DEZVOLTAREA ŞI ADMINISTRAREA WEBSITE-ULUI PROTOTIP CERT.RO PRINTR-UN INSTRUMENT SOFTWARE DE CONTENT MANAGEMENT BAZAT PE PROIECTUL OPEN SOURCE – JOOMLA

Marinescu Ion Alexandru

ionut@ici.ro

Institutul Naţional de Cercetare – Dezvoltare în informatică, ICI, Bucureşti

Rezumat: În acest articol vom prezenta modul de realizare al site-ului CERT.ro. Scopul acestui site este de a realiza un cadru informaţional adecvat în domeniul securităţii informaţiei la nivel naţional, prin constituirea unor baze de date cu incidente raportate de către diverse entităţi. Acest cadru informaţional furnizează răspunsuri la incidentele raportate, identifică formatele cele mai adecvate în transmiterea de date, facilitează cooperarea la nivel naţional şi internaţional, precum şi accesul la surse de informare externă.

Cuvinte cheie: CERT, CMS, Joomla, incidente de securitate, alerte de securitate, raportări incidente

Abstract: The paper presents the implementation of the CERT.ro site. The purpose of this site is to design an adequate information framework in the area of "cyber - security" on national level, by creating databases with incidents reported by vary entities. This information framework offers answers to reported incidents, identifies the most adequate information transfer media, facilitates national and international cooperation, as well as, access to external information resources.

Keywords: CERT, CMS, Joomla, security incidents, security alerts, reporting incidents

1. Introducere

Pentru a explica scopul site-ului CERT.ro, vom pleca de la definiţia unei structuri de tip CERT, folosită pe scară largă la identificarea, izolarea şi remedierea incidentelor de securitate şi a vulnerabilităţilor ce apar neîncetat odată cu dezvoltarea şi propagarea noilor tehnologii şi a internetului şi care pot pune în pericol chiar funcţionarea normală a societăţii umane atât de dependentă de aceste structuri tehnologice.

CERT – Computer Emergency Response Team reprezintă răspunsul la aceste incidente din reţelele şi sistemele de calculatoare, reprezentând o *comunitate* a echipelor de răspuns la incidente şi *un mediu de comunicare şi cooperare* între echipele specializate din orice organizaţie în managementul incidentelor de securitate, capabilă să mobilizeze resursele cele mai diverse ale unei organizaţii sau ale societăţii în scopul minimizării efectelor acestor incidente şi a recuperării rapide a funcţionalităţii afectate de incident.

La noi în ţară site-ul CERT.ro a fost gândit ca un nucleu de dezvoltare pentru viitoarele structuri de tip CERT (Computer Emergency Response Team) în mediul IT din România. CERT reprezintă un cadru informaţional pentru toţi utilizatorii sistemelor IT&C astfel încât aceştia să găsească o cale de rezolvare la problemele de securitate a informaţiilor cu care se confruntă la un moment dat, conform posibilităţilor fiecăruia dar şi cu sprijinul comunităţii IT&C.

CERT.ro *nu este o suprastructură a statului* care să impună reguli partenerilor implicaţi în schimbul şi prelucrarea de informaţii ci este un punct de contact şi un for de discuţii între toţi partenerii sociali cu interese în domeniul securităţii informaţiilor şi reţelelor IT&C.

2. Obiectivele şi publicul ţintă

2.1 De ce trebuie CERT.ro?

- pentru că se impune o viziune modernă, integratoare în domeniul securităţii şi în România, deşi securitatea informaţiilor şi a reţelelor de calculatoare şi de comunicaţii a fost şi este o preocupare permanentă a mediului IT&C din ţară;
- criminalitatea informatică este în creştere pe plan mondial, iar România este văzută din exterior ca un factor exportator de instabilitate în domeniu;
- continuarea dezvoltării serviciilor societăţii informaţionale necesită încredere din partea utilizatorilor. Această încredere poate fi periclitată prin proliferarea criminalităţii electronice, prin creşterea numărului de incidente din reţele şi a prejudiciilor produse de acestea;
- un nivel de securitate confortabil în reţelele IT&C poate fi atins numai în condiţiile cooperării tuturor factorilor cu responsabilităţi şi a tuturor participanţilor la "trafic".

2.2 Obiectivele activităţii site-ului CERT.ro

- constituirea unui centru naţional pentru diseminarea de informaţii privind instrumentele de securitate şi ghiduri de „bună purtare” în mediul virtual pentru diferite categorii de utilizatori, în limba română, adaptate mediului socio-profesional din ţară;
- constituirea unor baze de date, certe, utilizabile de specialiştii din domeniu pentru analize statistice aduse la zi, privind incidentele de securitate în care România este implicată, pentru a găsi cele mai adecvate măsuri de contracarare şi limitare a prejudiciilor;
- constituirea unei infrastructuri de comunicaţii şi baze de date privind securitatea mediului IT&C ca nucleu de coagulare a unei comunităţi de specialişti în domeniu;
- aducerea la aceeaşi „masă rotundă” de discuţii a specialiştilor IT&C ai autorităţilor, ofertanţilor de servicii IT&C, comercianţilor, producătorilor şi beneficiarilor pentru a analiza problemele cu care se confruntă, dar şi pentru a găsi soluţii viabile şi căi de cooperare în creşterea nivelului de securitate al mediului IT&C din România;
- efectuarea de activităţi de cercetare privind incidentele de securitate din reţelele IT&C şi a simptomelor acestora la nivelul sistemului, reţelei şi al societăţii constituind o sursă de informare pentru mediul IT, dar şi pentru publicul larg, utilizator de servicii IT;
- cristalizarea şi uniformizarea conceptelor specifice domeniului şi diseminarea acestora în comunitatea specialiştilor din domeniu;
- atragerea în activităţile centrului a unor specialişti de valoare, dedicaţi domeniului, capabili să lucreze în echipă.

2.3 Acest site se va adresa cu precădere:

- autorităţilor statului cu atribuţii în domeniul securităţii informaţiilor, a reţelelor, şi a dezvoltării şi implementării programelor privind serviciile e-Gov şi a societăţii informaţionale;
- membrilor Comitetului de Coordonare constituit prin HCSAT;
- specialiştilor din domeniul securităţii IT&C nevoiţi să repună în funcţiune sistemele afectate de incidente;
- specialiştilor din domeniul IT;
- providerilor de servicii IT&C;
- producătorilor şi vânzătorilor de produse IT;

- producătorilor şi comercianţilor de soluţii de securitate;
- utilizatorilor serviciilor IT&C:
    - structurilor de tip CERT deja înfiinţate cu o ofertă de cooperare;
    - structurilor de securitate din toate tipurile de organizaţii;
    - echipelor IT cu sarcini pe linie de securitate IT&C;
    - utilizatorilor de servicii IT&C cu pregătire tehnică;
    - utilizatorilor de servicii IT&C fără pregătire tehnică.

2.4 Accesul la informaţii

CERT.ro a fost proiectat astfel încât accesul la bazele de date din site să se realizeze pe următoarele niveluri:

- acces public neîngrădit la informaţiile privind legislaţia, politicile de securitate, ghiduri de bună practică, reglementările şi standardele din domeniu;
- acces public monitorizat, prin înregistrare şi confirmare, la informaţiile privind vulnerabilităţile cunoscute şi acoperite prin patch-uri de firmele producătoare precum şi a principalelor tipuri de atacuri utilizate. Accesul public va fi structurat pe două tipuri de informaţii:
    - pentru utilizatori experimentaţi;
    - pentru utilizatori neexperimentaţi.
- accesul autorităţilor – conform dreptului conferit de lege în baza necesităţii îndeplinirii atribuţiilor de serviciu.

CERT.ro oferă suport reactiv şi preventiv în privinţa incidentelor informatice precum fraudele electronice şi alte incidente. Accesul şi navigarea pe site este sunt monitorizate şi înregistrate.

3. Structura site-ului CERT.ro

Plecând de la obiectivele şi scopul site-ului CERT.ro, următorul pas constă în definirea design-ului funcţional sau ceea ce site-ul va permite utilizatorilor să realizeze.

În continuare vom prezenta:

- definirea funcţionalităţilor şi a conţinutului site-ului CERT.ro;
- determinarea secţiunilor care alcătuiesc site-ul CERT.ro şi a structurii paginilor web;
- navigare în CERT.ro.

3.1 Funcţionalităţile site-ului CERT.ro

A) Căutarea informaţiilor pe site

Funcţia de căutare avansată – returnează rezultate după mai multe criterii cum ar fi: articole, legături web, legături de contact, categorii, secţiuni, news feeds.

Căutarea se poate realiza după: toate cuvintele cheie, oricare dintre cuvinte, sau după fraza exactă. Ordonarea rezultatelor căutarii se poate face: alfabetic, după cel mai recent conţinut sau după cel mai vechi.

B) Servicii oferite utilizatorilor

RSS feeds, formular de raportare incidente, formular de raportare vulnerabilităţi, formular de raportare phishing, formular de raportare spam, asistenţă şi documentaţie CERT, politici şi proceduri CERT, ghid de bune practici, atenţionare incidente, atenţionare vulnerabilităţi, alerte, sfaturi de securitate, zonă privată comunitate CERT (acces permis pe baza de login si parolă),

educație şi învățare (training);

C) Media

Lista actualizată cu evenimente viitoare, arhivă evenimente, arhivă documente, documente cheie, interviuri şi articole (pdf), FAQ, foto & video (plug-ins, streaming), ilustrații, publicații, legislație (cadru reglementat), standarde, referințe, termeni şi condiții;

D) Interacțiune cu vizitatorii

Formular contact, informații de contact, oportunități de angajare, adresă poştală, localizare pe hartă, telefon, fax, email;

E) Accesibilitate

Modificare mărime text pagină, suport multilingvism, legături web externe, printare în pagină, transformare pdf, site-uri partenere, linkuri utile, dicționar terminologic, conținut personalizabil - Open Source Content Management System Joomla, declarație de accesibilitate, validare CSS, validare XHTML;

F) Navigare rapidă în site

Hartă site, breadcrumbs şi wayfinding (localizare în interiorul site-ului), back to the top links, cuvinte cheie;

3.2 Secțiunile site-ului CERT-RO şi structura paginilor web;

Site-ul CERT-RO este alcătuit din două secțiuni:

- secțiune publică;
- secțiune privată.

Secțiune publică – se înțelege acea parte generală din site ce poate fi consultată sub restricția termenilor şi condițiilor de utilizare, în orice moment. Această parte este compusă din documentație, atenționări incidente, vulnerabilități, raportări, contact.

Secțiune privată – reprezintă secțiunea destinată membrilor comunității CERT, accesibilă doar pe bază de înscriere şi emitere de către administratorul sistemului a unui login şi a unei parole. Aici se pot consulta documente specifice plus toate opțiunile destinate secțiunii publice.

Structura paginii este definită din şase zone:

A – zona superioară în care se găsesc elementele grafice de identificare şi meniul principal de navigație;

B – zona centrală în care este prezentat conținutul efectiv;

C – zona stângă în care este prezent meniul secundar 1 şi calendarul evenimentelor viitoare;

D – zona dreaptă împărțită în patru secțiuni pentru: modulul de căutare, alerte de securitate, incidente, vulnerabilități;

E – zona inferioară a paginii, împărțită în patru secțiuni, pe toată lățimea paginii cu informații specifice CERT;

F – ultima zonă a paginii care include informațiile despre copyright şi informații de reglementare în domeniul tehnologiilor web.

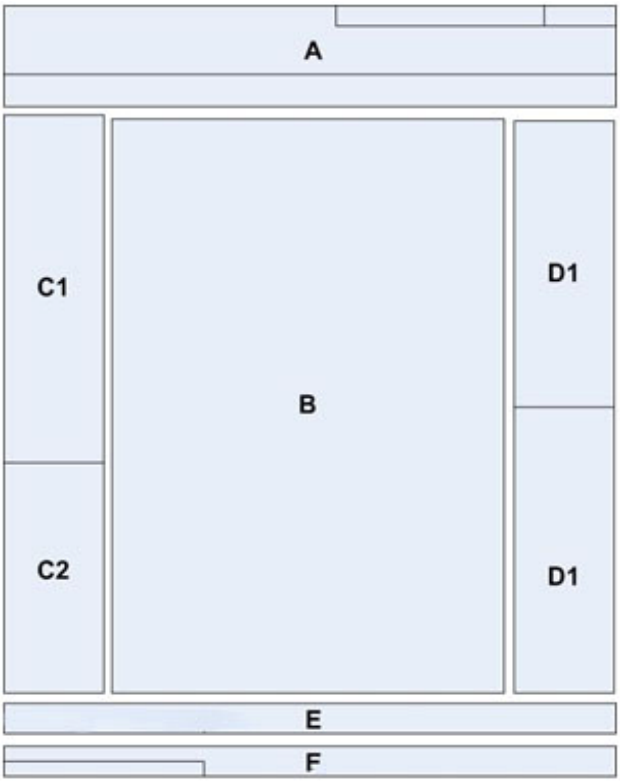

Figura 3.2-1. Structura paginilor web

3.3 Navigarea în site-ul CERT.ro

Navigarea în site-ul CERT.ro a fost gândită sub forma unui *meniu principal* (vezi fig.3.3-1) care asigură deplasarea între domeniile de interes ale site-ului prin selectarea subdomenilor aferente şi *patru meniuri secundare* care îmbunătățesc şi simplifică căutarea informațiilor dorite. Meniul principal este plasat în zona A din cadrul structurii paginilor web(vezi figura 3.2-1).

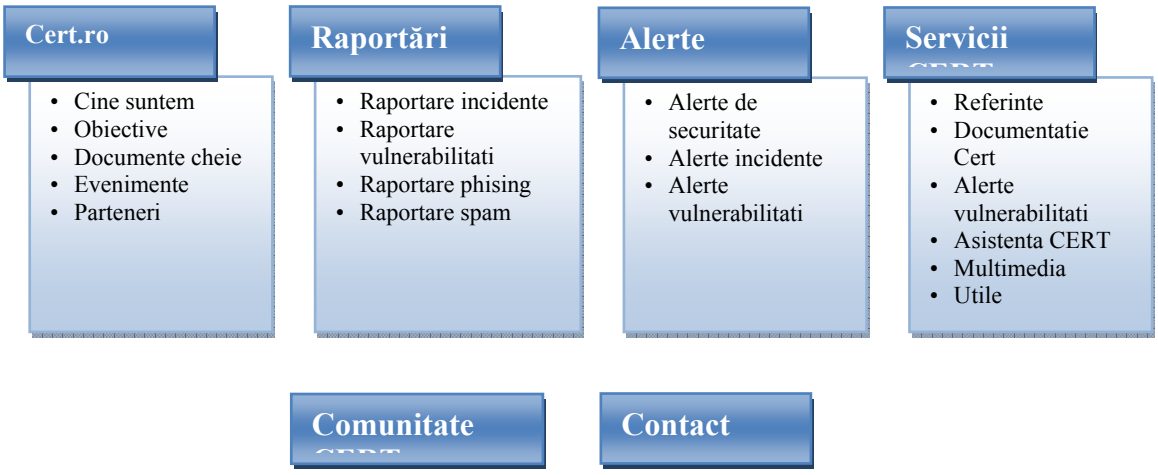

Figura 3.3-1. Meniul principal cu domeniile şi subdomeniile site-ului CERT.ro

Meniul secundar 1 (fig. 3.3-2) reprezintă o extensie a elementelor meniului principal, schimbându-şi componența funcție de domeniul selectat. Se regăseşte în secțiunea C1 din figura 3.2-1.

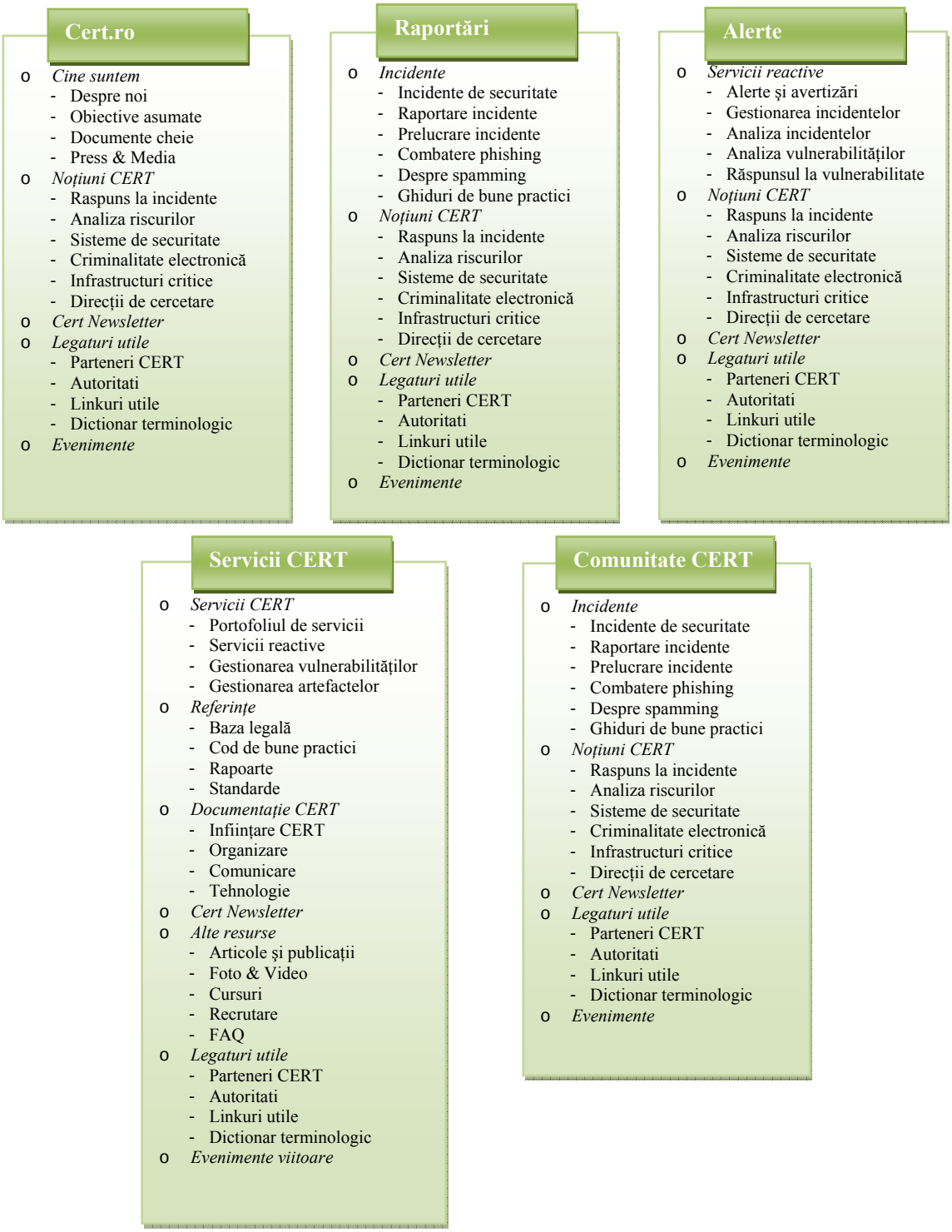

Figura 3.3-2. Meniul secundar 1

Meniul secundar 2 este împărţit în patru secţiuni: modul de căutare, alerte de securitate, incidente şi vulnerabilităţi. Se regăseşte în secţiunea D din figura 3.2-1.

Meniul secundar 3 (fig. 3.3-3) împărţit în patru secţiuni pe toată lăţimea paginii cu informaţii specifice CERT este fix şi disponibil în fiecare pagină a site-ului. Se regăseşte în secţiunea E din figura 3.2-1.

Figura 3.3-3. Meniul secundar 3 şi meniul secundar 4

Meniul secundar 4 conţine informaţiile de copyright şi de reglementare a condiţiilor de utilizare a site-ului. La fel ca meniul secundar 3, este un meniu fix ce îşi păstrează componenţa în toate paginile site-ului. Se găseşte sub meniul secundar 3 (vezi fig. 3.3-3), în secţiunea F din figura 3.2-1.

4. Dezvoltarea şi administrarea site-ului CERT.ro utilizând sistemul Joomla

În acest capitol va fi prezentat modul în care componentele sistemului Joomla au fost utilizate în realizarea site-ului CERT.ro.

Sistemul Joomla a permis ca în modul de proiectare a site-ului CERT.ro să existe o separare între aparenţa sa vizuală (aspectul) ca sumă a tuturor elementelor de formatare şi poziţionare a conţinutului în pagină şi conţinutul propriu-zis.

Joomla permite ca prin interfaţa sa de Front-end, vizitatorii şi utilizatorii înregistraţi cu drepturi restrînse (Author, Editor sau Publisher), stabilite de către administrator în interfaţa de administrare, pot avea acces la conţinutul şi funcţionalităţile site-ului CERT.ro.

Administrarea elementelor ce compun aspectul site-ului se realizează prin interfaţa de administrare (Back-end) de către utilizatori cu drepturi extinse de Administrator sau Super Administrator.

4.1 Componentele sistemului Joomla utilizate la site-ul CERT.ro

Componentele utilizate în structura paginilor site-ului CERT.ro sunt următoarele (vezi fig. 4.1-1):

- ✓ *Template*: container pentru toate elementele de ieşire de pe pagină. Acesta defineşte aspectul paginii şi locul fiecărui element.
- ✓ *Articles*: elemente de conţinut.
- ✓ *Modules*: furnizează elemente de ieşire şi de funcţionalitate în zona secundară de conţinut.
- ✓ *Plugins*: îmbunătăţeşte funcţionalitatea articolelor, componentelor şi modulelor.

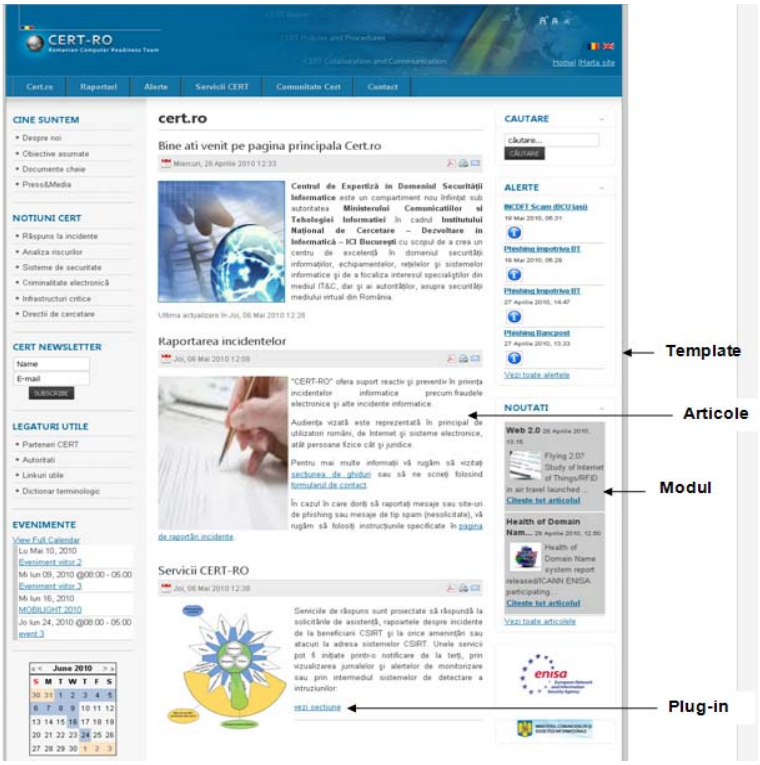

Figura 4.1-1. Interfaţa utilizator CERT.ro şi structura sa funcţională

4.1.1 Template-ul JaPurity - Şablonul utilizat pentru site-ul CERT.ro

Template-urile sunt elemente care determină aspectul paginii sau interfaţa site-ului. Template-urile sunt interschimbabile şi modificabile, în sensul că acelaşi conţinut poate fi afişat în structuri diferite. Template-urile pot fi văzute ca un pachet ce conţine în esenţă un fişier (index.php) ce stabileşte aşezarea modulelor în pagină şi un fişier (template_style.css) care stabileşte tema grafică / designul paginii. În jurul acestor două fişiere sunt adăugate restul componentelor, imaginilor şi funcţiilor ce dau dinamism şi culoare unui site web (spre exemplu funcţiile javascript). Template-urile sunt colectate în interiorul Template Manager (vezi fig. 4.12) iar de aici pot fi modificate.

Figura 4.1-2. Template Manager

Template-ul JaPurity este oferit odată cu instalarea pachetului Joomla şi a fost adoptat la realizarea CERT.ro deoarece îndeplineşte mai multe cerinţe pentru acest site şi anume: uşurinţă în realizarea meniurilor drop-down şi numărul mare de parametri modificabili care permit

modificarea lățimii şablonului, a schemei de culoare şi a altor elemente de design. S-a dorit ca păstrând funcționalitățile de bază neschimbate ele acestui template, să se poată implementa un design distinctiv prin elemente grafice originale şi poziționări în pagină diferite.

Pentru a ajunge la forma finală a site-ului, s-a modificat cu precădere fişierul template.css care controlează aspectul şi poziționarea elementelor din site, prin schimbarea elementelor de fundal din header, modificarea dimensiunilor paginii, a culorilor şi a poziției elementelor de navigare. În figurile 4.1-3 şi 4.1-4 se poate compara tempate-ul de bază şi aspectul acestuia modificat (lățimea paginilor, schema de culori, logo-ul de identificare, dispunerea modulului de căutare, modificarea meniurilor drop-down, afişarea articolelor-conținutului).

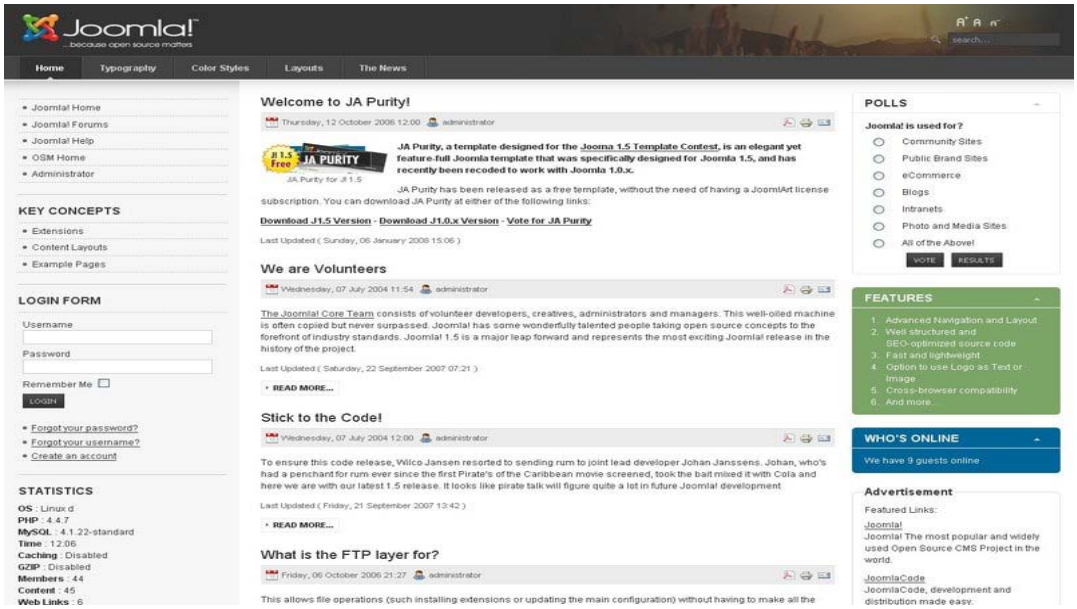

Figura 4.1-3. Template-ul JaPurity original

Figura 4.1-4. Template-ul JaPurity modificat

4.1.2 Module

Modulele (modules) ajută componentele sau site-ul să afişeze anumite porţiuni de conţinut sau anumite informaţii, pe marginile paginii sau în locuri special create pentru a fi ocupate de acestea. Un template Joomla are integrate poziţii în jurul conţinutului principal al paginii, pe stânga, dreapta, în antet şi subsol, deci modulele se vor afişa "în jurul" componentei care generează pagina. Cele mai importante module din site sunt cele de tip *meniu* (mod_mainmenu), *căutare* (mod_search*), feed RSS* (mod_syndicate) sau *login* (mod_login).

Într-o pagină din site-ul CERT.ro se pot observa diferitele tipuri de module utilizate (vezi fig.4.1-5), aşa cum apar ele în front-end-ul vizitatorilor site-ului.

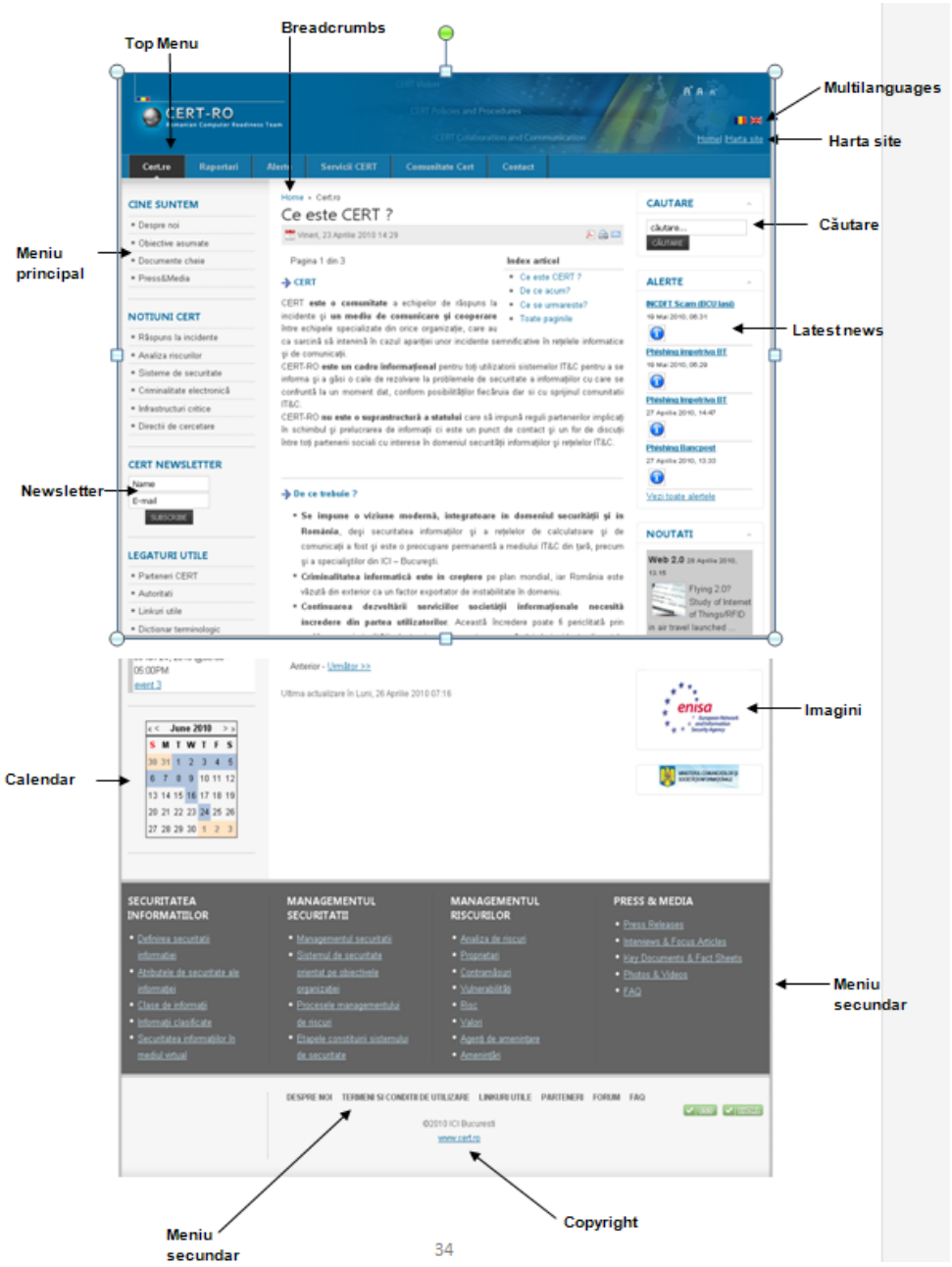

Figura 4.1-5. Tipuri de module utilizate

4.1.3 Structura paginii principale (Home)

Pagina principală CERT.ro (Home) prezintă informații despre CERT-RO ca pilon principal în securizarea informațiilor la nivel național, cu o scurtă prezentare în preambul a misiunii CERT-RO urmată de materiale ce descriu în rezumat cele mai recente acțiuni efectuate în cadrul organizației cu posibilitatea prezentării lor detaliate în alte secțiuni. Din pagina principală putem naviga către toate celelalte secțiuni ale site-ului prin intermediul meniurilor.

În cadrul paginii principale putem remarca existența următoarelor componente ce oferă informații importante utilizatorilor: alerte de securitate actualizate permanent, calendarul activităților viitoare precum şi un modul de căutare (vezi fig. 4.1-5).

4.2 Funcțiile site-ului CERT.ro

4.2.1 Secțiunea raportări incidente

O funcție importantă din site-ul CERT.ro este reprezentată de secțiunea raportări, regăsită cu uşurință în meniul principal al site-ului şi care, prin intermediul formularelor completate de către utilizatori, raportează patru tipuri de evenimente: incidente, vulnerabilități, phishing şi spam.

Pentru a înțelege cât mai bine importanța acestui serviciu oferit de site-ul CERT.ro şi a rolului său în încercarea de a preveni, limita sau rezolva problemele legate de securitatea informatică, va trebui definită noțiunea de incident de securitate.

Prin incident de securitate, se înțelege orice încălcare a politicilor de securitate care pot afecta atributele de securitate ale informației, ca urmare a unor cauze naturale sau provocate cu intenție. Referința principală față de care se raportează incidentele de securitate este politica de securitate a organizației – orice încălcare a politicii de securitate reprezintă incident de securitate.

Instrumentul de raportare incidente este format dintr-un formular (vezi fig. 4.2-1) transmis pe cale electronică din site-ul CERT.ro, în care se vor completa câmpurile necesare identificării cât mai exacte a incidentelor şi transmiterii în timp util a unui răspuns adecvat. Acest formular poate fi accesat şi trimis din meniul principal ***Raportări → Raportare incident***.

Stare

Site aflat sub atac	Incident petrecut in trecut	Incidente repetate . ..	Nerezolvat .....

Informații de contact

Nume:	Titlu: .....
Organizatie:	
Telefon direct:	E-mail: . ...
Numele persoanei juridice / legale? de contact: .	Telefon: ....
Locatie / Site-uri implicate:	
Telefon principal:	Fax: ....

Impactul atacului

Pierdere / compromitere a timpului de functionare corecta a sistemului de date:	
Pagube aduse sistemelor:	Sisteme ale altor organizatii afectate: ....
Pierderi financiare (suma estimata: .... $):.....	
Pagube privind integritatea sau livrarea de bunuri, servicii sau informatii critice:	

Figura 4.2-1 Conținutul formularului de raportare

Realizarea acestui formular în interiorul site-ului CERT.ro s-a făcut prin utilizarea unui component denumit Fabrik în variantă Open Source, creat special pentru a construi formulare utilizând Joomla. Pentru a înțelege modul lui de funcționare, trebuie să plecăm de la definiția unui component.

Componentele *(components) sunt cele mai importante extensii, deoarece ele generează conținutul paginilor. Există însă şi componente care nu generează conținut, aşa cum ar fi componenta JoomlaPack de back-up al site-ului sau componentele de newsletter. Componentele au propriile panouri de configurare accesibile prin meniul* ***Joomla Components*** *şi se folosesc împreună cu module şi pluginuri care sunt dezvoltate special pentru fiecare tip de component.*

Pe lângă generarea formularului, componentul Fabrik va gestiona şi datele culese de la utilizatori, salvându-le în baza de date MySql. În versiunea comercială a acestui produs, există mai multe opțiuni de salvare şi de procesare a datelor precum şi de obținere a rapoartelor aferente.

4.2.2 Secțiunea alerte

Serviciul de alertare incidente face parte din categoria servicii reactive oferite de site-ul CERT.ro. Aceste servicii sunt oferite ca reacție la apariția unor incidente detectate de către echipa sau echipele CERT.ro. Aceste servicii sunt destinate rezolvării problemelor pe termen scurt. Site-ul CERT.ro tratează şi informează utilizatorii despre două tipuri de probleme legate de securitatea informatică: incidente şi vulnerabilități.

Prin ***vulnerabilități*** *înțelegem gradul în care, resursele informatice sunt susceptibile de a fi degradate, distruse sau expuse unui agent sau factor ostil.*

Meniul Alerte – afişează legături URL către cele mai recente atenționări din cele două categorii de incidente, oferind posibilitatea de a fi detaliate, fiecare în parte, printr-un singur click pe titlul prescurtat al incidentelor identificate.

Aceste alerte informează beneficiarii în legătură cu noi dezvoltări cu impact pe termen mediu şi lung, de exemplu vulnerabilitățile nou găsite sau instrumentele intruşilor. Alertele permit beneficiarilor să-şi protejeze sistemele şi rețelele împotriva oricăror probleme nou găsite, înainte ca acestea să poată fi exploatate.

Publicarea alertelor ca şi conținut în site-ul CERT.ro se face cu ajutorul modulului Open Source AiDa News (vezi fig. 4.2-2), care oferă o multitudine de opțiuni de extragere a conținutului unor articole din categoriile şi secțiunile dorite de administrator, şi afişarea acestuia sub formă prescurtată, de alerte, în condițiile impuse tot de administrator sau de utilizatorii cu drepturi de acces la Modul Manager.

Figura 4.2-2. Secțiunea Moduls Manager – Opțiunile modulului AiDa News

4.2.3 Configurația de bază a site-ului

Joomla, oferă prin interfața de administrare (vezi fig. 4.2-3), posibilitatea setării configurației de bază a site-ului CERT.ro prin care se pot modifica opțiunile de bază ale site-ului, platformei şi accesului la server. Aceste modificări se realizează doar de către utilizatorii cu dreptul de Super Administrator.

Modificarea configurației globale a site-ului se realizează accesând meniul **Site→Global Configuration**. În fereastra afişată (vezi figura 4.2-3) cele trei opțiuni de bază sunt următoarele:

- Site - configurații de bază ale site-ului (dezactivarea site-ului, descrierea şi cuvintele cheie globale);
- System - configurații de bază ale platformei Joomla;
- Server - configurații de bază privind interacțiunea platformei cu serverul.

Pentru site-ul CERT.ro au fost păstrate opțiunile predefinite Joomla, doar în opțiunea Site, categoria Metadata Settings ce se referă la configurări de metadate necesare identificării site-ului mai rapid de către motoarele de căutare (cuvinte cheie, descriere globală site), a fost adaptată la nevoile şi conținutul CERT.ro.

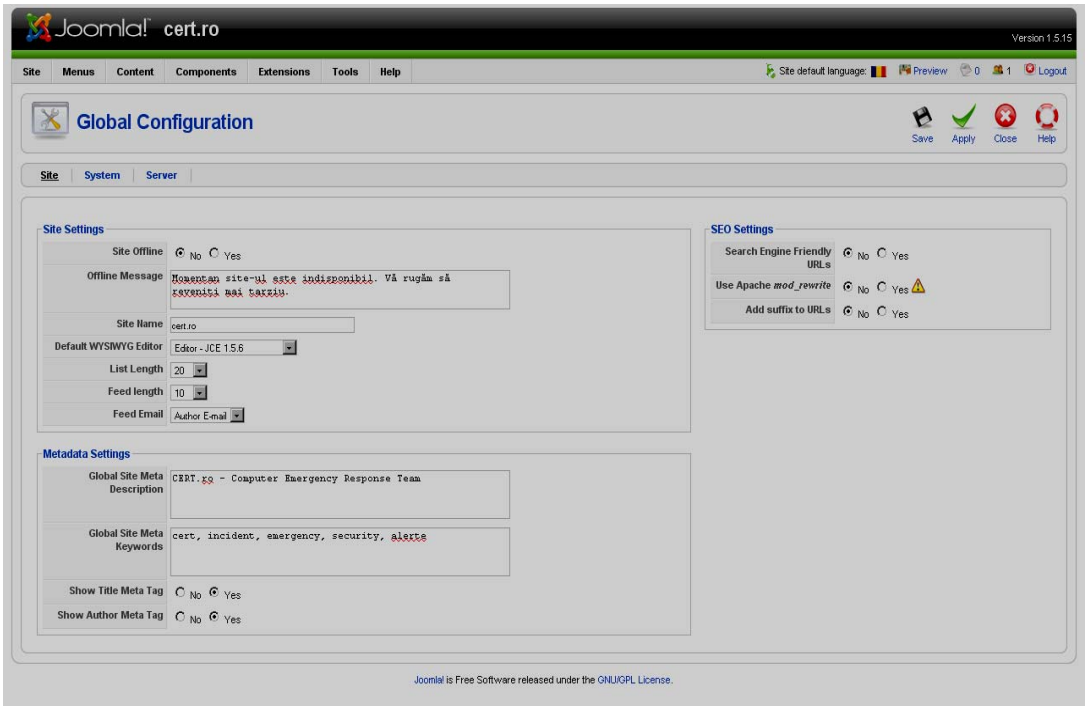

Figura 4.2-3. Secțiunea Global Configuration

5. Concluzii

Realizarea site-ului CERT.ro reprezintă un pas decisiv în construcția structurii CERT la nivel național ca un centru pilot de constituire a unei comunități a specialiştilor din domeniu şi de pregătire a lor. El va trebui să ofere servicii de mediere şi cooperare şi să ofere suportul tehnic şi informațional pentru activitatea structurilor de securitate din administrația de stat şi din mediul privat, cristalizarea şi uniformizarea conceptelor specifice domeniului şi diseminarea acestora în comunitatea IT.

Pentru a creşte gradul de utilizare şi interesul pentru secțiunile site-ului, accesul la bazele de date se va realiza pe două niveluri:

- acces public;
- acces public monitorizat.

Platforma de dezvoltare a acestui site face parte din categoria WCMS (Web Content Management System). S-a optat pentru soluția Joomla CMS. Acest instrument se poate utiliza în sistem liber (open source), nu necesită licențiere şi deci costurile de implementare şi utilizare sunt minime.

Pe tot parcursul procesului de realizare a site-ului, s-a urmărit realizarea unor interfețe intuitive şi prietenoase cu utilizatorul, în care orice informație să fie regăsită în cel mult trei click-uri de mouse, iar utilizatorul să ştie în permanență în ce secțiune a site-ului se găseşte.

Demonstrarea funcționalității acestui sistem pilot s-a realizat în cadrul departamentului **Centrului de Expertiză în Domeniul Securității Informatice**, compartiment nou înființat sub autoritatea **Ministerului Comunicațiilor şi Societății Informaționale,** în cadrul **Institutului Național de Cercetare – Dezvoltare în Informatică – ICI Bucureşti** urmând ca în urma analizelor, site-ul să devină public şi deplin funcțional.

BIBLIOGRAFIE

1. Improving CSIRT Communication Through Standardized and Secured Information Exchange – Teza de masterat - Sebastiaan Tesink 2005.
2. Joomla!Bible – Wiley Publishing, Inc – Ric Shreves.
3. http://www.cert-ro.eu/securitate_date/index.html
4. **MICAN, D., N. TOMAI, R. I. COROŞ:** Web Content Management Systems, a Collaborative Environment in the Information Society - Faculty of Economics and Business Administration, Babeş-Bolyai University.
5. Corporate Information Security Group – Reporting of the Best Practices and Metrics Team – SUA 2004.
6. Incident Management Capability Metrics – Software Engineering Institute 2007.
7. Incident Management Mission Diagnostic Method - Software Engineering Institute, 2008.
8. NIMS_core – National Incident Management System – SUA, 2008.
9. EISAS – European Information Sharing and Alert System - Studiu de fezabilitate ENISA 2006-2007.
10. **GRANCE, T., K. KENT, B. KIM:** Computer Security Incident Handling Guide — Recomandari NIST SP 800 – 61.
11. US-CCU Cyber-Security Chek List, John Bumgarner and Scott Borg, 2007.
12. Privacy Incident Handling Guidance – US Departament of Homeland Security, 2007.
13. Use of the Common Vulnerabilities and Exposures (CVE) Vulnerability Naming Scheme – Recomandari NIST – SP 800 – 51.
14. Guide to Malware Incident Prevention and Handling - Recomandari NIST – SP 800 – 83.
15. Guide to Integrating Forensic Techniques into Incident Response - Recomandari NIST – SP 800 – 86.
16. DIRECTIVA 2008/114/CE A CONSILIULUI din 8 decembrie 2008 privind identificarea şi desemnarea infrastructurilor critice europene şi evaluarea necesității de îmbunătățire a protecției acestora.