacurilor și incidentelor la întreg nivelul guvernamental, CERT va preveni cu siguranță pierderea a milioane de dolari.

Inexistența unui centru de colectare a tuturor informațiilor legate de securitatea IT la nivel guvernamental face ca puținele resurse dedicate să fie utilizate inefficient, multe dintre probleme fiind similare la diverse instituții publice.

Experiența altor țări demonstrează că o asemenea unitate este din ce în ce mai prezentă și mai utilă la nivelul sectorului guvernamental în condițiile creșterii numărului și complexității sistemelor IT implementate în sectorul public.

Mandatul unei unități CERT românești (CERT.ro)

S-a agreat faptul că SITIC poate servi, în termeni generali drept model, totuși este necesară o analiză atentă pentru a ne asigura că propunem ceva relevant pentru România. RITI dot-Gov face o primă propunere :

Misiune

Mandatul CERT.ro va fi de a susține societatea românească în protejarea împotriva incidentelor IT. CERT.ro va fi punctul central de raportare și coordonare privind incidentele de securitate relevante pentru guvern. CERT.ro va facilita schimbul de informații privind incidentele IT între organizațiile din societate și va disemina informațiile legate de noi probleme care ar putea împiedica funcționarea sistemelor IT guvernamentale. În plus, CERT.ro va asigura informații și consultanță privind măsuri pro-active și compilează și publică statistici.

Competență

CERT.ro se adresează tuturor gazdelor din domeniul guvernamental și adreselor desemnate pentru orice unitate guvernamentală locală sau națională. CERT.ro nu dă asistență tehnică incidentelor legate de utilizatori individuali.

Este important de menționat că CERT.ro nu va lucra direct cu sectorul privat sau utilizatori individuali. Totuși, unele dintre serviciile pro-active ale CERT.ro (informare, consultanță privind securitatea IT, statistici) ar trebui să fie disponibile pentru toată lumea, în special prin site-ul web al CERT.ro. sau prin liste de distribuție publică.

4) Confidențialitate

Toate documentele legate de CERT.ro ar trebui să fie publice cu excepția:

- documentelor clasificate, proprii sau emise de alte organizații/instituții și clasificate de către acestea,
- corespondenței purtate ca urmare a unor subiecte rezultate din documente precum cele de mai sus,

- documentelor (chiar ne-clasificate) ce ilustrează anumite situații de criză/pericol iminent la adresa unor sisteme la un moment dat, și a căror dezvăluire ar face aceste sisteme vulnerabile în fața amenințărilor,
- documentelor care în virtutea unor prevederi contractuale sunt confidențiale,
- documentelor pentru a căror divulgare ar fi necesar acordul unei terțe părți,
- altor documente considerate confidențiale la un moment dat (similare celor din lista de mai sus)

5) Personal: număr și calificare

Sugerăm un număr de maxim 10 persoane care să facă parte din personalul CERT.ro. Numărul poate fi mai mic la începutul activității și poate crește la numărul maxim, dacă este necesar.

Mai jos, dăm o descriere a fiecărei funcții. În **Anexa II** există o prezentare în detaliu care include calificările minime necesare fiecărei poziții și funcțiile esențiale.

1. Director, CERT-Ro

Directorul răspunde de planificarea, dezvoltarea și implementarea strategiilor operaționale, a inițiativelor, politicilor și programelor CERT-Ro. Acesta urmărește și evaluează succesul CERT-Ro în îndeplinirea planului său strategic.

2. Analist securitate Internet

Acesta este responsabil de asigurarea conducerii tehnice și strategice în cercetarea, examinarea și analizarea tendințelor și subiectelor legate de securitatea IT. Sarcinile sale includ:

- Testarea și analizarea „malicious codes”, software-ului vulnerabil, instrumentelor de securitate și actualizărilor disponibile
- Dezvoltarea relațiilor externe pentru asigurarea colectării de date pentru analiză
- Dezvoltarea sau asigurarea unei imagini globale a dezvoltării sistemelor și proceselor interne care să conducă la analize
- Analizarea și identificarea tendințelor în domeniul securității pe baza incidentelor, inclusiv analiza incidentelor și acțiunilor în timpul unor evenimente majore, analiza informațiilor publice și colaborarea cu alți experți în domeniul securității.
- Elaborarea de documente care să descrie cele mai bune practici pentru sistem și pentru administratorii de rețea, managerii tehnici, alți tehnicieni.
- Reprezentarea CERT-Ro la diverse forumuri tehnice
- Asigurarea de îndrumare tehnică pentru ceilalți membri ai CERT-Ro.
- Contribuție la elaborarea de planuri strategice și direcții de dezvoltare ale CERT-Ro.
- Dezvoltarea de procese și proceduri de monitorizare a „sănătății” Internetului prin monitorizarea informațiilor de rutare și a schimbărilor din informațiile de rutare, monitorizarea serverelor cheie DNS etc.

- Publicarea de informații pentru public și entități private asupra infrastructurii de rutare și stării infrastructurii DNS.
- Publicarea de lucrări și prezentări în colaborare cu părți interne și externe pe probleme avansate de securitate a rețelelor și Internetului.

3. Cercetător în domeniul vulnerabilităților IT

Responsabilitățile pentru această poziție sunt examinarea, analizarea, raportarea și efectuarea de schimbări în ingineria software. Sarcinile includ cercetarea în detaliu a vulnerabilității software, corespondență cu furnizori de software, cercetători, sponsori și alții, crearea de specificații și dezvoltarea de instrumente și procese pentru îndeplinirea scopului echipei, conducerea activităților de stabilire a direcțiilor de strategie în cercetarea vulnerabilității și identificarea, analizarea și prevenirea vulnerabilităților de software. Candidatul trebuie să fie un leader tehnic.

4. Specialist în remedierea vulnerabilităților IT

Responsabilitățile pentru această poziție sunt cercetarea, examinarea, analizarea, raportarea și efectuarea de schimbări în securitatea Internetului. Sarcinile includ cercetarea în detaliu a vulnerabilității software, corespondență cu vânzători de software, cercetători, sponsori și alții, crearea de specificații și dezvoltarea de instrumente și procese pentru îndeplinirea scopului echipei, conducerea activităților de stabilire a direcțiilor de strategie în remedierea vulnerabilității și identificarea și implementarea de noi abordări pentru identificarea, analizarea și prevenirea vulnerabilităților de software. Candidatul trebuie să fie un leader tehnic.

5. Specialist în dezvoltarea practicilor și instruire

Persoana din această poziție va lucra ca membru în Programul de dezvoltare a Practicilor și Instruire pentru dezvoltarea și predarea practicilor de îmbunătățire a securității și crearea de programe de instruire în asigurarea și siguranța informațiilor pentru administratori și manageri de sistem și rețea. Candidatul trebuie să lucreze bine în echipă și să poată comunica eficient cu ceilalți. Activitățile vor include lucrul cu clienții din diverse organizații, inclusiv agenții guvernamentale și alte instituții care se ocupă de infrastructuri critice.

6. Analist

Analistul statistic pentru securitatea rețelei va aplica principii solide statistice în dezvoltarea instrumentelor de analiză pentru studierea stării rețelei. Principalele responsabilități includ construirea de instrumente prototip de analiză, contribuții la dezvoltarea unui program de cercetare la nivel înalt pentru analiza datelor de securitate a rețelei și asigurarea unui rol de consultant pentru membrii echipei care fac analize statistice. Instrumentele prototip de analiză pot asigura următoarele capacități:

- Analiză de tendințe: urmărirea schimbărilor în compoziția și volumul traficului în rețea în timp
- Detectarea anomaliilor: găsirea punctelor de date care violează comportamentul normal de trafic în rețea
- Găsirea surselor comportamentale: identificarea surselor care arată comportament coordonat de atac
- Integrare date: unificarea unei game largi de tipuri de date pentru analiză și interferență.

7. Administrator de sistem

Acesta este responsabil de susținerea utilizatorilor și întreținerea software-ului și a echipamentelor cadrul CERT-Ro. Aceasta include înțelegerea necesităților echipei care folosește laboratorul, crearea și dezvoltarea de servicii de laborator care să răspundă acestor necesități, planificarea achizițiilor de echipamente, a configurației și întreținerii echipamentelor, a instalării și scoaterii din uz a echipamentelor pentru experimente, asistarea experimentelor după cum e cazul.

8. Specialist informare tehnică si relații publice

Pentru această poziție sunt necesare cunoștințe solide de limbă română și engleză. Un avantaj poate fi experiența în scrieri cu caracter tehnic, dar nu este obligatorie. Candidatul trebuie de asemenea să cunoască bine concepte generale de IT și terminologie de calculator în engleză și română. Cunoștințe în alte limbi reprezintă un avantaj, dar nu sunt obligatorii. Un alt avantaj ar fi capacități de editare/manipulare și cunoștințe generale de design/dezvoltare de web.

9. Consultant securitate

Necesită 2-4 ani de experiență în mediu de consultanță cu experiență demonstrată ca administrator de sistem sau rețea într-un mediu Windows sau UNIX, cunoștințe și experiență în arhitectură de sistem, soluții totale de securitate și protocoale și aplicații de Internet, experiență în configurarea și implementarea de soluții tehnice de securitate (firewalls și sisteme de detectare a intruziunilor). Se cer de asemenea capacități foarte bune de interfață cu clienții, bune capacități de comunicare verbală și în scris, capacități excelente de management de proiect, cunoștințe de protocoale și aplicații comune de Internet. Sunt de dorit certificate de tip MSCE, CCNA, CISSP, CISM or CISA.

10. Inginer de securitate (Security Response Engineer)

Se cere titlu de BS, preferabil într-un domeniu legat de calculatoare sau experiență echivalentă în industrie. Candidatul trebuie să arate o gamă largă de capacități inclusiv capacitatea de a citi și înțelege cod de asamblare x86, și cunoștințe de rețele TCP/IP, inclusiv cunoștințe de protocoale majore bazate pe TCP/IP. Trebuie să aibă o experiență de minimum doi ani în programare C/C++ pe platforme MS Windows și/sau Linux. În plus, poziția necesită cunoștințe de lucru în shell scripting, programare PERL și /sau Python pentru sarcinile zilnice.

6) Posibila locație a CERT-ului românesc

Discuțiile noastre în această privință au luat în considerare unele dintre caracteristicile pe care ar trebui să le aibă o astfel de instituție:

- *Un proiect susținut 100% guvernamental.* Deși am studiat problema realizării unui parteneriat public-privat, experiența europeană și tipul de activități ce se doresc a fi desfășurate ne arată că o asemenea posibilitate nu ar putea fi luată în calcul în momentul actual. În schimb, putem susține că o colaborare extrem de bine pusă la punct trebuie să existe între un CERT guvernamental, organizațiile de tip CERT private și ISP-iștii și organizațiile lor.
- *O instituție civilă.* Nu credem că o instituție militară ar putea să satisfacă necesitatea colaborării cu toate ministerele dar și cu industria privată. În toate țările din Uniunea Europeană unde există o unitate de tip CERT guvernamental aceasta este parte a unei instituții civile și nu militare.
- *Parte a unei instituții independente.* Această cerință se impune pentru separarea activităților de tip CERT de activitățile de stabilire a politicilor în domeniul securității IT. Instituția ar trebui să fie însă un pol de colaborare nu numai cu MCTI, în capacitatea sa de creator de politici în domeniul securității IT, dar și cu celelalte ministere și instituții implicate în domeniul securității IT, inclusiv la cel mai înalt nivel de securitate - CSAT (Consiliul Superior de Apărare al Țării).
- *Nu trebuie să fie o instituție de sine stătătoare.* Din cauza dimensiunilor relativ reduse din punct de vedere al personalului angajat (max. 10 persoane) și al nivelului de expertiză tehnică necesar al acestuia, CERT-ul ar fi împovărat de prea multe sarcini administrative dacă ar funcționa singur în cadrul unei instituții separate. Din aceste motive este de preferat “plasarea” acestuia în cadrul unei alte instituții și nu crearea unui organism separat care ar necesita destule resurse pentru a-i permite funcționarea în mod adecvat.
- *Angajații nu trebuie să fie funcționari publici.* Un statut de funcționar public i-ar împiedica pe aceștia să fie remunerați conform calităților necesare pentru o astfel de unitate.

O consultare publică pe tema alegerii organizației este recomandată pentru a fi siguri ca interesul tuturor părților implicate poate fi luat în calcul.

În cadrul prezentului document prezentăm 2 propuneri, pe care le detaliem mai jos, fără a exclude posibilitatea ca o altă instituție sa fie aleasă pentru găzduirea CERT.ro.

A. Considerăm că există posibilitatea creării unui CERT.ro guvernamental în cadrul Autorității Naționale de Reglementare în Comunicații (ANRC), care îndeplinește toate capacitățile mai sus menționate.

O asemenea ipoteză este întărită de experiența europeană care ne arată că în majoritatea statelor un asemenea CERT este realizat în cadrul autorității de reglementare în domeniul comunicațiilor electronice, ca un departament autonom, fiindu-i asigurată astfel independența de funcționare, dar și calitatea și plata corespunzătoare a personalului angajat.

Mai mult, asemenea atribuții în domeniul securității IT ar veni în completarea dispozițiilor *Legii nr. 506 din 17 noiembrie 2004 privind prelucrarea datelor cu caracter personal și protecția vieții private în sectorul comunicațiilor electronice* care dă competență ANRC în stabilirea unor condiții de securitate pentru furnizorii de servicii de comunicații electronice.

Art. 3: Măsuri de securitate

(1)Furnizorul unui serviciu de comunicații electronice destinat publicului are obligația de a lua toate măsurile tehnice și organizatorice adecvate în vederea garantării securității serviciului. În ceea ce privește securitatea rețelei, dacă este necesar, furnizorul serviciului de comunicații electronice va lua măsurile de securitate respective împreună cu furnizorul rețelei publice de comunicații electronice. Măsurile adoptate trebuie să garanteze un nivel de securitate proporțional cu riscul existent, având în vedere posibilitățile tehnice de ultimă oră și costurile implementării acestor măsuri.

(2)Autoritatea Națională de Reglementare în Comunicații, denumită în continuare ANRC, stabilește condițiile în care furnizorii trebuie să își îndeplinească obligația prevăzută la alin. (1).

Putem sugera ca un asemenea departament CERT să prezinte un raport anual de activitate în fața Parlamentului (ori numai a comisiilor specializate de IT&C) sau a CSAT (Consiliului Superior de Apărare a Țării)

B. O alta opțiune ar fi crearea unui CERT.ro ca departament autonom în cadrul unei instituții publice noi care să acopere și alte probleme de securitate IT

Poate fi considerată constituirea unei noi instituții publice în domeniul IT care să găzduiască o serie întreagă de activități din domeniul securității IT sau alte domenii adiacente care la ora actuală sunt în atribuțiile MCTI sau a altor organisme și care ar putea să fie realizate în cadrul unei instituții independente de Minister.² :

- Avizarea instrumentelor de plată cu acces la distanță conform Ordin nr. 218 din 14 iunie 2004
- Reglementarea și Supravegherea din domeniul semnăturii electronice conform legii semnăturii electronice
- Notificarea pentru serviciile de marcă temporală, conform legii 451/2004
- Realizarea de expertize tehnice în domeniul securității IT și a echipamentelor IT
- Promovarea de standarde în domeniul securității IT
- Audit independent al serviciilor de e-government
- Supravegherea aplicării legii comerțului electronic conform legii 365/2002 – art. 17
- Administrarea portalului efrauda.ro

Toate aceste activități pot fi realizate în cadrul unei instituții independente care să aibă ca domeniu general de competență securitatea IT. O parte din activitățile mai sus menționate pot fi și producătoare de venituri (fie prin servicii plătite – ca în cazul avizării

² De fapt, asemenea activități ar putea să facă obiectul de activitate și al CERT.ro în cazul în care aceasta ar fi creată ca un departament în cadrul ANRC

instrumentelor de plată, fie prin unele taxe de monitorizare - ca în cazul reglementării semnăturii electronice).

7) Buget

O estimare generală a bugetului pentru CERT.ro ar fi:

Asistență pentru consultanță de Proces, Management și Operațională, Management de Recrutare, Instruire	120.000 euro
Structură comunicații și IT (servicii, hardware și software)	130.000 euro
Facilități inițiale și mobilă	20.000 euro
Costuri operaționale pentru 1 an.....	440.000 euro
Total	710.000 euro

În mod evident costurile de funcționare sunt cea mai importantă parte a bugetului atâta vreme cât se dorește crearea unui grup de experți în securitatea IT foarte competenți și care, în consecință, trebuie să fie bine plătiți.

8) Surse de finanțare

Cheltuielile inițiale ale unui CERT.ro ar putea fi finanțate din mai multe surse

- Ar putea fi folosite posibile fonduri ale Uniunii Europene pentru susținerea creării CERT.ro. Prin PHARE 2005 ar putea fi finanțat un astfel de proiect prin asistență tehnică (consultanță) sau fonduri de investiție (echipamente, calculatoare etc.) sau prin proiecte de înfrățire „twinning projects” (în care expertiza unui CERT european ar putea fi împărtășită noii instituții românești). Disponibilitatea unei astfel de finanțări și a cerințelor specifice ar trebui verificate la Delegația UE din București începând cu luna februarie 2005. Ar trebui de asemenea să fim deschiși la orice surse de finanțare UE, inclusiv activități viitoare ale recent createi ENISA³
- Alte surse bilaterale de finanțare cum ar fi proiectul guvernului german IBD/GTZ
- Finanțare guvernamentală prin bugetul de stat
- USAID, prin proiectul RITI dot-Gov ar putea susține instruirea inițială în Statele Unite a 4 viitori membri ai CERT.ro, inclusiv participarea la o instruire CERT-CC în Arlington.

În funcție de planificarea în timp a realizării CERT.ro, o soluție optimă ar putea fi o combinație a surselor mai sus menționate sau cu alte surse de la donatori internaționali.

³ European Network and Information Security Agency - <http://www.enisa.eu.int/>

Pentru costurile de funcționare, toate opțiunile sunt deschise inclusiv alternative de finanțare prin bugetul de stat sau prin taxe și contribuții pentru servicii, atâta timp cât aceste servicii nu sunt privite ca activitate pur comercială.

9) Cooperarea cu alte organisme

Politica de securitate IT ar trebui elaborată de către MCTI, după consultări în detaliu cu industria IT, în special ISP. Este important ca politica de securitate IT să fie prezentată și discutată la cel mai înalt nivel al consiliului de strategie de apărare din România – CSAT.

Politica ar trebui implementată de către CERT.ro în cooperare cu toate instituțiile publice care au sarcini în acest domeniu în conformitate cu legislația națională.

Activitatea CERT.ro și implementarea politicii de securitate IT ar trebui supervizate de către Comisia de IT&C a Parlamentului. Comisia ar trebui să primească un raport public anual din partea CERT.ro cu privire la situația curentă a securității IT și implementării politicii de securitate IT. Comisia poate cere clarificări din partea conducerii CERT asupra unor anumite probleme și poate cere experți CERT pe anumite aspecte tehnice legate de securitate IT.

Cooperare cu alte structuri naționale

Experiența altor organizații CERT dovedește faptul că pentru îndeplinirea obiectivelor prevăzute în misiunea CERT este esențial a avea o bună relație de colaborare cu :

- Organizații comunitare (Autorități guvernamentale, organizații regionale și municipale) care ar trebui să transmită rapoarte de incidente de securitate IT la CERT.ro și să primească analize, statistici, consultanță specifică și instruire
- Alte echipe pentru incidente IT din România și străinătate dar și furnizori pentru schimb de informații privind noi probleme (ex. vulnerabilități și viruși)
- O strânsă cooperare cu alte instituții publice care au sarcini în domeniul securității IT.

Este recomandat crearea unui grup ne-formal cu celelalte CERT naționale și instituții publice care să se întâlnească cel puțin lunar să discute probleme operaționale, să împărtășească cunoștințe, să prezinte proiecte comune. Aceste întâlniri sunt importante pentru identificarea activităților care se suprapun din diverse instituții, dar și pentru a defini obiectivele și perspectivele naționale privind securitatea IT.

Trebuie creată o colaborare specială cu autoritățile de aplicare a legislației criminalității informatice. Informațiile ar trebui să meargă în ambele direcții:

- Organismele de aplicare a legii ar trebui să aibă un punct central de expertiză tehnică care să se ocupe de problemele tehnice ce trebuie clarificate
- Echipa CERT.ro ar trebui să informeze autoritățile de aplicare a legii cu privire la activitățile ilegale care au fost oprite sau identificate de către CERT.ro

Cooperare cu structuri internaționale

Cum cooperarea internațională în domeniul securității IT a devenit o necesitate, este esențial ca CERT.ro să dezvolte relații de colaborare cu alte organizații de tip CERT, precum și cu asociații ale acestora : FIRST, TICSIRTS, ECG⁴.

Ținând cont și de decizia de integrarea europeană a României o relație specială trebuie realizată cu ENISA.

10) Lista legislației ce ar putea fi modificată

Crearea unei instituții de tipul CERT.ro ar trebui să facă obiectul unei legi speciale, unde să se prevadă în mod specific cel puțin:

- statutul autonom
- structura de conducere
- obiectivele, atribuțiile și responsabilitățile acestuia
- modul de supraveghere și instituția însărcinată cu aceasta,
- modalitățile de finanțare a costurilor anuale
- relațiile cu alte instituții publice
- modul de angajare și salarizare al personalului CERT.ro
- aprobarea Bugetului anual de venituri și cheltuieli al ANRC.

În cazul în care CERT.ro va funcționa în cadrul unei alte instituții, atunci va trebui modificat și actul normativ care stabilește condițiile de funcționare ale acelei instituții.

De asemenea, în funcție de activitățile care vor cădea în sarcina CERT.ro sau a instituției care o vor găzdui, trebuie modificate și alte acte normative referitoare la acel domeniu (Ex. Semnătura electronică, avize mijloace de plată cu acces la distanță etc.).

Considerăm însă că este prea devreme a ne pronunța asupra acestor aspecte în detaliu.

⁴ Vezi secțiunea Tendințe internaționale pentru mai multe informații legate de aceste instituții/asociații.

Anexa 1

Report privind vizita de studiu pentru CERT Octombrie 2004

RITI dot-Gov a organizat o vizită de studiu legată de o unitate CERT (Computer Emergency Response Team) la Stockholm, Suedia, 22 Octombrie 2004. La această vizită au participat următoarele persoane:

Ministerul Comunicațiilor și Tehnologiei Informației

Liviu Nicolescu, Director General IT Reglementări IT, Standarde, Antifraudă și Securitate

Iulia Bumbac, Șef Serviciu, Antifraudă și Securitate rețele

Asociația Națională a Furnizorilor de Servicii Internet, ANISP

Gheorge Serban, Director Executiv.

RITI dot-Gov

Jerker Torngren, Project Director

Bogdan Manolea, Legal expert

Prima întâlnire a avut loc cu Michael Mohr, Director și Secretar Principal al Comisiei Guvernamentale de Apărare

A doua întâlnire a fost cu Johan Mårtensson, șef al Centrului Suedez de Incidente IT, SITIC, care este autoritatea suedeză oficială CERT.

Comisia de Apărare evaluează actualul sistem de protecție a securității privind criminalitatea informațională în societate și prezintă o propunere Guvernului privind posibilele modificări necesare ale sistemului. Comisia este puternic susținută de toate ministerele.

Pe baza unei propunerii a Comisiei, Parlamentul Suedez a decis în 2000 asupra actualei organizări a securității IT, inclusiv crearea SITIC. Comisia evaluează acum eficiența acestei organizații și posibilele modificări necesare datorate schimbărilor legate de diverse amenințări.

În plus, Comisia are rolul de coordonare a răspunsurilor la amenințările IT ne-militare.

În comisie participă toți reprezentanții sectorului public dar și sectorul privat participă frecvent în mod ad hoc.

În afara noii agenții SITIC, există alte trei agenții care au sarcini legate de securitatea IT:

- Agenția Suedeză de Management de Urgență, SEMA

- Administrația pentru Echipamente de Apărare (Defence Material Equipment Administration)
- Agenția de Apărare Radio

Ministerul Justiției este direct implicat prin Forța Națională de Poliție care are o echipă dedicată criminalității informatice și care susține și forțelor locale de poliție din punct de vedere al expertizei în domeniu.

Coordonarea dintre diversele autorități implicate se face prin Grupul de Coordonare unde toate agențiile se întâlnesc o dată pe lună pentru a prezenta programul fiecărei agenții pentru a evita duplicarea activităților.

S-a subliniat faptul că există un număr de companii private care îndeplinesc sarcini de tip “CERT” și pe baze comerciale. Unele dintre aceste companii pot oferi servicii în competiție cu SITIC. Această situație va fi analizată în continuare de Comisie pentru a obține o separare clară a responsabilităților și implicării din partea sectorului public și privat. Aceasta se va face pe baza faptului că responsabilitatea completă a problemelor de securitate trebuie să fie a sectorului public.

SITIC s-a creat ca prima unitate CERT Suedeză în 2002. Deși numărul de unități crește la nivel global, doar 8 țări europene au unități CERT guvernamentale. Totuși în aproape toate țările UE se află astfel de structuri de tip în cadrul mediului academic sau în sectorul privat.

SITIC are nouă angajați și este organizat ca un departament în cadrul autorității de reglementare a statului pentru poștă și telecomunicații, PTS, în primul rând pentru a beneficia de serviciile administrative și organizarea PTS. Nu s-a considerat eficientă crearea unei autorități separate doar pentru 9 oameni. Alegerea organizației gazdă nu a fost una evidentă, singur fapt clar fiind că trebuie să fie una civilă și nu legată de apărarea militară.

Numărul angajaților depinde de sarcinile pe care unitatea CERT trebuie să le îndeplinească și nu reflectă neapărat mărimea țării.

SITIC este finanțat direct de la bugetul statului și este parte integrantă din bugetul PTS. Bugetul anual SITIC se ridică la 15 milioane SKR ceea ce corespunde cu un total de aproximativ 1,6 milioane Euro. 2/3 din această sumă este cheltuită pe salariile angajaților care trebuie să fie în mod necesar foarte calificați în domeniul securității IT. Conform SITIC, o sumă mult mai mare este economisită anual datorită operațiunilor SITIC. Ca exemple s-au dat situația în care SITIC a evitat o amenințare care ar fi paralizat întregul sistem național de contribuții sociale și cazul în care s-a evitat o întrerupere totală a sistemului IT al Municipality din Stocholm.

Personalul trebuie să aibă experiență în a lucra cu rețele de calculatoare, să aibă capacități de analiză și comunicare și câteva cunoștințe de programare. Nu trebuie să știe în detaliu cum se scriu codurile de tip „malicious codes” ci cum funcționează acestea și cum se

dezvoltă în general. Trebuie de asemenea să fie la curent cu evoluția din domeniul securității IT.

SITIC cooperează cu alte agenții care au sarcini legate de securitatea IT dar și cu furnizori de echipamente, ISP-iști și alte echipe care se ocupă de incidente IT din Suedia și alte țări. .

Sarcina SITIC este de a ajuta societatea în eforturile împotriva incidentelor IT prin:

1. Capacitatea de a comunica rapid comunității informații legate de noi probleme care ar putea amenința sistemele IT;
2. Asigurarea de informații și consultanță privind eforturile de prevenire a incidentelor ;
3. Elaborarea și publicarea de statistici pentru îmbunătățirea muncii de prevenire;
4. Stabilirea unui sistem de schimb de informații privind incidentele IT între organizațiile comunității și echipă.

Aceasta se obține prin:

- Studii tehnologice pentru /descoperirea de noi probleme de securitate IT;
- Primirea de rapoarte privind incidente IT;
- Analize;
- Elaborarea de statistici;
- Asigurarea de consultanță.

Nu se consideră că aceste activități trebuie făcute 24 de ore zilnic, SITIC operând doar în timpul orelor normale de lucru.

SITIC a scos în evidență faptul că deseori funcțiile unei unități CERT sunt adesea confundate cu cele ale producătorilor de anti-virusi sau alți consultanți pe probleme de securitate IT. Diferența constă în modul de abordare pe care acele organizații îl au legat de „malicious codes” care apar zilnic.

Producătorilor de anti-virusi sau alți consultanți pe probleme de securitate IT li se dau informații legate de posibile vulnerabilități care pot fi peste 4 000 / an.

SITIC pe de altă parte se ocupă pe produsele majore de software și hardware existente în sectorul guvernamental și își concentrează activitățile și alertele pe acest segment guvernamental și tratează cam 200 vulnerabilități anual, ajutând audiența țintă să repare deficiențele de securitate și vulnerabilitățile înainte ca acestea să fie speculate. .

Anexa 2

Fișe de post

Detaliile pentru fiecare post sunt indicative, în funcție de ceea ce există pe piață putându-se modifica sau adăuga alte competențe necesare.

1. Director, CERT-Ro

Calificare:

Grad de MS în calculatoare sau echivalent

Cel puțin 15 ani experiență cu responsabilități progresive într-o organizație tehnologică sau de cercetare din învățământul superior, industrie sau guvern. Cel puțin 10 ani experiență în software inclusiv dezvoltare directă, conducere de echipă și management de proiect. Experiență demonstrată de management cu responsabilitate legată de proiecte, angajați, bugete și contracte.

O foarte bună și extinsă cunoaștere a sistemelor de calculatoare, a practicilor de securitate pentru calculatoare și a metodelor de evaluare a securității informațiilor, o foarte extinsă cunoaștere a scopurilor organizaționale, de management etc., capacitate managerială în diverse domenii și pe proiecte complexe, capacitatea de a influența, de a conduce și a lucra cu personal tehnic, capacitatea de a răspunde rapid și eficient priorităților în schimbare, excelente capacități analitice, organizatorice, de supervizare, de judecată și de rezolvare a problemelor, capacitatea de a interacționa eficient atât la nivel intern cât și extern, excelente capacități de comunicare verbală și în scris.

Capacitatea de a respecta termene limită, de a rămâne calm în timpul situațiilor dificile, de a lucra sub presiune și cu diverse întreruperi.

Capacitatea de a călători frecvent și de a-și adapta programul de lucru ce ar putea necesita lucrul în timpul sfârșitului de săptămână sau seara. Trebuie să poată trece o verificare de fond și să obțină anumite aprobări guvernamentale de securitate.

Funcții esențiale:

Conduce programele **CERT-Ro** pentru implementarea cu succes a planului strategic scopurilor și obiectivelor **CERT-Ro** și conduce activitățile zilnice operaționale ale **CERT-Ro**. Dezvoltă, implementează și urmărește planurile operaționale pe termen scurt și lung (financiare, de personal, infrastructură, proiecte).

Ghidează și monitorizează succesele **CERT-Ro** în îndeplinirea sarcinilor strategice. Evaluează rapoartele directe și face recomandări de salarizare pentru întreg personalul.

Conduce procesul de planificare strategică și contribuie la dezvoltarea planului strategic al **CERT-Ro**. Asigură actualizarea anuală a planului strategic, revizuieste fezabilitatea planului, identifică riscurile și definește strategia de abordare a riscurilor.

. .

Candidații trebuie să treacă o verificare de fond, să obțină aprobare de securitate și să fie cetățeni români.

2. Analist de Securitate Internet

Calificare

NOTA: Candidatul trebuie să treacă o verificare de fond, să obțină aprobare de securitate și să fie cetățean român.

PhD cu 6 ani experiență legată de domeniu sau MS în calculatoare sau domeniu asociat cu cel puțin 8 ani experiență.

BS MS în calculatoare sau domeniu asociat cu cel puțin 10 ani experiență.

Experiență: Cunoștințe expert în cel puțin câteva din următoarele subiecte:

- Instrumente de securitate
- Administrare sistem și/sau rețea
- Extragere de informații de securitate din instrumentele / aplicațiile de monitorizare rețea
- Detalii operaționale în sisteme de operare multiple
- Experiență în dezvoltare de software
- Experiență de programare în mai multe limbi.

Cunoștințe expert în următoarele:

- Sisteme de calculatoare și probleme de securitate în Internet
- Funcționare și limitări în tehnologiile folosite de către organizații ca elemente cheie de apărare de securitate a rețelei cum ar fi: „firewall”-uri sisteme de detectare a intruziunii, „proxy”-uri, scanere și încriptare
- Protocoale de baza Internet (TCP/IP, UDP, BGP, DNS, SMTP etc.).
- Protocoale de rutare pe Internet și chestiuni de securitate legate de rutarea pe routing
- Operații de server DNS, inclusiv servere root DNS și impactul infrastructurii Internet asupra modului de funcționare al serverelor DNS
- Cunoștințe detaliate privind metodele folosite de intruși pentru a ataca rețelele de sisteme
- Probleme de spațiu de adresa IP și de management global al numelor de domeniu
- Operarea infrastructurii de bază Internet
- Cele mai bune practici de dezvoltare a codului de securitate

- Inginerie de inversare a codurilor „malicious”
- Elemente de bază de securitate pentru computere
- dezvoltarea de instrumente de asistare a administratorilor de sistem și rețea
- colectarea, rezumarea și analizarea traficului Internet și a datelor de incidente pentru tendințele de securitate.

În plus, cunoștințe profunde sau familiarizare cu majoritatea sau toate subiectele următoare:

- Instrumente de securitate
- Administrare sistem
- Protocoale de bază Internet (TCP/IP, UDP, DNS, SMTP etc.).
- Tratarea răspunsului la incidente (mai mult decât RI)
- Vulnerabilități comune
- Baza teoretică a securității calculatoarelor
- Criptografie și instrumente de încriptare
- Detectarea intruziunii
- Inginerie de software
- Lucrări publicate și prezentări formale pe mai multe subiecte din următoarele subiecte:
 - BGP și alte probleme de securitate a protocolului de rutare
 - Cele mai bune practici pentru funcționarea în securitate a serverelor DNS, sisteme folosite în infrastructura de rutare
 - Posibile îmbunătățiri ale protocoalelor DNS de rutare
 - descoperirea vulnerabilităților la software
 - practici sigure de programare
 - inginerie inversa a software -ului (reverse engineering)
 - analiza de bază a sistemelor de calculatoare sau a altor echipamente electronice
 - analiza unui volum mare de informații de detectare a intruziunii sau date de rețea

Capacități

Capacitatea de a asigura conducere tehnică pentru personalul tânăr și nou angajat; capacitatea de a stabili priorități în domeniile tehnice, experiență demonstrată de vorbit în public și de comunicare eficientă cu un număr mare de colaboratori și parteneri externi și internaționali; capacitatea de a servi drept facilitator în coordonarea diverselor părți implicate în securitatea infrastructurii Internet și de a ajuta grupurile să ajungă la un consens tehnic.

Condiții normale de birou.

Capacitatea de a lucra bine sub presiune și cu termene limită. Capacitatea de a avea interacțiuni de nivel tehnic și managerial (sau ne-tehnic) cu un număr mare de colegi de vârste diferite.

Funcții esențiale

Dezvoltarea și implementarea rezultatelor, activități de tranziție inclusiv analiză de incident, artefact și vulnerabilitate. Verificarea colectării de date pentru susținerea eforturilor de analiză. Lucru cu personalul tânăr.

Cercetare în domenii de interes tehnic.

Reprezentarea **CERT-Ro** în alte grupuri (prezentări la conferințe, grupuri de lucru tehnologice etc.).

Tratarea problemelor de răspuns la incidente și vulnerabilitate.

Alte sarcini după cum e cazul.

3. Cercetător vulnerabilitate

Calificare minimă

BSc în calculatoare, informatică, management informatic sau echivalent 10 ani experiență ca administrator de sistem sau rețea, creator de software, administrator de baze de date sau similar sau MS în calculatoare, informatică sau management informatic sau echivalent plus 8 ani experiență ca administrator de sistem sau rețea, administrator de baze de date sau similar, PhD în calculatoare, informatică sau management informatic plus 6 ani experiență ca administrator de sistem sau rețea, creator de software, administrator de baze de date sau similar. Se iau în considerare și alte pregătiri de natură tehnică cu experiența descrisă mai sus.

Experiență sau cunoștințe substanțiale în:

- Probleme de securitate pe Internet
- Testare software
- Inginerie de software
- Forme comune de „malicious code”
- Metodologii comune de dezvoltare
- Defecte comune de software (ex. supraîncărcare buffer)
- Dezvoltare de software și programare în limbaje multiple
- Administrare de Sistem, baze de date și rețea
- Sisteme de operare multiple
- Protocoale comune Internet (ex: TCP/IP, ICMP, DNS, HTTP etc.).
- Teorie și practică avansată în criptografie

Lucrări publicate și prezentări formale în mai multe dintre următoarele subiecte

- descoperirea vulnerabilităților la software

- inginerie inversă de software
- analiză de bază a sistemelor de calculatoare sau a altor echipamente electronice.

Trebuie să aibă următoarele capacități:

- testare și evaluare software
- originalitate și creativitate
- capacități foarte bune de comunicare verbal și în scris
- capacitate de a stabili prioritățile de lucru
- lucru în echipă sub coordonare în caz de urgențe
- capacitatea de a lucra calm și bine sub presiune
- capacitatea de a avea de a face cu persoane dificile
- recunoașterea și tratarea în mod corespunzător a informațiilor confidențiale și sensibile
- capacitate de comunicare eficientă în situații normale sau de stres
- capacități de conducător și îndrumător

Capacitatea de a lucra sub presiunea limitelor de timp.

Trebuie să treacă verificarea de bază, să obțină aprobare și să fie cetățean român.

Funcții esențiale:

1. Examinare detaliată și testare software în căutare de noi vulnerabilități
2. Cercetare, specificare și dezvoltare de noi instrumente, procese și tehnici de îmbunătățire a testării și detectării vulnerabilității pentru a fi folosite de către inginerii de software
3. Scrierea și publicarea rezultatelor testelor
4. Corespondență cu furnizori de software, cercetători din domeniul vulnerabilității, sponsori și alte părți interesate
5. Reprezentarea **CERT-Ro** în alte grupuri (ex: conferințe, sesiuni de lucru etc.)
6. Asigurarea de asistență și contribuții altor echipe și proiecte
7. Îndrumarea personalului tânăr.

4. Specialist Remediere Vulnerabilitate

Calificare minimă:

BSc în calculatoare, informatică, management informatic sau echivalent 10 ani experiență ca administrator de sistem sau rețea, creator de software, administrator de baze de date sau similar sau MS în calculatoare, informatică sau management informatic sau echivalent plus 8 ani experiență ca administrator de sistem sau rețea, creator de software, administrator de baze de date sau similar, PhD în calculatoare, informatică sau management informatic sau echivalent plus 6 ani experiență ca administrator de

sistem sau rețea, creator de software, administrator de baze de date sau similar. Se iau în considerare și alte pregătiri de natură tehnică cu experiența descrisă mai sus.

Experiență și cunoștințe expert în:

- Probleme de securitate pe Internet
- Metodologii comune de dezvoltare
- Defecte comune de software (ex. supraîncărcare buffer)
- Dezvoltare de software și programare în limbaje multiple
- Administrare de Sistem, baze de date și rețea
- Sisteme de operare multiple
- Protocoale comune Internet (ex: TCP/IP, ICMP, DNS, HTTP etc.)
- Teorie și practică în criptografie

Lucrări publicate și prezentări formale în mai multe dintre următoarele subiecte

- posibile îmbunătățiri ale DND și protocoalelor de rutare cum ar fi BGP sau OSPF
- analiză de bază a sistemelor de calculatoare sau a altor echipamente electronice
- analizarea de volume mari de date de sistem și rețea pentru evaluare vulnerabilitate.

Trebuie să aibă următoarele capacități

- evaluarea rapidă a probelor
- separarea faptelor de păreri, speculații și posibilități
- dezvoltarea de planuri de acțiune în absența informațiilor complete pregătindu-se în același timp pentru orice evenimente neprevăzute
- informare pentru orice evenimente neprevăzute
- capacități foarte bune de comunicare în scris și verbal
- capacitatea de stabilire a priorităților de lucru
- interacționarea eficientă cu reporteri, administratori de sistem și rețea, furnizori, experți, utilizatori Internet, sponsori, persoane care elaborează politici în domeniu, manageri și personal
- lucru în echipă sub coordonare în caz de urgențe
- capacitatea de a lucra calm și bine sub presiune
- recunoașterea și tratarea în mod corespunzător a informațiilor confidențiale și sensibile
- capacitate de comunicare eficientă în situații normale sau de stres
- capacități de conducător și îndrumător

Capacitatea de a lucra sub presiunea limitelor de timp.

Trebuie să treacă verificarea de bază, să obțină aprobare și să fie cetățean român.

Funcții esențiale:

1. Dezvoltarea de strategii avansate legate remediere vulnerabilitate inclusiv strategii de comunicare cu furnizorii software, protecția infrastructurii critice, comunicare cu comunitatea IT, strategii avansate de management de acoperirea problemelor de securitate și alte tehnici legate de remedierea vulnerabilității.
2. Cercetare, specificare și dezvoltare de noi instrumente, procese și tehnici de îmbunătățire a tehnicilor de remediere a vulnerabilității și susținerea publicării, comunicării în siguranță și interacțiunii cu cei interesați
3. Scrierea și publicarea de documente care să descrie strategiile de atenuare a vulnerabilităților
4. Corespondență cu furnizori de software, cercetători din domeniul vulnerabilității, sponsori și alte părți interesate
5. Reprezentarea **CERT-Ro** în alte grupuri (ex. conferințe, sesiuni de lucru etc.)
6. Asigurarea de asistență și contribuții altor echipe și proiecte SEI.
7. Îndrumarea personalului tânăr.
8. Gata de a răspunde urgențelor pe Internet (în afara orelor normale de lucru)
9. Să acționeze ca supervisor pentru echipa care se ocupă de vulnerabilitate.

5. Practici, Dezvoltare și pregătire

Calificare minimă:

MS in Calculatoare, Inginerie Electronică sau Informatică cu un an experiență.

Cel puțin experiență relevantă și ca administrator de sistem/rețea într-un mediu TCP/IP sau foarte bune cunoștințe de UNIX/LINUX în mediu de instruire profesional. Aceasta include experiență în predare tehnică. Forte bună pregătire și cunoștințe de administrare securitate care să includă configurație firewall pentru tabele IP, Tripwire, Syslog, TCPDump și Snort, ca și implementări FreeSWAN IPSEC și scriptare shell/Perl. Experiență la scriere și dezvoltare curs și exerciții de securitate Linux. Experiență foarte serioasă de programare în C/C++. Java, XML și Perl.

Candidatul trebuie să poată stabili priorități de lucru și să respecte termenele de lucru, să ai capacitatea de rezolvare a problemelor tehnice, să aibă capacități foarte bune organizatorice analitice și de informare, capacități excelente de comunicare în scris și verbal, foarte bune capacități de predare tehnice. Trebuie să poată să lucreze la mai multe sarcini și să lucreze eficient cu mai multe echipe de proiect și sponsori/clienti. Se cer performanțe tehnice cu sistemele de operare și cunoștințe detaliate de protocoale de rețea.

Abilitate de a fi atent la detalii, de a respecta termenele limită, de a lucra sub presiune și de a comunica eficient.

Candidatul trebuie să treacă verificarea de bază, să obțină aprobare și să fie cetățean român.

Funcții esențiale:

1. Să elaboreze și să dezvolte documente tehnice și materiale de pregătire.
2. Să instaleze/configureze hardware și software inclusiv tehnologii noi care necesită examinare din punct de vedere al securității informaționale
3. Să facă pregătire tehnică și de management cu clienții
4. Să îndrume, ghideze și să interacționeze cu echipa și personalul
5. Să contribuie la planificare și strategia de tranziție .

6. Analist**Calificare minimă:**

BS în Calculatoare, Informatică sau echivalent cu 3 ani de experiență, MS în Calculatoare, Informatică sau echivalent cu 1 an de experiență, sau recent Ph.D în Calculatoare, Informatică sau echivalent .

Total 3 de experiență în elaborarea și analiza seturilor complexe de date, instrumente de construcție pentru analiză și generarea de rapoarte și limbaje de script și/sau programare în limbaje C++, JAVA, sau echivalent.

Abilități:

- Capabil să lucreze cu volum mare de lucru și să stabilească priorități
- Capacități foarte bune de rezolvare probleme
- Excelente capacități de comunicare în scris și verbal
- Capacitatea de a lucra atât independent cât și în echipă

Capacitatea de a lucra bine sub presiune și cu termene limită, de a stabili priorități, de a asista utilizatorii în varierea competențelor, de a interacționa cu furnizori, manageri și personalul tehnic, capacitate de a rezolva probleme tehnice, capacități foarte bune organizatorice, excelente capacități de comunicare în scris și verbal, menținerea confidențialității informațiilor.

Candidatul trebuie să treacă verificarea de bază, să obțină aprobare și să fie cetățean român.

Funcții esențiale

1. Participarea la elaborarea sistemelor de analiză
2. Participarea la analiza integrată a bazelor de date de evenimente
3. Conducerea realizării raportului de analiză al CERT-Ro
4. Contribuții la conferințe și întâlniri inclusiv prezentări; contacte de marketing cu clienții

5. Contribuții în revizuirea instrumentelor din literatura de specialitate și comerciale pentru interceptarea de date.

7. Administrator Sistem

Calificare minimă:

BS în Calculatoare, Informatică sau echivalent cu 8 ani de experiență, MS în Calculatoare, Informatică sau echivalent cu 5 ani de experiență, sau Ph.D în Calculatoare, Informatică sau echivalent cu 3 ani de experiență.

Experiență de management de proiect inclusiv experiență în crearea și actualizarea infrastructurilor de calcul.

Nivel de cunoștințe pentru administrator de sistem pentru sisteme de operare UNIX sau Windows, experiență în selectarea, configurarea și desfășurarea hardware și software asociat. Experiență și cunoștințe în utilizarea instrumentelor de administrare sistem pentru mai multe echipamente și configurații.

Cunoștințe de administrator de rețea pentru tehnologii de rețea inclusiv: TCP/IP, UDP, Ethernet, 802.11, protocoale de rutare, DNS. Experiență în arhitectură și implementare rețea.

- Capabil să lucreze cu volum mare de lucru și să stabilească priorități
- Capacități foarte bune de rezolvare probleme
- Excelente capacități de comunicare în scris și verbal
- Capacitatea de a lucra atât independent cât și în echipă
- Capacitatea de a lucra la mai multe proiecte
- Capacitatea de a face față cerințelor tehnice
-

Capacitatea de a lucra bine sub presiune și cu termene limită, de a stabili priorități, de a asista utilizatorii în varierea competențelor, de a interacționa cu furnizori, manageri și personalul tehnic, capacitate de a rezolva probleme tehnice, capacități foarte bune organizatorice, excelente capacități de comunicare în scris și verbal, menținerea confidențialității informațiilor.

Candidatul trebuie să treacă verificarea de bază, să obțină aprobare din partea autorităților de securitate și să fie cetățean român.

Funcții esențiale:

1. Colectează datele privind necesitățile de software și servicii necesare echipelor de Analiză de Artefact și Vulnerabilitate
2. Testează, evaluează și selectează hardware și software noi

3. Lucrează cu personalul CERT-Ro pentru elaborarea și/sau implementarea instrumentelor și proceselor de management și software și hardware din laborator, inclusiv executarea de experimente
4. Planificarea experimentelor, obținerea cerințelor experimentelor, executarea de instalări de laborator, asistență la experimente.

8. Specialist informare tehnică

Cerințe:

Poziția este responsabilă de calitatea finală a conținutului produs de către grupul CERT-Ro. Aceasta include producerea de alerte de securitate și descrieri tehnice detaliate ale amenințărilor de securitate în rețea sau web și informațiile necesare pentru atenuarea acestora de către clienții.

O parte cheie a poziției este lucrul cu omologi din toată lumea pe proiecte de dezvoltare conținut și pentru asigurarea consecvenței în informațiile de securitate oferite de alte unități de răspuns de securitate.

Candidatul va avea zilnic legătură strânsă cu echipa tehnică de răspuns de securitate pentru a înțelege fondul tehnic al problemelor clienților și a soluțiilor la acestea, verificând și editând conținutul asigurat de echipă unde este cazul pentru a adera la liniile directoare. Este de asemenea responsabil de monitorizarea web-site-urilor din domeniu pentru a obține informații legate de noi amenințări. Este de asemenea responsabil de editarea informațiilor pe site-ul CERT-Ro după aprobare.

În timpul unui incident de securitate, candidatul trebuie să lucreze ca parte a echipei de răspuns. I se va cere să adune informațiile de securitate fără a avea o înțelegere completă a naturii amenințării. Va fi responsabil de a hotărî care dintre informații sunt importante și trebuie date clientului imediat, ce informații se dau la nivel intern și ce informații necesită detalieri suplimentară.

9. Consultant Securitate

Cerințe:

Participă la proiecte de consultanță și implementare folosind concepte profesionale și politicile și procedurile companiei pentru a evalua și rezolva diverse probleme. Consultant la acest nivel va avea expertiză pe probleme la nivel mediu al portofoliului de soluții de securitate. Evaluează factorii și dă soluții în cadrul larg al practicilor și politicilor bine definite în selectarea metodelor, tehnicilor și criteriilor de evaluare pentru obținerea de rezultate. Ca parte a echipei poate conduce părți ale proiectelor și/sau poate conduce proiecte mici de consultanță inclusiv testarea, implementarea și documentarea soluțiilor de securitate.

10. Inginer Răspuns Securitate

Cerințe:

Acest rol combină responsabilități de răspuns rapid la noile amenințări de securitate în domeniu și răspuns la problemelor supuse de clienți echipei CERT-Ro. Principala responsabilitate a candidatului este de a revedea problemele supuse direct de către clienți fie fișierele scoase de pe Internet și de a crea informații și detectări de anti-virusi pentru aceștia care să fie puse pe website-ul CERT-Ro. Cum acestea sunt probleme tipice de client, mare parte a lucrului trebuie făcut în limite stricte de timp. Candidatul trebuie să identifice noi amenințări, să le dezasambleze și să le determine rapid funcționalitatea. Din propria sa analiza el trebuie să determine apoi metoda adecvată de detectare a amenințării și scrie o semnătură pe baza tehnologiei de detectare disponibile din produsele de securitate ale CERT-Ro. Se elaborează apoi un document care descrie amenințarea și modul de îndepărtare din sistemele afectate. Candidatul trebuie ocazional să lucreze în situații de mare tensiune rămânând în același timp concentrat pe sarcina de îndeplinit. Datorită lucrului cu alți membri ai CERT-Ro în multe cazuri din alte locații geografice, sunt necesare capacități excelente de comunicare în scris și verbal. Candidatul trebuie să poată lucra cu supervizare minimă și să asigure îndeplinirea atât a scopurilor proiectului cât și a cerințelor clienților. Se cer capacități foarte bune de rezolvare de probleme și depanare cum o soluție completă la problemele întâlnite poate să nu fie clară sau pur și simplu să nu existe.