CMS (Content Management System)
Instrument de comunicare online pentru Administraţia Publică

Costel Ciuchi

Cristian Botan

Victor Ciobanu

Bucureşti, 2014

CUPRINS

1. Comunicare în mediul virtual. Transparenţă instituţională 5

1.1. Accesul la informații și transparența instituțională 5

1.1.1. Responsabilitate, Răspundere și Receptivitate 6

1.1.2. Noțiunea de acces la informații (factori în favoarea adoptării legislației, caracteristici legislative comune, beneficii)....12

1.1.3. Transparența instituțională (obiect, beneficii, participarea cetățenilor, acțiuni în cazul lipsei de transparență) 22

1.2. Conceptul de comunicare online 28

1.2.1. Comunicarea în instituțiile publice 28

1.2.2. Comunicarea interpersonală în administraţia publică 31

1.2.3. Comunicarea online și interacțiunea cu cetățeanul....31

2. Servicii electronice şi aplicaţii în spaţiul virtual 35

2.1. Noţiuni de bază privind spaţiul virtual (Internet) 35

2.1.1. Introducere....35

2.1.2. Standarde şi modele de referinţă 43

2.1.3. Clasificarea reţelelor 50

2.1.4. Conexiuni şi medii de transmisie....52

2.1.5. Adrese IP. Arhitecturi de reţele. Arhitectura client-server 58

2.1.6. Porturi. Socket-uri 67

2.1.7. Nume de domenii. Sistemul DNS 68

2.1.8. Uniform Resource Locator (URL) 73

2.2. Servicii Internet 75

2.2.1. Serviciul World Wide Web 75

2.2.2. Serviciul transfer de fişiere....78

2.2.3. Serviciul poştă electronică 80

2.2.4. Chat şi mesagerie instant 82

2.2.5. Fluxuri web. Fişiere şi fluxuri multimedia 87
2.2.6. Conexiuni Peer-to-Peer. Acces la distanţă (REMOTE) 101
2.2.7. Reţele sociale. Comunicare şi colaborare 105
2.3. Aplicaţii în spaţiul virtual 109
2.3.1. Arhitectura unei aplicaţii web generice 109
2.3.2. Model de utilizare în tehnologia web 110
2.3.3. Dezvoltarea unei aplicaţii pentru gestionarea unui flux organizaţional 120
2.4. Securitate şi confidenţialitate în internet 132
2.4.1. Model de securitate pentru un sistem 133
2.4.2. Politica de securitate a unei organizaţii 137
2.4.3. Vulnerabilităţi şi ameninţări în sistemul informatic 141
2.4.4. Programe dăunătoare (malware) 144
2.4.5. Atacuri cibernetice de impact asupra instituţiilor publice 149
3. Content Management Systems 158
3.1. Introducere în CMS 158
3.1.1. Noțiunea de Content Management System 158
3.1.2. Tipuri de CMS 161
3.1.3. Conceptul Open Source 164
3.2. Administrarea platformei Wordpress 165
3.2.1. Instalarea și configurarea platformei 165
3.2.2. Structura ierarhică a nivelurilor de acces 170
3.2.3. Adăugarea și editarea conținutului - Tutorial publicare articole în Wordpress 172
4. BIBLIOGRAFIE 179
5. ANEXE 182
ANEXA 1. DOMENII DE NIVEL SUPERIOR (TOP-LEVEL DOMAIN) 182
ANEXA 2 – GOV.RO - Evoluţia www.gov.ro – 2000 – 2014 184
ANEXA 3 – Identitatea vizuală unică în comunicarea online 187
ANEXA 4 – SEO 189

1. Comunicare în mediul virtual. Transparenţă instituţională

1.1. Accesul la informații și transparența instituțională

Discursurile publice şi, în special, cele electorale din întreaga lume cuprind, fără echivoc, exprimări precum „îmi asum responsabilitatea", „voi trage la răspundere", etc.

În societăţile democratice, puterea suverană aparţine poporului. În ciuda faptului că reprezintă autorităţi mandatate prin vot public, nivelul la care Executivul este tras la răspundere pentru actele sale se află la pragul minimal. Această situaţie de fapt nu îl absolvă însă de responsabilitatea îndeplinirii interesului general.

Practica demonstrează că relaţiile de răspundere în faţa legii nu funcţionează conform aşteptărilor, fiind uneori perturbate de influenţe externe sau chiar de acte de corupţie. Instituţiile publice sunt acaparate de către cei puternici şi avuţi, iar pe cale de consecinţă, resursele publice sunt direcţionate în beneficiul acestora. Astfel, interesele particularilor şi diferenţele de putere fac ca sistemul să devină disfuncţional şi incapabil de a se reforma din interior.

Definirea unor relaţii clare de responsabilitate şi răspundere, adoptarea legilor corespunzătoare şi a normelor de aplicare a acestora pot reprezenta puternice mecanisme colective de normalizare şi de consolidare a integrităţii publice.

Astfel de mecanisme legitimează acţiunile autorităţilor şi acţionează ca o protecţie împotriva abuzului în exercitarea funcţiei, încurajând societatea spre negocierea contractului social pe termen lung.

Secțiunea de faţă se concentrează asupra elementelor cheie ce caracterizează conceptele de responsabilitate, răspundere şi receptivitate ale entităţilor publice în exercitarea autorităţii de stat, având ca scop diferenţierea noţiunilor şi clarificarea interpretărilor ambigue din jurul acestora.

Printre întrebările ce trebuie avute în vedere în discutarea acestui subiect se numără următoarele:

- În faţa cui sunt *responsabile* şi *răspund* persoanele care ocupă funcţii sau demnităţi publice?
- Ce atribuţii sau sarcini se află în *responsabilitatea* acestora şi pentru ce fapte *răspund* în faţa legii?
- În ce măsură ar trebui administraţia să fie *receptivă* faţă de nevoile şi solicitările grupurilor de interese, partidelor politice sau interesului general al poporului?

În definitiv, admiţând principiul democraţiei constituţionale, conform căruia puterea publică izvorăşte din popor, ne întrebăm, în ce măsură şi prin intermediul căror

mijloace administraţia caută să devină, prin sine însăşi, răspunzătoare în faţa acestuia?

1.1.1. Responsabilitate, Răspundere şi Receptivitate

RESPONSABILITATE

Relativ la politicile publice şi în general activitatea guvernamentală, termenul de *responsabilitate* comportă implicaţii de ordin moral cu privire la angajamente asumate de către ocupantul unei funcţii, anterior începerii mandatului sau pe parcursul acestuia. Nerespectarea lor atrage cu sine sancţiuni politice sau administrative, însă fără ca acest lucru să aibă repercusiuni de natură penală, nefiind în concret vorba despre o încălcare a legii de către acesta.

Doctrina constituţională a sistemului de guvernare Westminster constituie sursa pentru două dimensiuni ale responsabilităţii: *responsabilitatea individuală a fiecărui ministru* şi cea *colectivă a Cabinetului, privit ca întreg*.

În cazul celei dintâi, responsabilitatea finală pentru acţiunile ministerului şi ale departamentelor acestuia o poartă ministrul. Cu alte cuvinte, este aşteptat ca în situaţii dovedite de risipă a resurselor publice, corupţie sau orice alt tip de comportament inadecvat ce are loc într-un minister, ministrul să îşi asume responsabilitatea şi, în final, să demisioneze. Această pretenţie este aşteptată independent de faptul că ministrul nu a fost implicat şi nu avea cunoştinţă cu privire la acţiunile cercetate. Chiar şi cu îndeplinirea condiţiilor enunţate anterior, ministrul se face responsabil pentru că a angajat sau girat menţinerea în sistem a persoanelor implicate în activităţile ilegale.

Demisia prin aplicarea responsabilităţii ministeriale individuale nu produce consecinţe asupra activităţii întregului Cabinetul şi se aşteaptă ca partidul sau coaliţia majoritară să desemneze un nou ocupant al fotoliului ministerial. Principiul responsabilităţii ministeriale individuale este considerat esenţial în funcţionarea statului, întrucât garantează că un reprezentant al puterii este responsabil pentru fiecare activitate a structurii pe care o conduce, motivând, totodată, miniştrii să acorde atenţie sporită fiecărei componente şi fiecărui departament ministerial. Contraponderea principiului constă în aceea că succesele înregistrate prin eforturile administraţiei publice sunt asumate drept reuşite ale Executivului. Unul dintre exemplele de bază ale asumării responsabilităţii ministeriale citat de literatura dreptului administrativ[1] îl constituie scandalul politic iscat ca urmare a afacerii de la Crichel Down, rezultat cu demisia ministrului britanic al Agriculturii.

În mod evident, fiind mai degrabă o regulă morală decât o normă clar prevăzută, asumarea răspunderii din partea miniştrilor pentru activitatea structurilor din subordine nu este un act obligatoriu, însă perpetuarea unei astfel de stări poate

[1] Alexandru, Ioan – *Drept Administrativ European*, Editura Universul Juridic, Bucureşti, 2008, ISBN 978–973–127–081–4, p. 91.

aduce prejudicii întregului Cabinet. După cum afirmam anterior, a doua dimensiune izvorâtă din sistemul britanic se referă la responsabilitatea colectivă a Cabinetului. Conform acesteia, membrii Executivului trebuie să sprijine în mod public politicile guvernamentale, independent de faptul că aceştia le dezagrează în plan personal. Acest sprijin nu se rezumă doar la nivelul declaraţiilor, ci se aşteaptă ca membrii Cabinetului să voteze politicile guvernamentale în Parlament.

Principiul are la bază ideea conform căreia Executivul este responsabil în mod colectiv în faţa Parlamentului, în situaţia în care cel din urmă iniţiază un vot de neîncredere a cărui reuşită ar conduce la demiterea întregului Cabinet. Chiar şi în democraţiile civilizate, practica demonstrează că acest principiu întâmpină dificultăţi[2] în implementare. Revenind la ideea de început a acestei secţiuni, responsabilitatea constituie o îndatorire morală a celor însărcinaţi să înfăptuiască puterea publică. Această îndatorire nu ar trebui să se rezume însă doar la responsabilitatea faţă de puterea legislativă, ci şi la cea faţă de cetăţeni. Unii autori[3] argumentează că pregătirea unor „administratori publici" de carieră, cu expertiză tehnică şi un simţ dezvoltat al interesului general reprezintă unica modalitate prin care responsabilitatea serviciului public ar fi orientată şi către cetăţean. Dimpotrivă, alţii afirmă că fără restricţia puterii discreţionare în limita atribuţiilor şi implementarea unui sistem sancţionator al funcţionarilor ce fac abuz de putere, nu va fi posibilă responsabilizarea serviciului public în faţa cetăţenilor.

RĂSPUNDERE

Molière remarca faptul că „suntem răspunzători nu doar pentru acţiunile pe care le facem, ci şi pentru inacţiunile şi indeciziile noastre". Răspunderea se numără printre acele concepte de aur care, cel puţin la nivel declarativ, nu sunt vreodată contestate şi pe care toată lumea le lauda şi încurajează. Aceasta se regăseşte tot mai des în discursurile electorale şi în documentele de politică publică, întrucât conferă o imagine de transparenţă şi încredere.

Una dintre definiţiile larg acceptate ale acestei noţiuni spune că răspunderea reprezintă „mijloacele prin care indivizii sau organizaţiile sunt constrânse să raporteze în faţa uneia sau mai multor autorităţi cu atribuţii speciale în acest sens şi sunt considerate responsabile pentru acţiunile lor"[4]. Cu toate acestea, un număr îngrijorător de reprezentanţi ai spectrului politic, ai intelectualităţii şi, inclusiv mass-

[2] Precedentele cele mai notabile sunt: Executivul nu a sancţionat membrii liberali ce făceau parte din coaliţia de „Guvern Naţional" aflată la putere în Marea Britanie în anii 1930 care s-au opus introducerii tarifelor protective; prim-ministrul Harold Wilson le-a permis membrilor Cabinetului său să organizeze campanii pentru, dar şi împotriva referendumului din anii 1970 privind retragerea Marii Britanii din Comunitatea Economică Europeană; Tony Blair a păstrat-o în funcţie pe Clare Short, în ciuda faptului că aceasta se opusese public vehement la adresa războiului din Irak (2003).

[3] Relevante în acest sens sunt dezbaterile dintre Carl Joachim Friedrich (profesor de ştiinţe politice la Harvard University) şi Herman Finer (profesor al University of Chicago, originar din Basarabia) cu privire la raportul dintre miniştri şi funcţionarii publici.

[4] Edwards, Michael; Hulme, David – *Beyond the Magic Bullet: NGO Performance and Accountability in the Post-Cold War World*, Kumarian Press, 1996, ISBN 978–156–549–051–2.

media, perpetuează confuzia dintre responsabilitate şi răspundere, induşi probabil în eroare de caracterul simultan al celor două.

Aşa cum am arătat mai sus, responsabilitatea implică valori etice şi morale necesar a fi respectate în îndeplinirea unei funcţii sau demnităţi publice. Abaterea de la această regulă nu poate atrage cu sine sancţiuni de altă natură decât politică sau administrativă. De cealaltă parte, răspunderea are în vedere cadrul normativ al societăţii şi supunerea faţă de prevederile acestuia. În realizarea scopului său de protejare a valorilor sociale, răspunderea implică un sistem de sancţiuni ce poate conduce inclusiv până la pedepse privative de libertate, reprezentând astfel o expresie a condamnării de către stat a unei conduite ilicite.

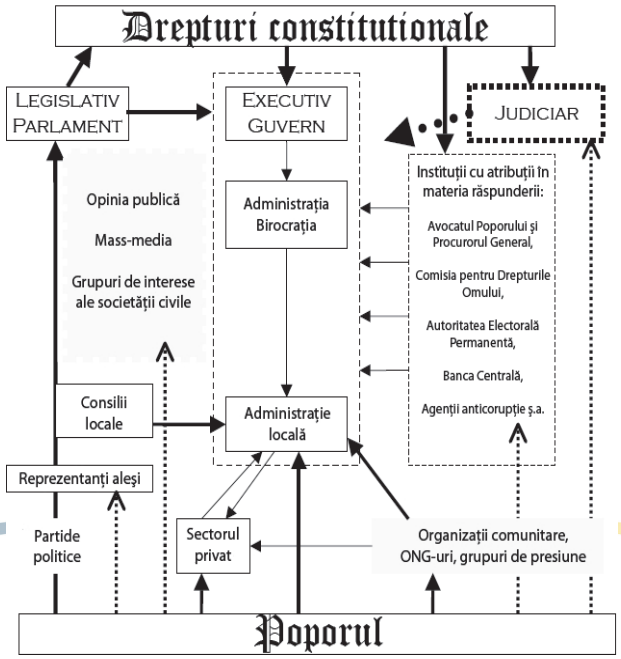
Dintre formele răspunderii juridice amintim: răspunderea *penală* (atunci când abaterea are un pericol social ridicat şi reprezintă o serioasă ameninţare asupra intereselor societăţii); răspunderea *civilă* (clasificată în *delictuală* – obligaţie legală cu caracter general pentru repararea prejudiciului cauzat de o faptă ilicită, respectiv *contractuală* – obligaţie legală, urmare a încălcării unor obligaţii contractuale preexistente); răspunderea *contravenţională* (fapte cu pericol social mai redus decât infracţiunea, expres prevăzute de lege sau alte acte normative săvârşite cu vinovăţie); răspunderea *materială* (obligaţia salariatului de a repara prejudiciul cauzat unităţii din vina sa şi în legătură cu munca sa); răspunderea *disciplinară* (fapte de încălcare cu vinovăţie de către orice persoană încadrată a obligaţiilor asumate prin contractul de muncă).

Profesorul J. Patrick Dobel[5] (Johns Hopkins University) argumentează că principalele angajamente pentru „administratorii publici" moderni ar trebui să aibă în vedere următoarele:

- să răspundă cu onestitate în faţa autorităţilor relevante sau în faţa cetăţenilor;
- să aprecieze valorile sociale ale regimului politic;
- să implementeze şi să menţină instituţii şi proceduri capabile să îşi îndeplinească misiunea;
- să asigure, în cadrul procesului de realizare a puterii publice, participarea corectă şi proporţională a actorilor interesaţi;
- să beneficieze de competenţă pentru realizarea eficace şi performantă a puterii publice;
- să militeze pentru eficienţă în afacerile Guvernului;
- să facă legătura între politicile publice, interesul cetăţenilor şi cel al actorilor interesaţi, în aşa fel încât scopurile niciunei categorii să nu fie subminate.

[5] Dobel, Patrick J. – *Public Integrity*, Johns Hopkins University Press, Maryland, 2001, ISBN 978–080–186–916–7, 2001, p. 21.

Literatura juridică face distincţie între două tipuri de răspundere relativă cu privire la activitatea actorilor implicaţi în administraţie: răspundere *verticală* şi răspundere *orizontală*.



Primul tip se referă la relaţia directă dintre cetăţeni şi reprezentanţii lor. Dincolo de manifestarea sprijinului sau a dezaprobării pentru un reprezentant în cadrul alegerilor electorale, răspunderea verticală este, totodată, o funcţie de control exercitată de către partidele politice, opinia publică, mass-media şi societatea civilă. Prin intermediul relaţiilor de răspundere pe orizontală – între puterile executivă, legislativă, judecătorească şi agenţiile de constrângere în această materie - instituţiile statului sunt trase la răspundere în mod reciproc, în numele poporului.

Reprezentarea grafică[6] constituie o hartă a principalelor relaţii de răspundere ce se regăsesc în majoritatea societăţilor democratice. Săgeţile pornesc de la elementul cu atribuţii pentru tragerea la răspundere şi conduc spre elementul care este tras la răspundere.

[6] Relaţiile cheie de răspundere. Sursă: Programul Naţiunilor Unite pentru Dezvoltare (UNDP), 2006.

RECEPTIVITATE

Receptivitatea este o noţiune relativ recentă în studiul administraţiei publice. În practică, se aşteaptă ca o administraţie *receptivă* să fie disponibilă şi să reacţioneze la nevoile specifice care rezultă din circumstanţele generate de implementarea politicilor publice. Receptivitatea se manifestă însă şi în sens opus, referindu-ne aici la receptivitatea cetăţenilor faţă de politicile publice şi implicarea acestora în găsirea unor noi răspunsuri sau remedierea politicilor deficitare.

În contrast, literatura de peste ocean utilizează termenul de *receptivitate* (responsiveness) pentru a descrie gradul la care aparatul birocratic al statului răspunde instrucţiunilor politice, ridicându-se problema că ocuparea funcţiei de preşedinte de către un membru aparţinând unei alte facturi politice decât predecesorul său, conduce la o stare de neîncredere cu privire la loialitatea administraţiei de la Casa Albă pentru ocupantul anterior. Cazul clasic invocat este primul mandat al lui democratului Franklin D. Roosevelt, ales preşedinte în 1933, după trei mandate consecutive ale republicanilor.

Ca răspuns faţă de acest tip de receptivitate, se marşează pentru *competenţa neutră* a administraţiei, descrisă de profesorul Herbert Kaufman (Yale University) drept acea „bogăţie de cunoştinţe şi calificări disponibile pe coridoarele birocraţiei pe care toţi aleşii, indiferent de convingerea politică, se pot baza, atât pentru informaţii utile, cât şi pentru consiliere lipsită de interes personal în proiectarea politicilor naţionale”[7].

Printre beneficiile receptivităţii administraţiei în accepţiunea definită iniţial se numără următoarele elemente:

- cetăţenii şi clienţii devin tot mai conştienţi în ceea ce priveşte disponibilitatea serviciilor publice şi dreptul lor de a le accesa;
- încurajarea vocilor care solicită un grad mai mare de accesibilitate şi de calitate a serviciilor publice;
- funcţionarii publici devin mai deschişi şi mai responsabili în faţa cetăţenilor;
- îmbunătăţirea gradului la care managerii publici împărtăşesc informaţiile şi se consultă reciproc; îmbunătăţirea gradului de responsabilitate al managerilor publici pentru îndeplinirea interesului general.

Reprezentarea, în mod eficient, a interesului general în cadrul politicilor publice implică un public *receptiv* faţă de însăşi politica propusă. Altfel spus, publicul trebuie să fie informat şi să vegheze efectiv activitatea autorităţilor şi instituţiilor publice, în principal din considerentul că receptivitatea publică motivează suplimentar factorii de decizie, în scopul reprezentării preferinţelor populaţiei şi, totodată, responsabilizează mediul politic.

CONCLUZII

[7] Kaufman, Herbert – *Emerging Conflicts in the Doctrines of Public Administration*, American Political Science Review (Volume 50), Cambridge University Press, 1956, p. 1057–1073.

Analizând în balanţă cele trei noţiuni, întărim accepţiunea conform căreia procesul realizării puterii publice se poate face numai în mod responsabil, cu răspundere faţă de limitele prevăzute în normele juridice şi în acord cu interesul general al celor administraţi. Managerul secolului XXI trebuie însă să beneficieze şi de atribute precum flexibilitate, receptivitate şi adaptabilitate faţă de nevoile în continuă schimbare ale populaţiei.

Pe parcursul acestei secțiuni, am căutat să arătăm elementele distinctive ale conceptelor de *responsabilitate*, *răspundere* şi *receptivitate*.

Rezumând cele enunţate anterior, responsabilitatea implică obligaţii de factură morală şi etică, fără existenţa în corpusul legislativ a unui set clar de drepturi şi îndatoriri în acest sens. De cealaltă parte, răspunderea are în vedere instrucţiuni specifice, menite a controla şi limita exercitarea puterii în acord cu opţiunile societăţii.

Astfel de instrucţiuni se regăsesc explicitate în norme juridice şi în dispoziţiile de aplicare ale acestora, iar încălcarea lor produce sancţiuni juridice. Receptivitatea bidirecţională (autorităţi ← cetăţeni, autorităţi → cetăţeni) are ca efect îmbunătăţirea calităţii serviciilor publice şi sporeşte, totodată, imaginea exterioară a administraţiei. În același timp, prin receptivitate problemele din comunitate sunt transmise mai uşor şi mai rapid către cei învestiţi pentru soluţionarea acestora.

1.1.2. Noțiunea de acces la informații (factori în favoarea adoptării legislației, caracteristici legislative comune, beneficii)

NOȚIUNEA DE ACCES LA INFORMAȚII

Dreptul accesului la informații publice reprezintă opțiunea fiecărui cetățean de a *cunoaște*, în speță de a-i fi puse la dispoziție elementele pe care acesta le consideră necesare pentru a putea alege ori întreprinde acțiuni în cunoștință de cauză.

Mai mult, acest drept la informare este asigurat și de procesul democratic prin care cetățenii își aleg reprezentanții în forurile legislative și administrative ale țării. Astfel, se creează cadrul care permite oricărui cetățean-contribuabil să se informeze și să fie informat cu privire la interesele sale și, prin aceasta, să exercite un control interelectoral cu privire la utilizarea adecvată a votului sau a contribuției sale financiare.

În consecință, cele trei dimensiuni ale dreptului cetățenilor în ceea ce privește accesul la informații sunt: (1) dreptul de a fi informat, din oficiu, de către instituțiile și autoritățile publice privind aspecte importante ale funcționării acestora; (2) dreptul de a solicita informații; (3) dreptul de a fi informat de către mass-media cu privire la diverse aspecte importante din sfera publică.

În acest context, informația reprezintă un instrument de control democratic exercitat asupra autorităților și instituțiilor publice, instrument ce se află în strânsă legătură cu noțiunea de *democrație participativă*, aceasta vizând diminuarea distanței dintre cetățean și administrație prin crearea unor canale de comunicare prin care membrii unei comunități să fie conștienți de actul de guvernare și să fie implicați în procesul de luare al deciziilor.

Concomitent, accesul la informații aduce beneficii de încredere și imagine guvernelor suverane.

Odată cu dezvoltarea tot mai accentuată a sectorului tehnologiei informației, guvernele au început să-şi concentreze o parte din eforturi pe introducerea de mijloace electronice care să asigure comunicarea continuă dintre cetățean și administrație.

FACTORI ÎN FAVOAREA ADOPTĂRII LEGISLAȚIEI

Există o gamă variată de factori interni și externi de presiune care au condus la adoptarea de către guvernele naționale a legislațiilor privind dreptul de acces la informațiile publice. În majoritatea statelor, grupuri nonguvernamentale precum asociațiile pentru combaterea corupției, pentru promovarea drepturilor mass-media și pentru protejarea mediului înconjurător au jucat un rol cheie în promovarea și adoptarea unor astfel de reglementări. Acestora li s-au alăturat presiunile din partea organizațiilor internaționale. În final, un alt factor de influență l-a reprezentat însăși conștientizarea de către state a importanței actelor normative în domeniu

pentru modernizarea actului de guvernare. În cele ce urmează, ne vom referi rezumativ la cei mai frecvenți astfel de factori.

Corupția și lipsa integrității

Adesea, crizele datorate lipsei de transparență au condus la adoptarea legislației în materia accesului la informații. Campaniile publice pentru combaterea fenomenului de corupție s-au dovedit a fi un real succes în statele aflate în tranziția către un regim democratic, în tentativa acestora de a schimba cultura publică.

În democrații consolidate, așa cum este cazul Irlandei, Japoniei sau al Regatului Unit al Marii Britanii și al Irlandei de Nord, legislația de profil a fost adoptată în final, ca urmare a campaniilor susținute de către societatea civilă și, în același timp, a scandalurilor politice din domeniul medical și cel al protecției mediului.

Totuși, ca o particularitate, o serie de state din Europa Centrală și de Est au adoptat astfel de acte normative în drumul lor către democrație și ca răspuns pentru dezastrul nuclear de la Cernobîl.

Presiunea internațională

Comunitatea internațională a jucat un rol deosebit de influent în ceea ce privește promovarea accesului la informații. Organisme internaționale precum Commonwealth-ul, Consiliul Europei și Organizația Statelor Americane au elaborat ghiduri și proiecte legislative menite a urgenta adoptarea juridică a accesului la informații. Mai mult, în 2003, Consiliul Europei a decis elaborarea primului tratat internațional privind accesul la informații.

Banca Mondială, Fondul Monetar Internațional și alte entități au exercitat, de asemenea, presiuni asupra statelor pentru adoptarea legislației menite să reducă prezența fenomenului de corupție și pentru a responsabiliza sistemele financiare naționale.

În acest registru trebuie subliniată și contribuția Convenției de la Aarhus, urmare a căreia zeci de state au adoptat acte normative reglementând accesul la informațiile privind mediul înconjurător.

Modernizarea și tehnologia informației

Expansiunea Internetului și pătrunderea acestuia în utilizarea zilnică au îmbunătățit considerabil cuantumul de solicitări adresate de către public, mediul de afaceri și entitățile din societatea civilă. În interiorul guvernelor naționale, nevoia de modernizare a sistemului de înregistrări și demersurile către e-guvernare au creat grupuri care promovează diseminarea informației prin intermediul tehnologiei moderne.

CARACTERISTICI LEGISLATIVE COMUNE

Majoritatea actelor normative naționale în domeniul accesului la informații se aseamănă în mod considerabil. O explicație a acestei situații se datorează faptului că doar câteva state au fost utilizate drept modele pentru adoptarea de noi sisteme, dintre acestea preponderent fiind vorba despre țările care au îmbrățișat timpuriu politica accesului la informații.

Unul dintre cele mai influente astfel de modele a reprezentat-o legislația din Statele Unite ale Americii. De cealaltă parte, exemplele Canadei și reglementările naționale, provinciale și locale din Australia au fost folosite proeminent în statele având la bază sistemul Westminster.

În ultimii ani s-a putut constata un fenomen de inovare în domeniul legislației privind accesul la informații. Au fost introduse noi prevederi precum *comisarul pentru informații*, având prerogative de executare, testări în interes public și o mai amplă acoperire a sferei de instituții cărora prevederile legale le sunt incidente. Aceste inovații au fost, de asemenea, adoptate în legile mai vechi care au fost supuse revizuirii.

Instituții aflate sub incidență

În general, legislația în domeniul accesului la informații se concentrează asupra organismelor executive și administrative care alcătuiesc statul birocratic modern. Aici includem:

- ministerele și agențiile responsabile în domeniul sănătății, mediului înconjurător;
- entitățile responsabile cu aplicarea legii;
- armata;
- sistemele de comunicații;
- transportul la nivel național;
- precum și instituțiile descentralizate aflate la nivel local.

Rareori, sub incidența legislației privind accesul la informații se încadrează și entitățile componente ale puterii juridice și cele ale legislativului.

Cazurile de bună practică recomandă folosirea unei definiții ample pentru entitățile publice care exercită funcții guvernamentale. Un exemplu în acest sens este reprezentat de Legea portugheză privind accesul la documente administrative, care se aplică „organismelor statelor sau aparținând regiunilor autonome însărcinate cu funcții administrative, organizațiilor, instituțiilor și asociațiilor publice, entităților din administrația locală, inclusiv asociațiilor și federațiilor, precum și altor entități care exercită autoritate publică conform legii”.

Informațiile accesibile

Legislațiile naționale în domeniul accesului la informații folosesc terminologii variate pentru a defini care sunt informațiile care poartă un caracter public. Actele normative cu vechime fac referire la dreptul de acces la înregistrări, documente oficiale sau fișiere, în timp ce normele recente folosesc referința generică ce include toate informațiile, indiferent de mediul lor de stocare.

Cu toate acestea, în țări precum Suedia, sintagma „document oficial" nu include materialele pregătitoare ori documentația care nu a fost folosită în elaborarea unei decizii finale, pierzându-se astfel seturi întregi de informație. Ca o particularitate, în India cetățenii sunt îndreptățiți să solicite mostre din hrana care este distribuită familiilor nevoiașe ori materiale folosite pentru construcția de drumuri.

În general, dreptul de acces la informație se aplică doar acelor date care sunt stocate. Acest fapt poate genera lacune întrucât o parte din informație se transmite pe cale verbală (cum este cazul anumitor întâlniri), chiar dacă acestea au stat la baza fundamentării unei decizii. O practică mai fericită sugerează introducerea obligației ca toată informația cunoscută să fie pusă la dispoziție.

În Danemarca, autoritățile care primesc pe cale verbală informații relevante pentru o decizie publică au obligația de a o înregistra în scris. În Noua Zeelandă, dreptul la informație este interpretat de maniera în care datele care sunt cunoscute unei agenții, însă nu au fost încă înregistrate, trebuie înregistrate în măsura în care acestea fac obiectul sau sunt relevante pentru o solicitare formulată. Această practică este, de asemenea, benefică pentru modificări ulterioare în cadrul procesului decizional, întrucât limitează abilitatea oficialilor publici de a omite informații pentru a evita divulgarea acestora, considerent pentru care se încurajează o stocare și o gestiune mult mai eficientă.

Solicitantul

Astăzi, un număr considerabil de state răspund solicitărilor de informații publice indiferent de interesul legal, cetățenia ori reședința persoanei. Țări precum Finlanda permit chiar ca solicitările să fie adresate în mod anonim, evitându-se astfel posibilitatea unei discriminări negative. Introducerea de limite în acest sens poate cauza prejudicii considerabile exercitării dreptului la informație. Spre exemplu, în India oficialii publici insistă în a obține acte de identitate din partea solicitanților înainte de a înregistra și procesa cererea acestora.

Excepțiile

Aproape toate legile privind accesul la informații conțin prevederi care stabilesc categorii de informații ce pot face obiectul excepției de la divulgare. Există o serie de situații comune ce pot fi regăsite în majoritatea situațiilor. Printre acestea se numără:

- informațiile ce privesc protejarea securității naționale și relațiile diplomatice;
- informațiile privind intimitatea personală, confidențialitatea comercială;

- informațiile privind ordinea publică și aplicarea legii;
- informațiile obținute pe canale confidențiale și discuțiile interne.

În multe sisteme parlamentare, documentele depuse la Guvern pentru formularea unei decizii și înregistrările întrunirilor membrilor Guvernului sunt excluse de la publicare pentru o perioadă de timp. În Irlanda, acest termen este de 10 ani. În Noua Zeelandă, documentele din ședințele executivului sunt divulgate pro-activ la intervale scurte de timp, fără a fi nevoie de solicitări anterioare.

Majoritatea actelor normative de profil obligă ca în situația refuzului de a furniza o informație, autoritatea responsabilă să argumenteze această decizie prin demonstrarea caracterului potențial dăunător.

Un număr tot mai important de reglementări prevăd un așa-numit *test al interesului public*. Astfel, entitatea responsabilă ori organismul de monitorizare trebuie să analizeze în balanță nedivulgarea unei informații în raport cu interesul public al divulgării acesteia. Astfel de prevederi permit ca anumite informații dăunătoare să fie divulgate în situațiile când nedivulgarea lor ar cauza prejudicii considerabile în raport cu interesul public. Spețe de astfel de situații includ, în general, încălcări ale legii sau acte de corupție în interiorul unei instituții.

Unele dintre legile privind accesul la informații impun ca odată ce pericolul s-a diminuat, documentele să fie divulgate. În alte circumstanțe, sunt introduse termene particulare. Exemplificând, Legea privind transparența federală din Mexic permite ca excepțiile sa fie invocate pentru nu mai mult de 12 ani.

Multe reglementări moderne prevăd în mod explicit că anumite informații nu pot fi invocate ca excepții de la divulgare. Spre exemplu, legea din Azerbaidjan stipulează o lungă listă de date, cuprinzând granturi, ajutoare compensatorii, statistici ș.a. În Mexic, Legea privind transparența federală și cea privind accesul la informații prevăd că „informațiile nu pot fi clasificate atunci când fac parte dintr-o investigație privind grave violări ale drepturilor fundamentale ale omului sau atunci când soarta umanității e în primejdie”.

Căi de apel și monitorizare

În prezent, există o varietate de mecanisme de apel și de impunere a legii. Acestea includ revizuirea administrativă, revizuirea judiciară ori impunerea ori monitorizarea din partea unei structuri independente. Gradul de eficiență al acestor mecanisme variază în mod considerabil. În general, se apreciază că organizarea unor comisii independente conduce la cel mai eficient sistem de monitorizare.

Prima cale de apel în aproape toate sistemele juridice o reprezintă revizuirea internă din cadrul instituției. În genere, aceasta implică adresarea unei solicitări către un superior ierarhic în cadrul entității respective pentru revizuirea considerentelor aflate la baza refuzului procesării unei cereri. În practică, astfel de demersuri produc rezultate mixte, însă de cele mai multe ori aceasta este o cale rapidă pentru revizuirea unei decizii. Cu toate acestea, există state în care

experiența demonstrează că în cadrul revizuirii interne instituțiile tind să-și apere decizia inițială de a nu divulga o informație, ceea ce rezultă în tergiversări procedurale mai degrabă decât în acces sporit. O statistică din 2005 relevă faptul că în ceea ce privește Regatul Unit, un procent de 77% dintre solicitările de revizuire internă adresate organismelor naționale au fost respinse în integralitate.

Odată ce căile interne de atac au fost epuizate, urmează solicitarea adresată unui organism extern. La nivelul analizei din 2005, în peste 20 de state Ombudsman-ul sau Avocatul Poporului (de regulă o instituție independentă numită prin decizia Parlamentului) poate fi solicitat să intervină pentru revizuirea unei decizii de nedivulgare, ca o componentă a atribuțiilor sale generice de a veghea la buna guvernare. Deși în general Ombudsman-ul nu are capacitate de coerciție în ceea ce privește hotărârile sale, în majoritatea statelor opiniile formulate de acesta sunt avute în vedere și sunt considerate a avea o largă sferă de influență, de cele mai multe ori instituțiile conformându-se recomandării acestuia.

Un trend tot mai larg sugerează crearea unei comisii independente privind accesul la informații. Comisia poate fi organizată drept o componentă a Parlamentului sau a unui alt organism guvernamental ori chiar a Cancelariei Prim-ministrului, așa cum este cazul Thailandei. În mod evident, există și scenariul în care această entitate acționează complet independent de orice altă putere în stat. Statisticile demonstrează că, în prezent, peste 22 de state au creat astfel de organisme.

Regatul Unit al Marii Britanii și al Irlandei de Nord, Germania, Elveția și Slovenia au corelat existența unei comisii pentru accesul la informații cu activitatea comisiei naționale privind protecția datelor. În Germania și Canada, această practică are loc și la nivel sub-național. În Irlanda, comisarul pentru informații ocupă concomitent și fotoliul de Ombudsman general. În ceea ce privește puterea și funcțiile unor asemenea comisii, scenariile sunt variate. În țări precum Canada și Franța, Comisia are abilități similare cu cele ale Ombudsman-ului. În Slovenia, Serbia, Irlanda și Regatul Unit, Comisia poate emite decizii cu caracter obligatoriu, limitate însă în anumite circumstanțe speciale prin intervenția unui ministru.

Adesea, comisarul pentru informații îndeplinește și alte îndatoriri dincolo de a judeca recursurile (monitorizarea generală asupra sistemului, organizarea de stagii de pregătire în materie, propunerea de modificări legislative și organizarea de campanii de conștientizare a populației). În Antigua și Barbuda, comisarul poate, de asemenea, să primească informații din partea avertizorilor de integritate. Unele state au optat pentru instituirea unor tribunale speciale pentru judecarea apelurilor. Aceste complete acționează relativ mai informal decât o instanță de judecată și ar trebui să se dovedească mai eficiente datorită caracterului lor specializat. În Australia, Tribunalul de Apeluri Administrative analizează sute de solicitări anual.

În Japonia, Comitetul extern pentru Revizuirea Divulgării de Informații procesează apelurile față de decizia inițială a entității în cauză. Cu toate acestea, entitățile pot întârzia transmiterea cazurilor către Comitetul de Revizuire, ceea ce a condus în practică la tergiversări lungi în multe situații. În Jamaica, cetățenii se confruntă, de

asemenea, cu întârzieri nejustificate și proceduri excesiv de formale în situația apelului față de o decizie de nedivulgare.

Regatul Unit este singurul stat în care funcționează atât o comisie specializată, cât și un comitet de revizuire. Tribunalul joacă un rol pozitiv în această construcție instituțională, încurajând creşterea transparenţei prin anularea frecventă a deciziilor comisarului pentru informație.

În fine, ultima cale de atac o reprezintă în majoritatea statelor o acțiune în instanțele naționale de judecată. În genere, instanțele au posibilitatea de revizui majoritatea deciziilor și de a emite hotărâri cu caracter obligatoriu. În anumite state în care există implementat un comisar pentru informații, jurisdicția instanței este limitată la probleme de natură juridică.

Un sistem cu atât mai puțin eficient se poate regăsi în Statele Unite ale Americii și în Bulgaria, acolo unde instanțele sunt singurele entități exterioare ce pot emite puncte de vedere. Acest fapt descurajează cetățenii să ducă o acțiune până la capăt din cauza cheltuielilor suplimentare și a întârzierilor semnificative până la aflarea verdictului final. Totodată, în general, instanțele dau dreptate organismelor publice, în mod particular atunci când este vorba de spețe care implicăinformații din spectrul securității naționale.

Sancțiuni

Aproape toate reglementările naționale în materia accesului la informații cuprind prevederi menite a sancționa autoritățile publice ori, după caz, angajații implicați, acolo unde informațiile nu sunt divulgate în mod contrar legii. În general, spețele se referă la situații în care o entitate publică ori un angajat din cadrul acesteia refuză nejustificat divulgarea unei informații, furnizează o informație alterată ori distruge documentele implicate. Sancțiunile pot fi impuse asupra entității publice ca atare, ori pe latura administrativă ori penală asupra angajatului răspunzător.

Majoritatea reglementărilor introduc amenzi ori chiar sancțiuni privative de libertate pentru abuzuri excepționale. Legislația poloneză în materia accesului la informații publice statuează că „orice persoană care, în ciuda obligațiilor sale, nu oferă acces la informații publice, este pasibil de amendă, libertate îngrădită sau chiar detenție în închisoare de până la un an”.

Sancțiunile reprezintă o componentă necesară a fiecărei legi pentru a demonstra caracterul indiscutabil al acesteia în cazurile de neconformare. În ciuda acestui fapt, există o reticență generală în cadrul entităților guvernamentale de a-și sancționa proprii angajați pentru situațiile în care aceștia încalcă legea, însă respectă politica generală a instituției.

Sentințele privative de libertate reprezintă rarități în acest domeniu. În anii trecuți s-au înregistrat foarte puține astfel de situații în Statele Unite, acestea fiind chiar, și așa, spețe la nivel de administrație locală.

În India, comisarii pentru accesul la informație au demarat o practică de amendare personală a ofițerilor responsabili de informație care refuzau ori întârziau nejustificat divulgarea unor informații sub incidența legii privind accesul la informații.

Sancțiunile care compensează cheltuielile suportate de solicitant pot fi, de asemenea, aplicate împotriva entităților publice care refuză divulgarea informației. În cazul Statelor Unite ale Americii, instanțele pot încuviința acoperirea cheltuielilor de judecată de către entitatea implicată atunci când se stabilește că aceasta se face responsabilă pentru reținerea nelegală a informației.

Accesibilitatea din oficiu

O altă trăsătură comună pentru majoritatea actelor ce reglementează accesul la informații o reprezintă îndatorirea agențiilor guvernamentale de a divulga din oficiu anume categorii de informații. Această listă include:

- informațiile privind organizarea juridică a instituției și conducătorii acesteia;
- documentele și normele de funcționare;
- politicile și propunerile de politică;
- formularele și deciziile întreprinse.

Divulgarea proactivă a informațiilor reprezintă, totodată, un exercițiu benefic chiar în favoarea instituției publice. Această procedură reduce volumul de sarcini administrative ce decurg din rutina formulării de răspunsuri la întrebări frecvente. Consiliul Uniunii Europene a remarcat, într-un raport anual de activitate, faptul că „odată ce numărul documentelor accesibile în mod direct din oficiu crește, numărul solicitărilor de documente descrește”. Totodată, statisticile Departamentului american pentru Justiție demonstrează faptul că volumul solicitărilor s-a redus considerabil odată cu publicarea din oficiu a documentelor în cadrul paginii oficiale de Internet.

Procedura online

Un alt trend ce trebuie avut în vedere în materia accesului la informații îl reprezintă nivelul tot mai crescut al sistemelor electronice, în vederea depunerii de solicitări și a primirii răspunsurilor. Multe legislații naționale impun, astăzi, îndatorirea ce revine structurilor publice de a divulga periodic anumite categorii de informații pe propria pagină de Internet. Conform prevederilor din Polonia, entitățile publice sunt obligate să publice informații detaliate privind politicile, structura de organizare, principiile de activitate, conținutul actelor și deciziilor administrative și bunurile publice aflate în gestiune, într-un raport privind informațiile de interes public, disponibil pe pagina de Internet.

În reglementările din Estonia, departamentele naționale și locale ale guvernului, precum și alte entități care gestionează informații publice au obligația de a menține actualizată pagina de Internet, precum și de a publica o listă exhaustivă de informații, inclusiv: statisticile economice și cele privind infracționalitatea, statutele

și alte prevederi legale aplicabile, fișele de post ale funcționarilor publici, adresele acestora de e-mail, calificările și nivelul salarial, informațiile privind sănătatea și securitatea, bugetele și proiectele de buget, informațiile despre politica privind mediul înconjurător, precum și proiectele de acte, reglementări și planuri, inclusiv memorandumurile și notele de fundamentare. Instituțiile sunt obligate să se asigure că informația este actuală, exactă și clară.

Politica Consiliului Uniunii Europene în acest domeniu este de a pune la dispoziție, în mod automat, materialele pe care le produce sub incidența propriilor reglementări de acces la informații în cadrul registrului său electronic – http://register.consilium.eu.int.

Solicitanților li se permite din ce în ce mai frecvent să depună solicitări folosind poșta electronică sau formulare online. În Turcia, principalele ministere sunt active în folosirea rețelelor electronice pentru publicarea informațiilor, inclusiv încurajând utilizatorii să depună solicitări și să obțină notificări de actualizare cu privire la formularele depuse online. În Mexic, sistemul informatic de solicitări coordonat de Institutul Federal pentru Accesul la Informații Publice furnizează o soluție integrată pentru toate instituțiile publice.

BENEFICIILE ACCESULUI LA INFORMAȚII

Principalele beneficii ce derivă din existența accesului la informații fac referire la:

- participarea cetățenilor și la nivelul acestora de înțelegere a acțiunilor guvernamentale;
- protejarea drepturilor cetățenești;
- eficientizarea activității entităților publice.

În ceea ce privește **participarea cetățenilor**, trebuie avut în vedere faptul că puterea politică este împuternicită cu responsabilitățile actului de guvernare prin liberul consimțământ al cetățenilor, exprimat prin vot. Astfel, autoritățile sunt datoare, în schimb, să informeze în mod constant cetățenii cu privire la activitățile pe care le întreprind, recunoscând dreptul acestora de a participa la luarea deciziilor. Implicarea pertinentă a cetățenilor în procesul decizional poate surveni numai în prezența unei legături strânse și a unui flux continuu de informații între guvernanți și cei guvernați.

Campaniile publice având drept obiectiv **îmbunătățirea nivelului de conștientizare a cetățenilor** privind raționamentul aflat la baza deciziilor publice pot îmbunătăți sprijinul cetățenesc al unui demers și pot reduce considerabil nivelul de insatisfacție cauzat de absența informațiilor. De asemenea, reprezentanții puterii legislative pot exercita atributul lor de supraveghere a executivului mult mai eficient atunci când acesta din urmă acționează cu celeritate și deschidere.

Un alt beneficiu direct al legiferării dreptului privind accesul la informații îl reprezintă **protejarea drepturilor cetățenești**. Exemplificând, în India sunt folosite solicitări de acces la informații pentru identificarea cazurilor de distribuire irațională

și ineficientă a ajutoarelor de hrană pentru cetățenii cu probleme sociale. Rezultatul acestor analize a condus la consolidarea cadrului legal pentru limitarea arbitrariului exercitat de autoritățile locale în acest proces. Similar, solicitări de informații adresate autorităților din Thailanda au dus la identificarea unor cazuri de favoritism în ceea ce privește admiterea unor copii din familii influente din punct de vedere financiar, în unități de învățământ de elită, contrar rezultatelor obținute de aceștia în cadrul testărilor naționale.

În Statele Unite ale Americii, legislația accesului la informații a permis descoperirea practicilor de tortură din instituțiile de detenție și detectarea practicilor ilegale de supraveghere exercitate de guvern asupra cetățenilor. Anumite legi privind exercitarea dreptului la informații permit cetățenilor accesul la propriul dosar administrat de diferite entități statale. Astfel, aceștia se pot asigura că informațiile cu privire la persoana lor sunt corecte și complete, în așa fel încât să beneficieze de serviciile sociale sau de altă natură care le sunt cuvenite.

În ultimul rând, un alt beneficiu semnificativ datorat accesului la informații îl reprezintă **capacitatea entităților publice de a-şi îmbunătăți activitatea** și a-şi modifica aspectele procedurale pentru optimizarea rezultatelor. Deciziile care trebuie comunicate public sub incidența legislației privind accesul la informații vor trebui justificate prin argumente obiective și raționale.

Astfel, accesul la informații se dovedește a fi un instrument cheie nu numai în ceea ce privește lupta împotriva corupției, în spețe precum licitațiile pentru achiziții publice, dar și în verificarea ulterioară ce poate fi întreprinsă de cetățeni asupra stadiului unei lucrări în raport cu specificațiile tehnice prevăzute în contract.

1.1.3. Transparența instituțională (obiect, beneficii, participarea cetățenilor, acțiuni în cazul lipsei de transparență)

TRANSPARENŢĂ DECIZIONALĂ

1. Ce este legea transparenţei?

Legea transparenţei asigură deschiderea activităţii administraţiei publice centrale şi locale către cetăţeni prin intermediul a două mecanisme importante:

a) Participarea publicului la procesul de elaborare a reglementărilor;

b) Participarea publicului la procesul de luare a deciziilor.

Legea transparenţei nu trebuie confundată cu legea privind accesul la informaţiile de interes public şi nici cu democraţia directă. Spre deosebire de legea accesului la informaţiile de interes public, care permite accesul cetăţeanului la informaţiile publice gestionate de diverse entităţi publice, legea transparenţei oferă posibilitatea cetăţenilor de a participa activ la procesul de elaborare de reglementări, prin sugestii adresate autorităţilor administraţiei publice.

De asemenea, spre deosebire de democraţia directă, legea transparenţei nu conferă cetăţenilor dreptul de a lua decizia finală cu privire la reglementările care vor fi adoptate. Acest rol va fi în continuare asumat de autorităţile administraţiei publice care vor decide dacă includ sau nu în proiectele de reglementări informaţiile şi sugestiile primite din partea cetăţenilor, organizaţiilor neguvernamentale şi asociaţiilor de afaceri.

2. Cui se adresează această lege?

Legea transparenţei implică o colaborare între doi parteneri: administraţia publică şi destinatarii reglementărilor elaborate de aceasta (cetăţeni, organizaţii neguvernamentale, asociaţii de afaceri). Pe lângă administraţia publică, legea face referire la instituţii publice şi la servicii publice, deşi aceste organisme nu au atribuţii directe în procesul de adoptare a reglementărilor.

3. Ce presupune legea?

Autorităţile administraţiei publice centrale şi locale, precum şi celelalte instituţii publice care utilizează resurse financiare publice au obligaţia de a face publice proiectele de reglementări înainte ca acestea să fie adoptate. După acest moment, destinatarii reglementărilor, persoane fizice sau juridice, au posibilitatea de a formula sugestii şi recomandări cu privire la reglementările care le-au fost prezentate în stadiu de proiect.

Sugestiile astfel formulate vor fi analizate de către autorităţile iniţiatoare care vor decide asupra necesităţii includerii în textul final al reglementărilor. Cu privire la participarea publicului la procesul de luare a deciziilor, legea prevede posibilitatea celor interesaţi de a participa şi de a-şi exprima punctele de vedere în cadrul şedinţelor organismelor menţionate mai sus.

4. Obiectul Legii transparenţei

Potrivit Legii transparenţei, cetăţenii şi organizaţiile constituite de aceştia îşi vor putea exprima opiniile şi interesele în legătură cu elaborarea de acte normative şi în legătură cu luarea unor decizii administrative. Instrumentele disponiblie sunt dreptul de a fi consultaţi de autorităţile publice în legătură cu proiectele de acte normative şi participarea la şedinţele publice ale respectivelor autorităţi.

5. Care sunt beneficiile legii?

- Pentru administraţia publică:
  - obţine în mod gratuit informaţii suplimentare cu privire la sectoarele de activitate care urmează să fie afectate de reglementările propuse;
  - explică necesitatea reglementărilor propuse;
  - înlătură problemele de implementare a reglementărilor datorate necunoaşterii acestora de către destinatari;
  - înlătură problemele de implementare datorate deficienţelor de redactare ale reglementărilor;
  - câştigă încrederea opiniei publice.
- Pentru beneficiarii reglementărilor:
  - iau cunoştinţă de proiectele de reglementări propuse de administraţia publică;
  - îşi exprimă punctele de vedere cu privire la aceste proiecte;
  - îşi adaptează activitatea din timp la cerinţele care urmează a fi introduse.

6. Ce pot schimba cetăţenii prin transparenţă?

Autorităţile publice a căror activitate cade sub incidenţa Legii transparenţei adoptă sau redactează în mod constant acte normative şi iau decizii care influenţează viaţa sau activitatea oamenilor. Legea transparenţei permite cetăţenilor să comenteze proiectele de acte normative şi să îşi spună cuvântul referitor la deciziile care sunt adoptate de autorităţile publice în cadrul unor şedinţe publice.

Proiectele de acte normative pot fi clasificate în proiecte elaborate în cadrul unor organe ale administraţiei publice şi proiecte elaborate în afara administraţiei. Toate actele adoptate de autorităţi administrative, cu excepţiile prevăzute de lege, intră sub incidenţa Legii transparenţei.

Excepţii! Nu are loc un proces de consultare în cazul elaborării unor acte normative:

- privind apărarea naţională, siguranţa naţională şi ordinea publică;
- privind interesele strategice, economice şi politice, ale ţării;
- conţinând valori, termene de realizare şi date tehnico-economice ale unor activităţi comerciale sau financiare, dacă publicitatea acestora aduce atingere principiului concurenţei loiale;
- privind datele personale.

În situaţia în care autorităţile publice vor folosi scuza exceptării de la consultare pentru a nu iniţia procesele reglementate de lege, este important ca astfel de decizii să fie contestate prin memorii adresate respectivei instituţii sau, în lipsa unei reacţii pozitive, prin intermediul instanţelor. Astfel, instanţele de judecată vor putea clarifica limitele aplicării legii.

În situaţii care, datorită circumstanţelor excepţionale, impun adoptarea unor soluţii imediate, pentru evitarea unei grave atingeri aduse interesului public, este prevăzută posibilitatea de a adopta acte normative fără a urma un proces consultativ. Această reglementare îşi poate dovedi utilitatea în situaţii de criză.

Legea transparenţei face de mai multe ori precizarea că opiniile exprimate de cetăţeni sau organizaţii în timpul consultărilor au doar valoare de recomandare. Decizia rămâne la latitudinea autorităţii publice. Actul normativ va fi trimis, după consultări, spre analiză şi avizare, potrivit procedurii legale privind elaborarea actelor normative. Acesta va include modificări redactate pe baza acelor opinii, exprimate în procesul de consultare, care au fost selectate de către funcţionarii publici responsabili de redactarea actului respectiv.

Autorităţile publice sunt obligate de lege să precizeze, în raportul anual privind transparenţa decizională, numărul de recomandări incluse în proiectele de acte normative. Se poate dovedi util ca cetăţenii să solicite instituţiilor publice motivarea alegerii făcute. Acest lucru nu este expres prevăzut de lege, dar autorităţile publice pot să facă publice motivele includerii doar a unor puncte de vedere sau a respingerii altora. Şedinţele publice la care se referă Legea transparenţei sunt, în fapt, toate şedinţele care sunt necesare pentru desfăşurarea activităţii autorităţii publice respective şi pe care autoritatea respectivă le declară ca fiind publice. Excepţiile sunt expres reglementate de lege.

Excepţii! Cetăţenii şi asociaţiile legal constituite nu pot participa la şedinţele în care sunt prezentate informaţii:

- privind apărarea naţională, siguranţa naţională şi ordinea publică;
- privind interesele strategice economice şi politice ale ţării;
- conţinând valori, termene de realizare şi date tehnico-economice ale unor activităţi comerciale sau financiare, dacă publicitatea acestora aduce atingere principiului concurenţei loiale;
- privind datele personale.

Definiţia dată de lege şedinţelor publice lasă la latitudinea autorităţilor respective declararea acestora ca publice, prin regulamentul lor de organizare şi funcţionare.

7. Cum pot participa cetăţenii?

Pentru a influenţa decizii sau acte normative, persoanele pot participa fie individual, în calitatea lor de cetăţeni, fie organizaţi în asociaţii legal constituite. Legea nu limitează în nici un fel accesul la mecanismele prevăzute de aceasta, oricine având dreptul de a participa, indiferent de interesul reprezentat. Cetăţenii

pot participa la procesele reglementate de Legea transparenţei fără deosebire de rasă, naţionalitate, origine etnică, limbă, religie, sex, opinie, apartenenţă politică, avere sau origine socială.

Organizaţiile pot participa şi ele, prin reprezentanţii lor. Legea transparenţei dă dreptul de participare numai organizaţiilor „de reprezentare civică", adică a organizaţiilor neguvernamentale, sindicatelor şi altor organizaţii non-profit recunoscute legal. Nu pot folosi direct mecanismele acestei legi societăţile comerciale, organizaţiile cooperatiste, asociaţiile agricole, partidele politice. Ele pot să intervină fie prin intermediul unor persoane (cum ar fi proprietari, membri, persoane cu funcţii de conducere), fie prin intermediul unor organizaţii neguvernamentale create pentru a le reprezenta interesele. Un punct de vedere poate fi susţinut de o persoană, de o asociaţie fără personalitate juridică, de o persoană juridică non-profit sau de o coaliţie.

8. Cum îşi pot expune cetăţenii punctul de vedere?

Consultarea cu privire la acte normative este un proces în care agenda este stabilită de către instituţiile publice. Instituţiile publice decid, în funcţie de conjunctură sau de priorităţile lor, ce acte vor fi elaborate. Acest fapt cere atenţie permanentă, pentru a vedea ce acte din sfera dumneavoastră de interes sunt în discuţie la un moment dat. Primul pas este informarea cu privire la actele care sunt supuse consultărilor.

Informarea din partea autorităţilor publice asupra proiectelor de acte normative ce vor fi supuse consultărilor se face în prealabil şi din oficiu. Sursele de informare cu privire la proiectele de acte normative supuse consultărilor sunt:

- anunţ pe pagina de Internet a instituţiei publice;
- anunţ afişat într-un spaţiu accesibil publicului din sediul instituţiei;
- mass-media, dacă aceasta preia anunţul trimis de instituţia respectivă.

Anunţul va cuprinde:

- nota de fundamentare a proiectului, expunerea de motive sau referatul de aprobare;
- textul complet al proiectului de act normativ;
- termenul de trimitere al comentariilor (cel puţin 10 zile) şi
- modul în care cei interesaţi pot trimite în scris comentariile.

O altă modalitate importantă de a primi informaţia referitoare la consultările asupra proiectelor de acte normative este procedura depunerii unei cereri la autoritatea publică respectivă. În cazul actelor normative cu relevanţă asupra mediului de afaceri, instituţia publică iniţiatoare va transmite anunţul către asociaţiile de afaceri şi către alte asociaţii legal constituite, pe domenii specifice de afaceri.

Potrivit legii, participarea la elaborarea de acte normative se poate face în procesul de redactare a unui proiect de act normativ, anterior supunerii spre analiză şi avizare autorităţii publice care l-a elaborat. Cetăţenii au la dispoziţie un timp limitat, stabilit de autoritatea publică şi făcut public în anunţul iniţial. Acest termen nu

poate fi însă mai scurt de 10 zile de la data publicării anunţului.

Comentariile, prevăzute de lege ca „propuneri, sugestii, opinii cu valoare de recomandare, vor fi primite de o persoană desemnată special de conducătorul autorităţii publice.

O altă modalitate de consultare, pe lângă comunicarea de comentarii în scris, o reprezintă organizarea de dezbateri publice. Dezbaterile publice pot fi solicitate în scris de către o asociaţie legal constituită sau de o altă autoritate publică, iar autoritatea publică iniţiatoare a proiectului de act normativ este obligată să le organizeze.

9. Cum pot participa cetăţenii la şedinţele publice?

Autoritatea publică este obligată să facă public anunţul cu privire la şedinţă cu cel puţin trei zile înainte de desfăşurarea acesteia. Anunţul va fi făcut public prin:

- afişare la sediul autorităţii;
- inserare în site-ul web;
- comunicare către mass-media.

Anunţul va conţine:

- data, ora şi locul de desfăşurare;
- ordinea de zi.

Participarea la şedinţă se va face în limita numărului de locuri din sala în care se va desfăşura şedinţa. Pentru a determina cine sunt persoanele care au prioritate, legea introduce noţiunea de „ordine de precădere || şi lasă la dispoziţia persoanei care conduce şedinţa să stabilească priorităţile interesului pentru participare. Mass-media are acces preferenţial la şedinţă, trecând peste ordinea de precădere.

Acelaşi preşedinte de şedinţă mai dispune de un instrument de control al şedinţei - posibilitatea de a avertiza sau chiar de a evacua din sală un participant, în cazul în care acesta nu respectă regulamentul de organizare şi funcţionare a şedinţelor, parte a regulamentului instituţiei publice respective.

Cei care nu pot participa la şedinţă vor avea acces, în condiţiile legii accesului la informaţiile de interes public, la minuta şedinţelor publice.

Ca şi în cazul actelor normative, contribuţiile participanţilor la şedinţele publice au valoare de recomandare, adoptarea deciziilor ţinând de competenţa exclusivă a autorităţilor publice.

10. Acţiuni în cazul lipsei de transparenţă

Legea transparenţei prevede căi de atac în cazul în care nu este respectată. Conform art. 13 din legea privind transparența decizională, persoanele sau organizaţiile au dreptul de a ataca în contencios administrativ instituţiile publice care nu respectă legea.

Cel care face plângerea în instanţă va trebui să facă dovada lezării unui drept sau

interes legitim al său prin neaplicarea sau aplicarea eronată a Legii transparenţei. Persoana respectivă va trebui să urmeze, în prealabil, procedura de plângere administrativă la instituţia publică care a permis lezarea dreptului.

Dacă un funcţionar nu permite accesul la şedinţele publice sau împiedică implicarea în consultările cu privire la proiecte de acte normative, poate fi sancţionat pentru abatere disciplinară. Trebuie arătat că legea se referă la funcţionar, adică la orice angajat al unei instituţii publice.

Sancţionarea se face diferenţiat dacă este vorba despre un funcţionar public sau de alt funcţionar al instituţiei publice respective. Cei împiedicaţi să participe la şedinţe sau consultări trebuie să adreseze un memoriu superiorului direct sau comisiei de disciplină, prin care să ceară sancţionarea funcţionarului. Pentru angajaţii instituţiilor publice care nu sunt funcţionari publici, sancţionarea se face sub regimul Codului Muncii.

Conducătorii instituţiilor publice care nu sunt funcţionari publici, fiind demnitari, aleşi, sau consilieri lor personali, nu pot fi sancţionaţi în acest mod. Singura cale rămâne cea prevăzută de Legea contenciosului administrativ.

Legea prevede şi un instrument ce poate fi folosit de cetăţeni pentru verificarea modului în care a fost aplicată legea de către autorităţi: raportul anual privind transparenţa decizională. Prin intermediul raportului se va evalua, cel puţin din punct de vedere cantitativ, în ce măsură a fost pusă în aplicare legea. Nepublicarea raportului anual de către toate autorităţile publice vizate poate să fie atacată în justiţie.

1.2. Conceptul de comunicare online

1.2.1. Comunicarea în instituțiile publice[8]

Comunicarea poate fi formal definită ca orice proces prin care premisele decizionale sunt transmise de la un membru al unei instituţii la altul. Comunicarea însoţeşte activitatea instituţiilor publice, contribuind la realizarea în bune condiţii a acesteia. Comunicarea publică se referă atât la schimbul şi difuzarea de informaţii de utilitate publică, cât şi menţinerea liantului social[9].

Comunicarea în instituţii este un proces bilateral: el presupune atât transmiterea ordinelor, informaţiei şi sfaturilor la un centru de decizie (adică un individ învestit cu responsabilitatea de a lua decizii), cât şi transmiterea deciziilor luate de la acest centru în alte părţi ale instituţiei. Mai mult, este un proces care se desfăşoară în plan vertical şi orizontal în mod bidirecţional în instituţie.

Canalele de comunicare în instituţiile publice pot fi de două feluri: formale şi informale. Prin canalele formale se transmit fluxurile informaţionale oficiale. Canalele informale de comunicare se stabilesc în general între persoane şi grupuri informale. Acestea sunt formate din angajaţi care au interese sau afinităţi comune. Informaţiile transferate prin aceste canale sunt neoficiale şi au un caracter personal sau general: ele nu sunt verificate.

COMUNICAREA CU ROL DE PROMOVARE

Comunicarea instituţională este o comunicare extraorganizaţională prin care instituţia din administraţia publică urmăreşte să-şi întărească imaginea, să suscite în jurul ei un climat de încredere şi simpatie din partea cetăţenilor[10].

Comunicarea externă a instituţiei publice contribuie la notorietatea şi imaginea organizaţiei în instituţie. Ea îndeplineşte atfel, totodată, funcţia de promovare a instituţiei publice a statului şi a unităţilor administrativ-teritoriale. Comunicarea cu rol de promovare reprezintă, în realitate, un caz aparte, pentru că, deşi literatura de specialitate o considera fără excepţie ca făcând parte din comunicarea externă, ea se desfăşoară unilateral, dinspre instituţia publică către mediul exterior al acesteia. În această situaţie, nu mai sunt membrii organismului public cei care intreţin legatura cu exteriorul, ci organizaţia ca instituţie. Ea dă informaţii despre serviciile pe care le oferă, încearcă să-i amelioreze imaginea de ansamblu sau, pur si simplu, vrea să facă cunoscute şi să-şi promoveze valorile[11].

Prin însăşi natura ei, administraţia publică depinde de comunicare:

- comunicarea între diferitele niveluri ale administraţiei publice;
- comunicarea pe acelaşi nivel;
- comunicarea între administraţie şi executivul social;
- comunicarea între administraţie şi autoritatea politică;

---

[8] Cf. administratiepublica.ro
[9] P. Zémor – La Communication Publique, Presses Universitaires de France, Paris, 1995
[10] Alexandru Nedelea – *Marketing în Administraţia Publică*
[11] V. A. Munteanu – *Marketing public*, Ed. Sedcom Libris, Iaşi, 2006

- comunicarea în mediul social;

Devine din ce în ce mai importantă atât pentru administraţie, cât şi pentru clienţii acesteia - contribuabili, cetăţeni, grupuri de interese, autoritatea politică - dezvoltarea canalelor de comunicare cu "lumea de afaceri". Formele principale prin care se concretizează acest tip particular de comunicare sunt:

- publicitatea – prin mass-media sau prin propriile materiale publicitare;
- sponsorizările – finanţarea activităţilor culturale sau sportive;
- mecenatul – ajutor financiar sau logistic acordat artiştilor, organizaţiilor umanitare sau non-profit;
- articole care prezintă organizaţia în publicaţiile de specialitate;
- organizarea de standuri la târguri şi forumuri;
- organizarea de zile ale porţilor deschise;
- acţiuni de consiliere şi ajutorare a altor instituţii, similare (dar care în mod real nu sunt concurenţiale) prin detaşarea temporară de personal.

Există, aşadar, o multitudine de forme de promovare a imaginii, valorilor sau serviciilor specifice instituţiei publice. Cea mai eficientă şi mai ieftină formă de promovare este însă, cel mai adesea, ignorată. Ea se află la îndemâna tuturor funcţionarilor şi constă în reliefarea permanentă a aspectelor pozitive ale organismului public din care fac parte, cu ocazia contactelor cu mediul extern, fie acestea personale sau profesionale. Ideea este că fiecare funcţionar public îşi poate asuma fără probleme rolul de comunicator extern, mesajul său fiind centrat pe seriozitatea, eficienţa şi calitatea de care dă dovadă instituţia. Acest lucru presupune ca funcţionarul public *să ştie* (ceea ce ţine de eficienţa comunicării interne), *să creadă* (este vorba de coerenţa dintre discursul pe care îl afişează şi acţiunile sale concrete) *şi să vrea* (adică să simtă nevoia să vorbească despre instituţia de administraţie publică, ceea ce trimite la ideea de motivaţie).

Comunicarea în instituţiile publice se realizează prin:

- comunicarea orală (verbală) – de exemplu comunicarea dintre funcţionar şi cetăţean la ghişeu sau la birou;
- comunicarea scrisă;
- Instituţiile din administraţia publică urmăresc ca, prin intermediul comunicării, să obţină următoarele facilităţi[12]:
- identificarea - ce răspunde nevoilor instituţiilor administrative de a-şi asigura notorietatea şi de a-şi face cunoscute competenţele;
- informarea - care urmăreşte să facă cunoscută corpului social acţiunea administrativă;
- realizarea unei educaţii sociale – ce corespunde, sub forma de sfaturi, recomandări, rolului din ce în ce mai important al instituţiilor publice în cadrul vieţii sociale.

Autoritatea publică urmăreşte, prin comunicare, o relaţie de proximitate cu cetăţeanul, apropiindu-se de acesta şi intrând în dialog, pentru a-i cunoaşte

[12] F. Dubois – Les politiques de communication externe des collectivités territoriales, Université de Lille III, Lille, 1994

cerinţele, doleanţele[13]. În procesul de comunicare pot apărea următoarele **bariere comunicaţionale:**

a) **La nivelul emiţătorului şi al receptorului:**

- starea emoţională a receptorului;
- rutina, care influenţează receptivitatea;
- imaginea de sine a emiţătorului şi a receptorului şi imaginea despre interlocutor;
- caracterizarea diferită a situaţiei de comunicare de către emiţător şi receptor;
- lipsa atenţiei în receptarea mesajului;
- concluzii grăbite asupra mesajului;
- lipsa de interes a receptorului faţă de mesaj;
- sentimentele şi intenţiile participanţilor la situaţia de comunicare.

b) **La nivel de limbaj:**

- aceleaşi cuvinte primesc sensuri diferite pentru persoane diferite, în special din cauza diferenţelor în planul pregătirii şi al experienţei;
- dificultăţi de exprimare; exprimarea cu stângăcie a mesajului de către emiţător;
- utilizarea de cuvinte sau expresii confuze.

c) **La nivelul contextului:**

- context fizic necorespunzător (poluare fonică ridicată);
- suporţi informaţionali necorespunzători.

Diversitatea cauzelor care determină dificultăţile şi perturbările aferente procesului de comunicare face obligatorie existenţa în cadrul respectivului sistem a posibilitaţilor de reglare, de adaptare şi de transformare[14]. Elementul central al acestei reglări este reprezentat de feed-back, care îi permite receptorului (de exemplu, cetăţeanul) să-şi emită reacţiile, iar emiţătorului (de exemplu, funcţionarul public, purtătorul de cuvânt al instituţiei, etc) să le înregistreze. Abilitatea comunicatorului de a răspunde adecvat feed-back-ului este determinantă pentru eficienţa comunicării. Funcţiile feed-back-ului sunt următoarele[15]:

a) funcţia de control al înţelegerii, al receptării în bune condiţii a mesajului;
b) funcţia socio-afectivă: feed-back-ul creşte siguranţa internă şi satisfacţia actorilor.
c) funcţia de adaptare a mesajului la caracteristicile actorilor, la dificultăţile întâmpinate sau alte evenimente care presupun o modificare a conţinutului sau a formei;

[13] V. A. Munteanu – Marketing public, Ed. Sedcom Libris, Iaşi, 2006
[14] I. Chiru – Comunicare interpersonală, Ed. Tritonic, Bucureşti, 2003
[15] J. C. Abric – Psihologia comunicării, Iaşi, 2002

d)funcţia de reglare socială prin flexibilitatea rolurilor şi funcţiilor îndeplinite de diverşi actori, în măsură să faciliteze înţelegerea punctului de vedere al celuilalt;

1.2.2. Comunicarea interpersonală în administraţia publică

Una dintre dificultăţile derulării unui proces de comunicare eficient este generată de *disonanţa cognitivă*. Aceasta presupune selectarea surselor de informare în conformitate cu propriile convingeri ale entităţilor implicate în transmiterea sau receptarea mesajului comunicat.

Fenomenul disonanţei cognitive este frecvent în administraţia publică. Astfel, când un grup se constituie pentru a discuta diferite probleme, constatăm că, de la şefii departamentelor, la ministere, la directori generali, la secretari de stat, etc, fiecare găseşte grupul în care ceilalţi au aceeaşi viziune asupra problemelor. Când întâlnirea începe şi membrii grupului îşi expun opiniile personale, ei aud propriile puncte de vedere prezentate în cuvinte diferite şi pleacă întăriţi în convingerile lor iniţiale, care sunt asemănătoare cu ale celorlalţi.

În plus şi în rândul funcţionarilor publici se manifestă un mecanism psihologic care acţionează în sensul respingerii şi al deformării informaţiilor şi realităţilor care nu sunt în concordanţă cu propriile convingeri.

De asemenea, pot fi identificate situaţii în care funcţionarii publici s-au dovedit total opaci, nereceptivi faţă de faptele care le-au fost prezentate de administraţie publică, prin procesul de comunicare cetăţean-instituţie. Se întâlnesc frecvent situaţii în care funcţionarul oferă impresia că ascultă, deşi, în realitate, nu este atent. Este doar politicos, rămânând liniştit până când îi vine rândul să vorbească, timp în care îşi trece în revistă propriile argumente. Răpunsul său este, aproape în întregime, nepotrivit cu cele spuse de vorbitorul anterior, ignorând complet punctele de vedere expuse de cetăţean. Ca urmare, asemenea respingere evidentă pune o problemă reală de comunicare şi trebuie recunoscută ca atare[16]. Pentru reducerea influenţei barierelor în comunicarea scrisă şi chiar înlăturarea acestora, materialul informativ trebuie elaborat în funcţie de receptor.

1.2.3. Comunicarea online și interacțiunea cu cetățeanul

COMUNICAREA EXTERNĂ A ADMINISTRAŢIEI PUBLICE

Aflată într-un contact permanent şi direct cu mediul social, instituţia publică preia “şocurile” provenite de la acesta şi încearcă să le răspundă prin iniţierea, la nivel organizaţional, a unor demersuri orientate spre schimbări, transformări, reechilibrări[17]. Pe de altă parte, orice transformare sau schimbare este resimţită şi în exterior, administraţia influenţând şi modelând, la rândul ei, mediul social.

[16] H. A. Simon, V.A. Thompson, D. W. Smithburg – Administraţia publică
[17] Lucica Matei – Management public

În cadrul proceselor de comunicare externă a administraţiei publice este posibil să apară **bariere comunicaţionale:**

- între diferitele instituţii ale administraţiei publice, din cauza gradului ridicat de specializare a fiecăreia, neacordării importanţei cuvenite colaborării între instituţii;
- între administraţia publică şi cetăţeni.

COMUNICAREA ÎNTRE INSTITUŢIA PUBLICĂ ŞI CETĂŢENI

Autorităţile publice trebuie ca, prin întreaga lor activitate, să urmărească satisfacerea interesului general al populaţiei, iar instituţiile administraţiei publice au obligaţia să se apropie de membrii colectivităţilor locale şi să menţină un contact permanent cu aceştia. În acest sens, administraţia publică trebuie să comunice, să fie deschisă dialogului, să respecte şi să ia în considerare cetăţeanul.

Instituţiile administraţiei publice recurg la comunicare în cadrul acţiunilor întreprinse sau al relaţiilor pe care le stabilesc.

Comunicarea publică reprezintă forma de comunicare ce însoţeşte activitatea instituţiilor publice, în vederea satisfacerii interesului general. Mesajele transmise cuprind informaţii de utilitate publică. Astfel, comunicarea publică trebuie să facă cunoscute cetăţenilor existenţa oraganizaţiilor din sectorul public, modul de funcţionare şi atribuţiile acestora, legalitatea şi oportunitatea deciziilor adoptate. Totodată, prin comunicarea publică se urmăreşte cunoaşterea nevoilor şi dorinţelor populaţiei pentru ca instituţiile publice, prin rolul şi atribuţiile pe care le deţin, să vină în întâmpinarea acestora, realizând astfel un interes general.

Comunicării publice îi revine rolul de a convinge, prin politicile instituţionale realizate, precum şi prin deciziile publice adoptate, că se urmăreşte un interes general, obţinându-se astfel adeziunea cetăţenilor.

Cetăţeanul trebuie să fie informat cu privire la existenţa şi modul de funcţionare a serviciilor publice, trebuie ascultat când îşi exprimă nemulţumirea, trebuie să-i fie luate în considerare dorinţele şi nevoile. În literatura de specialitate întâlnim următoarele categorii de comunicare publică[18]:

- comunicarea instituţiei prezidenţiale;
- comunicarea parlamentară;
- comunicarea guvernamentală: a guvernului, ministerelor şi celorlalte structuri subordonate guvernului;
- comunicarea organismelor publice, altele decât cele incluse în cadrul comunicării guvernamentale, precum şi a întreprinderilor de interes public;

De exemplu, în cadrul instituţiilor publice locale, comunicarea publică are următoarele forme:

[18] A. Martereau – Communication publique teritoriale, Les editions de C.N.F.P.T., Paris, 1996

- punerea la dispoziţia cetăţenilor a informaţiilor de interes local;
- prezentarea şi promovarea serviciilor publice oferite de colectivităţile locale;
- promovarea instituţiilor publice şi a colectivităţilor teritoriale.

Cetăţenii vin în contact cu instituţiile publice locale şi, ca urmare, au nevoie să ştie cum se adresează pentru satisfacerea unui interes legitim, ce documente trebuie să completeze, ce proceduri trebuie să urmeze. Instituţiilor publice locale le revine obligaţia de a pune la dispoziţia publicului informaţii cu caracter practic, de natură să facă cunoscute cetăţenilor regulile pe care trebuie să le respecte în demersurile lor, să faciliteze accesul acestora la serviciile publice locale[19].

O relaţie deschisă, de parteneriat, va uşura fluxul de informaţii în ambele sensuri. Iniţiatorul acestei relaţii trebuie să fie instituţia administrativă, care are obligaţia să caute modelele cele mai eficiente şi specifice pentru realizarea feed-back-ului şi pentru cunoaşterea resurselor locale. Buna funcţionare a comunicaţiilor facilitează administrarea şi controlul proceselor de prestare, al operaţiilor din care se compun diferitele procese şi are un impact puternic asupra comportamentului funcţionarilor publici, a eficienţei şi oportunităţii în interacţiunile cu diverse categorii de cetăţeni.

Prin **comunicaţiile interne** raţional organizate şi funcţionale, personalul este în mod continuu informat despre tot ceea ce se întâmplă în cadrul instituţiei administrative. Comunicaţiile interne joacă un rol important şi pe linia instruirii şi a motivării personalului, contribuind, în acest fel, la realizarea calităţii prestaţiilor şi la o mai bună satisfacere a nevoilor şi exigenţelor cetăţenilor[20].

Instituţiile publice pot recurge la o paletă largă de tehnici şi mijloace de comunicare precum: publicaţii, broşuri specializate, afişaj, canale de televiziune, presă.

COMUNICAREA ÎNTRE FUNCŢIONARUL PUBLIC ŞI CETĂŢEAN

În procesul comunicării, relaţia funcţionar public-cetăţeni constituie substanţa actului de administraţie publică.

Unităţile comunicaţionale, respectiv funcţionarul public (ca emiţător) şi cetăţeanul (ca receptor de mesaje) au obiective clare:

- **emiţătorul** îşi propune să informeze, să convingă, să îndrume, să capteze interesul, să fie eficient;
- **receptorul** se va strădui să fie atent, să înţeleagă, să reţină.

Comunicarea cu cetăţenii se realizează prin: expuneri, activităţi de informare, dezbateri, sesiuni de comunicări, programe de investigare, activităţi cu caracter cultural-educativ, participare la concursuri, publicaţii proprii, afişiere, transmiterea prin forme scrise sau orale de informaţii diverse spre şi dinspre structurile de conducere şi de specialitate ale instituţiilor administraţiei publice.

---

[19] F. Coman – Kund – Politica de comunicare externă a colectivităţilor locale, Editura Economică, Bucureşti, 2000

[20] A. Vorzsak (coord.) – Marketingul serviciilor, Presa Universitară Clujeană, Cluj-Napoca, 2004

Liderii din administraţia publică trebuie să acorde o atenţie deosebită antrenării funcţionarilor publici în facilitarea comunicării dintre aceştia şi cetăţeni. În acest sens, putem identifica următoarele sarcini:

- diagnosticarea problemelor;
- culegerea, verificarea şi diseminarea informaţiilor;
- trasmiterea rezultatelor evaluării informaţiilor;
- rezolvarea conflictelor.

Pentru realizarea acestor sarcini, pot fi avute în vedere următoarele căi de rezolvare:

- ascultarea activă;
- stimularea autoanalizării problemelor;
- controlul tonului vocii;
- cultivarea întelegerii şi toleranţei;
- detensionarea atmosferei.

Parteneriatul interactiv funcţionar public-cetăţean presupune circulaţia informaţiei în ambele sensuri. Dincolo de aspectele oficiale, instituţionale, relaţia funcţionar public-cetăţean trebuie să conţină o anumită doză de informaţii.

Comunicarea este absolut esenţială pentru organizare. Este evident că fără comunicare nu poate fi organizare, căci atunci nu există posibilitatea ca grupul să influenţeze comportamentul individului. Pe lângă aceasta, disponibilitatea anumitor tehnici de comunicare va determina, în mare parte, modul în care funcţiile de luare a deciziilor pot şi trebuie distribuite în instituţie[21].

Din punct de vedere al legislaţiei în vigoare, instituţiilor publice le revine responsabilitatea informării cetăţenilor (informare exactă şi simplă), a primirii lor în audienţă şi a consultării acestora în problemele care-i privesc.

[21] Herbert A. Simon – Comportamentul administrativ

2. Servicii electronice şi aplicaţii în spaţiul virtual

2.1. Noţiuni de bază privind spaţiul virtual (Internet)

2.1.1. Introducere

Reţeaua mondială Internet reprezintă o modalitate de comunicare, fiind un mecanism de stocare şi propagare a informaţiilor, un mediu de colaborare şi interacţiune între indivizi (prin dispozitivele pe care le controlează), fără a ţine cont de localizarea lor geografică. Internet-ul este exemplul cel mai sugestiv referitor la beneficiile pe care le poate aduce investirea solidă în cercetare şi în dezvoltarea infrastructurilor de comunicaţii.

Reţeaua Internet poate fi prezentată ca o colecţie globală de echipamente de comunicaţii (staţii de lucru, servere, dispozitive de interconectare şi periferice) organizate sub forma unei imense reţele. Principalele atribute ale reţelei Internet sunt:

- este o grupare masivă de echipamente hardware, soluţii software, informaţii, oameni, cu o arie de acoperire planetară, aflate într-o permanentă interacţiune;
- nu are un proprietar, însă există reguli şi mecanisme care contribuie la buna ei funcţionare; reţeaua funcţionează după standarde reglementate de organisme internaţionale independente;
- nu este concepută ca o reţea cu un scop unic;
- este o vastă matrice de reţele de calculatoare (locale, metropolitane, naţionale) care susţin o mare varietate de tehnologii şi aplicaţii: poşta electronică (*e-mail*), World Wide Web (*WWW*), biblioteci de fişiere, aplicaţii de comunicaţii de voce VoIP (*Voice-Over IP*), comerţ electronic (*e-commerce*), învăţământ la distanţă (*e-learning*) etc;
- dispozitivele (sisteme de calcul, echipamente periferice) care compun reţeaua Internet, sunt identificate printr-o adresă unică (*adresa IP)*, iar comunicarea dintre ele se realizează prin transmiterea şi recepţia pachetelor de date.

Un aspect important îl reprezintă modul de utilizare a cuvântului "**INTERNET**":

- **Internet** - scris cu majusculă identifică reţeaua globală de calculatoare interconectate
- **internet** - scris cu litere mici face referire la orice reţea de calculatoare, adică o reţea ce interconectează mai multe echipamente de comunicaţii care aparţin unei organizaţii, companii, universităţi sau grup de persoane.

Prima dată semnificativă în realizarea reţelei Internet o reprezintă anul 1957, când Uniunea Sovietică lansează satelitul Sputnik (pe 4 octombrie). Ca urmare, în Statele Unite ale Americii (*SUA*) se formează, în cadrul **DoD** (*Department of Defense* - Departamentul Apărării), grupul **ARPA** (*Advanced Research Projects Agency*). Scopul acestui grup era de a menţine SUA în fruntea evoluţiei tehnologice, în special în domeniul apărării. Prima însemnare oficială legată de

dezvoltarea unei reţele globale datează din 1962 de la conducătorul grupului ARPA, J.C. Licklider, care a emis ipoteza realizării unei reţele globale de sisteme de calcul interconectate prin care să se obţină acces în timp real la date şi informaţii fără a depinde de poziţionarea geografică.

În cadrul organizaţiei non-profit RAND (*Research ANd Development Corporation*), a cărei activitate în anii ’60 - ’70 se concentra asupra problemelor din domeniul militar, cercetătorul Paul Baran a emis două ipoteze care au revoluţionat dezvoltarea conceputului de comunicare în cadrul reţelei ARPANET prin realizarea:

- unei **reţele de calculatoare distribuite**;
- unei tehnici (standardizări) de transmitere a datelor, denumită ulterior "**comutare de pachete**".

Ideea de bază de la care s-a pornit a fost necesitatea practică de a asigura un sistem de comunicaţii funcţional la nivelul întregului teritoriu al Statelor Unite în diferite situaţii (cum ar fi un conflict nuclear), precum şi din nevoia segmentării nodurilor de comunicaţii (astfel încât distrugerea unui nod să nu implice nefuncţionarea întregului sistem de comunicaţii).

MAI MULTE CĂI DE COMUNICAŢII (NODURI DISTRIBUITE)

La vremea respectivă existau două modele de bază pentru construirea unei reţele de comunicaţie:

- **centralizată** - toate nodurile sunt conectate la un distribuitor (comutator central) denumit Switch. Datele de la un nod sunt trimise către nodul central care le transmite (rutează) spre destinaţie; dacă nodul central este distrus, toată comunicaţia este întreruptă şi reţeaua devine nefuncţională;
- **descentralizată** - utilizează mai multe noduri de comutare centrale, fiind organizată pe principiul mai multor reţele centralizate interconectate. În cadrul acestui model, fiecare nod este dependent de nodul de comutaţie de care aparţine şi de calea (ruta) până la acesta. Este un model de reţea fiabilă faţă de varianta centralizată, dar reţeaua încă depinde de distribuitoare.

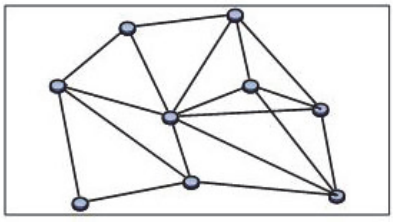


Fig. 1.1. Reţea cu noduri distribuite (conform teoriei lui Paul Baran)

Conform conceptului enunţat de către Paul Baran, **reţeaua distribuită** are un model de comunicare de la sursă la destinaţie prin mai multe căi (rute) alternative,

fiecare nod fiind conectat la mai multe noduri, fără a exista un comutator central. Există astfel mai multe rute de a trimite datele spre o anumită destinaţie. În cazul distrugerii unui nod, comunicarea între noduri este realizată folosind căile alternative asigurate prin nodurile vecine (figura 1.1).

COMUTAREA DE PACHETE

Tehnica de transmitere a datelor constă în împărţirea mesajului original în mai multe blocuri de mesaje scurte la sursă, trimiterea acestora separat prin reţea, iar la destinaţie, mesajul original se reface din blocurile componente recepţionate. Cercetătorul britanic Donald Davies a realizat un sistem în care blocurile componente ale unui mesaj, denumite **pachete** (*packets*), sunt transmise secvenţial şi nu în mod continuu, permiţând un transfer eficient al datelor.

Reţelele de comunicaţii tradiţionale, cum ar fi reţeaua telefonică, lucrează cu linii dedicate unei anumite convorbiri (comutare de circuite). Astfel, când se iniţiază un apel, se dedică o linie (un circuit) pentru acel apel şi aceea linie de comunicaţie nu poate fi utilizată cât timp apelul este în derulare. Dacă se efectuează o pauză în convorbire, linia este în continuare ocupată şi nu este disponibilă pentru alţi utilizatori, iar circuitul nu este utilizat în mod eficient.

Paul Baran a construit o reţea de noduri care au rol de comutare şi transmit (rutează) pachetele de la un nod la altul până la destinaţie, nodurile utilizând schema de lucru numită ”**Hot Potato Routing**”.

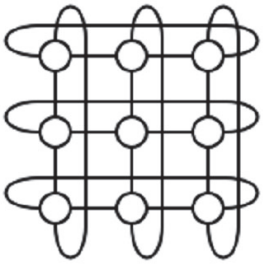


Fig. 1.2. Modelul Hot Potato Routing

Prin utilizarea de calculatoare digitale pe post de noduri, operaţia poate fi făcută foarte rapid, permiţând transferul aproape în timp real. Calculatoarele pot utiliza statistici constant actualizate despre starea reţelei şi a nodurilor acesteia pentru a putea determina în fiecare moment calea (ruta) cea mai bună către o anumită destinaţie. Dacă un nod nu este disponibil (are probleme tehnice, a fost distrus), pachetele pot fi transmise (rutate) pe o cale alternativă.

EVOLUŢIA REŢELEI LA NIVEL MONDIAL

La începutul dezvoltării sale, reţeaua ARPANET nu a fost proiectată ca model de reţea pentru a fi utilizată în timpul unui conflict militar, ci doar pentru a simplifica comunicarea între cercetătorii din cadrul echipei ARPA şi pentru a permite utilizarea în comun a datelor şi a resurselor sistemelor de calcul de la distanţă.

Conceptul lui Paul Baran referitor la realizarea unei reţele fiabile de comunicaţii era foarte eficient şi a fost imediat adoptat de către echipa de cercetători din cadrul reţelei ARPANET (**metoda reţelei distribuite** şi **a comutării de pachete**). Nodurile erau constituite din calculatoare denumite IMP (*Interface Message Processors*) care au devenit apoi dispozitive de alegere a căilor (*routers*).

ARPANET a pornit cu 4 noduri şi în august 1969 a fost livrat primul IMP la UCLA (University of California, Los Angeles), iar peste o lună, al doilea IMP la Stanford Research Institute. Cele două centre au fost conectate şi astfel s-a născut prima conexiune din cadrul ARPANET. Până la sfârşitul anului erau conectate alte două centre, University of Utah şi UCSB - University of California, Santa Barbara.

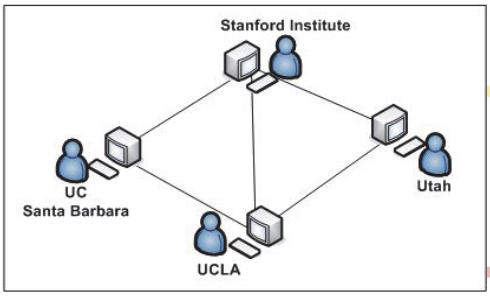


Fig. 1.3. Prima reţea ARPANET în anul 1969

Protocolul reprezintă **un set de reguli şi convenţii utilizate pentru a transmite informaţia într-o reţea de calculatoare**. Prin protocol se defineşte **modul în care sunt trimise datele în reţea** şi **tipul informaţiei de control (adrese, lungime) ataşate**. Fiecare calculator conectat în aceste reţele a fost denumit generic gazdă (*host*). Acesta trebuie să folosească un limbaj (protocol) comun pentru a putea interpreta corect datele transmise/recepţionate.

În următorii ani, numărul de calculatoare care se conectau la reţeaua ARPANET a crescut rapid (în 1971 existau în reţea 15 noduri şi erau conectate 23 host-uri), dar au început să apară alte reţele, cum ar fi BITNET şi CSNET (realizate pentru comunicarea în cadrul comunităţii academice şi respectiv industriale).

Iniţial, în reţeaua ARPANET se asigurau doar 3 servicii de comunicaţie: conectarea la distanţă, transferul de fişiere şi tipărirea la distanţă, iar în 1972 a fost introdus serviciul de poştă electronică şi a apărut primul program de poştă electronică pentru reţea distribuită. În aceeaşi perioadă, a început dezvoltarea unui nou protocol care ulterior a primit numele "Transmission Control Protocol/Internet

Protocol" (prescurtat TCP/IP), un protocol care să permită oricărei reţele conectarea la ARPANET, fără a fi necesare schimbări interne în arhitectura reţelei.

Prima versiune TCP/IP a apărut în 1973, însă a fost acceptat ca protocol standard abia la **1 ianuarie 1983**, când reţeaua ARPANET a trecut complet de la protocolul NCP la TCP/IP.

Noua reţea care funcţiona pe baza protocolului TCP/IP a fost denumită Internet, aceasta fiind considerată "data de naştere" a Internet-ului. În figura 1.4 sunt evidenţiate momentele de referinţă în evoluţia reţelei Internet.

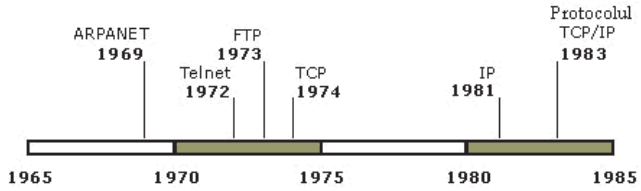


Fig. 1.4. Evoluţia reţelei Internet

Alte repere importante în dezvoltarea reţelei Internet au fost:

1973	Au fost conectate primele noduri internaţionale aflate în Anglia şi Norvegia
1974	Numărul host-urilor a crescut la 62
1979	Apare USENET, o reţea de calculatoare pentru cercetare, cu acces dial-up, bazată pe protocolul UUCP (*UNIX-to-UNIX Copy*). USENET oferea acces la servicii de e-mail şi ştiri (*Usenet News*).
1982	Reţeaua se extinde la 235 de host-uri, iar în 1983 conecta 500 de centre
1984	Reţeaua avea aproximativ 1.000 de host-uri. A fost introdus sistemul DNS (*Domain Name System*), un sistem care a înlocuit vechiul mecanism de preluare periodică a tabelei de corespondenţă domeniu - adresă IP de la NIC (*Network Information Center*) unde se ţinea evidenţa calculatoarelor conectate la ARPANET.
1986	NSF (*National Science Foundation*) creează reţeaua NSFNET pentru a conecta centrele de cercetare dotate cu super-calculatoare din peste 100 de universităţi printr-o magistrală (*backbone*) de mare viteză, la acea vreme (56 kbps). NSFNET a permis conectarea la Internet fără restricţiile impuse de ARPANET, ceea ce a declanşat o explozie de conectări, de la aproximativ 2.000 host-uri în luna februarie, la 5.000 în luna noiembrie.
1987	Se măreşte rata de transfer a magistralei de comunicaţii la 1,544 Mbps şi apoi, în 1991, la 45 Mbps, o creştere de circa 800 de ori faţă de rata iniţială, în decursul a 5 ani. După apariţia NSFNET, peste 10.000 host-uri au fost conectate, iar după 2 ani existau peste 60.000.
1990	Reţeaua originală ARPANET se desfiinţează, după ce toate organizaţiile care erau conectate au trecut la NSFNET. Tim Berners-Lee, fizician la CERN Geneva, dezvoltă protocoalele de comunicaţie

	pentru **World Wide Web**, realizând **limbajul HTML** (*Hypertext Markup Language*) care are la bază termenul de *hypertext* introdus de Ted Nelson (1965).
1992	Apar primele pagini Web disponibile prin serviciul World Wide Web. În reţea sunt peste 2 milioane de host-uri, la fiecare 30 de secunde adăugându-se un nou calculator la Internet. Se înfiinţează ISOC (*Internet Society*).
1993	**Era Web 1.0** debutează cu lansarea serviciului WWW către publicul larg. Web-ul are conţinut static, read-only (informaţia poate fi doar citită de către publicul larg). WWW conţine pagini Web între care există legături (*hyperlinks*). Primul program pentru navigare (*browser*) performant - denumit Mosaic - este lansat pe piaţă, întâi pe platforme Unix cu sistemul X-Windows, apoi pe platformele Apple MacIntosh şi Microsoft Windows.
1995	Erau conectate peste 50.000 de reţele pe toate cele 7 continente, cu peste 29.000 de reţele din S.U.A. (în total peste 4 milioane de host-uri) - NSFNET îşi încetează activitatea, accesul la Internet fiind asigurat doar prin firme specializate (*Internet Service Providers*). Sunt lansate **yahoo.com** şi **msn.com** (directoare de link-uri). Apare noţiunea de comerţ online (e-commerce), apoi încep să se dezvolte primele magazine online: amazon.com, ebay.com, buy.com.
1998	Reţeaua Internet înregistrează circa 300 milioane utilizatori. Se lansează oficial motorul de căutare **Google**.
2001	Marketingul pe Internet devine o realitate din ce în ce mai prezentă. Peste 600 de milioane de utilizatori accesează reţeaua Internet.
2003	Apar tehnicile SEO de optimizare a codului unui site Web.
2004-2010	**Era Web 2.0**: se dezvoltă concepte precum blog, social media, social networking, wiki, feeds, XML, file sharing, comunitate online. Web-ul devine read-write (suportă conţinut adăugat de utilizatori).
2011	**Era Web 3.0**: apar termeni precum "*Semantic Web*", caracterizat prin capacitatea de înţelegere a semnificaţiei informaţiei de către maşini, “personalizarea Website-urilor” (modificare în funcţie de profilul individului şi context), "căutări inteligente”.

ORGANIZAŢIILE INTERNET

INTERNET SOCIETY (ISOC - "Societatea Internet-ului") este o organizaţie internaţională, non-profit, neguvernamentală, care are ca membri peste 150 de organizaţii şi peste 6.000 de persoane din 170 de ţări. Rolul este de a superviza dezvoltarea reţelei mondiale de Internet, prin stabilirea standardelor şi tehnologiilor care fac posibilă comunicarea în cadrul acestei reţele întinse la nivel planetar. Principalele responsabilităţi ale ISOC sunt:

- dezvoltă standardele Internet prin grupurile IAB (*Internet Architecture Board*), IETF (*Internet Engineering Task Force*), IESG (*Internet Engineering Steering Group*), IRTF (*Internet Research Task Force*) - vezi figura 1.5.;

- activează în domenii cum ar fi cenzura şi libertatea de exprimare sau proprietatea intelectuală;
- contribuie la educarea managerilor din lumea Tehnologiei Informaţiei (*IT - Information Technology*).

IAB (*Internet Architecture Board*) - se ocupă cu definirea arhitecturii Internet şi de managementul nivelului superior al numelor de domenii, având rol de supervizare a grupului IETF.

IETF (*Internet Engineering Task Force*) - este responsabil de proiectarea şi dezvoltarea protocoalelor. Reprezintă comunitatea tuturor cercetătorilor şi proiectanţilor de reţele care produc, la nivel mondial, specificaţiile tehnice ale arhitecturii Internet, fiind organizată pe grupuri de lucru axate pe diverse domenii (rutare, transport, securitate etc.).

IESG (*Internet Engineering Steering Group*) - asigură managementul tehnic al grupului IETF, precum şi aprobarea de standarde, fiind format din responsabilii de zonă AD (*Area Director*) din cadrul IETF.

IRTF (*Internet Research Task Force*) - se ocupă de aspecte ale protocoalelor Internet, aplicaţiilor, arhitecturilor şi tehnologiilor.

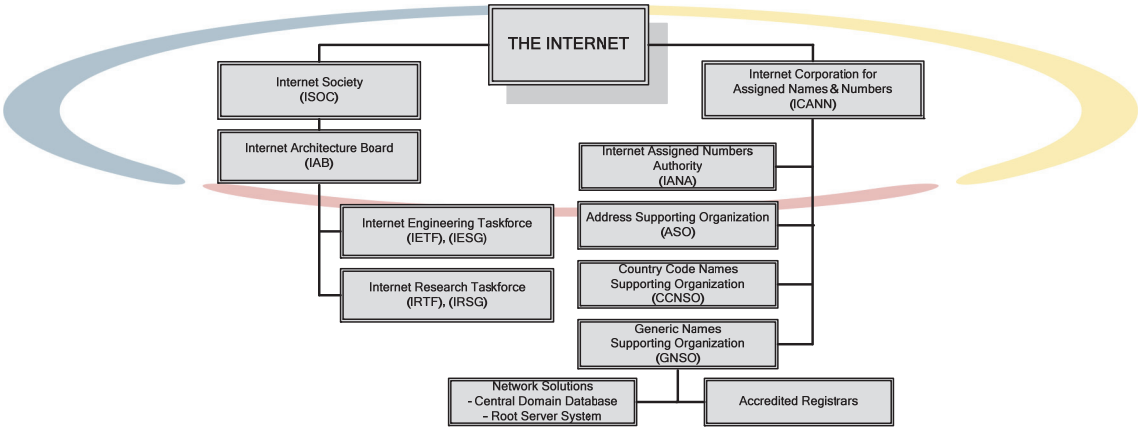


Fig. 1.5. Organizaţiile Internet

ICANN (*Internet Corporation for Assigned Names and Numbers*) coordonează din punct de vedere tehnic implementarea standardelor pentru Internet. Aceasta a fost creată în 1998 cu efortul conjugat al mediului de afaceri, tehnic şi academic, prin asumarea şi implementarea unui set de standarde tehnice, fiind formată din:

- **ASO** (*Address Supporting Organization*) - reglementează adresele IP şi modul de alocare a acestora;
- **CCNSO** (*Country Code Names Supporting Organization*) - pentru alocarea numelor de domenii;

- **GNSO** (*Generic Names Supporting Organization*) - reglementează politicile privind numele de domenii.
- **IANA** (*Internet* Assigned *Numbers Authority*) supervizează:
  - alocarea globală a adreselor IP şi a altor resurse prin intermediul unor registre locale RIR (*Regional Internet Registry*);
  - administrarea datelor din NS (nameserver-ele) de la primul nivel (nivelul de root) al DNS;
  - tipurile de formate media utilizate în cadrul Internet-ului: MIME type (*Multipurpose Internet Mail Extensions*) este un identificator prin care se deosebesc tipurile de fişiere utilizate pe Internet (de exemplu: image/jpeg, audio/mpeg, text/html);
  - alte aspecte specifice protocoalelor de comunicaţii (schemele URI - *Uniform Resource Identifier*, codarea caracterelor etc.).

REŢEAUA INTERNET ÎN ROMÂNIA

Dezvoltarea reţelelor de calculatoare şi de comunicaţii în România debutează în anul 1953, când a fost lansat proiectul "Primul calculator românesc". CIFA-1 a fost realizat la Institutul de Fizică al Academiei - Institutul de Fizică Atomică Măgurele de echipa condusă de ing. Victor Toma. Principalele momente în evoluţia şi dezvoltarea reţelei Internet în ţara noastră, au fost:

1971	Demarează la ICI primele studii privind reţelele de calculatoare.
1975	Sunt fabricate primele modem-uri româneşti la IPA (Institutul de Proiectări pentru Automatizare) şi sunt testate primele linii de comunicaţii pentru transmisia de date (ICI şi MTTc - Ministerul Transporturilor şi Telecomunicaţiilor).
după 1976	ICI experimentează transmisii de date atât pe linii de telecomunicaţii, cât şi printr-o reţea locală în care erau conectate micro şi minicalculatoare.
1984	ICI şi MTTc creează reţeaua de calculatoare electronice RENAC/RENOD (Reţeaua Naţională de Calculatoare/Reţeaua Nodală de Comunicaţii), proiectul primei reţele de calculatoare de arie largă (WAN) din România încheiat cu succes după 12 ani de cercetări. Iniţial, reţeaua a legat 3 noduri (Bucureşti, Bacău şi Cluj-Napoca), ajungând în 1989 la 18 noduri funcţionale.
1991	Se aprobă finanţarea din bugetul de stat a unui proiect de conectare la subreţeaua EARN (*European Academic Research Network*), având ca noduri ICI, IFA (Institutul de Fizică Atomică) şi IPB (Institutul Politehnic din Bucureşti).
1992	Primul nod românesc care realizează legătura internaţională cu EARN prin Universitatea din Viena devine operaţional la ICI. Se prezintă conceptul unei reţele pentru cercetare şi învăţământ superior (RNC - *Romanian National Computer Network*).
1993	ICI devine prima entitate din România conectată la Internet, pe 26 februarie

	având loc conectarea oficială a României la Internet. Domeniul ".ro" devine recunoscut la IANA şi apare primul furnizor comercial de servicii Internet, S.C. EUNET SRL. Infrastructura de comunicaţii a Universităţii POLITEHNICA Bucureşti devine operaţională în luna iunie.
1995	Se stabilesc prioritățile pentru dezvoltarea societății informaţionale din România în cadrul Strategiei de aderare la Uniunea Europeană.
1998	Peste 15.000 de calculatoare sunt conectate în domeniul ".ro", înregistrându-se o creştere continuă a conexiunilor la Internet, a furnizorilor de servicii şi a ratei de transfer.
2001	ANISP (Asociaţia Naţională a Providerilor de Internet din România) se înființează la 31 ianuarie, având ca principal scop "promovarea şi sprijinirea furnizorilor de reţele şi servicii de comunicaţii electronice".
2002	În iunie se desfăşoară la Bucureşti reuniunea ICANN.
2008	Din datele INS (Institutul Naţional de Statistică) reiese că 27% din gospodăriile din România au acces la reţeaua Internet, din care 88,1% situate în mediul urban. Numărul de utilizatori de Internet din România era de aproximativ 7 milioane.
2010	România ocupă locul 4 în lume şi primul loc în Europa la viteza medie a conexiunilor Internet (7 Mbps). Constanţa este oraşul european cu cea mai bună viteză medie pe Internet (8,8 Mbps).

2.1.2. Standarde şi modele de referinţă

Principiile şi ideile care stau la baza tehnologiei Internet, rezultate din cercetările agenţiei ARPA, includ un set de standarde ce stabilesc modul în care calculatoarele comunică, precum şi o serie de convenţii utilizate pentru interconectarea reţelelor şi dirijarea traficului de date.

În continuare vor fi analizate:

- Modelul de referinţă OSI;
- Modelul TCP/IP;
- Clasificarea reţelelor după localizare geografică, accesibilitate şi mod de conectare.

Organizarea generală a majorităţii reţelelor este făcută sub forma unor straturi (niveluri) care poartă numele generic "*layers*", fiecare dintre acestea având un set prestabilit de funcţii pe care le realizează pentru a realiza comunicaţia.

Numărul acestor niveluri, numele, conţinutul şi funcţiile variază de la un model de reţea la altul. Fiecare nivel depinde doar de nivelul imediat inferior, iar scopul unui nivel este de a oferi anumite servicii nivelului imediat superior, protejându-l de detaliile privitoare la implementarea efectivă a serviciilor oferite.

Comunicaţia între nivelurile corespondente se realizează prin parcurgerea tuturor nivelurilor inferioare acestora.

Modelul de referinţă OSI

ISO (*International Organization for Standardization*) este organizaţia internaţională care a dezvoltat şi realizat arhitecturi de reţele precum DECNET, SNA, TCP/IP. **Modelul de referinţă OSI** (*Open System Interconnection*), realizat în 1984, reprezintă o schemă descriptivă care a oferit producătorilor standardele necesare asigurării compatibilităţii şi interoperabilităţii între diferitele tehnologii.

Modelul OSI reprezintă un model de bază utilizat pentru standardizarea transmisiilor în reţele de comunicaţii, fiind structurat în 7 niveluri (vezi figura 1.6):

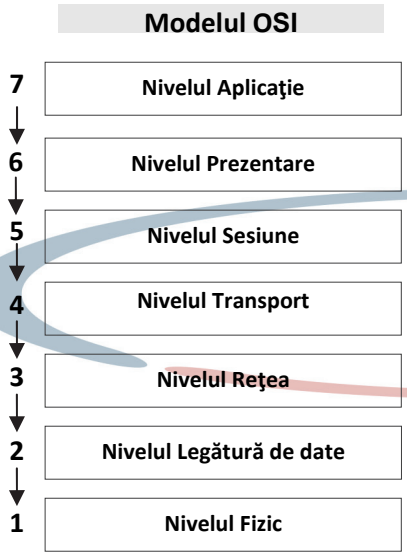


Fig. 1.6. Modelul OSI

Nivelul 7: Aplicaţie (Application Layer)

Este nivelul situat cel mai aproape de utilizatori şi oferă servicii pentru aplicaţiile acestora. Nivelul determină disponibilitatea partenerului de comunicaţie, sincronizează aplicaţiile între ele şi stabileşte procedurile pentru controlul integrităţii datelor şi erorilor. De asemenea, identifică dacă există suficiente resurse pentru desfăşurarea unei transmisii între două sisteme de calcul. Exemplu: browser Web.

Nivelul 6: Prezentare *(Presentation Layer)*

Este nivelul care se asigură că informaţiile pe care le transmite nivelul Aplicaţie al unui sistem pot fi citite de către nivelul Aplicaţie al altui sistem.

Când este necesar, nivelul Prezentare face translaţie între diferitele formate ale datelor, folosind un format comun pentru reprezentarea acestora. Exemplu: codificarea datelor.

Nivelul 5: Sesiune *(Session Layer)*

Prin sesiune se înţelege dialogul între două sau mai multe echipamente. Nivelul Sesiune stabileşte, gestionează şi finalizează sesiunile de comunicaţie între aplicaţii. Acest nivel sincronizează dialogul între nivelurile Sesiune ale echipamentelor şi gestionează schimbul de date între acestea. În plus, oferă mecanisme de verificare în ceea ce priveşte expedierea datelor, clase de servicii şi raportarea erorilor.

Nivelul 4: Transport *(Transport Layer)*

Este nivelul la care are loc segmentarea şi reasamblarea datelor. Acest nivel furnizează un serviciu pentru transportul datelor către nivelurile superioare şi, în

special, verifică disponibilitatea transportului prin reţea. Nivelul Transport oferă mecanisme prin care stabileşte, întreţine şi ordonă închiderea circuitelor virtuale, detectează căderea unui transport şi dispune refacerea acestuia, controlează fluxul de date pentru a preveni rescrierea acestora.

Nivelul 3: Reţea *(Network Layer)*

Este unul dintre cele mai complexe niveluri; asigură conexiunea şi selecţia căilor de comunicaţie între două sisteme ce pot fi localizate în zone geografice diferite. De asemenea, nivelul Reţea este responsabil de selectarea căilor de comunicaţie, switching, adresare şi rutare.

Nivelul 2: Legătură de date *(Data Link Layer)*

Este nivelul care asigură tranzitarea datelor de la nivelul fizic pe baza adresării fizice, topologiei reţelei, notificării erorilor, ordonării frame-urilor şi controlului fluxului informaţional.

Nivelul 1: Fizic *(Physical Layer)*

Defineşte specificaţiile electrice, mecanice, procedurale şi funcţionale necesare activării, întreţinerii şi dezactivării legăturii fizice între sisteme. Specificaţiile vizează nivelul tensiunii, ratele de transmisie a datelor, distanţa maximă de transmisie, conectorii fizici, mediul de transmitere.

Modelul TCP/IP

Chiar dacă modelul OSI este recunoscut pe plan internaţional ca modelul universal în domeniul reţelelor, standardul utilizat pentru reţeaua Internet este **modelul TCP/IP** (*Transmission Control Protocol/Internet Protocol*) şi suita sa de protocoale. Un sistem de calcul este conectat la Internet dacă utilizează stiva de protocoale TCP/IP, are asociată o adresă IP şi poate trimite pachete IP către toate celelalte sisteme din cadrul reţelei Internet. Spre deosebire de modelul OSI, modelul TCP/IP are doar 4 niveluri (vezi figura 1.7).

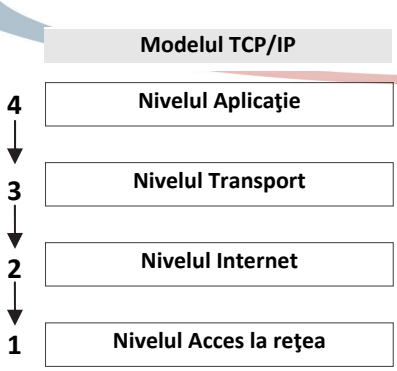


Fig. 1.7. Modelul TCP/IP

Nivelul 4: Aplicaţie *(Application Layer)*

Proiectanţii TCP/IP au considerat că protocoalele de nivel înalt din acest model trebuie să includă detalii cu privire la sesiunile de lucru şi modul de prezentare. Astfel, într-un singur nivel sunt combinate toate facilităţile legate de reprezentarea datelor sau codificarea şi controlul dialogului.

Nivelul 3: Transport *(Transport Layer)*

Acest nivel vizează controlul fluxului de date, detectarea şi corecţia erorilor. La nivelul Transport întâlnim două protocoale: **Transmission Control Protocol** (TCP) şi **User Datagram Protocol** (UDP).

Nivelul 2: Internet *(Internet Layer)*

Scopul acestui nivel este de a trimite pachetele sursă din orice reţea către o altă reţea, astfel încât aceste pachete să ajungă la destinaţie indiferent de calea aleasă şi de reţeaua din care au fost transmise. Protocolul utilizat la acest nivel este **Internet Protocol**, funcţiile îndeplinite de acesta fiind determinarea rutelor şi comutarea pachetelor (asemănător cu sistemul poştal).

Nivelul 1: Acces la reţea *(Network Access Layer)*

Numele acestui nivel este generic şi de multe ori generează confuzie. Este nivelul care include detalii despre tehnologiile LAN/WAN, precum şi toate detaliile incluse în nivelurile Fizic şi Legătură de date din modelul OSI. La acest nivel au loc procesări logice, cum ar fi reprezentarea, codarea, dialogul.

Comparaţie între modelul OSI şi modelul TCP/IP

Similitudini:

- sunt alcătuite din niveluri de lucru (layers);
- au un nivel denumit Aplicaţie, dar realizează servicii diferite;
- nivelurile Reţea şi Transport sunt comparabile.

Diferenţe:

- TCP/IP combină nivelurile Prezentare şi Sesiune din modelul OSI în cadrul nivelului Aplicaţie;
- la TCP/IP nivelurile Legătură de date şi Fizic sunt combinate într-unul singur, numit ”Acces la reţea”;
- TCP/IP are o structură simplificată, având mai puţine niveluri;
- TCP/IP reprezintă un model standardizat în baza căruia s-a dezvoltat reţeaua Internet.

Mediul Internet este construit în jurul conceptului de niveluri de lucru şi reprezintă o reţea de comutare de pachete (PSN - *Packet Switching Network*). Comunicarea (transferul informaţiilor) în mediul Internet se realizează prin colecţii de date denumite **pachete de date** (*packets*) pentru protocoale, orientate pe conexiune (exemplu: TCP), respectiv **datagrame** (*datagrams*) pentru protocoale, neorientate pe conexiune (exemplu: UDP, IP). Reţelele de comunicaţii sunt proiectate astfel încât două sisteme de calcul, localizate oriunde în lume, să fie capabile să comunice între ele, indiferent de configuraţia hardware a acestora (PC, Mac,

mainframe) sau platforma software utilizată (Windows, Linux, Solaris, Mac OS), iar acest lucru este posibil prin utilizarea unui limbaj comun numit **protocol**.

Protocolul este definit ca un set formal de reguli şi convenţii cu ajutorul cărora este reglementat schimbul de informaţii între echipamentele unei reţele. Conceptul de **nivel** este folosit pentru a înţelege mai uşor, respectiv pentru a dezvolta acţiunile şi procesele ce apar în timpul circulaţiei informaţiilor de la un calculator la altul. Nivelul “n” al unui calculator poate comunica cu nivelul “n” al altuia, iar regulile utilizate în comunicare se numesc **protocoale de nivel “n”**.

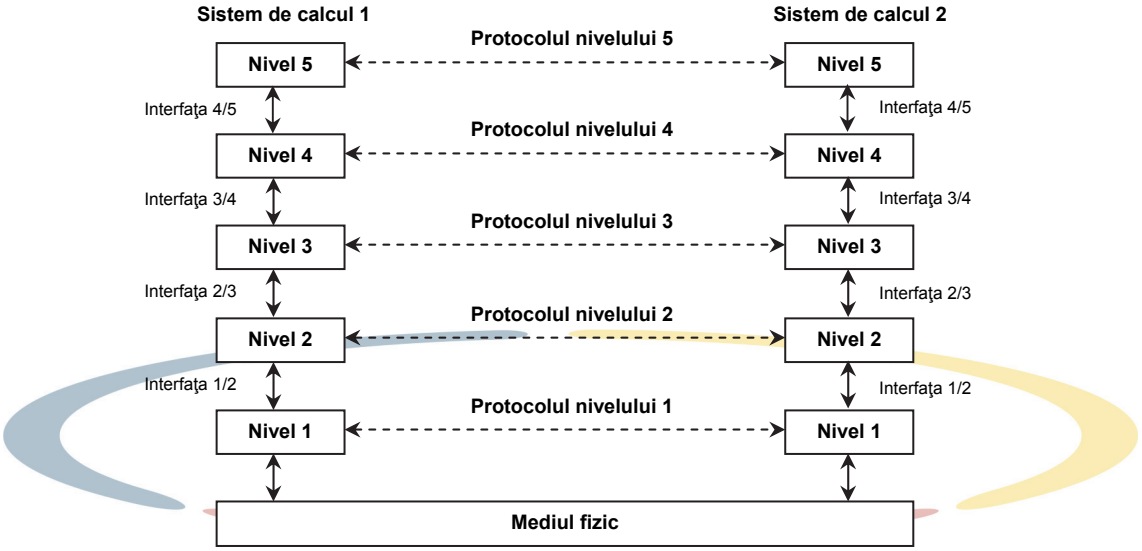


Fig. 1.8. Modul de lucru al unui protocol

Datele folosite de nivelul “n” de pe sistemul de calcul 1 nu sunt transferate direct nivelului “n” de pe sistemul de calcul 2, ci trec prin nivelurile inferioare ale sistemului 1 (nivelurile n-1, n-2, etc.) până la nivelul cel mai de jos. La acest nivel se face trecerea (prin mediul fizic de conexiune) către sistemul 2, urmând ca datele să "parcurgă" (nivelurile 1, 2, ...) spre nivelul “n” al acestuia (vezi figura 1.8).

Regulile utilizate în mediul Internet pentru a decide cum şi unde să se transmită pachetele de date formează aşa-numitele **protocoale de comunicaţii**, acestea constituind software-ul mediului Internet.

Protocoalele de comunicaţii cuprind un set de protocoale de reţea care specifică detaliile comunicaţiilor între calculatoarele (nodurile) interconectate, împreună cu convenţiile de interconectare a reţelelor şi de dirijare a informaţiilor în reţea. În prezent, majoritatea reţelelor conectate la Internet funcţionează pe baza modelului TCP/IP, iar această suită este constituită din următoarele protocoale:

- la nivelul Transport: TCP (*Transmission Control Protocol*) şi UDP (*User Datagram Protocol*) ;
- la nivelul Internet: IP *(Internet Protocol*);

TCP (*Transmission Control Protocol*) este un protocol orientat pe conexiune (între cele două sisteme de calcul care schimbă pachete de date există o legătură neîntreruptă prin care comunică permanent).

UDP (*User Datagram Protocol*) este un protocol neorientat pe conexiune, care oferă un număr limitat de servicii (nu asigură mecanisme pentru siguranţa datelor la recepţie).

IP (*Internet Protocol*) este un protocol de bază al nivelului Internet (în modelul de implementare TCP/IP) care asigură transferul pachetelor între calculatoarele conectate la Internet doar pe baza adreselor IP şi suportă fragmentarea datelor şi reasamblarea pachetelor la destinaţie.

În continuare sunt prezentate pe scurt principalele protocoale de comunicaţii utilizate în Internet:

DHCP (Dynamic Host Configuration Protocol)

Protocol care permite dispozitivelor să obţină automat informaţiile necesare funcţionării într-o reţea TCP/IP (alocare dinamică de adresă IP, mască subreţea, adresă gateway etc.).

DNS (Domain Name System)

Mecanism pentru obţinerea adresei IP (valoare numerică), pornind de la numele de domeniu (şir de caractere).

FTP (File Transfer Protocol)

Protocol utilizat la copierea fişierelor pe sau de pe un sistem de calcul la distanţă într-o reţea TCP/IP.

GOPHER

Protocol proiectat în 1991 ca alternativă la World Wide Web, utilizat pentru distribuirea şi căutarea de documente pe Internet.

HTTP (Hypertext Transfer Protocol)

Protocol utilizat pentru transportul cererilor de la un browser la un server Web şi pentru transportul paginilor de la serverele Web înapoi la clientul care le-a solicitat. Este un protocol de tip text, nesigur pentru transmiterea unor date confidenţiale.

HTTPS (Hypertext Transfer Protocol Secure)

Variantă a protocolului HTTP care asigură criptarea şi transmiterea datelor printr-un port sigur. HTTPS (elaborat de Netscape) îi permite protocolului HTTP să ruleze în cadrul unui protocol de securitate cunoscut sub denumirea de SSL (*Secure Sockets Layer*).

ICMP (Internet Control Message Protocol)

Protocol Internet utilizat la nivelul Reţea (nivelul 3 al modelului de referinţă OSI) ce asigură corecţia erorilor şi oferă informaţii privitoare la prelucrarea pachetelor IP.

IMAP (Internet Message Access Protocol)

Protocol pentru accesarea mesajelor pe un server e-mail la distanţă (*remote server*). IMAP

permite crearea de copii locale ale mesajelor e-mail (aducerea lor pe calculatorul local), însă în general este utilizat pentru gestionarea centralizată a mesajelor, permiţând mai multor clienţi accesarea aceleiaşi adrese e-mail.

IRC (Internet Relay Chat)

Formă de trimitere în timp real a mesajelor pe Internet, comunicare în grup sau prin mesaje private.

MIME (Multipurpose Internet Mail Extensions)

Standard care extinde suportul mesajelor de poştă electronică pentru alte seturi de caractere (pe lângă setul ASCII) sau ataşarea de fişiere binare.

MMS (Microsoft Media Server)

Protocol realizat şi licenţiat de Microsoft pentru furnizarea unor fluxuri de date multimedia.

POP3 (Post Office Protocol 3)

Protocol pentru a descărca (de obicei printr-o conexiune TCP/IP) mesaje e-mail stocate pe diverse servere. Versiunea curentă a standardului Post Office Protocol este 3 (de unde şi numele POP3).

PPP (Point-to-Point Protocol)

Protocol folosit pentru stabilirea unei conexiuni directe între două noduri de reţea (autentificare, compresie, criptare).

RTP (Real time Transport Protocol)

Format standardizat pentru transportul şi livrarea datelor audio şi video prin Internet (telefonie, video conferinţă).

SAP (Session Announcement Protocol)

Protocol pentru emiterea informaţiilor sesiune multicast (mod de furnizare a informaţiei unui grup de destinaţii simultan).

SMTP (Simple Mail Transfer Protocol)

Protocol dedicat pentru trimiterea unor mesaje e-mail de la un calculator la altul prin reţea.

SSH (Secure Shell)

Protocol care permite schimbul datelor între două dispozitive printr-o conexiune securizată.

SSL/TLS (Secure Sockets Layer/Transport Layer Security)

Protocoale ce folosesc metode criptografice pentru a securiza segmentele într-o conexiune la nivelul Transport. Protocolul TLS este succesorul lui SSL, ambele fiind folosite în aplicaţii precum navigare Web, poştă electronică, mesagerie instant şi telefonie VoIP.

TELNET

Protocol pentru conectarea la distanţă, nesecurizată, pe un sistem de calcul (la linia de comandă).

2.1.3. Clasificarea reţelelor

Practic, prin Internet se înţelege o ierarhie de reţele, fiecare calculator conectat la Internet făcând parte dintr-o subreţea din această ierarhie. Reţelele mici şi utilizatorii acestora se conectează la furnizorii locali de Internet (ISP) care, la rândul lor, beneficiază de serviciile unor furnizori de nivel regional sau naţional, aceştia fiind conectaţi la magistrala de transport (*backbone*) a Internet-ului.

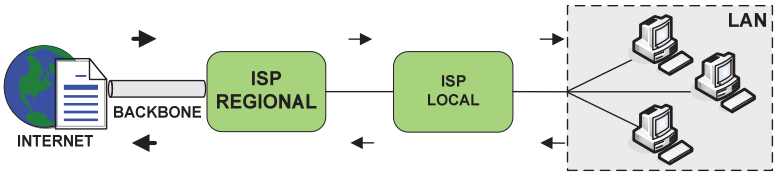


Fig. 1.9. Internet-ul ca o ierarhie de reţele

Principalele avantaje ale reţelelor de calculatoare sunt:

- partajarea accesului (*sharing*) la diverse resurse: fie hardware (unităţi magneto-optice, imprimante, scannere, camere video), fie software (fişiere de date, programe sau servicii - tipărire, partajarea conexiunii la Internet), indiferent de locul în care sunt stocate acestea în cadrul reţelei;
- posibilitatea de comunicare şi schimb de date între utilizatori prin accesarea unor aplicaţii şi servicii disponibile în cadrul reţelei.

O reţea de calculatoare reprezintă o combinaţie de elemente:

- **hardware:**
  - sisteme de calcul fixe (PC, workstation) sau mobile (laptop, smartphone);
  - adaptoare (plăci) de reţea (*Network Interface Card*) montate on-board sau extern, pe diverse magistrale (pentru calculatoare desktop) sau plăci PCMCIA (pentru calculatoare mobile);
  - mediul fizic prin care se transmite: cablu, fibră optică sau unde radio;
  - alte echipamente de interconectare (repetoare, hub-uri, switch-uri);
- **software:**
  - protocoale de comunicaţie;
  - programe pentru operarea sau managementul reţelei.

Principalele criterii după care sunt clasificate reţelele de calculatoare sunt:

După localizarea geografică

- **Reţele globale** (GAN - *Global Area Network*) reprezintă un model de asigurare a comunicaţiilor, care combină diferite tipuri de conexiuni mobile fără fir (tip WLAN sau satelit);
- **Reţele mari** (WAN - *Wide Area Network*) sunt reţelele care acoperă sau interconectează o arie geografică întinsă (oraşe, regiuni, ţări);

- **Reţele metropolitane** (MAN - *Metropolitan Area Network*) sunt reţele localizate la nivel de cartier, zonă economică sau chiar la un oraş;
- **Reţele academice** (CAN - *Campus Area Network*) se întind pe suprafaţa unui campus studenţesc şi fac legătura între diverse departamente (facultăţi) ale unei universităţi (între LAN-urile entităţilor componente). O reţea CAN permite utilizatorilor (studenţi, profesori, angajaţi) accesul gratuit la diverse resurse ale universităţii, inclusiv la Internet.
- **Reţele locale** (LAN) sunt reţele localizate într-o singură clădire sau în câteva clădiri învecinate şi au dimensiuni relativ restrânse, de până la câteva sute de metri;
- **Reţele personale** (PAN - *Personal Area Network*) sunt reţele formate pe distanţe foarte scurte (5-10 metri) între diverse dispozitive interconectabile (PDA - *Portable Digital Assistant*, smartphone, dispozitive GPS). Conectarea se poate face prin cablu (USB, Firewire) sau prin tehnologii fără fir (IrDA - unde infraroşii, Bluetooth - unde radio).

DUPĂ VIZIBILITATE ŞI ACCESIBILITATE

- **Intranet** este o reţea privată bazată pe protocolul TCP/IP, care aparţine unei organizaţii şi nu este neapărat conectată la Internet. Intranet-ul este accesibil numai utilizatorilor autorizaţi, în general din interiorul unei organizaţii (membri, angajaţi).
- **Extranet** este o reţea privată care extinde reţeaua Intranet a unei organizaţii pentru utilizatori din afara acesteia, oferind acces securizat la anumite informaţii furnizorilor, clienţilor, partenerilor de afaceri.
- **Reţea virtuală privată** (VPN - *Virtual Private Network*) este o reţea întâlnită de obicei în cadrul unor companii sau organizaţii multinaţionale, ce permite interconectarea mai multor puncte de lucru aflate în locaţii geografice diferite, într-o reţea "virtuală". Mediul de conectare folosit este reţeaua publică Internet (o reţea prin definiţie nesigură), utilizându-se pentru securizarea accesului şi a transferului datelor diverse protocoale de autentificare şi criptare.

DUPĂ MODUL DE CONECTARE

- Reţea realizată cu cablu (*wired*): pe linia telefonică (Dial-up, linie închiriată ISDN, DSL), cablu TV, reţeaua electrică, reţea locală, mod de conectare denumit şi Wired Ethernet; acesta se poate realiza prin cablu coaxial, cablu torsadat sau fibră optică;
- Reţea realizată fără cablu (*wireless*):
  - Wi-Fi, GSM, Broadband wireless, Satelit.

Alegerea tipului de conexiune se face în funcţie de condiţiile tehnice, costuri, viteza de lucru necesară sau poziţia geografică.

2.1.4. Conexiuni şi medii de transmisie

Utilizarea reţelei Internet în tot mai multe activităţi curente a condus la dezvoltarea şi standardizarea unor medii noi de transmisiune a informaţiei, precum şi la definirea unor arhitecturi funcţionale (hardware şi software) de implementare a reţelelor.

Conectarea la Internet poate fi realizată în diverse moduri: prin cabluri terestre (linie telefonică, linii închiriate DSL sau ISDN, fibră optică, cablu coaxial, cablu TV), Wi-Fi, satelit sau dispozitive mobile, dar esenţial pentru orice tip de conexiune este timpul de conectare şi rata de transfer a datelor. Funcţia de bază a mediului de transmisiune este de a transporta informaţia sub formă de biţi şi bytes de la sursă către destinaţie. Cele mai utilizate medii de transmisiune sunt:

- conductorii pe bază de cupru, de tip:
  - UTP (*Unshielded Twisted Pair*) - rate de 10/100 Mbps, distanţa maximă circa 100 m;
  - Cablu coaxial - 1/10 Mbps, distanţa maximă 185 - 500 m, în funcţie de tip;
- fibra optică - 100/1000 Mbps, distanţa maximă 2 - 60 km, în funcţie de tip;
- unde radio - 11 - 54 Mbps (reţele wireless WLAN, distanţa maximă de zeci de metri);

CONEXIUNE PRIN LINIE TELEFONICĂ

Un modem (modulator-demodulator) realizează conexiunea la un furnizor de servicii prin intermediul unei linii telefonice. Acest tip de acces permite conexiuni la rate de transfer teoretice de maxim 56 kbps, influenţate însă foarte mult de zgomotul de pe liniile telefonice (practic se ating rate de 40 - 50 kbps, însă rata de transfer pe o linie cu mult zgomot poate fi şi de 20 kbps).

Pentru conectarea unui calculator la un furnizor de servicii se utilizează protocolul PPP (*Point-to-Point Protocol*), realizându-se o conexiune modem-la-modem, la preţul unei convorbiri telefonice până la ISP (de obicei preţul unei convorbiri locale).

(a) (b) (c)

Fig. 1.10. Modem-uri: a. intern, hardware; b. extern; c. PCMCIA

CONEXIUNE PRIN LINIE ÎNCHIRIATĂ

ISDN (*Integrated Services Digital Network*)

Este un serviciu specific reţelei telefonice cu comutaţie de circuite, care permite transmiterea digitală atât a vocii, cât şi a datelor, prin intermediul aceleiaşi legături de fire din cupru, realizându-se o îmbunătăţire considerabilă a calităţii şi vitezei de transfer a datelor în comparaţie cu sistemele analogice.

Fig. 1.11. Modem ISDN

DSL (*Digital Subscriber Line*)

DSL este o tehnologie apărută la sfârşitul anilor '80, care permite transmisia digitală a informaţiilor pe liniile telefonice la viteze net superioare tehnologiei ISDN. DSL foloseşte banda de frecvenţe înalte şi nu afectează funcţionarea simultană a serviciului de voce (este necesară utilizarea unui filtru care să evite interferenţele între echipamentele analogice şi serviciul DSL). Există mai multe variante de implementare a tehnologiei DSL:

- ADSL (*Asymmetric DSL*) - se caracterizează prin transmiterea asimetrică a datelor, astfel că cea mai mare parte a canalului este utilizat pentru transmiterea informaţiei către utilizator (download) şi o mică parte pentru a primi informaţii de la acesta (upload). Rate de transfer tipice: 256 kbps - 8 Mbps downstream/1 Mbps upstream. Prin utilizarea unor tehnici de codare digitală, tehnologiile mai noi (ADSL2+) permit rate superioare de ordinul 26 Mbps/3 Mbps. ADSL poate fi furnizat pe distanţe mici (în general mai mici de 4 km faţă de punctul de conexiune - centrala telefonică sau 8 km dacă permite tipul de cablu utilizat). De obicei, modemul ADSL are o interfaţă Ethernet (conector RJ-45) sau conector USB pentru conectarea calculatorului.

- SDSL (*Symmetric DSL*) - este opusul ADSL, deoarece banda este împărţită pe jumătate între download şi upload (simetric). Distanţa maximă de conectare: 3 km. Viteza de download/upload: 1,5 Mbps/1,5 Mbps.
- HDSL (*High Bitrate DSL*) - printre primele variante de DSL, este de tip simetric. Lucrează la 1,544 Mbps (America de Nord) sau 2,048 Mbps (Europa).
- VDSL, VHDSL (*Very High Bitrate DSL*) - 2001 - permite rate ridicate pentru aplicaţii gen HDTV, VoIP sau acces Internet de mare viteză. Valori tipice pentru rata de transfer: 13 - 52 Mbps download/2 - 3 Mbps upload.
- G.Lite (*DSL Lite*) - o variantă mai lentă de ADSL care nu necesită scindarea liniei la utilizator, aceasta realizându-se în centrala telefonică. Valori tipice pentru conexiune: 1,544 Mbps - 6 Mbps download/128 kbps - 384 kbps upload.

Fig. 1.12. Modem ADSL

CONEXIUNE PRIN CABLU TV

Este utilizată infrastructura televiziunii prin cablu (CATV), folosindu-se pentru accesul la Internet ca mediu de transmisiune cablul coaxial. Deoarece semnalele TV ocupă doar o mică parte a benzii suportate de cablul coaxial, au fost introduse noi servicii, precum *Internet prin cablu* şi *telefonie prin cablu*.

Fig. 1.13. Modem CATV

CONEXIUNE PRIN REŢEAUA ELECTRICĂ

BPL (Broadband over Power Lines) utilizează pentru conectarea la Internet reţeaua de distribuţie a energiei electrice. Rata de transfer a datelor este echivalentă unei conexiuni prin cablu TV sau DSL, între 500 kbps şi 3 Mbps.

Fig. 1.14. Modem BPL

CONEXIUNE PRIN REŢEAUA LOCALĂ

În cazul în care calculatorul face parte dintr-o reţea de tip LAN care este conectată la Internet, atunci acel calculator dispune de o **conexiune Internet permanentă prin LAN**. Conexiunile prin reţeaua locală reprezintă o alternativă la conexiunile prin liniile telefonice închiriate, principalele sale caracteristici fiind ratele de transfer ridicate şi întinderea pe suprafeţe geografice relativ mici (zeci sau sute de metri, la nivel de birou, clădire sau chiar acasă).

Standardul IEEE 802.3 reprezintă un set de standarde pentru cablare şi semnalizare definite la nivelul Fizic şi al Legăturii de date (primele două niveluri ale modelului de referinţă OSI, care stabilesc tehnologiile de tip Ethernet pentru reţele LAN. Transmisia datelor se poate realiza prin:

- cabluri coaxiale (10BASE5, 10BASE2);
- cabluri torsadate (10BASE-T, 100BASE-T, 1000BASE-T, 10GBASE-T);
- fibră optică - în general pentru "coloana vertebrală" a reţelei (10BASE-F, 100BASE-FX, 1000BASE-SX, -LX, -CX, 10GBASE-SR, -LR, -ER, -SW, -LW, -EW);
- unde radio (Wireless LAN);

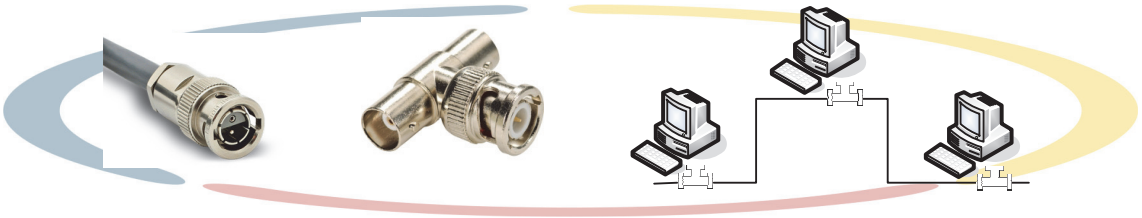


Fig. 1.15. Conectori şi mod de conectare 10BASE2 "Thinnet"

CONEXIUNE WI-FI

Wi-Fi este denumirea comercială a tehnologiilor utilizate pentru produse certificate, bazate pe setul de standarde IEEE 802.11 care garantează interoperabilitatea între diverse dispozitive fără fir (wireless) - sisteme de calcul, laptop-uri, PDA-uri, smartphone-uri, console de jocuri şi alte dispozitive periferice.

Fig. 1.16. Echipamente de conectare wireless: placă de reţea şi router

WLAN (Wireless LAN)

Este o reţea locală fără fir formată din două sau mai multe sisteme de calcul sau alte dispozitive (de exemplu, imprimante) care comunică între ele într-o arie limitată, la viteze comparabile cu cele ale reţelelor Ethernet pe cablu.Versiunea iniţială 802.11a (octombrie 1999) operează în banda de 5 GHz la o rată de transfer maximă de 54 Mbps. Versiunile 802.11b (octombrie 1999) şi 802.11g (iunie 2003) operează în banda de 2,4 GHz la o rată maximă de 11 Mbps, respectiv 54 Mbps, şi o distanţă de circa 34 metri, dar operarea în această bandă poate produce interferenţe temporare cu alte dispozitive (cuptoare cu microunde, dispozitive Bluetooth sau telefoane fără fir). O nouă versiune a acestui standard, 802.11n, lansată în 2009, atinge rate de transfer de 150 Mbps şi o rază de acţiune de circa 70 metri.

CONEXIUNE WIRELESS BROADBAND

Asigură rate de transfer între 128 kbps şi 1 Mbps, comparabile cu conexiunile terestre prin cablu de tip ADSL sau modem CATV. Furnizorii acestui tip de serviciu denumit WISP (*Wireless Internet Service Providers*) extind reţeaua Internet în zone rurale sau unde nu sunt disponibile legături terestre care să ofere viteze optime, prin intermediul unor antene montate în locuri cu vizibilitate maximă.

Fig. 1.17. Antenă bază şi antenă client

Ambele capete al legăturii radio trebuie, de regulă, să fie direct vizibile între ele (*direct line of sight*) pentru a beneficia de performanţele maxime oferite de acest tip de conexiune.

CONEXIUNE SATELIT

O legătură de tip satelit este utilizată în zonele unde legăturile terestre nu sunt disponibile din cauza costurilor ridicate de implementare. Pentru a utiliza o conexiune satelit este necesară o antenă cu un receptor, un transmiţător şi un IDU (*InDoor Unit*) care realizează comunicaţia cu sistemul de calcul. Aceste echipamente sunt numite sistem terestru VSAT (*Very Small Aperture Terminal*) datorită dimensiunii reduse a antenei (între 0,55 şi 1,2 m).

Fig. 1.18. Antenă utilizată la conexiunea de tip satelit

Sistemul VSAT oferă rate de transmisie de până la 52,5 Mbps la legătura de ieşire (de la Hub la VSAT) şi 307,2 kbps la legătura de intrare (de la VSAT la Hub).

CONEXIUNE GPRS

GPRS *(General Packet Radio Service*) este un serviciu pentru date mobile disponibil utilizatorilor de telefonie mobilă GSM (*Global System for Mobile*) atât în sistemul 2G (la rate de 56 - 114 kbps), cât şi în 3G (până la 14,4 Mbps la download). GPRS permite aplicaţii Internet pentru dispozitive inteligente (telefoane mobile, PDA, smartphone) folosind protocolul WAP (*Wireless Application Protocol*).

(a)

(b)

Fig. 1.19. Echipamente de conectare GPRS: a. Modem-uri PCMCIA; b. Modem-uri USB

IrDA (*Infrared Data Association*) este standardul utilizat pentru transferul de date pe distanţe foarte scurte folosind raze infraroşii. Cele două dispozitive trebuie să aibă vizibilitate directă unul faţă de celălalt, distanţa standard fiind de 1 metru.

Bluetooth este un protocol wireless pentru transferul de date pe distanţe mici între echipamente fixe şi mobile (care formează aşa-numitele *Personal Access Network*). A fost realizat ca o alternativă la standardul RS232 care utiliza portul serial al calculatorului şi un cablu de date pentru transmiterea datelor.

DECT (*Digital Enhanced Cordless Telecommunications*) este un standard pentru telefoane fără fir utilizate local, în domeniul casnic sau birouri. Unitatea mobilă se conectează la o unitate de bază prin intermediul undelor radio în banda de frecvenţe 1880-1900 MHz (în Europa).

WUSB (*Wireless USB*) este un protocol creat pentru a elimina conexiunea prin cablu între un calculator şi diverse echipamente periferice.

G.hn este standardul creat pentru reţele de mici dimensiuni (*Home Network*) aflat în dezvoltare la Uniunea Internaţională a Telecomunicaţiilor - Departamentul Standardizări în Telecomunicaţii (ITU-T). Viitorul aparţine tehnologiei G.hn, care este propus să devină standard universal pentru reţele de date bazate pe cabluri (linii electrice, linii telefonice, cablu coaxial) cu rate de transfer de până la 1 Gbps.

2.1.5. Adrese IP. Arhitecturi de reţele. Arhitectura client-server

Serviciile oferite de reţea se bazează, în marea lor majoritate, pe un sistem de date distribuite. Fiecare pachet de date dintr-un mesaj este tratat independent, fiind împachetat şi trimis secvenţial spre destinaţie pe rute diferite. Nu există o conexiune directă între sursă şi destinaţie, ruta aleasă pentru pachete depinzând de mai multe criterii prestabilite. Rutele se pot schimba de la un pachet la altul (de unde şi numele de "reţele comutate"), pachetele fiind asamblate la destinaţie. Din punct de vedere funcţional, în Internet se identifică trei tipuri de sisteme:

- ***Host*** (calculator gazdă) - calculator cu acces la Internet pe unul din cele patru niveluri (utilizator, local, naţional şi mondial) de la care se pot obţine servicii Internet.
- ***Gateway*** (calculator de legătură) - furnizează legătura între nivelurile reţelei Internet şi realizează conectarea între două reţele distincte. Gateway poate fi şi un server proxy care nu modifică cererile şi răspunsurile primite (de la staţiile locale, respectiv de la serviciile accesate).
- ***Router*** (calculator de dirijare) - furnizează servicii de dirijare a informaţiilor între două noduri prin emisie-recepţie. Sistemele de calcul tip router iau decizii asupra modului de dirijare a pachetelor de date la fel cum serviciul poştal direcţionează scrisorile spre destinaţie. Pentru ca un pachet să ajungă la recepţie se utilizează o informaţie de adresă (destinaţie). Un sistem de calcul tip router primeşte informaţia despre adresă şi, pe baza acesteia, decide pe unde să fie trimis pachetul, stabilind “conducta” (*pipe*) optimă pentru ca pachetul să ajungă la destinaţia indicată de adresa respectivă.

Există posibilitatea ca unele pachete să se rătăcească pe drumul de la sursă la destinaţie; protocolul IP conţine mecanisme de identificare a pachetelor pierdute, mecanisme prin care se emit cereri de retransmisie. Ordonarea pachetelor la destinaţie revine în responsabilitatea nivelului Transport. Fiecare host conectat la Internet trebuie să aibă o identitate (adresă) unică pentru a putea avea acces la reţeaua mondială. Această adresă se numeşte **adresă IP** (*Internet Protocol*) şi este

formată din 32 de biţi (4 octeţi) pentru adrese IP versiunea 4 (notat IPv4), formatul iniţial de adresă apărut în anii '80.

Din numărul de biţi ai unei adrese IPv4 rezultă că în total pot fi 4.294.967.296 valori unice (adică 2^{32} adrese), din care efectiv utilizabile sunt doar 3.706.650.624 adrese, deoarece:

- 536.870.912 sunt ocupate de clasele D (IP multicast) şi E (adrese experimentale), câte 2^{28} adrese fiecare;
- 17.891.328 adrese sunt rezervate pentru reţele private;
- 33.554.432 adrese sunt pentru reţelele 0 (*default route*) şi 127 (*loopback*), câte 2^{24} pentru fiecare caz.

Evoluţia rapidă a reţelei Internet începând cu anii '90 a dus la scăderea numărului de adrese disponibile, accelerată în ultimii ani atât de creşterea numărului de utilizatori, cât şi de înmulţirea într-un timp foarte scurt a dispozitivelor conectate permanent (modem-uri, routere) sau a echipamentelor mobile (laptop-uri, tablete PC, telefoane mobile sau PDA-uri). În figura 1.20 este reprezentată evoluţia alocării adreselor IPv4, conform IANA. Implementarea unei noi versiuni (denumită **IPv6**, publicată în 1998) reprezintă singura soluţie viabilă pe termen lung la problema epuizării adreselor IPv4.

Alocarea adreselor IP se face controlat, printr-o autoritate centrală care trebuie contactată de un solicitant (un ISP sau orice organizaţie care doreşte conexiune la Internet). Spaţiul adreselor IP din zona europeană este reglementat de către RIPE (*Réseaux IP Européens*), iar în România autoritatea care gestionează alocarea adreselor IP la nivel naţional este RNC (*Reţeaua Naţională de Calculatoare*).

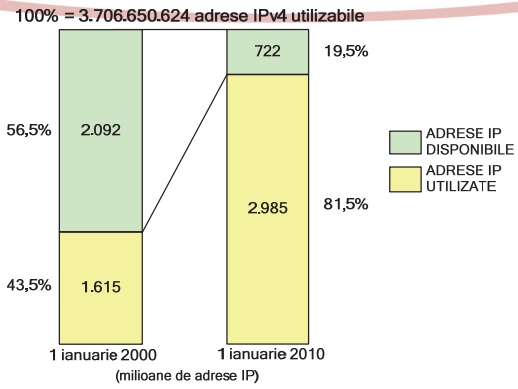


Fig. 1.20. Evoluţia alocării adreselor IPv4

Adresa IPv4. Adresarea pe clase.
Adresa IPv4, pe 32 de biţi, este structurată în două părţi distincte, ambele formate dintr-un număr de biţi multiplu de 8 (obligatoriu pentru adresarea pe clase):

- **secţiunea de reţea** (*Network*) - reprezintă identificatorul reţelei (*network-id*), cu rolul de a identifica reţeaua din care face parte calculatorul;
- **secţiunea de gazdă** (*Host*) - reprezintă zona prin intermediul căreia un dispozitiv se identifică, în mod unic, într-o reţea.

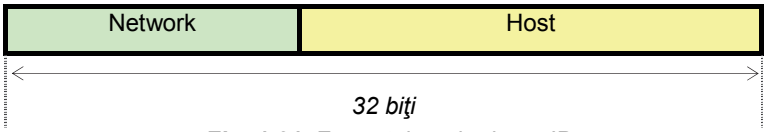


Fig. 1.21. Formatul unei adrese IPv4

Într-o reţea, host-urile pot comunica între ele doar dacă au acelaşi identificator de reţea. Dacă au identificatori de reţea diferiţi, host-urile pot partaja acelaşi segment fizic de reţea, dar nu pot comunica decât dacă există un alt dispozitiv care să realizeze conexiunea între segmentele logice ale reţelei. Forma generală a unei adrese IPv4 este: **xxx.xxx.xxx.xxx**

141.85.147.1 sau 10001101.01010101.10010011.00000001

Cei 4 octeţi sunt utilizaţi pentru a crea aşa numitele **clase de adrese** care pot fi atribuite unor organizaţii, instituţii, companii sau utilizatori casnici. Primii biţi ai adresei codifică poziţia separatorului dintre cele două secţiuni (Network şi Host), delimitând 5 clase de adrese IP dintre care doar primele 3 sunt folosite efectiv pentru comunicaţii unicast (clasele A, B şi C). Ultimele două clase, D şi E, au scopuri speciale.

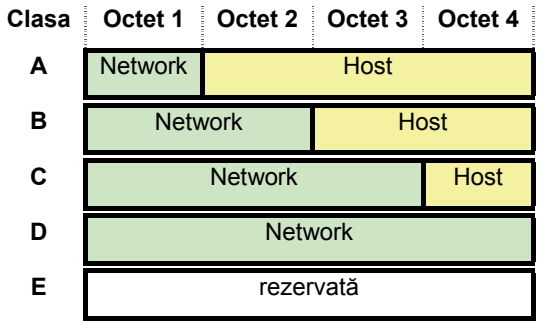


Fig. 1.22. Clase de adrese IP

CLASA A - 0 x x x x x x x . x x x x x x x x . x x x x x x x x . x x x x x x x

- este cea mai extinsă împărţire, realizată de IANA;
- adresa de reţea (Network) este pe 8 biţi, iar primul bit este 0;

- există 128 de reţele (2^7) din care se pot defini doar 126 reţele: 0.x.x.x este rezervată pentru *default route* (ruta implicită), iar 127.x.x.x pentru *loopback*;termen nedefinit
- fiecare reţea suportă maximum 2^{24}-2 host-uri;
- fiind disponibile 2^{31} adrese (2.147.483.648), deoarece primul bit este întotdeauna 0, rezultă că spaţiul adreselor de clasă A ocupă 50% din spaţiul total de adrese.

CLASA B - **10xxxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx**

- se utilizează pentru reţele extinse (ISP sau companii mari);
- adresa de reţea (Network) are 16 biţi, iar primii 2 biţi sunt 10;
- există maximum 16.384 de astfel de reţele (2^{14});
- se pot defini 2^{16}-2 host-uri pentru fiecare reţea;
- fiind disponibile 2^{30} adrese (1.073.741.824), rezultă că spaţiul adreselor de clasă B ocupă 25% din spaţiul total de adrese.

CLASA C - **110xxxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx**

- este cea mai întâlnită clasă, fiind utilizată pentru reţele LAN mici sau medii;
- adresa de reţea (Network) este pe 24 biţi, iar primii 3 biţi sunt 110;
- există maximum 2.097.152 de astfel de reţele (2^{21});
- se pot defini 2^8-2 host-uri pentru fiecare reţea;
- fiind disponibile 2^{29} adrese (536.870.912), rezultă că spaţiul adreselor de clasă C ocupă 12,5% din spaţiul total de adrese.

CLASA D - **1110xxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx**

- adresele din această clasă sunt rezervate pentru IP Multicast (metodă de trimitere a datagramelor către un grup de receptori printr-o singură transmisie, specifică aplicaţiilor multimedia pentru streaming şi televiziune pe Internet);
- are adresa de reţea (Network) de 32 biţi şi primii 4 biţi 1110;
- nu are host-uri;
- sunt maximum 268.435.456 de astfel de reţele (2^{28}).

CLASA E - **1111xxxx.xxxxxxxx.xxxxxxxx.xxxxxxxx**

- este rezervată pentru dezvoltări ulterioare.

Din punct de vedere arhitectural există trei tipuri de noduri în reţeaua Internet:

- de nivel înalt (corespunzătoare adreselor IP din clasa A);
- continentale (pentru adrese din clasa B);
- locale (noduri din clasa C).

Pentru a comunica, o staţie trebuie să cunoască adresa IP şi adresa MAC a staţiei de destinaţie, iar căutarea automată a adresei MAC pe baza adresei IP este făcută de protocolul ARP din cadrul suitei de protocoale TCP/IP. Tabelele ARP conţin adresele IP şi MAC ale tuturor echipamentelor conectate în aceeaşi reţea, precum şi maparea unică a unei adrese IP pe o adresă MAC. În cazul în care adresa MAC a destinaţiei nu este identificată, staţia sursă emite o cerere ARP - *ARP Request*, trimiţând un pachet tuturor staţiilor din reţea printr-o adresă de broadcast.

Avantajele adresării pe clase:

- utilizarea împărţirii pe octeţi;
- uşurinţa rutării prin codificarea clasei în primii biţi ai adresei IP.

Dezavantajele acestei metode de adresare:

- risipă de adrese prin utilizarea ineficientă a spaţiului de adrese alocat;
- creşterea numărului de intrări în tabelele ARP.

ADRESE IPv4 Speciale (rezervate)

Loopback - Adresele de clasă A de forma 127.xxx.xxx.xxx (echivalente cu *localhost* sau 127.0.0.0/8) sunt rezervate şi nu sunt utilizate pentru a adresa o reţea sau un host, ci pentru interfaţa de reţea software a unui calculator numită **interfaţă loopback**. Această interfaţă nu are hardware asociat, nu este fizic conectată la reţea şi este utilizată pentru a efectua teste de reţea fără a crea probleme de trafic.

Adrese locale nerutabile (adrese private) - Fiecare din clasele de adrese A, B şi C au câteva adrese cu o semnificaţie specială. Acestea nu sunt niciodată atribuite unui echipament conectat direct la Internet, ci servesc ca adrese IP pentru Intranet-ul unei organizaţii. Adresele IP rezervate pentru reţelele private sau Intranet-uri mai sunt numite **adrese nerutabile**, pentru că nu pot fi rutate spre Internet.

Tabel 1.1. Adrese IP pentru reţele private

Clasa	Adrese IP private	Număr adrese	CIDR (subnet)
A	10.0.0.0 - 10.255.255.255	16.777.216	10.0.0.0/8 (255.0.0.0)
B	172.16.0.0 - 172.31.255.255	1.048.576	172.16.0.0/12 (255.240.0.0)
C	192.168.0.0 - 192.168.255.255	65.536	192.168.0.0/16 (255.255.0.0)

Spre deosebire de celelalte adrese IP, adresele destinate reţelelor private nu sunt gestionate central, ci pot fi utilizate şi organizate la nivelul fiecărei reţele locale în funcţie de necesităţi.

SOLUŢII LA PROBLEMA EPUIZĂRII ADRESELOR IP. ADRESE IPv6

Adresele IPv6 sunt pe 128 biţi (16 octeţi) şi sunt formate din 8 grupuri a câte 4 cifre scrise în hexazecimal (baza 16 de numeraţie), iar grupurile sunt separate de caracterul ":". **xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx:xxxx**

Dacă există unul sau mai multe grupuri de 4 cifre egale cu 0000, acestea se pot suprima prin "::" (lucru valabil o singură dată în cadrul unei adrese IPv6, pentru a se evita confuziile).

0123:4567:8abc:deff:edcb:a876:5432:1000
aaaa:0000:0000:0000:ffff:3231:dd87:1000 poate fi scris ca:
aaaa::ffff:3231:dd87:1000

Spaţiul IPv6 suportă în jur de $3,4x10^{38}$ adrese posibile, fiind acceptat nativ de sistemele de operare moderne (Windows Vista, Mac OS X sau Linux).

Trecerea spre IPv6 este încă în fază incipientă, dar din ce în ce mai accentuată (la sfârşitul anului 2008 rata de implementare a IPv6 era sub 1% din toate host-urile conectate la Internet, iar la începutul lui 2011, aceasta era de 5%).

Internet Society a stabilit data de 8 iunie 2011 ca "Ziua Mondială IPv6", o zi în care, pentru 24 de ore, furnizori importanţi de aplicaţii pe Internet (Google, Yahoo, Facebook) au asigurat acces direct utilizatorilor la servicii şi conţinut cu conectivitate pe infrastructură IPv6. Scopul acestei acţiuni a fost unul de motivare a organizaţiilor din industria Internet - ISP-uri, producători de hardware, producători de sisteme de operare şi companii care activează în domeniu - să îşi pregătească sistemele pentru o tranziţie reuşită către sistemul de adrese IPv6. Arhitecturile reţelelor de calculatoare se pot împărţi în funcţie de relaţiile funcţionale care există între elementele componente, în:

- Active Networking - arhitectură de reţea în care nodurile se comportă ca elemente active, fiind programate să opereze diverse acţiuni (rutare, comutare şi executare de cod) asupra mesajelor care traversează această reţea.
- Peer-to-Peer - model de configuraţie a unei reţele formată din utilizatori care oferă direct (fără intermedierea vreunui server sau a altei staţii de lucru) o parte din resursele proprii (putere de calcul, spaţiu de stocare, bandă alocată) celorlalţi utilizatori ai reţelei.
- Client-server

ARHITECTURA CLIENT-SERVER

Această arhitectură permite implementarea efectivă a serviciilor Internet. Conceptul se bazează pe existenţa a două tipuri de participanţi în schimbul de informaţii: **Servere** şi **Clienţi**.

SERVERE - Noţiunea de **server** poate fi abordată din punct de vedere:

- **hardware** - reprezintă un calculator specializat (dedicat) care oferă servicii altor calculatoare din reţea (stochează fişiere, partajează imprimante etc.);

- **software** - reprezintă un set de programe ce rulează pe un calculator şi oferă servicii clienţilor (conectare pe baza unui username şi a unei parole la reţeaua locală, publicarea unui site Web, gestiunea poştei electronice, operaţii cu baze de date etc.).

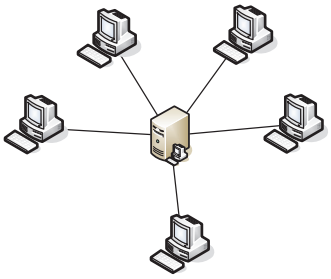


Fig. 1.23. Arhitectura cu server central

Serverele trebuie să fie capabile să răspundă unui număr cât mai mare de solicitări De aceea, trebuie luate în considerare puterea de calcul necesară aplicaţiilor care vor fi instalate, traficul, precum şi numărul de conexiuni la care se estimează că vor fi supuse. Aplicaţia de tip server este pornită, de obicei, la punerea în funcţiune a calculatorului şi, după iniţializare, intră în starea de aşteptare a cererilor venite din partea aplicaţiilor de tip client.

O clasificare a programelor tip server, după funcţia pe care o realizează, este următoarea:

- **Servere WWW**: sunt servere de fişiere care conţin componentele unui site Web. Protocolul utilizat este, de obicei, HTTP (*Hypertext Transfer Protocol*), iar accesul la conţinutul unui site Web se face printr-un program client denumit navigator (*browser*);
- **Servere de fişiere**: stochează fişiere de diverse tipuri şi le furnizează la cererea clientului; protocolul utilizat, de obicei, este FTP (*File Transfer Protocol*), iar accesul se face prin programe client FTP (fie un browser, fie programe dedicate);
- **Servere de poştă electronică**: permit recepţia, stocarea şi trimiterea de mesaje prin serviciul e-mail (poştă electronică). Gestionarea acestor mesaje se face cu programe specializate (clienţi e-mail);
- **Servere de baze de date**: stochează colecţii mari de date structurate sub forma unor baze de date şi furnizează servicii de manipulare şi interogare a acestora, folosind limbajul SQL (*Structured Query Language*);
- **Servere de groupware**: facilitează unui grup de participanţi să lucreze împreună într-un mediu partajat;
- **Servere de imprimare** (*Print Server*): furnizează clienţilor servicii de imprimare la o imprimantă comună, partajată în reţea;

- **Servere de obiecte**: stochează obiecte şi permit programelor client să trimită mesaje acestor obiecte;
- **Servere de aplicaţii**: sunt dedicate uneia sau mai multor aplicaţii particulare şi conţin programele specifice aplicaţiei respective.

CLIENŢI – reprezintă programe executate şi controlate de utilizatori, care solicită unui **Server** diverse informaţii sau servicii şi primeşte răspunsul acestuia. Clientul trimite cereri, iar serverul răspunde la aceste cereri, cele două părţi (client şi server) comunicând pe baza unui limbaj comun (protocol). Câteva exemple de programe client uzuale în utilizarea informaţiilor disponibile pe Internet:

- **Clienţi Web**: browsere care afişează conţinutul paginilor din Internet - Internet Explorer, Mozilla Firefox, Google Chrome, Opera, Apple Safari, Netscape Navigator;
- **Clienţi e-mail**: programe folosite de utilizatori pentru a gestiona mesaje de poştă electronică - Microsoft Outlook, Mozilla Thunderbird, IncrediMail, Eudora, Pegasus Mail, Windows Live Mail;
- **Clienţi FTP**: programe utilizate pentru transferul binar al fişierelor pe şi de pe servere FTP, pe calculatorul utilizatorului - FileZilla, WinSCP, CuteFTP, FireFTP.

Programele tip client sunt, de obicei, executate pe sisteme uzuale, însă şi aici trebuie avute în vedere destinaţiile unui sistem de calcul pentru a-l "dimensiona" conform utilizării (programe de birou, programe de grafică, jocuri, calcule matematice). Programele de tip client şi server pot coexista şi rula simultan chiar şi pe acelaşi calculator, însă, de obicei, se află pe maşini separate. Avantajele oferite de sistemele client-server au condus în multe domenii din mediul business la o migrare de la staţii mainframe sau PC către acest tip de arhitectură.

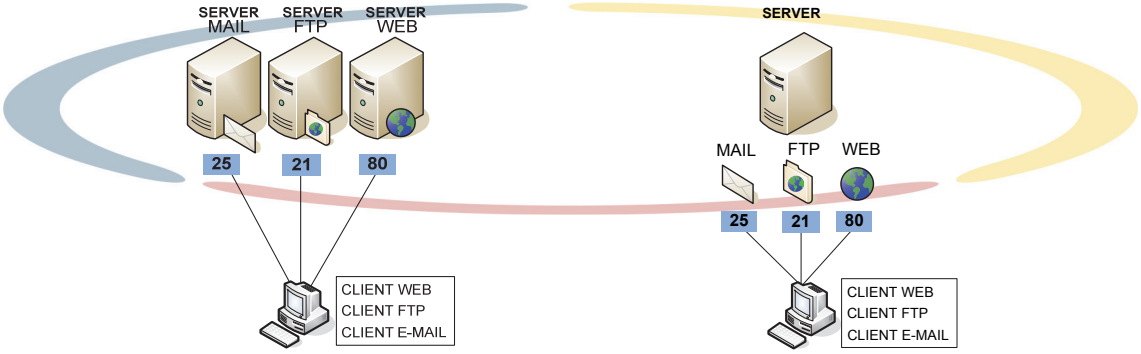
Printre **avantajele** sistemelor client-server putem enumera:

- **securitatea superioară** - este dată de restricţiile care pot fi impuse utilizatorilor prin drepturi de acces - aceştia nu pot accesa fişiere decât în conformitate cu drepturile (de acces, citire, scriere) pe care le au asociate;
- **performanţe ridicate** - o proiectare optimă hardware şi software a serverului poate determina o bună gestionare a calităţii serviciilor oferite utilizatorilor care accesează simultan diverse resurse;
- **raportul ridicat calitate/preţ** - puterea de calcul necesară sistemului client este una obişnuită la un preţ accesibil; pentru performanţe ridicate ale sistemului de tip server este necesară achiziţionarea unui echipament cu o capacitate mare de procesare, deci un preţ crescut.

Dezavantajele sistemelor client-server constau în:

- **complexitate ridicată** - în cazul aplicaţiilor complexe, configurarea şi administrarea sistemelor client-server nu sunt uşor de realizat, datorită ariei de răspândire;
- **volum relativ mare de resurse hardware** - pentru a suporta un număr cât mai mare de utilizatori, serverele din sistemele de tip client-server au nevoie de resurse hardware complexe (două sau mai multe procesoare, mai multă memorie RAM, mai mult spaţiu pe disc).
- **preţ** - necesitatea de a dedica sistemele (serverele) numai unui anumit tip de activitate conduce la costuri ridicate. Deoarece performanţele unui server scad pe măsură ce numărul de utilizatori simultani creşte, prin existenţa unor sisteme dedicate se menţin în limite acceptabile aceste performanţe, însă serverele dedicate conduc la un preţ ridicat pe ansamblu sistemului.

Privit ca echipament (hardware), un server poate găzdui una (figura 1.24.a) sau mai multe (figura 1.24.b) aplicaţii de tip server (software). Astfel, pot coexista pe acelaşi echipament un server Web, unul pentru FTP şi unul pentru poşta electronică. Folosind clienţi specifici fiecărui tip de serviciu, utilizatorul se conectează la acelaşi host (acelaşi IP), accesarea resursei dorite (o pagină Web, un fişier, un mesaj e-mail) realizându-se de către programul client.



(a) (b)

Fig. 1.24.

a. mai multe servicii pe mai multe echipamente; b. mai multe servicii pe acelaşi echipament

Programul client comunică echipamentului de tip server (hardware) la care resursă se conectează (ce serviciu doreşte să acceseze). Selectarea unui serviciu din setul de aplicaţii de tip server care rulează pe un sistem de calcul este realizată prin porturi (*Ports*). Fiecare aplicaţie de tip server (software) ”ascultă” pe un anumit port dedicat (prestabilit) solicitările, iar clientul va trebui să transmită/recepţioneze pachetele de date pe acel port.

2.1.6. Porturi. Socket-uri

Portul reprezintă un număr întreg fără semn (unsigned integer) pe 16 biţi, cu valori posibile de la 0 la 65.535 (2^{16}-1), prin care se identifică în mod unic procesele care rulează pe un sistem de calcul. Orice aplicaţie care rulează şi realizează o conexiune în cadrul unei reţele trebuie să ataşeze un număr de port acelei conexiuni. În cazul în care nu se face o specificare implicită/explicită a unui port, transferul de date către client nu va avea loc.În lipsa portului specificat (în acest exemplu portul 8000), browserul se va conecta pe portul implicit pentru protocolul HTTP (portul 80). Conform IANA, porturile sunt separate în 3 categorii:

- porturi folosite implicit de diverse servicii (*Well-Known Ports*), de care IANA se ocupă efectiv: intervalul 0 - 1023;
- porturi ce pot fi folosite de diverse procese executate de utilizatori obişnuiţi (*Registered Ports*): intervalul 1024 - 49151;
- porturi dinamice şi/sau private (*Dynamic or Private Ports*): intervalul 49152 - 65535.

Câteva dintre porturile implicit utilizate pentru diverse servicii uzuale sunt prezentate în tabelul 1.2.

Tabel 1.2. Porturi utilizate de principalele protocoale sau servicii

Protocol (serviciu)	Rol	Port
FINGER	Obținere informații despre utilizatori	79
FTP	Protocol acces server fișiere	21
HTTP	Protocol acces server Web	80
HTTPS	Acces server Web prin conexiune securizată	443
IMAP	Organizare, sincronizare e-mail	143
IRC	Internet Relay Chat	194
MMS	Streaming Microsoft Media Server	1755
NAMESERVER	Legătura IP - nume server	53
NNTP	Protocol pentru servere de ştiri (*newsgroups*)	119
NTP	Sincronizare ceas calculator	123
POP3	Descărcare e-mail	110
RTMP	Fluxuri multimedia prin tehnologia Flash	1935
RTSP	Protocol pentru fluxuri media	554
SMTP	Rutare e-mail între servere	25
SSH	Conexiune la distanță (securizată)	22
TELNET	Conexiune la distanță (nesecurizată)	23
VNC	Conexiune la distanță (interfață grafică VNC)	5900

O adresă de tip **SOCKET** reprezintă o combinaţie între o adresă IP (identitatea sistemului de calcul) şi un port (conectat la procesul din programul de aplicaţie), într-o identitate unică.

Socket-urile sunt fundamentale pentru programarea în reţele de comunicaţii care utilizează suita de protocoale TCP/IP. Un socket oferă un canal de comunicaţii bidirecţional cu un alt socket pentru trimiterea/primirea datelor, conexiunile de acest tip fiind realizate între două calculatoare din cadrul unui LAN sau prin Internet, dar pot fi utilizate şi pentru comunicarea între procese pe un singur computer.

Termenul *Internet socket* este utilizat pentru o interfaţă de programare a aplicaţiei (API - *Application Programming Interface*) din cadrul TCP/IP furnizată, de obicei, de sistemul de operare.

Cele mai utilizate librării de socket-uri sunt Berkeley Socket (pentru Linux/Unix) şi Winsock (pentru sistemele Windows).

2.1.7. Nume de domenii. Sistemul DNS

Accesul la o resursă (serviciu sau fişier) necesită cunoaşterea adresei IP (un şir de cifre) la care este disponibilă. Pentru utilizatorii obişnuiţi este mai uşor de reţinut un şir de caractere (un nume, o denumire) apropiat de limbajul natural, decât un şir de cifre (adresa IP). Translaţia dintr-un şir de cifre într-un şir de caractere este realizată de **sistemul numelor de domeniu** (DNS - *Domain Name System*).

Sistemul numelor de domeniu, conceput de Paul Mockapetris în 1984, este un sistem distribuit de stocare şi interogare a unor date ierarhizate (pentru Internet aceste date sunt reprezentate de numele de domenii şi adresele IP).

La nivelul TCP/IP există o rutină software denumită *name resolver* care interoghează serverul DNS pentru a obţine corespondenţa (translatarea) între numele de domeniu şi adresa IP. Deoarece pachetele se transmit prin Internet folosind adrese IP, scopul sistemului DNS este de a obţine adresa IP corespunzătoare numelui de domeniu al unui host pe care un utilizator doreşte să-l acceseze.

Principalul avantaj al acestui serviciu îl reprezintă adresa URL a unei resurse, care se păstrează constantă atunci când se schimbă rutele către un anumit domeniu (când se modifică serverul de găzduire, de exemplu). Nu contează unde este stocată fizic o resursă (fişier sau serviciu), deoarece numele de domeniu va fi transferat automat de sistemul DNS către adresa IP a serverului gazdă.

Tabel 1.3. Nume de domenii şi adresele IP corespondente

Nume domeniu	Adresa IP
www.gov.ro	85.120.75.150
sgg.gov.ro	193.151.29.6
www.posturi.gov.ro	193.151.29.22
www.mai.gov.ro	81.181.207.71

Sistemul DNS are o organizare ierarhizată în care fiecare nod sau frunză a acestei structuri de tip arbore conţine informaţii despre resursele asociate pentru un nume de domeniu. Baza de date este distribuită în toată reţeaua Internet, adică nu există un calculator de tip nod central care să stocheze toată informaţia necesară translaţiei între adresele IP şi numele de domenii. Fiecare domeniu sau subdomeniu menţine informaţia asociată host-urilor sale, având definit propriul server DNS.

Spaţiul numelor de domenii este împărţit pe **zone**, începând cu **zona de root** (rădăcină). Responsabilităţile pe anumite zone se pot diviza, realizându-se astfel zone adiţionale.

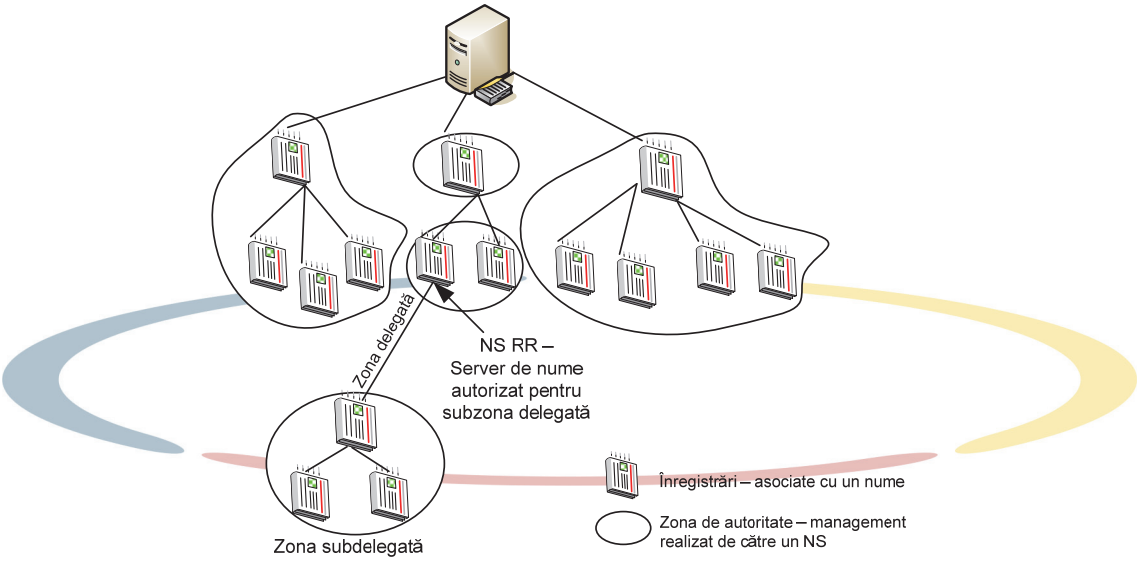


Fig. 1.25. Organizarea domeniilor şi a subdomeniilor

MODUL DE LUCRU AL SISTEMULUI DNS

Presupunem că dorim să accesăm adresa www.google.com. Se tastează adresa în caseta de adrese a browserului Web, iar acesta contactează serverul DNS local pentru a afla adresa IP a domeniului www.google.com.

Dacă serverul a mai primit de curând o cerere pentru acelaşi domeniu, adresa IP este stocată în memoria serverului DNS local, fiind transmisă imediat calculatorului care a solicitat adresa respectivă.

Dacă adresa IP nu se află în memoria serverului DNS, acesta trimite o cerere la unul din **serverele de bază** (*root nameservers*) care răspund de domeniile din nivelul superior (în cazul nostru, ".com").

După ce obţine adresa serverului DNS primar care deţine informaţii despre domeniul .com, serverul DNS local trimite o cerere acestuia. Serverul DNS primar va furniza adresa serverului DNS responsabil de domeniul google.com. Ultima etapă o reprezintă transmiterea unei cereri de la serverul DNS local la ultimul server DNS identificat, în urma căreia se va obţine adresa IP a serverului www.google.com, precum şi o valoare TTL (*Time to Live*), adică timpul cât un server DNS local poate reţine în memoria sa cache adresa IP a numelui de domeniu www.google.com (TTL are valori uzuale între o zi şi o săptămână). Odată aflată adresa IP a serverului solicitat, browserul va contacta acel host şi va transfera pagina returnată de serverul Web.

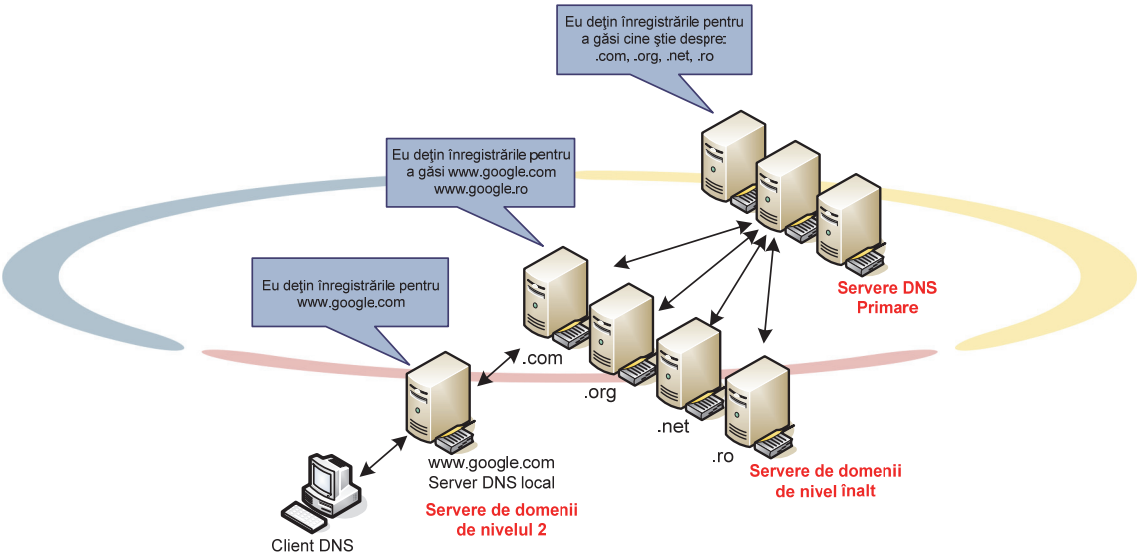


Fig. 1.26. DNS - Mod de lucru

STRUCTURA NUMELOR DE DOMENII

Formatul general al numelor de domenii conţine două sau mai multe etichete (*labels*) separate prin punct (".").Forma generală este:

hostname.secondlevel.firstlevel

- **firstlevel** - primul nivel (eticheta din dreapta), denumit nivelul superior sau TLD (*Top-Level Domain*), este mai puţin specific şi indică tipul organizaţiei sau ţara căreia îi aparţine domeniul/host-ul respectiv. Există sute de nume de

domenii în acest nivel, printre care .com, .edu, .mil, .gov, .org şi combinaţii de două litere pentru fiecare ţară.

- **secondlevel** - fiecare din etichetele spre stânga specifică un subdomeniu (o subdiviziune) a domeniului corespunzător din dreapta. În fiecare TLD există foarte multe domenii la nivelul doi (subdomenii) care identifică organizaţia, cum ar fi Google, Yahoo sau MSN (Microsoft).
- **hostname** - face referire la un nume de domeniu care are asociată una sau mai multe adrese IP.

Trebuie să se facă deosebirea între un domeniu (de exemplu: "gov.ro", domeniul alocat Guvernului României) şi un host (de exemplu: "posturi"). Domeniul reprezintă un grup de subdomenii sau un grup de host-uri, iar host-ul este cel mai de jos nivel al ierarhiei.

Structura ierarhică formată din domenii şi subdomenii este definită în funcţie de diferite unităţi de organizare sau de diverse domenii de activitate. Numele în primul nivel sunt unice, însă la nivelul doi (secondlevel) pot exista duplicate, în TLD-uri diferite (de exemplu, linux.com şi linux.org). Orice organizaţie poate înregistra un nume de domeniu la nivelul doi, cu condiţia ca numele respectiv să nu existe deja. Subdomeniul este, în general, numele sau prescurtarea numelui organizaţiei (de exemplu, gov.ro sau guv.ro pentru Guvernului României). Pot exista mai multe niveluri de subdomenii (teoretic, până la 127), dar rar sunt utilizate mai mult de patru.

Deoarece numele de domenii trebuie să fie unice, există o singură organizaţie la nivel de ţară, care controlează această listă pentru a se asigura unicitatea numelui unui domeniu. Aceste organizaţii menţin şi actualizează o bază de date la nivel naţional care conţine informaţii de identificare despre proprietarul unui domeniu şi serverele DNS asociate pentru fiecare domeniu. Sarcina de a gestiona nivelurile TLD (zona de root DNS) îi revine organizaţiei ICANN, prin autoritatea IANA. În România, organizaţia care gestionează numele de domenii este RNC.

Existenţa unei organizaţii centrale pentru administrarea numelor de domenii din primul nivel este importantă, însă aceasta nu poate menţine informaţia legată de fiecare subdomeniu, unde pot fi definite zeci sau sute de host-uri. Astfel, subdomeniile menţin informaţiile legate de host-urile lor şi au responsabilitatea asigurării numelor unice în domeniul respectiv.

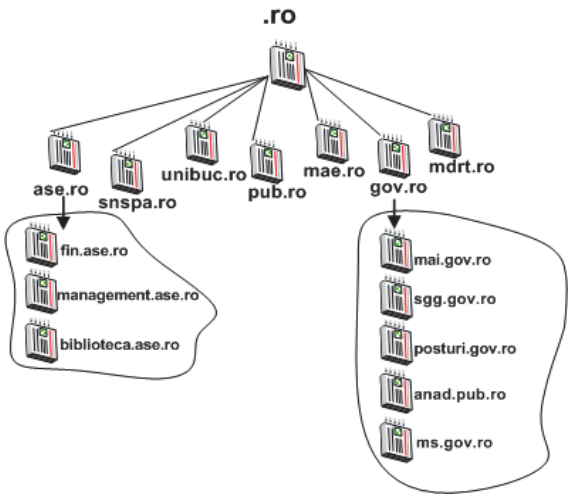


Fig. 1.27. Exemple de domenii şi subdomenii în .ro

În acest moment TLD este împărţit în 2 categorii:

- **ccTLD (*Country-Code Top-Level Domain*)** - secvenţă formată din două litere care descriu o ţară sau teritoriu, conform cu standardul ISO 3166.
- **gTLD (*Generic Top-Level Domain*)** - secvenţă formată din 3 sau mai multe litere prin care se identifică specificul (profilul) site-ului sau domeniul de activitate.

Lipsa restricţiilor la înregistrarea numelor de domenii a dus la apariţia unor domenii (aşa-numitele "*domain hacks*") care folosesc ccTLD pentru a forma nume, expresii, titluri sau mărci, în scopuri de marketing. Câteva exemple:

- expresii cu o anumită semnificaţie în limba engleză: I.am (Armenia), tip.it (Italy), start.at (Austria), go.to (Tonga), its.me (Montenegro);
- cuvinte sau diverse mărci: blo.gs (South Georgia and the South Sandwich Islands), del.icio.us (United States), cr.yp.to (Tonga), fa.st (Sao Tome and Principe), e.xplo.it (Italy), itun.es (Spain), goo.gl (Greenland);
- arii de interes, grupuri sau organizaţii: .cd (Democratic Republic of the Congo) - prescurtare pentru Compact Disc-uri, .dj (Djibouti) - comunitatea Disc Jockeys, .fm (Federated States of Micronesia) - posturi de radio FM, .im (Isle of Man) - mesagerie instant, .ms (Montserrat) - proiecte Microsoft, .tm (Turkmenistan) - Trade Mark, .tv (Tuvalu) - industria televiziunii.

În **Anexa 1** sunt sintetizate codurile de ţară (ccTLD) pentru zona europeană şi domeniile gTLD generale, de infrastructură a reţelei Internet, rezervate şi sponsorizate. Fiecare resursă disponibilă pe Internet (fie că este un serviciu sau

orice tip de fişier) are o adresă care descrie în mod unic localizarea acesteia pe "harta" Internet-ului.

2.1.8. Uniform Resource Locator (URL)

URL (*Uniform Resource Locator*) reprezintă punctul cheie al localizării şi interpretării informaţiilor din Internet, fiind o modalitate de descriere atât a locaţiei unei resurse Web, cât şi a conţinutului acesteia (implicit a mecanismului de obţinere şi utilizare a acelei resurse). URL reprezintă un şir de caractere cu următoarea formă generală:

tip_resursă://domeniu:port/cale/fişier?query#ancoră

Semnificaţiile elementelor componente din cadrul sintaxei asociate mecanismului de localizare URL sunt:

- **tip_resursă**: specifică schema utilizată pentru accesarea resursei. În funcţie de schemă, sintaxa ce urmează are diverse forme. Schemele uzuale conţin, de obicei, numele protocolului folosit pentru accesarea resursei:
  - ***http*** (pentru accesarea unei pagini Web)
    http://*<host>*
  - ***https*** (pentru accesarea unei pagini Web aflată pe un server securizat)
    https://*<host>*
  - ***ftp*** (pentru accesarea unui server FTP)
    ftp://*<host>*
    ftp://*<username>*:*<password>*@*<host>*
  - ***mailto*** (specificarea unei adrese e-mail)
    mailto:*<address>[?<header1>=<value1>[&<header2>=<value2>]]*
  - ***file*** (accesarea unui fişier din reţeaua locală)
    file:*//<path>/<file>*
  - ***rtsp*** (*Real Time Streaming Protocol*) sau **rtmp** (*Real Time Messaging Protocol*) pentru fluxuri media în diverse formate (mpeg, avi, mov, Flash)
    rtsp:*//<path>*
    rtmp:*//<path>*
  - ***news*** (ştiri Usenet)
    news:*<newsgroupname>*
    news:*<message-id>*
  - ***gopher*** (protocol Gopher)
    gopher:*//<host>:<port>/<item type>/<path>*
  - ***telnet*** (utilizare cu protocolul Telnet)
    telnet:*//<user>:<password>@<host>[:<port>/]*

În exemplele de mai sus s-au folosit notaţiile: *<nume>* - pentru valoarea unei entităţi (text sau numeric) din adresa URL şi *[nume]* - pentru o expresie opţională (care poate să lipsească). Alte scheme uzuale de accesare, dar neoficiale, sunt:

- ***about*** (funcţii interne ale browserului);
- ***feed*** (abonare la un flux Web);
- ***javascript*** (executare cod Javascript);
- ***magnet*** (clienţi cu conexiune directă, Peer-to-Peer);
- ***mms*** (streaming media prin Microsoft Media Server);
- ***aim***/***msnim***/***ymsgr*** (conversaţii prin AOL Instant Messenger/Windows Live Messenger/Yahoo Messenger);
- ***skype***, ***callto*** (conversaţii prin Skype);
- ***ssh*** (conexiuni securizate prin protocolul SSH).

```
http://www.google.com sau http://74.125.87.99/
https://www.cia.gov
ftp://ftp.lug.ro
ftp://utilizator:parola@example.com
mailto:user@domeniu?subject=Subiect&body=Continut%20mesaj
file://../imagini/img1.gif
```

- **domeniu**: numele domeniului, numele calculatorului gazdă sau adresa IP unde se află resursa căutată. În general, domeniul nu este *case sensitive* (poate fi scris cu litere mari sau mici).

```
http://www.yahoo.com sau http://WWW.YAHOO.COM duc la aceeaşi adresă
```

- **port**: atunci când un serviciu nu utilizează portul implicit alocat, fiind necesară specificarea portului pentru a accesa resursa solicitată.

```
http://www.example.com:8080
```

- **cale**: structura de directoare (foldere) în care se află fişierul căutat, separate prin semnul "/" (slash). De obicei calea este *case sensitive*; serverele Microsoft Windows nu fac diferenţa între litere mari sau mici.

```
http://www.example.com/html/language/
```

- **fişier**: numele fişierului şi extensia sa (sunt *case sensitive* pe sisteme de operare Linux).

```
http://www.example.com/images/gif/IMG1.gif
```

- **query**: în unele cazuri se pot specifica anumite variabile cu valorile atribuite (de exemplu în preluarea datelor din formularele Web sau în scripturile .cgi, .asp sau .php).

```
http://www.example.com/example.php?field1=value1&field2=value2
```

- **ancoră**: pentru fişiere tip .html permite saltul direct la o ancoră (*bookmark*) definită cu marcajul <a>.

```
http://www.example.com/example.html#cap1
```

2.2. Servicii Internet

2.2.1. Serviciul World Wide Web

Evoluţia tehnologiilor de transmisie şi resursele variate pe care le pune la dispoziţie reţeaua Internet au condus la dezvoltarea unor servicii complexe, disponibile atât pentru organizaţii, cât şi utilizatorilor obişnuiţi. Până la începutul anilor '90 Internet-ul era dedicat aplicaţiilor şi cercetărilor ştiinţifice din diverse domenii de activitate (industrial, guvernamental, academic), dar odată cu dezvoltarea unui nou serviciu, WWW (*World Wide Web*), reţeaua a început să fie accesată de zeci de mii, sute de mii, apoi milioane de noi utilizatori.

WWW a fost dezvoltat de fizicianul şi informaticianul englez Timothy Berners-Lee în 1989 la CERN (Centrul European de Cercetare a Energiei Nucleare, Geneva, Elveţia). Numărul de servere Web a ajuns, la nivel mondial, la 500, în 1993, traficul Web ocupând circa 1% din traficul total pe Internet, iar un an mai târziu erau peste 10.000 de servere şi în jur de 10 milioane de utilizatori. În ianuarie 1995 se înfiinţează W3C (*World Wide Web Consortium*), principala organizaţie care reglementează standardele în domeniul Web (HTML, CSS, XML, CGI şi altele).

WWW reprezintă o colecţie de fişiere (text, multimedia sau alte tipuri) şi servicii, interconectate prin legături (*hyperlinks*) într-un uriaş sistem hypertext. Documentele hypertext disponibile pe Internet sunt create într-un limbaj special de marcare (HTML - *HyperText Markup Language*) care permite realizarea unui document structurat, în vederea prezentării lui pe ecran folosind un program specializat (cel mai adesea un browser Web).

HTML este un format text care poate fi vizualizat şi modificat atât cu un editor text simplu, cât şi cu programe complexe de tip WYSIWYG (*What You See Is What You Get*), adică editare vizuală, în mod grafic (Microsoft Frontpage, Macromedia Dreamweaver, Microsoft Word). Limbajul HTML se bazează pe utilizarea marcajelor (*tags*) încorporate în cadrul textului, astfel încât browserul să afişeze textul într-un anumit mod. Aceste marcaje oferă posibilitatea de a introduce stiluri şi culori pentru text, inserarea unor imagini, tabele, secvenţe audio-video, legături spre alte tipuri de documente.

Participanţii la mediul WWW se împart în două categorii:

- utilizatori - accesează informaţiile disponibile la o adresă folosind un program client (browser) care solicită diverse resurse de la aplicaţii tip server;
- pagini de Internet (site-uri Web) - colecţii de fişiere găzduite pe servere Web şi organizate pentru a oferi pagini cu text, imagini, sunet, video şi legături spre alte fişiere din cadrul aceluiaşi site sau către un alt site din spaţiul WWW.

Browserele Web utilizează protocoalele HTTP, HTTPS şi FTP pentru a reprezenta conţinutul paginilor Web pe ecranele utilizatorilor (interpretează atât marcajele

limbajului HTML, cât şi alte tipuri de informaţii - fişiere text, imagini, animaţii, sunete). Browserele mai conţin programe suplimentare (*plugins*) capabile să ruleze anumite secvenţe de cod inserate în conţinutul paginilor Web (scripturi Javascript, applet-uri Java) sau să interpreteze diverse tipuri de documente (PDF, Flash, Java sau alte tehnologii).

Un hyperlink poate indica spre orice tip de fişier; în cazul în care nu poate deschide acel tip de fişier, browserul va oferi utilizatorului posibilitatea să îl descarce (*download*) sau să-l deschidă cu un alt program instalat local în sistemul de operare.

Tabel 2.1. Cele mai utilizate cinci browsere Web (februarie 2014, conform Neowin.net)

Browser	Procent
Microsoft Internet Explorer	58,5%
Mozilla Firefox	17,68%
Google Chrome	16,84%
Apple Safari	5,67%
Opera	1,23%

La ora actuală, pe piaţa browserelor supremaţia este disputată între Microsoft Internet Explorer (care deţinea până nu demult o cotă impresionantă) şi Mozilla Firefox, dar o creştere semnificativă a numărului de utilizatori înregistrează Google Chrome şi Safari de la Apple.

Protocolul HTTP

HTTP (*Hypertext Transfer Protocol*) este un protocol de tip text care rulează la nivelul Aplicaţie din modelul de referinţă TCP/IP, fiind utilizat pentru accesarea informaţiilor disponibile în spaţiul WWW. Prima versiune a protocolului (HTTP/0.9) a fost realizată în 1990 de Tim Berners-Lee şi a fost îmbunătăţită prin versiunea HTTP/1.0 (1996). În prezent, versiunea utilizată este HTTP/1.1.

Protocolul HTTP ilustrează foarte bine noţiunile de cerere (*request*) şi răspuns (*response*) caracteristice arhitecturii client-server: clientul (browserul) solicită, iar serverul Web răspunde. HTTP presupune ca pe calculatorul destinaţie să ruleze un program care înţelege acest protocol. Fişierul transmis la destinaţie poate fi un document de tip HTML, un fişier tip imagine, sunet, animaţie, video, un fişier text sau orice tip de fişier binar (programe executabile, arhive, baze de date şi altele).

Accesarea unei resurse (fişierul *example1.html*) situate pe un server Web la adresa *www.example.com*, folosind protocolul *HTTP* se va face cu sintaxa:

http://www.example.com/example1.html

Etapele în accesarea acestei resurse (o pagină Web) sunt:

- în programul client, utilizatorul introduce în bara de adrese resursa pe care doreşte s-o acceseze, specificând URL-ul acesteia;

- numele domeniului este convertit de sistemul DNS într-o adresă IP;
- browserul stabileşte împreună cu host-ul de la adresa IP aflată în pasul anterior, o conexiune TCP pe portul 80 (portul implicit), unde serverul Web instalat pe acel host "ascultă" solicitările unor eventuali clienţi;
- după realizarea conexiunii, browserul solicită resursa (fişierul *example1.html* din exemplul de mai sus), iar serverul Web furnizează resursa solicitată sau răspunde cu diverse mesaje (de eroare dacă informaţia cerută nu este disponibilă sau cu alte informaţii).

Protocolul HTTPS

HTTPS (*Hypertext Transfer Protocol Secure*) este o combinaţie între protocolul HTTP (text clar, nesecurizat) şi un protocol criptografic care permite transferul securizat prin intermediul WWW (realizează un canal sigur într-o reţea nesigură).

HTTPS a fost dezvoltat de Netscape Communications în anul 1994 din nevoia de a proteja datele confidenţiale de eventuale interceptări şi/sau modificări, fiind utilizat în tranzacţii financiare pe Web sau în schimbul de informaţii private.

Protocolul HTTP lucrează la nivelul Aplicaţie, în timp ce datele se criptează/decriptează la un nivel inferior, folosindu-se protocoalele SSL (*Secure Sockets Layer*) şi TLS (*Transport Layer Security*). Portul implicit utilizat de protocolul HTTPS este 443. Schema utilizată în specificarea URL-ului este *https*, ca în exemplul de mai jos:

https://www.example.com

Un avantaj prezentat de protocolul SSL este că permite protejarea fluxului de informaţii chiar dacă doar una din părţi (de obicei serverul) se autentifică. Astfel, protocolul HTTPS devine şi o metodă de autentificare a serverului Web printr-un certificat digital care este examinat şi acceptat de către client. Browserul solicită acest certificat digital, serverul se autentifică, după care poate fi realizat transferul criptat al datelor.

Certificatul digital este o colecţie de date obţinută de la o autoritate recunoscută (CA - *Certificate Authority*), prin care serverul îşi certifică identitatea.

Browserele includ o listă a principalelor autorităţi de certificare (de exemplu Verisign) şi pot verifica certificatele emise de acestea. Certificatul digital conţine informaţii despre domeniul respectiv, datele de identificare ale deţinătorului domeniului, informaţii suplimentare despre perioada de validitate a certificatului sau numele autorităţii emitente.

Pentru domeniile care nu au un certificat digital valid se afişează un mesaj de avertizare (într-o fereastră separată, pentru browserele mai vechi, sau chiar în pagina respectivă - pentru browserele noi), iar domeniile cu certificate valide sunt evidenţiate în bara de adrese (pentru versiunile noi ale celor mai multe browsere).

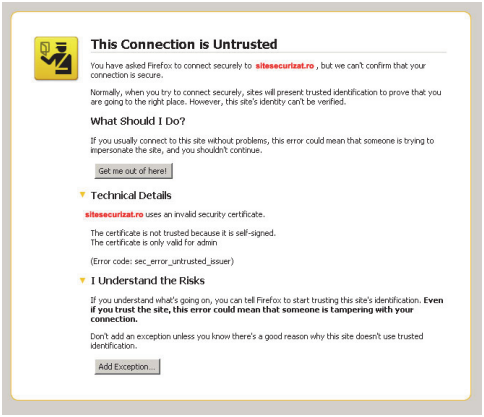


Fig. 2.1. Mecanismul de validare a certificatului digital în browserul Firefox

2.2.2. Serviciul transfer de fişiere

Transferul de fişiere este termenul utilizat pentru operaţiunile de descărcare, respectiv, trimitere de fişiere, indiferent de conţinut, printr-o reţea de calculatoare şi/sau prin reţeaua Internet. Metodele uzuale de transfer al fişierelor prin Internet sunt:

- poşta electronică - are de obicei limitări în ceea ce priveşte mărimea fişierelor ataşate. Este o metodă indicată pentru fişiere mici sau de dimensiuni rezonabile, în funcţie de furnizorul serviciului şi cota alocată fiecărui utilizator - de exemplu, Yahoo şi GMail permit fişiere ataşate de maxim 25 MB.
- serverele FTP - permit upload-ul şi stocarea fişierelor de dimensiuni mai mari. Dezavantajul constă într-un mecanism cu mai mulţi paşi de implementat: crearea unui cont cu parolă pe un server FTP, upload-ul fişierelor cu un client FTP sau prin interfaţa Web - dacă este pusă la dispoziţie această facilitate, informarea persoanei interesate de acele fişiere.
- programele de mesagerie instant, care necesită prezenţa online simultană a celor două părţi. Deşi este o metodă uşor de implementat pentru transferuri uzuale, nu este recomandată pentru fişiere de mari dimensiuni.

Transferul datelor se poate face atât **spre utilizator** (*download*) - receptorul datelor, cât şi **dinspre utilizator** (*upload*) - în acest caz utilizatorul este furnizorul datelor.

Transferul fişierelor se realizează la mai multe niveluri:

- în reţele locale de calculatoare prin mecanismul partajării (*sharing*) unor foldere sau directoare. Operaţiunile de transfer sunt transparente pentru utilizator; acesta poate accesa resursa partajată indiferent de sistemul de

operare, sistemul de fişiere, arhitectura hardware sau software a calculatoarelor sau dispozitivelor pe care este stocată resursa;

- între sistemul de calcul şi un dispozitiv periferic ataşat la acesta (unităţi externe de stocare a datelor, dispozitive multimedia, camere foto/video etc.);
- transferuri explicite folosind servicii dedicate precum HTTP sau FTP;
- prin reţele Peer-to-Peer (*Bittorrent*)
- utilizând programele de mesagerie instant în reţele locale sau prin Internet;
- prin porturile seriale ale calculatorului, utilizând fie o legătură directă cu alt calculator, fie un modem conectat la linia telefonică.

Protocolul din suita TCP/IP utilizat pe scară largă pentru transferul de fişiere (text sau binare) între calculatoare interconectate (la intranet sau Internet), în diverse arhitecturi hardware şi sisteme de operare este protocolul FTP (*File Transfer Protocol* - protocolul de transfer fişiere).

Pentru a utiliza protocolul FTP este nevoie de un **server FTP** (din punct de vedere hardware este un calculator care rulează programe speciale denumite generic "*Server FTP*", gestionează cererile şi stochează fişierele dorite) şi un **client FTP** (aplicaţie executată pe calculatorul utilizatorului pentru a accesa resursele puse la dispoziţie de serverul FTP). Conexiunea între un client şi un server FTP se realizează pe două porturi:

- unul pentru control/comenzi (valoarea implicită a portului este 21);
- unul pentru date (o valoare uzuală pentru acest port este 20).

TRANSFER FIŞIERE DE MARI DIMENSIUNI

Creşterea spaţiului ocupat de date sau aplicaţii (DVD-uri, jocuri, filme, programe) a dus la apariţia unor servicii dedicate stocării şi transferului fişierelor de dimensiuni medii şi mari. Astfel, au fost dezvoltate site-uri specializate care stochează pe o perioadă limitată fişiere de dimensiuni mari (uzual de ordinul 1-2 GB) pentru a fi descărcate ulterior doar de către destinatarul lor (legăturile sunt cunoscute doar de expeditor şi de persoana căreia i se adresează, care primeşte automat un mesaj e-mail cu hyperlink-ul respectiv). Exemple: wetransfer.com. transfer.ro, FileServe, Hotfile, RapidShare, Microsoft Skydrive. Printre avantaje site-urilor care oferă servicii de File Hosting pot fi enumerate:

- nu necesită crearea unui cont sau instalarea unor programe suplimentare;
- transfer sigur, rapid şi discret;
- adresele fişierelor stocate nu sunt publice, putând fi descărcate doar de cei cărora le sunt adresate.

BACK-UP ONLINE

Din această categorie fac parte site-urile care funcţionează ca "hard-disk-uri" online pentru backup sau stocări de date de mari dimensiuni, prin utilizarea unui program client care realizează sincronizarea dintre folder-ul local şi cel online. În funcţie de compania deţinătoare şi modul de abonare (gratuit sau plătit), spaţiile puse la dispoziţie ajung până la 50 GB pentru fiecare utilizator. Exemple: Dropbox, Adrive.

2.2.3. Serviciul poştă electronică

E-MAIL (*Electronic Mail*) este unul din primele servicii implementate în mediul Internet, bucurându-se de o largă răspândire şi o popularitate ridicată. Poşta electronică permite schimbul de mesaje sau date (fişiere) între un expeditor şi unul sau mai mulţi destinatari, serviciul fiind utilizat pentru:

- corespondenţă obişnuită (mesaje text);
- transferul unor fişiere de dimensiuni reduse (prin ataşare la mesaj);
- obţinerea unor informaţii prin interogarea unor adrese e-mail speciale la care se pot solicita un document sau o informaţie (căutarea unui cuvânt într-un dicţionar, consultarea prognozei meteo etc.);
- abonarea la liste de adrese - prin înscrierea într-o listă de adrese se primesc periodic mesaje de la ceilalţi membri ai listei, persoane cu pasiuni, probleme sau obiective comune.

Mecanismul de lucru al serviciului e-mail

În figura 2.2 este prezentată calea parcursă de un mesaj prin intermediul serviciului de poştă electronică. Se identifică următorii paşi:

A. Expeditorul creează mesajul e-mail într-un MUA (*Mail User Agent*). MUA este reprezentat de clientul e-mail sau o interfaţă Web, utilizate de expeditor pentru crearea şi citirea mesajelor e-mail.
B. Mesajul este trimis către MTA (*Mail Transport Agent*, denumit şi *smtpd* - *SMTP daemon*). MTA este responsabil doar de trimiterea unui mesaj de la un computer la altul. Acesta poate primi mesaje de la un alt MTA (*relay*) sau de la un MUA. Exemple de aplicaţii MTA sunt: *sendmail*, *postfix*, *exim*, *qmail* (pe sisteme Linux) sau *Microsoft Exchange Server* (pentru sisteme Windows).
C. În funcţie de destinaţia mesajului (în aceeaşi reţea sau în altă reţea), mesajul e-mail trece numai prin reţeaua companiei ("REŢEA") sau prin reţeaua mondială ("INTERNET").

D. Mesajul aşteaptă în coada serverului MTA (*e-mail queue*) până când va fi expediat. Pot exista întârzieri cauzate de numărul mare al mesajelor din coada de aşteptare sau de dimensiunea mare a fişierelor ataşate.

E. Până să ajungă în spaţiul Internet, mesajul trece prin mai multe sisteme de verificare şi filtrare implementate pentru protecţia serverului de e-mail emitent, în ordine: anti-virus (program care scanează mesajul de viruşi şi alte aplicaţii malware), anti-spam (program de filtrare a mesajelor nesolicitate) şi firewall (sistem de protecţie al serverului).

F. MTA-ul expeditorului se va ocupa de toate aspectele furnizării mesajului până la destinaţie, unde va primi acceptare sau respingere din partea MTA-ului destinatarului. Mesajul trece prin mai multe servere, MTA cerând de fiecare dată de la sistemul DNS adresa următorului server în drumul spre destinatar. Calea aleasă depinde parţial de disponibilitatea serverelor. Termenul "*Mail server*" se referă şi la un computer care acţionează ca un MTA, rulând software adecvat. MTA comunică prin protocolul SMTP (de unde şi numele de *SMTP server* sau *Outgoing mail server*).

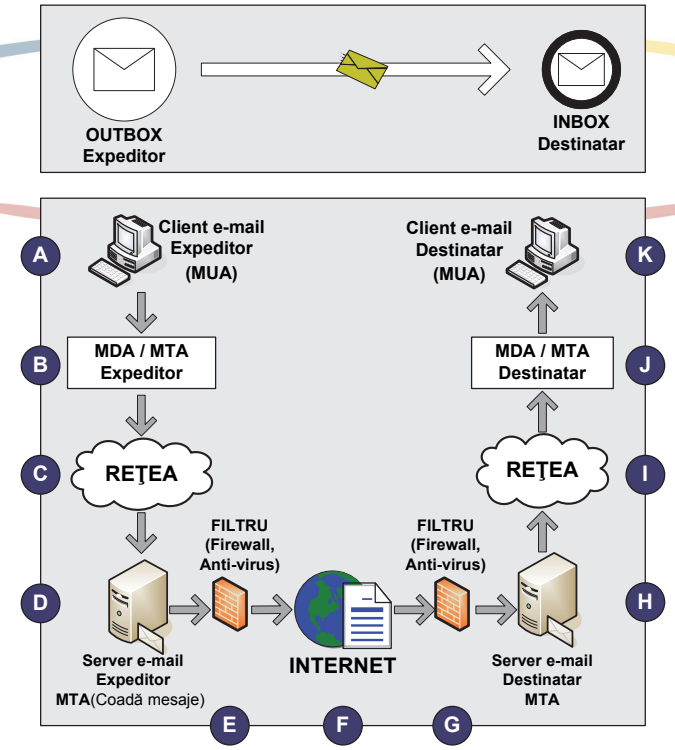


Fig. 2.2. Traseul parcurs de un mesaj prin serviciul de poştă electronică

G. Până să ajungă la MTA-ul destinatarului, mesajul poate trece prin mai multe sisteme de filtrare, în ordine: firewall, program anti-virus şi program de filtrare anti-spam.

H. Dacă trece de sistemele de filtrare, mesajul urmează aceeaşi cale de la expediţie, dar în sens invers, până ajunge în MTA-ul destinatarului.

I. Mesajul sosit în MTA trece (eventual) prin reţeaua companiei sau ajunge direct la MDA (*Mail Delivery Agent*) de la destinaţie.

J. Mesajul este preluat de MDA, un program ce se ocupă de pregătirea mesajului pentru a fi livrat în căsuţa poştală a destinatarului, imediat cum acesta soseşte pe server. MTA şi MDA sunt implementate, de obicei, de acelaşi program sau pachet (un MTA poate juca şi rolul unui MDA, aplicaţiile esenţiale fiind doar MTA şi MUA). Aplicaţiile MDA dedicate au însă implementate facilităţi în plus. Cele mai folosite MDA sunt *procmail* şi *maildrop*.

K. Destinatarul citeşte mesajul printr-un client e-mail (MUA) sau folosind interfaţa Web. Dacă se utilizează un client e-mail, mesajul poate fi accesat prin două protocoale:

   a. POP3, utilizat pentru aducerea mesajelor şi, eventual, lăsarea unei copii pe server;

   b. IMAP, protocol care păstrează implicit o copie pe server şi permite gestionarea stării mesajelor (citit, şters, mutat), astfel încât să fie realizată o sincronizare uşoară a acestora.

2.2.4. Chat şi mesagerie instant

Spre deosebire de serviciul e-mail (asincron), comunicarea în timp real este sincronă şi presupune conectarea simultană a utilizatorilor la acelaşi server de aplicaţie, doar în acest caz putându-se realiza o conversaţie online. Printre mijloacele de comunicare online se numără:

- chat-urile de pe site-urile Web (folosind diverse limbaje de programare şi scripturi - Java, ASP, Javascript, PHP - se pot implementa module de chat în interiorul unei pagini Web fără a fi necesară instalarea unui program client);
- programele IRC (*Internet Relay Chat*);
- programele IM (*Instant Messaging*).

IRC (*Internet Relay Chat*)

IRC este un protocol de tip text bazat pe TCP şi opţional TLS, care permite utilizatorilor să comunice pe Internet prin mesaje text, în forumuri de discuţii. Comunicarea se face în timp real, având ca suport numeroase reţele de servere

IRC (de exemplu Undernet - cea mai utilizată în ţara noastră, DALnet, Efnet, IRCnet, QuakeNet).

Reţele IRC asigură canale comune publice (*channels*) sau camere de conversaţie (*chat rooms*) pe diverse subiecte (*topics*), dar şi suport pentru discuţii private (între doi sau mai mulţi utilizatori). Folosind un nume unic de identificare (*nickname*), utilizatorul se poate conecta (*join*) la un canal de comunicaţie sau iniţia un nou canal (caz în care utilizatorul este operator - *channel operator* sau *op*). Rolul operatorului este să asigure respectarea regulilor unui canal (drepturi şi obligaţii ale utilizatorilor, respectarea limbajului civilizat etc.), el putând elimina temporar (*kick*) sau definitiv (*ban*) un utilizator. Conectarea la un server dintr-o reţea de IRC se poate realiza:

- printr-un program client instalat la utilizator (de exemplu: mIRC, Pirch);
- prin interfaţa Web - pentru aceasta sunt necesare:
  - un browser care să permită rularea unui *applet* pentru conectarea la serverul IRC;
  - instalarea unui *plugin* (modul suplimentar) care asigură suportul pentru limbajul Java în browserul Web.

IM (*Instant Messaging*)

Programele tip IM (*Instant Messaging*) sunt o formă de *comunicare directă în timp real* între două sau mai multe persoane conectate simultan la acelaşi server. Ca şi la IRC, diferenţa între programele IM şi serviciul e-mail o constituie comunicarea sincronă (utilizatorii trebuie să fie conectaţi - *online* - simultan pentru ca discuţia să poată avea loc). Versiunile noi ale anumitor programe IM permit şi trimiterea *offline* a mesajelor care pot fi citite de utilizator atunci când se conectează. Modalitatea de bază a comunicării o constituie mesajele text, însă versiunile actuale de clienţi IM permit şi facilităţi multimedia (telefonie, voce, video). Principalele funcţii pe care le îndeplineşte un program actual de IM sunt:

- schimb de mesaje text, permiţând formatarea textului (font, dimensiune, stil, culoare), conversia automată a link-urilor, inserarea unor *emoticons*;
- conversaţie audio (sunt necesare un microfon şi boxe/căşti) tip PC-la-PC şi PC-la-telefon;
- facilităţi video-conferinţă (sunt necesare o cameră Web, microfon şi boxe/căşti);
- transfer direct de fişiere şi partajare de fişiere (*file sharing*);
- conferinţă (text sau video) cu mai mulţi utilizatori;
- gestionare centralizată a agendei de adrese, a altor servicii şi opţiuni;

- partajarea activităţii utilizatorului pe site-urile de *social networking*;
- trimiterea mesajelor offline;
- posibilitatea de a salva discuţia în arhivă;
- existenţa unor *blacklist* (liste cu utilizatori ignoraţi de la care nu se pot primi mesaje).

Apărute la sfârşitul anilor '60, odată cu primele sisteme de operare multi-user, programele de comunicare online au evoluat în timp datorită dezvoltării protocoalelor de tip Peer-to-Peer (*talk*, *ntalk*, *ytalk*) sau protocoalelor care necesită conectarea la un server (*talker*, *irc*).

În anii '80 s-au dezvoltat BBS-urile (*Bulletin Board System*), un mediu care permitea utilizatorilor conectarea folosind un program tip *Terminal*, iar unele programe înglobau facilităţi specifice mesageriei instant. La începutul anilor '90 a apărut sistemul de service online "Quantum Link" pentru calculatoarele Commodore 64 (precursorul binecunoscutului America OnLine Instant Messaging - AIM, disponibil din 1997).

La mijlocul anilor '90 încep să apară programele IM în mod grafic (GUI - *Graphic User Interface*) aşa cum sunt cunoscute în zilele noastre; primele au fost PowWow şi ICQ. Între timp, alte companii dezvoltă aplicaţii cu protocoale şi clienţi proprietari, pentru fiecare server de IM fiind nevoie de rularea câte unei aplicaţii client.

În 2000 apărea Jabber, o aplicaţie *open-source* (codul sursă este public şi nu există restricţii de copyright) bazată pe un protocol *open* (disponibil publicului larg), care utilizează librării particularizate pentru unele dintre protocoale proprietare (acţiona ca un gateway prin care se reducea numărul programelor client folosite).

Diferenţele existente între diferitele platforme utilizate de principalii furnizori de servicii IM (Yahoo!, Microsoft şi AOL) nu au permis adoptarea unui standard universal pentru unificarea platformelor de comunicaţie IM. Totuşi, versiunile noi de Yahoo Messenger şi Windows Live permit adăugarea reciprocă de utilizatori din cealaltă reţea (dar şi din reţelele IBM Lotus Sametime şi LCS - *Microsoft Live Communication Server*).

Au fost dezvoltate versiuni ale programelor client de IM pentru cele mai importante sisteme de operare (Windows, Linux sau Mac OS X). Unele aplicaţii realizează conectarea simultană (furnizând numele de utilizator şi parola pentru fiecare cont) pe mai multe reţele:

- programe tip *Multi Protocol Instant Messengers* (Pidgin, Trillian, Miranda);
- website-uri (ebuddy.com, iloveim.com, meebo.com) care nu necesită instalarea unui program client.

Tabel 2.2. Programe tip *Multi Protocol Instant Messengers*

Program	An	Reţele acoperite
Pidgin (ex-Gaim)	1999	AIM, Bonjour, Gadu-Gadu, Google Talk, Groupwise, ICQ, IRC, MSN, MySpaceIM, QQ, SILC, SIMPLE, Sametime, XMPP, Yahoo!, Zephyr
Miranda	2000	AIM, Bonjour, Battle.net, Fetion, Gadu-Gadu, Inter-Asterisk eXchange, ICQ, IRC, Jabber, Google Talk, Lotus Sametime, NetSend, MySpace, MSN, QQ, SIP, Skype, Tlen.pl, Xfire, Yahoo! Messenger
Trillian	2002	AIM, ICQ, Windows Live Messenger, Yahoo! Messenger, IRC, Novell GroupWise Messenger, Bonjour, Jabber, Skype
Digsby	2008	AIM, MSN, Yahoo, Google Talk, ICQ, Jabber, Facebook Chat

O tendinţă actuală o reprezintă conectarea conturilor IM cu cele din reţelele sociale (Facebook, Myspace, Twitter, LinkedIn), realizându-se sincronizarea informaţiilor postate între aceste aplicaţii.

APLICAŢII IM PENTRU WINDOWS

Microsoft Netmeeting - Este un client pentru video-conferinţă şi VoIP inclus în versiunile Windows 95 OSR2 până la Windows XP. Netmeeting a fost un client popular pentru discuţii şi video-conferinţe prin Internet, înainte de apariţia programelor IM gratuite. Versiunea Windows Vista nu mai include această aplicaţie (deşi se poate instala ulterior printr-un hotfix), ci recomandă utilizatorilor săi noile aplicaţii Windows Meeting Space, Remote Desktop Connection, Remote Assistance, Windows Live Messenger şi Microsoft Office Live Meeting.

Windows Live Messenger - Aplicaţia care poartă acest nume începând cu 2005 (a purtat numele MSN Messenger din 1999) este un client realizat de Microsoft pentru acces la setul de servicii online Windows Live. Se utilizează protocolul proprietar MSNP (Microsoft Notification Protocol) şi identificarea pe baza unui cont comun (Windows Live ID) pentru mai multe tipuri de servicii (Hotmail - e-mail, MSNBC - canal de ştiri pe cablu, MSN - colecţie de servicii Internet, Xbox Live - joc online multiplayer, sau alte servicii afiliate).

Yahoo! Messenger - Aplicaţia lansată în 1998 este un client gratuit cu ajutorul căruia se pot accesa şi alte servicii precum e-mail, calendar, ştiri şi alte module particularizate în funcţie de opţiunile selectate de către utilizator.

AOL Instant Messenger (AIM) - Aplicaţia dezvoltată de către compania AOL în 1997 utilizează protocoalele proprietare OSCAR (Open System for CommunicAtion in Realtime), protocol utilizat şi de programul ICQ (pe care compania AOL l-a cumpărat în 1998), şi TOC (Talk to OSCAR Protocol), un protocol cu mai puţine facilităţi decât OSCAR, dar folosit de cei ce doresc doar discuţii prin mesaje text.

Google Talk (GTalk) - Aplicaţia apărută în 2005 este gratuită pentru IM şi VoIP, dar disponibilă doar pentru sistemele de operare Windows XP şi versiunile ulterioare; Schimbul de date se realizează prin protocolul XMPP (*Extensible Messaging and Presence Protocol*), un open-protocol extensibil, care acum

beneficiază de suport pentru conversaţii de tip VoIP, multimedia - protocolul Jingle - şi transfer de fişiere.

Unele companii proprietare permit conectarea la servere şi prin intermediul interfeţei Web (aşa numitul *Web Messenger*); astfel nu mai este necesară instalarea pe sistemul de calcul a unui program client, ceea ce facilitează accesul din reţele unde restricţiile de securitate nu permit instalarea sau conectarea clientului de IM. Un applet creat prin diverse tehnologii (Java, Flash) permite conectarea la o gamă restrânsă de servicii chiar din pagina Web.

În era comunicaţiilor mobile, un mare accent se pune pe facilităţile de conectare, utilizând dispozitivele mobile (telefon mobil, tabletă PC, smartphone sau PDA). Prin serviciul MIM (*Mobile Internet Messaging*) este posibilă utilizarea aplicaţiilor tip messenger, însă funcţiile puse la dispoziţie de versiunile mobile ale acestora sunt mai puţin dezvoltate decât la variantele desktop. Există versiuni mobile pentru cele mai importante aplicaţii IM, sub diverse sisteme de operare mobile (Windows Mobile, Symbian, Blackberry sau Android).

PROGRAME PENTRU CHAT ÎN REŢEAUA LOCALĂ

O altă categorie de programe pentru mesagerie instant o reprezintă programele utilizate pentru chat în reţeaua locală. Principalele caracteristici sunt:

- rulează în interiorul reţelei, fiind accesibilă doar utilizatorilor din cadrul LAN-ului (celor din spatele firewall-ului);
- datele/informaţiile nu pot ieşi în afara reţelei;
- programele trebuie instalate local, pe fiecare calculator unde se doreşte acces şi, de obicei, nu necesită un server dedicat;
- pot identifica automat conturile utilizatorilor, precum şi alte informaţii despre alte sisteme de mesagerie existente în reţea.

Pentru sistemele Windows, primul program de chat utilizat într-o reţea locală a fost WinPopup, inclus în versiunile 3.1 (1992) până la Millenium Edition, fără versiunile bazate pe NT. Începând cu versiunile NT/2000/XP, în Windows există un serviciu (program rezident care rulează în fundalul sistemului de operare) destinat comunicării text în reţea, denumit *Messenger service* (implicit dezactivat în Windows XP Service Pack 2).

Pentru sistemele de operare Unix există comanda *talk* utilizată în schimbul local de informaţii în mod text, iar pentru interfaţa grafică X Window din sistemele Linux, se utilizează aplicaţia LinPopUp. Aceasta foloseşte Samba, un protocol care permite partajarea fişierelor şi tipărirea pentru sistemele de operare Windows şi Linux. LinPopUp permite schimbul de mesaje text cu un calculator pe care rulează programul WinPopup sau cu un alt program LinPopUp de pe un sistem de operare diferit (prin protocolul Samba).

2.2.5. Fluxuri web. Fişiere şi fluxuri multimedia

Un flux Web (*feed*, *Web feed* sau *channel*) este un format de date prin care se oferă utilizatorilor informaţii actualizate frecvent. Printr-un Web feed se poate oferi:

- informaţia completă (titlu şi conţinut);
- un sumar ce conduce, printr-un link, la conţinutul informaţiei;
- doar legătura către o pagină care conţine informaţia completă.

Termenul "sindicalizare Web" (*syndication*) se referă la punerea la dispoziţia utilizatorilor a fluxurilor de distribuţie ale unui site, astfel încât aceştia să beneficieze de conţinutul său actualizat. Tot mai multe agenţii de ştiri, ziare, site-uri cu conţinut dinamic adoptă acest model de informare, publicând cele mai noi ştiri, informaţii, articole sau mesaje postate pe forumuri şi în format feed. Avantajele fluxurilor Web constau în:

- sunt utile ambelor părţi, atât pentru site-ul sursă (care îşi creşte expunerea pe mai multe pagini Web, implicit traficul şi publicitatea), cât şi pentru site-urile care publică aceste fluxuri (îşi actualizează şi îmbunătăţesc astfel conţinutul);
- modul de abonare la noutăţi: se adaugă adresa feed-ului fără a fi necesară înscrierea cu o adresă e-mail (ca la newsletters), astfel că utilizatorul nu mai este mai expus ameninţărilor asociate cu serviciul de poştă electronică (spam, viruşi, phishing şi furt de identitate);
- dezabonarea este definitivă şi se realizează prin ştergerea fluxului din programul client utilizat pentru accesare.

CREARE ŞI UTILIZARE

Etapa 1. Generarea unui flux Web

Web feed-ul este generat în limbajul **XML** (*eXtensible Markup Language*), un limbaj de marcare care provine din limbajul general SGML (*Standard Generalized Markup Language*) şi stă la baza altor limbaje de marcare, cum ar fi: XHTML, MathML sau GraphML. Limbajul XML este destinat structurării, depozitării şi transportului informaţiei. După cum sugerează şi numele, este un limbaj extensibil, adică autorul poate defini propriile marcaje (*tags*), pe care le poate interpreta după dorinţe (spre deosebire de limbajul HTML unde marcajele trebuie cunoscute de browser pentru a fi interpretate). Sintaxa de bază pentru un element este:

<nume_element atribut="valoare">Conţinut Element </nume_element>

Împreună cu datele "vizibile" pe ecran, printr-un flux Web se transmit şi alte tipuri de informaţii (*metadata*) care descriu diferite atribute asociate unui flux Web. Acestea sunt de mai multe tipuri:

- informaţii înglobate în fişiere de date care descriu:

- pentru un document - data creării, autorul;
- pentru un fişier imagine - sursa (camera foto), rezoluţia (biţi per pixel);
- pentru un fişier mp3 - titlul piesei, artistul, albumul, data şi genul muzical.

- în fişiere HTML sunt informaţii (introduse cu marcajul <meta>) accesate şi utilizate de roboţi (*Internet bots*) şi de motoarele de căutare;
- în fişiere XML acestea se referă la autor sau data actualizării/publicării fluxului.

Pentru scrierea corectă a unui document XML se au în vedere:

- structura - trebuie respectate integral regulile sintactice XML; orice marcaj de început (< >) trebuie închis (< />), altfel documentul nu este considerat XML;
- validarea - un document este valid dacă respectă regulile semantice definite în XML Schema - DTD (*Document Type Definition*); orice element nedefinit duce la invalidarea întregului fişier.

Etapa 2. Publicarea unui flux Web

Fişierul .xml generat va fi salvat pe serverul Web (direct sau prin upload), iar fluxul va fi actualizat dinamic, ori de câte ori este necesar. Prezenţa unui flux Web într-o pagină trebuie marcată vizual prin introducerea unui link către fişierul .xml, iar pentru ca browserele să detecteze acest flux, în secţiunea <head> a paginii Web trebuie plasat marcajul:

<link href="feed.xml" type="application/rss+xml" title="RSS Feed">

unde feed.xml este numele fişierului generat.

O altă etapă o constituie promovarea feed-ului prin înscrierea lui în motoare de căutare specializate sau în directoare de feed-uri.

Etapa 3. Accesarea unui flux Web

Se realizează folosind link-ul pus la dispoziţie de distribuitorul de flux, utilizatorul putând deschide acest flux Web astfel:

- printr-un serviciu online (Google Reader, Bloglines) sau suită de servicii care oferă pagini şi gadget-uri personalizate (iGoogle, My Yahoo, MyMSN);
- prin programe de navigare (versiunile noi ale browserelor interpretează şi salvează astfel de fluxuri);
- cu un program dedicat (*aggregator* sau *feed reader*) instalat pe calculatorul propriu sau pe un dispozitiv mobil (Blackberry, smartphone, tabletă PC, PDA). Printre cele mai utilizate programe se numără Feed Demon, NewsGator, Pluck, NetNewsWire.

Prin abonarea (*subscribe*) la un flux Web, adresa lui este salvată în lista de feed-uri preferate, fapt care permite actualizarea conţinutului în programul sau serviciul utilizat pentru accesarea acestui tip de informaţii. Fluxurile Web sunt citite de utilizatorii finali (persoanele care doresc să fie informate) sau preluate şi redistribuite de alte site-uri Web, blog-uri sau producători de podcast-uri.

FORMATE DE FLUXURI WEB

Formatele utilizate pentru generarea unui flux Web sunt:

RSS (*Really Simple Syndication*) - formatul iniţial de fişier pentru fluxuri Web (prima versiune, RSS 0.9, apărută în 1999) a evoluat până la versiunea 2.0 (2002), fiind adoptată iniţial de Mozilla Firefox, apoi de Internet Explorer şi Outlook, urmate de browserul Opera.

```
<?xml version="1.0"?>
<rss version="2.0">
<channel>
<title>...</title>
<link>http://....</link>
<description>....</description>
<language>en-us</language>
<pubDate>...</pubDate>
<lastBuildDate>...</lastBuildDate>
<item>
<title>...</title>
<link>...</link>
<description>...</description>
<pubDate>...</pubDate>
</item>
</channel>
</rss>
```

ATOM - format creat ca alternativă la RSS, în scopul de a clarifica ambiguităţile, consolida versiunile multiple şi extinde capabilităţile. La sfârşitul anului 2003 a apărut versiunea Atom 0.3 care s-a răspândit odată cu adoptarea sa de către serviciile Google (GMail, Google News, Blogger), iar în octombrie 2007 a apărut versiunea 1.0 a acestui format.

```
<?xml version="1.0" encoding="utf-8"?>
<feed xmlns="http://www.w3.org/2005/Atom">
<title>...</title>
<subtitle>...</subtitle>
<link href="http://..."/>
<updated>...</updated>
```

```
<author>
<name>...</name>
<email>...</email>
</author>
<entry>
<title>...</title>
<link href="http://..."/>
<updated>...</updated>
<summary>...</summary>
</entry>
 </feed>
```

PODCAST

Reprezintă o metodă de a pune la dispoziţia utilizatorilor fişiere multimedia (audio, video) prin formatul flux Web, fişierele putând fi redate online, dar şi descărcate pentru acces offline, atât pe calculatoare, cât şi pe echipamente mobile (telefoane, tablete PC, playere multimedia). Numele provine de la combinaţia termenilor *iPod* (un dispozitiv media portabil al firmei Apple Computer) şi *broadcast* (difuzare). *Podcaster* este persoana care publică un podcast, iar *podcatcher* este programul care poate identifica noile fişiere asociate cu un flux Web de tip podcast (exemple: Apple iTunes, Nullsoft Winamp, Juice Receiver, jPodder).

BLOG

Prescurtarea de la *Web log* (jurnal pe Web), blog-ul este un tip de pagină de Internet care conţine o serie de articole, comentarii, descrieri de evenimente, materiale audio sau video, aranjate, de obicei, în ordine invers cronologică publicării (cel mai recent articol postat este aşezat primul).

Un blog poate fi definit ca un site actualizat cu regularitate, care conţine text, link-uri la alte blog-uri sau pagini Web, împreună cu material multimedia, majoritatea acestora permiţând postarea comentariilor vizitatorilor. În general, blog-ul are un caracter personal, tip jurnal online, dar sunt şi blog-uri care aparţin unor organizaţii, companii sau persoane private, orientate pe diverse subiecte (fotografie, călătorii, muzică, politică, artă). Există aplicaţii care uşurează procesul de adăugare şi actualizare a blog-urilor, printre cele mai cunoscute platforme fiind Wordpress (open source) şi Blogger (Google). Totalitatea blog-urilor poartă numele generic de *blogosferă*.

Blog-urile reprezintă o componentă importantă a generaţiei Web 3.0, conţinutul lor generat atât de autor, cât şi de ceilalţi utilizatori, fiind strâns integrat cu reţelele de socializare şi alte tehnologii moderne. Accesarea informaţiilor multimedia pe Internet se realizează prin două metode distincte, ***download*** şi ***streaming***. Alegerea modului de publicare a fişierelor sau a fluxurilor multimedia depinde de la

situaţie la situaţie (necesitate, uşurinţă în implementare, costuri, posibilităţi tehnice etc.).

DOWNLOAD

Metoda constă în salvarea întregului fişier multimedia pe calculator, astfel încât acesta să fie disponibil pentru accesare şi/sau editare ulterioară, offline. Un fişier multimedia poate fi descărcat ca orice alt fişier pe Internet, prin accesarea link-ului disponibil în pagina Web. Acesta permite accesul la fişier fără vreun software suplimentar sau setări speciale ale serverului Web. Pentru deschiderea fişierului multimedia salvat este necesară instalarea unui program ("multimedia player") pe calculatorul local. Pentru link, în sursa paginii Web se introduce un cod HTML de forma: Vezi fişier avi

Avantaje:

- odată salvat, fişierul permite accesul rapid (pentru deschidere sau editare);
- nu se consumă timp şi bandă decât o singură dată, la descărcarea fişierului;
- poate fi vizualizat de pe discul local, fără a necesita conexiune Internet.

Dezavantajele acestei metode:

- fişierul ocupă spaţiu pe discul local şi durează un timp până când tot fişierul este transferat (mai ales pentru fişiere de mari dimensiuni şi conexiuni lente);
- se utilizează când serverul care furnizează datele are un trafic moderat; dacă se realizează multe conexiuni concurente, metoda de download prin protocoalele HTTP/FTP nu este eficientă şi duce la o supraîncărcare a serverului;
- protocoalele HTTP sau FTP permit doar descărcarea integrală al fişierelor înainte de a putea fi deschise cu player-ele asociate;
- nu se poate detecta viteza conexiunii utilizatorului; se pot realiza mai multe versiuni ale fişierului (calitate mai bună înseamnă mai mult spaţiu ocupat şi timp de descărcare mai mare), iar utilizatorul poate să aleagă versiunea în funcţie de performanţele conexiunii.
- O altă metodă care utilizează protocolul HTTP pentru transferul fişierelor multimedia de la un server Web către un client este **download-ul progresiv** (sau *HTTP streaming*). Aceasta reprezintă o metodă hibridă (combinaţie între download şi streaming) care constă în rularea fişierului multimedia (*play*) după ce doar o porţiune din el a fost descărcată (nu se aşteaptă descărcarea întregului fişier). Saltul (*fast-forward*) la un anumit moment din materialul multimedia nu este posibil decât după încărcarea porţiunii corespunzătoare din fişier. Pentru rularea fişierului se foloseşte un program multimedia dedicat,

executat în propria fereastră, separată, sau direct în browser-ul Web (printr-un plug-in suplimentar).

STREAMING

Emisia pe Internet (*webcast*) a unui fişier multimedia reprezintă o tehnică prin care este creat un flux constant şi continuu de date (*streaming*). Un server de streaming este un software specializat care acceptă cereri pentru furnizarea de fişiere audio/video, cunoaşte formatul fişierelor şi lăţimea de bandă, iar uneori negociază cu player-ul local condiţiile de transfer al datelor. Serverul de streaming conferă următoarele avantaje:

- permite accesul foarte rapid la diverse părţi (momente de timp) ale fişierului dorit, fără a se mai aştepta descărcarea întregului material;
- saltul în materialul multimedia este un avantaj atât pentru consumator, care poate vedea doar ce-l interesează, cât şi pentru furnizor, pentru că poate implementa aplicaţii interactive pentru căutare sau playlist-uri personalizate;
- furnizează doar cantitatea de date necesare pentru rularea fişierului;
- permite monitorizarea utilizatorilor care urmăresc un anumit material (numărul lor, durata conexiunii);
- optimizează lăţimea de bandă, deoarece nu se transferă tot fişierul;
- fişierul nu ocupă spaţiu pe discul local al utilizatorului (după rulare, fişierul descărcat temporar este şters).

Accesul la fişierul multimedia se face cu o mică întârziere cauzată de viteza de download pe Internet, de gradul de ocupare al serverului şi de buffer-ul solicitat de programele de vizualizare. Comparativ cu metodele tipice de emisie audio-video (staţii/studiouri), emisia pe Internet are următoarele avantaje:

- posibilitatea de adresare către un public mult mai numeros, fără să existe restricţii tehnice sau financiare;
- distribuţia nu este limitată geografic (nu este necesară utilizarea unor antene care să distribuie semnalul, astfel că oricine, indiferent de poziţia sa geografică, poate accesa prin Internet emisia postului radio/TV);
- informaţiile pot fi distribuite în direct (în cazul transmiterii unor evenimente live, în timp real) sau la cerere (pentru materiale înregistrate);
- costurile asociate amenajării unui studio pentru emisia online sunt mult mai scăzute;
- se pot distribui mai uşor emisiuni destinate unui anumit public ţintă;
- posturile cu emisie pe Internet nu se supun regulilor valabile pentru posturile cu emisie prin unde electromagnetice (referitoare la audienţă, formatul programului etc.).

Printre dezavantaje se pot enumera:

- este necesară o conexiune Internet stabilă şi o lăţime de bandă adaptată traficului estimat/calculat;
- în funcţie de sistemul de operare, utilizatorul trebuie să instaleze anumite programe (client, decoder) pentru a urmări emisia postului radio/TV;
- în cazul în care se atinge numărul maxim de clienţi acceptaţi, conexiunea nu se mai realizează.

Furnizorii de materiale multimedia (audio şi video) pot oferi informaţia:

- live (postul radio/TV emite atât "clasic", prin aer sau cablu, cât şi webcast);
- înregistrată, materialele disponibile (emisiunile deja înregistrate şi stocate pe server) putând fi accesate la cerere de către utilizatori.

Programele emise pot fi realizate:

- conform unei grile de program, de către persoane din cadrul postului (ascultătorii nu pot interveni);
- interactiv, de către utilizatori (mai ales la posturile radio personale, utilizatorii pot modifica, de exemplu, programul muzical alegând ce melodie să urmeze).

Radio prin Internet (*Web radio* sau *net radio*) este un serviciu de emisie audio transmis prin intermediul reţelei Internet. Primul post de radio a emis pe Internet în anul 1994, iar astăzi există zeci de mii de posturi de radio, personale sau ale unor companii. Pentru a uşura găsirea unui post de radio online s-au dezvoltat site-uri specializate care oferă informaţii organizate sau căutare după criterii precum nume post, ţară, gen muzical, număr de ascultători, tipul şi rata de codare.

Televiziunea pe Internet (*Internet TV* sau *ITV*) constă în furnizarea serviciului TV prin intermediul reţelei Internet. Metodele utilizate sunt:

- *Broadcatching* - descărcarea conţinutului digital făcut disponibil prin mecanismul RSS. Este utilizat în sistemul P2PTV (aplicaţii Peer-to-Peer destinate redistribuirii fluxurilor video în timp real într-o reţea P2P; fluxurile video redistribuite sunt, de obicei, canale TV din întreaga lume);
- *Streaming* - este modelul iniţial prin care un flux video (semnal TV sau alt semnal video) era emis de un site Web.

Din ce în ce mai multe posturi radio sau TV au şi o emisie alternativă în mediul online (Internet). Problema care apare este suprasolicitarea reţelei, “gâtuirile” fiind inerente în această situaţie, iar soluţia o constituind-o menţinerea unei lăţimi de bandă continuă a reţelei. Conexiunea punct-la-punct (*unicasting*) presupune transmiterea aceluiaşi flux de informaţii pentru toţi utilizatorii care îl solicită.

Deoarece transmiterea unui flux video prin reţeaua Internet nu reprezintă un mod eficient de emisie şi încarcă traficul prin reţea, a fost dezvoltat un protocol denumit *multicasting*. Metoda multicasting presupune ca semnalul emis să fie redistribuit în mod egal de un echipament dedicat (router sau splitter) către toţi solicitanţii pe care îi deserveşte; clientul şi serverul negociază calea cea mai eficientă pentru a primi fluxul. Pentru ca emisia şi recepţia unui flux multimedia să se desfăşoare în bune condiţii este nevoie de:

- codarea (comprimarea) informaţiei la emisie;
- utilizarea unor protocoale de transmisie adecvate;
- un program de redare (*player*) la recepţie.

CODAREA INFORMAŢIEI LA EMISIE

Un fişier multimedia se poate obţine prin:

- conversia unui fişier multimedia existent (se utilizează programe utilitare de conversie care permit schimbarea formatului fişierului). Conversia este posibilă nu numai din audio în audio sau din video în video, ci şi prin obţinerea unui fişier audio din unul video (extragerea componentei audio);
- utilizarea unui program pentru captură, editare şi conversie audio-video (printre programele populare se numără Adobe Premiere sau Final Cut Pro).

Odată creat, fişierul multimedia trebuie publicat pe serverul Web. În codul paginii Web se introduce marcajul HTML corespunzător pentru modalitatea de accesare a fişierului, prin:

- un link (marcajul <a>) care indică URL-ul fişierului (audio, video sau în general pentru orice alt tip de fişier);
- inserarea materialului ca obiect (marcajele HTML <object> sau <embed>).

Domeniul AUDIO

Pentru codarea fluxului de date se folosesc codec-uri cu pierderi, cele mai utilizate formate fiind:

- **MP3** (Moving Picture Experts Group - MPEG);
- **OGG** (Xiph.org Foundation);
- **Windows Media Audio** (Microsoft);
- **Real Audio** (Real Networks);
- **AAC** (Advanced Audio Coding).

MP3 (.mp3)

MPEG-1 Audio Layer 3 este un format de codare cu pierderi adoptat ca standard în 1991. Principalul avantaj al formatului constă în dimensiunea redusă a fişierului, obţinută cu preţul scăderii din calitate. Codarea se realizează eliminând sunetele care nu pot fi sesizate de urechea umană, prin utilizarea unui model psiho-acustic. Encoder-ul cel mai utilizat în acest moment este LAME, un program open-source care oferă o calitate maximă la comprimarea MP3.

OGG (.ogg)

Este un format realizat pentru comprimarea de fişiere şi fluxuri de date pe Internet. Fişierele de tip .ogg pot fi atât audio, cât şi video. Printre encoder-ele open-source folosite se pot enumera:

- audio - Vorbis, Speex (compresia vocii umane), FLAC (codare fără pierderi);
- video - Theora, Tarkin (3D);
- text - Writ (pentru a include subtitrări sau titluri de capitole).

Windows Media Audio (.wma)

Tehnologie proprietară Microsoft, formată din 4 codec-uri distincte:

- Standard (concurent al tehnologiilor MP3 şi Real Audio);
- Professional (suportă multi-channel şi audio de înaltă definiţie);
- Lossless (codare audio fără pierderi de calitate);
- Voice (destinat compresiei vocii, la rate de biţi scăzute).

Real Audio (.ra)

Este un format dezvoltat de Real Networks (prima versiune fiind lansată în 1995) care acoperă un domeniu vast, de la formate transmise prin dial-up (pe linii telefonice cu modem) până la formate high-fidelity (pentru muzică). Formatul este din ce în ce mai puţin utilizat pentru audio streaming în varianta *progressive download*.

AAC (Advanced Audio Coding)

Proiectat ca urmaş al tehnologiei MP3, AAC este un format de comprimare cu pierderi, implicit pentru dispozitivele iPhone (Apple Computer), iPod, iTunes şi Sony PlayStation 3. O versiune optimizată pentru aplicaţii cu rate scăzute (gen audio streaming) este HE-AAC (*High-Efficiency Advanced Audio Coding*). În funcţie de tipul browserului şi de configurarea plugin-urilor asociate, fişierul audio poate fi ascultat direct din pagina Web sau din fereastra player-ului multimedia instalat (după download).

1. Inserarea unui link la un fişier audio într-o pagină Web (file.mp3)
Fişier mp3

2. Conectarea la adresa Web a fluxului multimedia sau a fişierului de tip playlist (.m3u sau .pls)
Ascultă LIVE
Ascultă LIVE

Domeniul VIDEO

Principalele formate media distribuite ca fluxuri video pe Internet sunt:

- **Windows Media Video** (Microsoft);
- **QuickTime** (Apple Computer);
- **MPEG-4** (Moving Picture Experts Group - MPEG);
- **Real Video** (Real Networks);
- **Flash/Shockwave** (Macromedia, acum marcă Adobe).

Windows Media Video (.wmv)

Este un format comprimat de fişier video creat de Microsoft, iniţial pentru a face faţă competitorului Real Video. Formatul .wmv este caracterizat printr-o calitate bună şi o dimensiune redusă a fişierului. Fiind un format proprietar Microsoft, poate fi incompatibil pe alte platforme non-Windows sau în alte browsere (non-Internet Explorer). Includerea unui fişier .wmv într-o pagină Web se realizează cu marcajele:

- <a> (link direct, va fi deschis sau salvat pe disc);
- <object> (rulat direct în pagină).

1. Cu marcajul <a>
Vedeţi fişierul video

2. Cu marcajul <object>
<object id="mediaplayer" width="192" height="190" classid="clsid:22d6f 312-b0f6-11d0-94ab-0080c74c7e95" standby="Se incarca..." type="application/x-oleobject">
<param name="filename" value="videofilename.wmv">
<param name="showcontrols" value="true">
<param name="showstatusbar" value="false">
<param name="showdisplay" value="false">
<param name="autostart" value="false">
<embed type="application/x-mplayer2" src="fisier.wmv" name="media" width="192" height="190" showcontrols="1" showstatusbar="0" showdisplay="0" autostart="0"></embed>
</object>

QuickTime (.mov)

Printre facilităţile unice ale acestui format se numără interactivitatea, imaginile panoramice şi realitatea virtuală (*QuickTime Virtual Reality*). Inserarea unui fişier .mov cu marcaje HTML se realizează cu marcajele HTML:

- <a> (link direct, va fi deschis sau salvat pe disc);
- <object> (rulat direct în pagină).

1. Cu marcajul <a>

```
<a href="videofilename.mov">Vedeţi fişierul video</a>
```

2. Cu marcajul <object>

```
<object classid="clsid:02bf25d5-8c17-4b23-bc80-d3488abddc6b" width="320" height="180"
codebase="http://www.apple.com/qtactivex/qtplugin.cab">
<param name="src" value="videofilename.mov">
<param name="autoplay" value="true">
<param name="controller" value="false">
<embed src="videofilename.mov" width="320" height="180" autoplay="true"
controller="false" pluginspage="http://www.apple.com/quicktime/download/"></embed>
</object>
```

MPEG-4 (.mp4)

Reprezintă un set de metode utilizate pentru compresia datelor digitale audio-video, care includ tehnologii de compresie pentru Web (streaming), CD, voce (telefon, videotelefon) şi televiziune pe Internet. Include multe facilităţi ale vechilor standarde MPEG-1 şi MPEG-2, dar şi noi facilităţi precum suport VRML (*Virtual Reality Modeling Language*) pentru randări tridimensionale (*3D rendering*) şi suport pentru DRM (*Digital Rights Management*), o metodă de a controla drepturile de utilizare pentru un produs media. Modurile de includere ale unui fişier .mp4 într-o pagină Web folosind marcajele <a> şi <object> sunt prezentate mai jos.

1. Cu marcajul <a>

```
<a href="videofilename.mp4">Vedeţi fişierul video</a>
```

2. Cu marcajul <object>

```
<object classid="clsid:02bf25d5-8c17-4b23-bc80-d3488abddc6b"
codebase="http://www.apple.com/qtactivex/qtplugin.cab" width="160" height="136">
<param name="src" value="videofilename.mp4">
<param name="autoplay" value="true">
<embed src="videofilename.mp4" type="image/x-macpaint" width="160" height="136"
pluginspage="http://www.apple.com/quicktime/download" autoplay="true"></embed>
</object>
```

Real Media (.rm, .ram)

Este un format comprimat de fişier multimedia realizat de către RealNetworks şi folosit împreună cu RealVideo (suită proprietară de protocoale video) şi RealAudio pentru streaming multimedia în reţeaua Internet. Transmisiile sunt realizate în format CBR (*Constant Bitrate*). Recent, RealNetworks a dezvoltat un format de transmisie cu rată variabilă pentru fluxurile multimedia, denumit RMVB (*RealMedia Variable Bitrate*). Majoritatea playerelor multimedia de pe diferite sisteme de operare (Windows, Macintosh, Linux) oferă suport pentru formatele RealMedia. Player-ul oficial pentru formatele Real (audio, video) este RealPlayer.

Inserarea unui link către un fişier RealMedia se poate realiza:

- direct spre fişierul .rm (marcajul <a> va duce la descărcarea fişierului înaintea vizualizării);
- către un metafişier (.ram) care conţine un link spre fişierul .rm efectiv;
- cu marcajul <object>.

1. Link direct spre fişierul video

```
<a href="videofilename.rm">Vedeţi fişierul video </a>
```

2. Link spre un metafişier

```
<a href="videofilename.ram">Link spre metafişier</a>
```

unde *videofilename.ram* este un fişier text care conţine adresa secvenţei video videofilename.rm, ca mai jos: http://www.example.com/video/videofilename.rm

3. Cu marcajul <object>

```
<object id=”rvocx” classid="clsid:cfcdaa03-8be4-11cf-b84b-0020afbbccfa" width="180" height="159">
<param name="src" value=" videofilename.rm">
<param name="autostart" value="false">
<param name="controls" value="imagewindow">
<param name="console" value="video">
<embed type="audio/x-pn-realaudio-plugin" src="videofilename.rm" width="180" height="159" autostart="false" controls="all" console="video"></embed>
</object>
```

Flash video (.flv, .swf)

Este un format de fişier video pe Internet, accesibil prin intermediul unui plug-in Adobe Flash Player, un important player de fluxuri video. Versiunea 10 a formatului suportă standardele H.264 (pentru video) şi HE-AAC (pentru audio). Un fişier Flash video poate fi furnizat în mai multe formate:

- .flv (fişier de sine stătător);
- .swf (înglobat în acest format cu programe speciale);

- download progresiv prin protocolul HTTP (necesită utilizarea unui server Web obişnuit; deşi simulează difuzarea în timp real, este cea mai utilizată metodă de publicare pe site-urile Web);
- difuzat prin protocolul RTMP, folosind aplicaţia FMS (*Flash Media Server*).

1. Inserarea unui fişier Flash (.swf) de pe discul local cu marcajul <object>

```
<object classid="clsid:D27CDB6E-AE6D-11cf-96B8-444553540000"
codebase="http://download.macromedia.com/pub/shockwave/cabs/flash/swflash.cab#
version" width="200" align="right" height="160" hspace="2">
<param name="movie" value="example.swf">
<param name="quality" value="High">
<param name="uiMode" value="full">
<param name="scale" value="NoBorder">
<param name="bgcolor" value="#008000"></object>
```

2. Integrarea unui film de pe site-ul Youtube

```
<object>
<param name="movie" value="http://www.youtube.com/v/xxxxxxxxxxx">
<param name=bgcolor value=#000000>
<embed src=http://www.youtube.com/v/xxxxxxxxxxx&autoplay=0&rel=0
type= application/x-shockwave-flash width=265 height=180 bgcolor=#000000
wmode=transparent></embed>
</object>
```

PROTOCOALE DE TRANSMISIE

Domeniul AUDIO - Printre cele mai importante servere pentru fluxuri audio se numără:

- SHOUTcast - realizat de Nullsoft în 1998, este un software freeware şi cross-platform, cu licenţă proprietară;
- Icecast - aplicaţie realizată de Xiph.org Foundation în 1999 pentru platforme UNIX şi Windows.

Domeniul VIDEO - Implementarea unui server pentru fluxuri video (*Streaming Video Server*) se poate realiza prin:

- achiziţionarea unui serviciu specializat de streaming de la un ISP.
- instalarea şi operarea unui server propriu: pe lângă serverul Web (Linux sau Windows), trebuie instalate pachete suplimentare (exemple: Helix Universal Server - pentru fluxuri de tip RealMedia, Windows Media, Quicktime şi MPEG-4, Apple Quicktime Streaming Server - pentru MPEG-4 şi 3GPP, Macromedia Communication Server - pentru formatul Flash video);

PROTOCOALE FOLOSITE

- **RTSP** (*Real Time Streaming Protocol*) este utilizat pentru controlul serverelor de fluxuri media, fiind un protocol care permite comenzi de tipul Play şi Pause în rularea în timp real a fişierelor media. RTSP este utilizat pentru fluxurile de tip Windows Media, Real Media şi QuickTime video.
- **RTP** (*Real-time Transport Protocol*) realizează transportul efectiv al datelor.
- **MMS** (*Microsoft Media Server*) este un protocol unicast folosit pentru transferul datelor în Windows Media Services (Microsoft este proprietarul acestui protocol). Printre programele care suportă protocolul MMS se numără Windows Media Player, Winamp şi VLC Media Player.
- **RTCP** (*RTP Control Protocol*) realizează doar controlul protocolului RTP (fără a transporta datele efectiv) şi furnizează periodic statistici referitoare la calitatea serviciului (QoS - *Quality of Service*).
- **UDP** transmite fluxul media sub forma unor pachete de dimensiuni mici. Deşi simplu şi eficient, nu are implementat un mecanism prin care să fie garantată sosirea pachetelor la destinaţie. Aplicaţia de la recepţie realizează, prin diferite tehnici de corecţie a erorilor, verificarea integrităţii şi recuperarea datelor.
- **TCP** garantează transmiterea corectă a fiecărui bit din fluxul media. Este dificil de implementat, deoarece acest protocol are un sistem de time-out şi reîncercări care retrimite datele când se înregistrează pierderi. În acest caz, are loc o încetinire sau o blocare a fluxului de date, lucru care poate fi evitat la recepţie prin utilizarea unui buffer (memorie tampon) în programul de redare.

RECEPŢIA FLUXURILOR MULTIMEDIA

La recepţie utilizatorul poate:

- deschide pentru ascultare sau vizualizare informaţia multimedia printr-o aplicaţie denumită generic *media player*. Aceste aplicaţii realizează doar redarea informaţiei descărcate sau emise în flux continuu pe Internet.
- edita (modifica) un fişier multimedia salvat pe disc cu programe specializate denumite, în general, editoare (*editors* sau *processors*);
- translata (converti) între diferitele formate necesare pentru utilizarea lor în diverse scopuri.

Unele programe de tip media player sunt specializate pe redarea unui anumit tip de format (audio sau video), însă majoritatea pot gestiona ambele tipuri de informaţii. Sistemele de operare Microsoft Windows conţin, implicit în secţiunea de programe utilitare, o aplicaţie numită Windows Media Player (atât pentru desktop, cât şi pentru dispozitive mobile - Pocket PC, Smartphone sau tablete PC).

Un alt player intens utilizat în Windows este Winamp; acesta suportă o mare varietate de fişiere multimedia (atât audio, cât şi video). Sistemele de operare Mac OS X conţin implicit player-ul QuickTime Player şi iTunes, iar pentru Linux se utilizează implicit VLC media player.

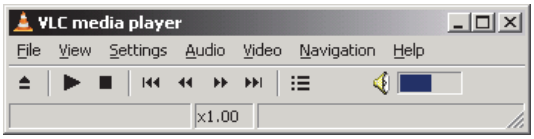


Fig. 2.3. Aplicaţia VLC media player

VLC media player este o aplicaţie completă, gratuită şi de tip open-source, care permite accesarea a numeroase formate de fişiere (atât audio, cât şi video), precum şi citirea conţinutului direct de pe unităţile de discuri (CD, DVD), din fluxuri Web şi de la plăcile de captură, oferind suport pentru majoritatea codec-urilor utilizate momentan.

2.2.6. Conexiuni Peer-to-Peer. Acces la distanţă (REMOTE)

După domeniile în care activează, reţelele Peer-to-Peer (P2P) sunt utilizate în:

- partajarea fişierelor (*file sharing*);
- telefonie VoIP;
- difuzarea fluxurilor multimedia (audio, video);
- programe de mesagerie instant (IM).

Termenul "*sharing*" reprezintă punerea în comun a resurselor (hardware/software) în vederea accesării lor de către mai mulţi utilizatori. La nivel hardware acest lucru semnifică posibilitatea partajării echipamentelor (de exemplu, o imprimantă) conectate la un calculator (server sau staţie de lucru). Din punct de vedere software, unele sisteme de operare permit partajarea fişierelor şi a folderelor/directoarelor, cu posibilitatea de a controla accesul utilizatorilor la acestea. Astfel, pentru *file sharing* există următoarele tipuri de arhitecturi:

- server central: este metoda cea mai simplă, în care se stochează toate fişierele de partajat pe un server (server de reţea, server Web);
- Peer-to-Peer: fiecare utilizator pune la dispoziţia celorlalţi utilizatori, propriile fişiere, direct pe staţia de lucru, fără a fi necesar un server central.

În cadrul arhitecturii Peer-to-Peer, fiecare utilizator are dublu rol: server (permite altor utilizatori să descarce fişiere de pe discul său local) şi client (descarcă fişiere de la alţi utilizatori). Prin această descentralizare:

- se realizează o creştere a performanţei întregului sistem (mai multe servere disponibile, lăţime de bandă mai mare, mai mult spaţiu de stocare, putere de calcul sporită);
- există o robusteţe mai mare a reţelei: în cazul căderii unui nod, informaţia poate fi găsită în alte noduri;
- este dificil de stabilit responsabilitatea cuiva pentru distribuirea ilegală de materiale protejate de legea drepturilor de autor.

Prima reţea specializată de file sharing a fost Napster (1999), o reţea centralizată care oferea gratuit fişiere audio (muzică). În urma unui proces intentat de către RIAA (*Recording Industry Association of America*) pentru nerespectarea legislaţiei drepturilor de autor, a fost închisă temporar. Napster continuă să funcţioneze astăzi ca serviciu plătit, acoperind ţări precum Canada, Germania, Marea Britanie şi Japonia. Cu un catalog de peste 8.000.000 de melodii, Napster a devenit unul din cele mai mari magazine de muzică online.

Alte aplicaţii populare pentru file sharing pe Internet sunt FastTrack (Kazaa), eDonkey (eMule, iMesh) sau Gnutella.

BITTORRENT

Conform unui studiu din februarie 2009, BitTorrent este unul dintre cele mai utilizate protocoale pentru partajare de fişiere, fiind responsabil de circa 43% din traficul total pe Internet, în special pentru transferul fişierelor de mari dimensiuni.

Avantajele utilizării acestui protocol constau în viteza mare de download şi lăţimea de bandă minimă utilizată. Aceste caracteristici sunt realizate prin împărţirea fişierului de descărcat în mai multe segmente de dimensiuni mai mici (*Segmented downloading* sau *Swarming download*) şi download-ul acestora de la utilizatorii care le-au descărcat deja. Mai mult, protocolul selectează automat cele mai rapide conexiuni pentru fragmentele de fişiere solicitate.

DIRECT CONNECT

Protocolul *Direct Connect* permite conectarea mai multor clienţi la un server central (denumit *hub*) care oferă funcţii de căutare şi descărcare a fişierelor stocate de aceştia. Prin acest protocol de transfer în mod text, necriptat, sunt posibile şi discuţii online (chat). Deoarece conexiunea se realizează printr-un un nod central, lăţimea de bandă a acestuia trebuie să fie ridicată; transferurile fişierelor se realizează, însă, direct între cei 2 clienţi.

Conectarea la distanţă (*remote*) pe un alt sistem presupune utilizarea unui program specializat prin care se realizează autentificarea utilizatorului pe respectivul sistem. După autentificare, utilizatorul beneficiază de aceleaşi drepturi de acces şi posibilităţi de lucru ca şi cum ar lucra direct pe sistemul respectiv (şi nu ar fi la

distanţă). Sesiunile de lucru la distanţă pot fi iniţiate prin intermediul unor aplicaţii tip Terminal, Remote Desktop sau Remote Browser.

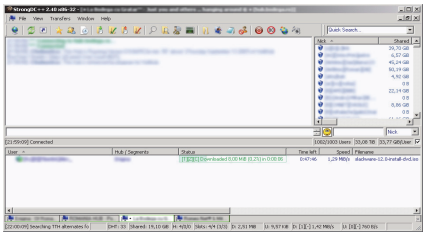


Fig. 2.4. Clientul StrongDC

CONECTARE LA LINIA DE COMANDĂ (*TERMINAL*)

Telnet (*Telecommunication network*) este un protocol dezvoltat în 1969 care permite autentificarea la o staţie de lucru printr-o interfaţă text cu o linie de comandă, folosind portul TCP 23. Un *terminal* (*consolă*) este o interfaţă în mod text care permite introducerea comenzilor şi afişarea rezultatelor.

În interfaţa grafică oferită de sistemele de operare moderne există programe care simulează aplicaţii tip terminal. Acestea permit conectarea în mod text (consolă) la diverse tipuri de servere, în special de tip Unix, şi introducerea comenzilor la linia de comandă a sistemului de operare.

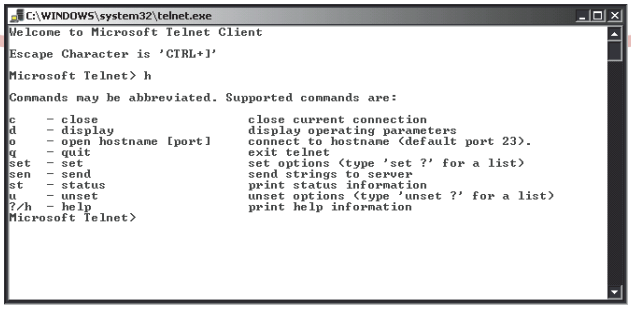


Fig. 2.5. Clientul Telnet

Datorită condiţiilor de securitate scăzute pe care le oferea (Telnet nu cripta informaţiile transmise, parole sau date efective, astfel că acestea puteau fi uşor interceptate), protocolul Telnet nu a mai fost utilizat, fiind înlocuit, practic, cu protocolul **SSH** (*Secure Shell*) - lansat în 1995.

Protocolul SSH are implementată o criptare puternică (pentru a se evita posibile interceptări ale datelor) şi o autentificare cu chei publice.

Unul din cei mai utilizaţi clienţi SSH este PuTTY, un emulator de terminal, gratuit şi open source, folosit ca aplicaţie client pentru protocoalele SSH, Telnet, Rlogin (conexiune pe portul TCP 513), Raw TCP (pentru depanarea altor servicii Internet) sau Serial (pe porturile seriale ale calculatorului).

CONECTARE ÎN MOD GRAFIC (REMOTE DESKTOP)

Remote Desktop Software reprezintă o categorie de programe utilizate pentru conectarea la distanţă la un sistem de calcul printr-o interfaţă grafică.

Principalele protocoale utilizate sunt:

- **VNC** (*Virtual Network Computing*), un protocol pe multiple platforme. VNC are o componentă de server (instalată pe calculatorul unde se doreşte accesul de la distanţă) şi o componentă de client, prin care unul sau mai mulţi utilizatori se pot conecta simultan la serverul VNC;
- **RDP** (*Remote Desktop Protocol*), un protocol specific mediului Windows, preinstalat în Windows XP şi Vista. Microsoft face referire la RDP ca *Terminal Services* sau *Remote Desktop Services*.

Printre aplicaţiile grafice de conectare la distanţă pot fi enumerate:

- **RealVNC** - utilizează protocolul VNC pentru accesul la distanţă la desktop-ul altui sistem;
- **Remote Administrator** (***Radmin***) - conţine două module: un server (ce se instalează pe calculatorul ce va fi accesat la distanţă) şi un viewer (aplicaţie folosită pentru vizualizarea desktop-ului sistemului unde a fost instalat modulul server);
- **LogMeIn** - utilizează un protocol proprietar de conexiune la distanţă transmis securizat prin SSL. Un certificat SSL este realizat pentru fiecare maşină la care se face conexiunea la distanţă şi folosit pentru a securiza transferul datelor între cele două părţi.
- **TeamViewer** - aplicaţie sub Windows, Mac OS X, Linux, care permite controlul la distanţă, partajarea desktop-ului şi transferul de fişiere.
- **FreeRDP** - aplicaţie client de tip open-source care utilizează protocolul RDP pentru acces la distanţă, cu suport pentru sistemele Windows, Mac OS X, Linux şi Free BSD.

2.2.7. Reţele sociale. Comunicare şi colaborare

Web 2.0 este un termen apărut recent, în perioada 2004-2005, care face referire la noi moduri de a considera şi exploata capabilităţile de comunicare şi informare ale reţelei mondiale Internet. Web 2.0 reprezintă o nouă abordare conform căreia conţinutul şi informaţia de pe Internet nu sunt furnizate doar de *industrial media* (firme, organizaţii, trusturi, guverne), ci şi de *social media* (persoane obişnuite care contribuie, prin intermediul Web-ului şi al reţelelor de telecomunicaţii mobile, la răspândirea informaţiilor).

Iniţial, spaţiul World Wide Web era compus din pagini statice care erau actualizate manual, necesitând cunoştinţe solide de limbaj HTML pentru publicarea datelor şi informaţiilor. Pentru ca actualizarea să poată fi realizată în timp real de utilizatori mai puţin instruiţi, au fost dezvoltate sisteme de gestiune automată a informaţiilor dintr-un site Web, denumite CMS (*Content Management Systems*). Aceste sisteme sunt utilizate pentru crearea, editarea, gestionarea şi publicarea informaţiilor digitale în format text sau multimedia prin interfeţe grafice (GUI) intuitive şi uşor de utilizat, care facilitează introducerea datelor şi actualizarea rapidă a conţinutului.

Se consideră că, începând cu anul 2005, reţeaua Internet oferă informaţii/date de o calitate superioară prin creşterea considerabilă a numărului celor care publică şi/sau comentează aceste informaţii.

Utilizarea de noi tehnici de lucru şi termeni a condus la dezvoltarea conceptului Web 2.0, care se diferenţiază faţă de varianta anterioară (Web 1.0) prin următoarele concepte:

- stocarea datelor utilizatorilor se realiza pe calculatorul local, urmând să fie publicate în Web ulterior. Acum, datele se pot prelucra şi publica direct în Web (de exemplu fotografiile private). Programele instalate local au implementate şi componente prin care se accesează online aplicaţiile Web, fiind proiectate pentru a menţine o legătură permanentă cu Web-ul şi pentru a realiza sincronizarea datelor.
- majoritatea programelor conţin module specializate pentru auto-actualizare, contactând producătorul programului în mod automat sau la cerere;
- browserul devine cel mai important program al utilizatorului, deoarece cu ajutorul lui pot fi implementate şi accesate aplicaţii Web din ce în ce mai complexe;
- rolurile de "creator" şi "consumator" în mediul Web încep să capete un nou sens, deoarece "consumatorii" de până acum încep să contribuie activ la realizarea de conţinut nou (de exemplu blogurile), toţi participând direct la răspândirea prin Web a informaţiilor şi opiniilor;
- apariţia termenului *mashup* - o pagină Web sau o aplicaţie care utilizează şi combină date din două sau mai multe surse pentru a dezvolta noi servicii.

Termenul "reţea socială" identifică o comunitate online formată în jurul utilizatorilor care au pasiuni, interese şi activităţi comune, persoane care doresc să cunoască experienţele similare ale altor utilizatori, dar şi să împartă din propriile experienţe de viaţă sau să-şi exprime punctul de vedere.

Zelist Monitor a prezentat în 2013 o statistică (publicată pe site-ul www.zelist.ro/) a celor mai accesate aplicaţii Web 2.0 în Romania:

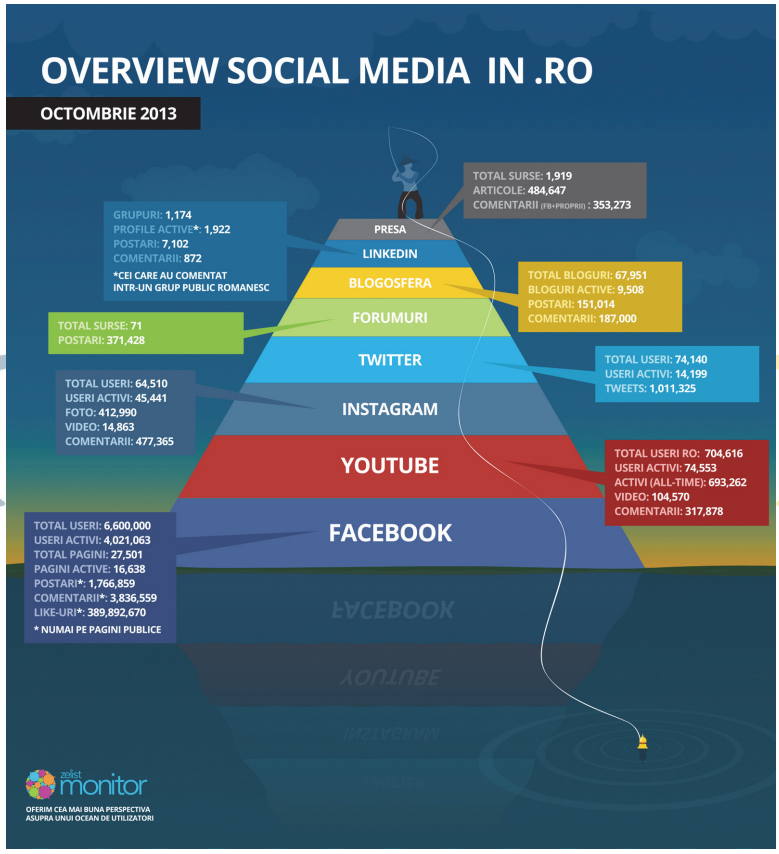


Fig. 2.7. Topul reţelelor sociale utilizate în România (2013)

Reţelele sociale sunt aplicaţii care utilizează servicii online în timp real (chat, mesagerie instant), însă prezintă şi o componentă asincronă care constă în schimbul informaţiilor prin e-mail sau fluxuri Web, postarea mesajelor, a comentariilor sau elementelor multimedia prin interfeţele de administrare specifice fiecărei aplicaţii.

Aplicaţiile online specifice erei Web 2.0 se pot clasifica astfel:

COMUNICARE

- **forumuri**: site-uri cu conţinut generat de utilizatori, format din mesaje şi discuţii organizate pe topici. Tehnologiile cele mai utilizate sunt vBulletin şi phpBB. O categorie specială este forumul de tip Q&A (*Questions & Answers*).

  Yahoo! Answers, Google Answers

- **grupuri**: servicii în care grupuri de utilizatori poartă discuţii pe diverse teme de interes comun.

  Google Groups, Yahoo! Groups, MSN Groups

- **blog** (*weblogs*, *social blogs*): jurnale online, unele orientate pe teme de interes public, altele (cele mai multe) sunt personale.

- **micro-blogging**: o formă redusă a serviciului blog, caracterizată prin transmiterea de mesaje scurte şi fişiere multimedia de dimensiuni mici.

  Twitter, Plurk

- **podcast**: mecanism de difuzare a informaţiilor multimedia (audio/video) prin sindicalizare Web (ca flux RSS).

  BBC radio

- **reţele sociale** (*social networking*): serviciu orientat pe organizarea unor comunităţi online a utilizatorilor care au în comun aceleaşi interese sau activităţi. Aceste website-uri încurajează noi metode de comunicare şi partajare a informaţiilor (imagini, text, audio, video).

  MySpace, Facebook, Hi5, Tagged, Windows Live Spaces, LinkedIn

- **motoare de căutare în social media**: există motoare de căutare speciale pentru bloguri, fluxuri RSS şi site-uri social media în general.

  Technorati

- **agregatoare de reţele sociale**: se bazează pe colectarea informaţiilor de la mai multe reţele sociale şi reunirea într-un singur profil.

  FriendFeed, Youmeo

COLABORARE

- **wiki**: colecţie de pagini Web create prin contribuţia utilizatorilor (*collaborative websites*) care folosesc un limbaj de marcare (*markup language*) simplu.

  Wikipedia

- **opinii şi recenzii**: utilizatorii publică păreri despre produse, servicii sau companii. Prin aceste analize (*reviews*), un viitor client găseşte recenzii despre achiziţionarea unui produs, colaborarea cu o anumită companie etc.

  epinions.com, yelp.com

- **social bookmarking**: serviciul de salvare, căutare şi organizare a locaţiilor paginilor Web. Adresele paginilor Web (salvate ca *bookmarks*) sunt identificate pe baza cuvintelor cheie şi a altor meta-informaţii adăugate de către utilizatori. De aici şi numele de "*social tagging*" asociat acestui serviciu în care utilizatorii colaborează între ei şi adaugă *tag*-uri (descrieri pentru un element sau informaţie). Această metodă de adnotare şi împărţire pe categorii a conţinutului de către utilizatori, fără un set impus de reguli în ceea ce priveşte declararea sau definirea tag-urilor, poartă numele de *folksonomy* - combinaţia termenilor *folk* (lume, oameni) şi *taxonomy* (ştiinţa legilor de clasificare).

  Delicious, StumbleUpon

- **social news**: se referă la site-uri unde utilizatorii postează ştiri, link-uri la diverse pagini sau comentează alte articole, ordinea de afişare fiind stabilită de scorul obţinut în urma voturilor celorlalţi utilizatori. Serviciul *social news* a dus la apariţia conceptului de "*citizen journalism*", prin care utilizatori obişnuiţi joacă un rol activ în colectarea, raportarea şi analiza informaţiilor şi a noutăţilor. Scopul jurnalismului public este furnizarea informaţiilor independente, relevante, corecte şi de larg interes.

  Slashdot, Digg, Reddit

MULTIMEDIA

- **audio sharing**: comunităţi virtuale pe baza preferinţelor muzicale. Pagini de prezentare a artiştilor, a evenimentelor muzicale, posturi de radio online, topuri şi alte informaţii din domeniu se regăsesc pe aceste site-uri.

  last.fm, imeem

- **video sharing**: permite upload, vizualizare şi partajare materiale video de mici dimensiuni. Compania gazdă a acestui serviciu permite utilizatorilor (membrilor) upload-ul materialelor video pe care apoi le găzduieşte şi le pune la dispoziţie tuturor vizitatorilor. Se pot publica scurte materiale video, cum ar fi înregistrări personale, videoclipuri, extrase din diverse emisiuni, reclame.

  Youtube, Dailymotion, Flickr, Google Video, Metacafe, Photobucket, Yahoo Video.

- **photo sharing**: constă în transferul pozelor digitale şi publicarea lor online. Operaţiile sunt facilitate de aplicaţii care uşurează încărcarea şi afişarea fotogaleriilor: generatoare de albume, organizarea imaginilor pe galerii, partajarea publică sau privată, multi-view sub formă de thumbnails sau slideshow-uri, adăugarea unor comentarii şi adnotări.

  Flickr, Imageshack, Panoramio, Photobucket, Picasa

- **art sharing**: comunitatea online a artiştilor, este un loc unde au loc expoziţii virtuale şi discuţii despre diversele aspecte ale artei.

  deviantART, Elfwood, Gfxartist

2.3. Aplicaţii în spaţiul virtual

2.3.1. Arhitectura unei aplicaţii web generice

În spaţiul virtual, o aplicaţie web reprezintă o colecţie interconectată de pagini Web, având un conţinut generat dinamic sau static, dezvoltată cu scopul de a oferi o funcţionalitate specifică.

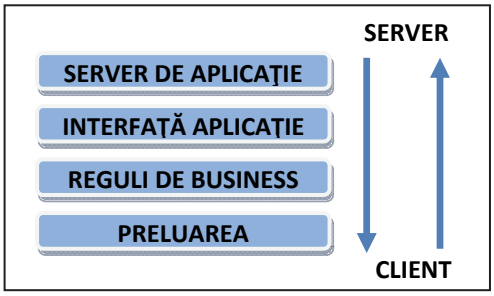


Fig. 3.1. Arhitectura generică a unei aplicaţii client-server

Arhitectura unei aplicaţii web este fundamentată pe principiul separării aplicaţiei în module independente care pot fi executate în spaţii de memorie diferite. În acest tip de arhitectură, modulul care face interogările joacă rolul de "client" (cel care cere un anumit serviciu), iar modulul care este interogat devine "server" (cel care satisface acel serviciu).

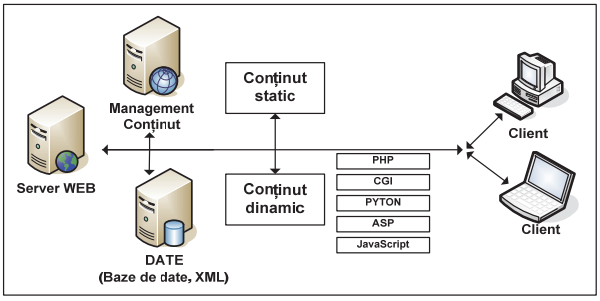


Fig.3.2. Arhitectura generală pentru o aplicaţie web

Deşi interacţiunea între cele două module se poate desfăşura în cadrul aceluiaşi calculator, această arhitectură oferă o modalitate eficientă de interconectare a serviciilor distribuite. Preluarea informaţiilor:

- la nivel de preluare a informaţiilor, datele sunt obţinute de la utilizator şi transformate în format accesibil sistemului de calcul şi invers; este important de subliniat că în această etapă nu este verificată corectitudinea datelor transmise, ele fiind doar adaptate necesităţilor de utilizare;
- la nivelul regulilor de business se stabilesc "regulile jocului", adică se validează datele. La acest nivel nu se procesează niciun fel de cerere venită de la client, ci doar se stabileşte corectitudinea datelor venite de la acesta necesare serverului, sau invers.
- interfaţa aplicaţiei este nivelul care răspunde de transformarea datelor din formatul transmis de client în formatul necesar serverului pentru a putea da un răspuns clientului (de exemplu, această etapă va transpune cererea clientului într-o instrucţiune SQL pe care o va transmite etapei finale);
- serverul de aplicaţie este nivelul final de procesare a datelor şi obţinere a rezultatelor cerute de client. Aplicaţiile client-server sunt structurate pe patru niveluri. Modul de împărţire a aplicaţiei între client şi server (care nivel va fi situat pe partea de client a aplicaţiei şi care va fi situat pe partea de server) rămâne la latitudinea dezvoltatorului.

De-a lungul timpului, au apărut variante care au la bază modelul client-server, cum ar fi: 1-tier, 2-tier, 3-tier şi N-tier.

2.3.2. Model de utilizare în tehnologia web

Arhitectura de tip 3-tier este o arhitectură de tip client-server, în care modelul logic de funcţionare, accesul la date, baze de date şi interfaţa cu utilizatorul sunt dezvoltate şi optimizate ca module independente pe platforme hardware şi software diferite. Acest tip de arhitectură a rezultat din raţiuni practice în procesul de proiectare software, fiind un cadru fundamental pentru modelarea logică a sistemelor şi devenind un model de bază în dezvoltarea de software. Componentele de bază ale acestei arhitecturi sunt:

- **nivelul prezentare** - nivelul de servicii pentru utilizatori asigură accesul la aplicaţie. Este nivelul de interfaţă cu utilizatorul, care prezintă date şi, opţional, permite introducerea şi manipularea acestora. Există 2 tipuri de interfeţe cu utilizatorul pentru acest nivel: interfaţa dedicată (de aplicaţie) şi interfaţa de tip Web. Exemplu: programe client dedicate, browser Web.
- **nivelul logic** - nivelul de logică a aplicaţiei realizează modelarea proceselor şi a datelor. Este nivelul care controlează funcţionalităţile aplicaţiei prin efectuarea unor prelucrări detaliate pe baza unor reguli, conform proceselor definite în cadrul aplicaţiei. Componentele acestui nivel sunt utilizate pentru îndeplinirea regulilor definite în cadrul proceselor, cum ar fi algoritmi şi metode, dar şi reguli de acces la date. Exemplu: server de aplicaţie.

- **nivelul de date** - acesta interacţionează cu informaţii aflate în baze de date sau depozite de date. Este nivelul reprezentat de serverul de baze de date, unde sunt depozitate şi de unde sunt extrase informaţiile. Alocarea unui nivel dedicat pentru date, separat de restul nivelurilor dintr-un sistem, îmbunătăţeşte scalabilitatea şi performanţa acestuia. Exemplu: server baze de date.

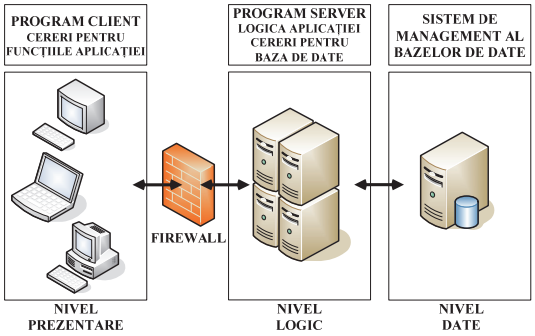


Fig. 3.3. Model de arhitectură 3-tier

Cel de-al treilea nivel include, de obicei, aplicaţii software care furnizează informaţii pentru serverul Web. Acesta poate folosi informaţiile aplicaţiilor software pentru a răspunde cererilor, în loc să caute o pagină Web sau un fişier pe discul local.

Arhitecturile care au patru, cinci sau mai multe niveluri sunt, în general, denumite arhitecturi de tip n-tier, conţin un nivel pentru aplicaţiile software (în mod asemănător cu arhitecturile 3-tier), dar includ bazele de date şi aplicaţiile sistemului de management al bazelor de date care lucrează împreună cu aplicaţiile software pentru generarea informaţiei pe care un server Web o transformă în pagini transmise la client.

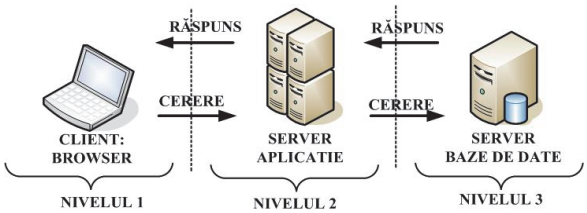


Fig. 3.4. Arhitectura 3-tier în tehnologia Web

În cazul dezvoltărilor bazate pe tehnologii Web, arhitectura de tip 3-tier este utilizată, în special, în aplicaţiile pentru comerţ electronic. În general, implementările folosind arhitectura 3-tier au următoarea structură:

1. un nivel de interfaţă cu utilizatorul: în aplicaţiile de tip Web, interfaţa (*front-end*) prezintă conţinutul extras de un program specializat de tip browser;
2. un nivel intermediar de prelucrare şi generare a conţinutului realizat prin diverse tehnologii cum ar fi: Ruby on Rails, Java EE, ASP.NET, PHP, ColdFusion, Perl sau un server Web care asigură distribuţia de conţinut (static sau dinamic);
3. un nivel de suport al bazelor de date sau al depozitelor de date - cuprinde colecţii de date, sistemul de management al datelor sau SGBD (*Sistem de Gestiune a Bazelor de Date*) care administrează şi asigură accesul la date.

Adăugarea unui nivel suplimentar asigură îndeplinirea cerinţelor de funcţionare şi utilizare a aplicaţiilor de tip distribuit pe arie largă. Funcţionalităţile asigurate de nivelul suplimentar pot fi rezumate astfel:

- se relaţionează cu serverul şi sistemul de management al bazelor de date;
- diferite componente şi formate ale datelor pot fi reutilizate în alte aplicaţii;
- oferă acces la diferite tipuri de sisteme de management al datelor fără conlucrarea cu partea de client;
- oferă un plus de flexibilitate unui server de baze de date prin posibilităţile de adăugare sau actualizare a diverselor sisteme de management asociate, cu modificări minore în serverul Web;
- viteza de procesare a serverului de baze de date depinde doar de viteza de procesare a serverului Web;
- integrarea autorizărilor pe serverul Web oferă o securitate mai bună.

Principalele beneficii ale modelelor pe niveluri de tip N-tier/3-tier sunt:

- mentenabilitatea - fiecare nivel este independent de celelalte, actualizările sau modificările pot fi efectuate fără a afecta întreaga aplicaţie;
- scalabilitate - nivelurile se bazează pe implementarea în straturi, iar extinderea unei aplicaţii este destul de simplă;
- flexibilitate - fiecare nivel poate fi gestionat sau extins independent de celelalte niveluri;
- disponibilitate - aplicaţiile pot valorifica arhitectura modulară prin utilizarea unor componente scalabile, care asigură creşterea disponibilităţii.

CREAREA PAGINILOR WEB UTLIZÂND LIMBAJUL HTML (HYPERTEXT MARKUP LANGUAGE)

HTML este un limbaj prin care se schimbă modul de prezentare a textului, folosindu-se un sistem de coduri de marcare (*tags*) inserate chiar în interiorul textului (spre deosebire de formatul .doc de exemplu, care este un format binar, special codat). Documentele HTML (fișiere cu extensiile tipice **.htm** sau **.html**) conțin doar text, iar prin codurile speciale de marcare:

- se controlează formatarea textului (font, paragraf);
- se pot defini legături către orice document stocat pe computer, în rețeaua locală sau pe Web;
- se inserează imagini, tabele, simboluri, alte elemente grafice;
- se pot afișa obiecte (elemente multimedia, animații Flash etc.);
- sunt create formulare interactive pentru preluarea unor opțiuni;
- se introduc scripturi (scrise de obicei în limbajul Javascript);
- se definește aspectul și macheta paginii Web (sau a întregului site) folosind stiluri (CSS - *Cascading Style Sheets*).

Versiuni:

- HTML 1.0 (*HTML Tags*) (sfârşitul lui 1991, limbaj propus de Tim Berners-Lee, "inventatorul" Internet-ului);
- HTML 2.0 (1995);
- HTML 3.2 (1997);
- HTML 4.0 (decembrie 1995) în formatele *Strict* (marcaje învechite sunt interzise), *Transitional* (marcaje învechite sunt permise) şi *Frameset* (sunt permise doar marcaje referitoare la cadre);
- HTML 4.01 (1999);
- HTML5 (2008).

Codurile de marcare sunt încadrate de două caractere speciale de delimitare pentru a le deosebi de textul propriu-zis al documentului: semnele mai mic „<” şi mai mare „>”. Toate marcajele HTML conţin aceste caractere şi fiecare caracter de început "<" trebuie să aibă un caracter de încheiere ">": <cod>

Un **element de marcare** este în general format din 2 coduri de marcare (de deschidere şi de închidere) care înconjoară conţinutul. Cele mai multe coduri - dar nu toate - trebuie să apară în perechi, pentru a identifica blocul asupra căruia se aplică respectivul cod.

<cod> ...*conţinut...* </cod>

Există elemente de marcare formate şi dintr-un singur cod (fără codul de încheiere), însă acestea nu se aplică unui anumit conţinut, ci sunt de sine

stătătoare. Cerinţele limbajelor XHTML, XML şi ale versiunilor actuale de HTML impun închiderea tuturor elementelor. Atunci când elementul de marcare nu are cod de încheiere se va folosi expresia <cod />.

<cod><cod />

Elementele de marcare se pot imbrica, dar trebuie păstrată structura ierarhică (un element trebuie să se închidă în interiorul elementului ierarhic superior):

<cod1> ...*conţinut...* <cod2> ...*conţinut...* </cod2> ...*conţinut...* </cod1>

Atributele definesc diferite proprietăţi pentru un element de marcare şi se adaugă doar la marcajul de început al acestuia, de forma:

<cod atribut1="valoare1" atribut2="valoare2"... >

Numele atributelor nu sunt *case sensitive* (nu contează dacă se scriu cu majuscule sau litere mici), dar valorile pe care le iau atributele pot fi. Enumerarea mai multor atribute pentru acelaşi element se face separându-le prin spaţiu.

Comentarii - Introducerea unui bloc de comentarii în HTML se face astfel:

<!-- ...comentarii... -->

Comentariile, deşi nu sunt vizibile în pagina Web afişată, se pot vedea dacă se deschide codul sursă al paginii (View - Page Source). Un alt tip de comentariu, recunoscut doar de browserul Internet Explorer, este comentariul condiţional:

<!--[if IE 8]> Folosesti Internet Explorer 8 <![endif]-->

Forma generală a unui document HTML

Un document (fişier) HTML este construit pe următoarea structură:

```
<!DOCTYPE HTML>
<HTML>
<HEAD>
...
</HEAD>
<BODY>
...
</BODY>
</HTML>
```

Prima linie defineşte tipul documentului, pentru ca browserele să poată identifica mai bine sintaxa folosită în codul sursă, iar pagina să fie afişată corect. Există diverse declaraţii pentru HTML 4.01. HTML 5 sau XHTML 1.0., dar uzual se foloseşte:

<!DOCTYPE HTML PUBLIC "-//W3C//DTD HTML 4.01 Transitional//EN"
"http://www.w3.org/TR/html4/loose.dtd">

pentru HTML 4.01 Transitional sau

<!DOCTYPE HTML>

pentru HTML5.

Există 2 marcaje ce delimitează documentul, declarându-l de tip HTML. Acestea sunt <HTML> şi </HTML> ce se plasează la începutul, respectiv sfârşitul documentului. În interiorul acestei structuri există 2 blocuri:

- **Zona de antet** (*Head*) delimitată de marcajele <HEAD> … </HEAD> conţine informaţii generale despre document, cuprinzând marcaje ce descriu titlul, informaţii despre autor, cuvinte-cheie despre categoria şi conţinutul site-ului, includerea unor fişiere externe (stiluri CSS, scripturi Javascript);
- **Cuprinsul** (*Body*) delimitat de <BODY> … </BODY> este cel mai important şi mai cuprinzător marcaj. Aici se găseşte practic întregul conţinut vizibil al documentului. Marcajul <BODY> acceptă următoarele atribute:
  - **BGCOLOR**="#rrggbb" | "rgb(r,g,b)" | "nume_culoare" - stabileşte o culoare pe fundalul paginii, unde:
    - #*rrggbb* este o combinaţie de 6 cifre hexazecimale, nu neapărat identice, din cele 16 posibile (0-9, A-F) pentru a obţine combinaţii de roşu - verde - albastru (**R**ed - **G**reen - **B**lue);
    - rgb(*r*,*g*,*b*) - este specificată o culoare folosind valori întregi în intervalul 0...255 pentru a obţine combinaţii de roşu - verde - albastru;
    - *nume_culoare* este un nume standardizat de culoare recunoscut de browser-ul Web.
  - **BACKGROUND**.="fişier_imagine" - specifică fişierul imagine (precedat eventual de calea relativă dacă nu este în acelaşi folder cu pagina) care va fi folosit pe fundal. Atributul BACKGROUND suprascrie o eventuală culoare de fundal (stabilită cu atributul BGCOLOR).
  - **TEXT**="#rrggbb" | "rgb(r,g,b)" | "nume_culoare" - specifică o culoare pentru textul din pagină;
  - **LINK**="#rrggbb" | "rgb(r,g,b)" | "nume_culoare" - specifică o culoare pentru link-urile din pagină;
  - **VLINK**="#rrggbb" | "rgb(r,g,b)" | "nume_culoare" - specifică o culoare pentru link-urile vizitate din pagină;
  - **ALINK**="#rrggbb" | "rgb(r,g,b)" | "nume_culoare" - specifică o culoare pentru link-urile active din pagină (link-urile pe care se ţine apăsat indicatorul mouse-ului).

Exemple:

```
<BODY BACKGROUND="fundal.gif"> Această pagină are o imagine pe fundal.</BODY>
<BODY BGCOLOR="#FF0000">Această pagină are fundal roşu.</BODY>
<BODY BGCOLOR="rgb(255,0,0)">Această pagină are fundal roşu.</BODY>
<BODY LINK="#808000" VLINK="#800080" ALINK="#008080" TEXT="#008000"
BGCOLOR="rgb(15,25,100)">Exemplu de utilizare a atributelor marcajului BODY</BODY>
```

FORMATAREA PAGINILOR WEB PRIN INTERMEDIUL STILURILOR CSS (CASCADING STYLE SHEETS)

CSS *(Cascading Style Sheets)* este un standard pentru formatarea elementelor unui document HTML. Stilurile se pot atașa elementelor HTML prin intermediul unor fișiere externe sau în cadrul documentului, prin elementul <style> și/sau atributul style. CSS se poate utiliza și pentru formatarea elementelor XHTML, XML și SVGL. Un CSS descrie modul de reprezentare al unei pagini HTML, într-un fişier separat. CSS are următoarele avantaje:

- Separă conţinutul de prezentare
- Permite definirea modului de afişare şi layout-ul tuturor paginilor de pe un server web intr-un singur loc;

CSS *(Cascading Style Sheets)* au fost adăugate începând cu HTML 4.0 şi definesc modul de prezentare al elementelor HTML, stilurile pot fi aplicate:

- unui singur marcaj HTML (nerecomandat; stilul se aplică doar acelei apariţii a marcajului)

```
<p style="color: red; margin-left: 20px">Paragraf care foloseste un stil </p>
```

- în interiorul secţiunii <HEAD> (se utilizează când un singur document foloseşte acel stil)

```
<head>
<style type="text/css">
hr {color: blue}
p {margin-left: 20px}
body {background-color: green}
</style>
</head>
```

- într-un fişier extern (extensia tipică: .css) (ideal pentru a fi aplicat mai multor pagini; aspectul întregului site se controlează dintr-un singur fişier; metodă recomandabilă de utilizare a stilurilor)

```
<head> <link rel="stylesheet" type="text/css" href="stil.css"> </head>
```

Sintaxa - selector {property: value}

- selector – marcajul căruia dorim să-i modificăm o proprietate
- property – proprietatea (atributul) pe care dorim să o modificăm
- value – valoarea atributului de modificat

Exemple

```
body { color: black }; p { font-family: "sans serif" }; p { text-align: center; color: red }
h1,h2,h3,h4,h5,h6 { color: green }
```

PHP / MYSQL

Adaptarea la noile provocări pe care le oferă dezvoltarea reţelei Internet necesită adoptarea unor noi strategii privind dezvoltarea unor tehnologii pentru utilizarea resurselor în îndeplinirea obiectivelor organizaţiilor. Una dintre cerinţele absolut necesare pentru o aplicaţie este de a fi dinamică şi interactivă. În aceste condiţii, una dintre cele mai bune soluţii tehnologice este reprezentată de utilizarea unui limbaj *server-side*. Astfel, a apărut **PHP** (*Hypertext Preprocessor*), limbaj utilizat pe scară largă în dezvoltarea paginilor şi aplicaţiilor Web dinamice. De obicei, este utilizat în combinaţie cu **MySQL**, un sistem de gestiune a bazelor de date relaţionale asociate aplicaţiilor Web şi **Apache**, un server Web care asigură procesarea cererilor şi transmiterea către nivelul aplicaţie şi al bazelor de date.

PHP, un limbaj de programare care se evidenţiază prin simplitate în modul de utilizare şi caracteristici dintre cele mai complexe, a devenit un model în fruntea tehnologiilor de dezvoltare a aplicaţiilor Web cu conţinut dinamic. PHP se remarcă prin următoarele caracteristici:

- *sintaxa simplă, uşor de utilizat*: variabilele PHP nu trebuie declarate şi pot reţine orice tip de obiecte;
- *similitudinea sintaxei* cu cea a limbajelor de programare structurată consacrate precum C şi Perl. Cu o sintaxă ce satisface toate aşteptările de la un limbaj de programare atât interpretat, cât şi compilat, structurat sau orientat-obiect, PHP versiunea 5 permite dezvoltarea unor aplicaţii complexe cu un efort minim;
- *independenţa de platformă*: a fost portat pe toate sistemele de operare majore, incluzând UNIX, Linux, Windows şi MacOS şi interacţionează cu majoritatea serverelor Web;
- *open-source*: spre deosebire de produsele comerciale similare, care necesită licenţă şi nu oferă acces la codul sursă, un dezvoltator are libertatea de a modifica şi completa limbajul după propriile nevoi;
- *librărie open-source şi de module*: beneficiind de o comunitate foarte răspândită de dezvoltatori software, PHP oferă un număr impresionant de module reutilizabile şi uşurinţă (datorită sintaxei) în crearea de componente reutilizabile şi modulare. Astfel, extensiile PHP oferă suport pentru acces la API (*Application Programming Interface*) pentru Windows, managementul proceselor pe sisteme de operare din clasa UNIX-ului, manipularea formatelor de comprimare zip/gzip/bzip2, generarea de documente în format PDF, Flash şi multe alte tehnologii;
- *eficienţă*: este optimizat pentru timp scurt de răspuns (necesar aplicaţiilor Web), poate fi utilizat ca modul al server-ului Web şi astfel îmbunătăţeşte suplimentar timpul de răspuns;
- *interfaţa prietenoasă de conectare la o gamă foarte mare de servere de baze de date*: în conformitate cu necesităţile aplicaţiilor Web de a interacţiona în

mod dinamic cu utilizatorul, în vederea prezentării informaţiilor păstrate într-o bază de date, scripturile PHP care conţin numai 2 sau 3 linii rezolvă probleme simple de conectare şi executare a instrucţiunilor SQL asupra bazelor de date;

- începând cu versiunea 4.0, deţine *suport minimalist pentru programarea orientată-obiect*, suport devenit complet în versiunea 5.0.

Conform rapoartelor W3tech referitoare la utilizarea limbajelor de programare în dezvoltarea aplicaţiilor Web din mediul online, se confirmă popularitatea limbajului PHP.

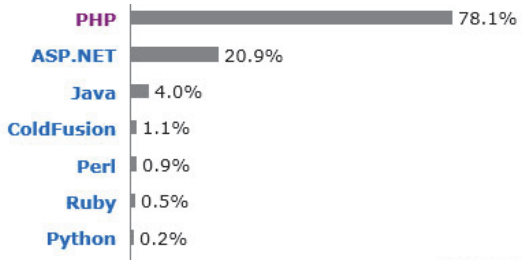


Fig. 3. 5. Procentul de utilizarea a limbajelor de programare server-side în spaţiul virtual

MySQL - bazele de date au devenit o parte integrantă a componentei operaţionale pentru majoritatea organizaţiilor. Fără o structurare a datelor în structuri organizate precum bazele de date, gestiunea datelor ar fi un proces dificil, poate chiar imposibil. Majoritatea organizaţiilor (bănci, universităţi, biblioteci etc.), prin operaţiunile pe care le desfăşoară, depind în mare măsură de bazele de date şi modul de gestionare a acestora. Procese precum utilizarea motoarelor de căutare sau comerţul electronic sunt activităţi care prin modul de proiectare nu s-ar putea desfăşura fără utilizarea bazelor de date.

Un SGBD (*Sistem de Gestiune a Bazelor de Date*) reprezintă un ansamblu de programe utilizate pentru gestionarea datelor sau un mediu de programare destinat gestiunii datelor şi informaţiilor dintr-o bază de date, care asigură:

- încărcarea bazei de date;
- actualizarea şi interogarea acesteia;
- interfaţa cu sistemul de operare în vederea simplificării accesului la date.

Un sistem de gestiune a bazelor de date care gestionează interfaţa cu aceste date formează ceea ce se numeşte un server de baze de date. MySQL este unul dintre cele mai răspândite sisteme de gestiune a bazelor de date relaţionale, rapid şi robust, dezvoltat pentru a efectua operaţiuni cu baze de date într-un mod eficient şi

securizat. MySQL este un server multi-user şi multi-thread care utilizează limbajul standard de interogare a bazelor de date (SQL - *Standard Query Language*). Popularitatea MySQL se datorează, în primul rând, multiplelor facilităţi oferite de acesta, dintre care voi aminti:

- *viteza de execuţie*: conform dezvoltatorilor de aplicaţii MySQL este cel mai rapid sistem de gestiune a bazelor existent la ora actuală pe piaţă;
- *uşurinţa în utilizare*: este un sistem de gestiune a bazelor de date cu performanţe ridicate, dar relativ simplu de utilizat, a cărui configurare şi administrare sunt mult mai simple decât în cazul unor SGBD similare;
- *accesul concurent la date de către un număr nelimitat de utilizatori*: acceptă conexiuni de la mai mulţi clienţi simultan. De asemenea, clienţii pot utiliza mai multe baze de date simultan şi pot obţine acces la MySQL în mod interactiv, folosind interfeţe care permit introducerea de interogări şi vizualizarea rezultatelor.
- *conectivitatea şi securitatea:* poate fi utilizat în reţele, bazele de date fiind accesibile din reţeaua locală sau de oriunde din Internet, oferind posibilitatea partajării datelor; MySQL are dezvoltat un modul complet de control al accesului cu drepturi explicite de citire şi scriere.
- *distribuţia liberă:* fiind gratuit, a constituit principalul motiv al popularităţii în utilizare şi dezvoltare.

Principalele motive pentru utilizarea pe scară largă a MySQL sunt viteza, stabilitatea şi facilitatea în utilizare. De asemenea, în dezvoltarea MySQL au fost avute în vedere o serie de caracteristici importante pentru mediul online, cum ar fi faptul că a fost proiectat încă de la început pentru gestionarea unui volum foarte mare de date, conectivitate şi viteză mare, precum şi o securitate ridicată. Toate aceste caracteristici fac din MySQL unul din cele mai utilizate produse pentru gestiunea bazelor de date pe Internet.

Apache (proiect *Apache Software Foundation*) este rezultatul unui efort colectiv cu scopul declarat de a dezvolta şi întreţine un server Web care oferă servicii *http* pentru sistemele de operare (UNIX, Linux, Windows), fiind caracterizat de următoarele calităţi: open-source, securizat, eficient şi extensibil.

Ajuns la versiunea 2.4.3., depăşeşte din punct de vedere al funcţionalităţilor şi performanţelor servere comerciale ale unor firme de prestigiu, prin:

- *opţiunile de configurare şi design-ul modular*: simplitate în scrierea de module personalizate care să asigure o anumită funcţionalitate, în cazul în care acestea nu sunt deja implementate în librăria proprie;
- *portabilitate*: versiunea originală a serverului Apache a fost dezvoltată pentru UNIX, dar versiunile actuale rulează sub OS/2, Windows şi alte platforme.

Câteva caracteristici ale serverului Apache sunt:

- *facilităţi multiple*: oferă suport XML, incluziune de fişiere pe parte de server, rescrierea URL-urilor, găzduire virtuală etc.;
- *modular*: dacă se doreşte folosirea unei facilităţi care nu este implementată în nucleul de bază Apache, aceasta poate fi instalată separat;
- *extensibil*: codul sursă fiind gratis, dacă nu se găseşte un modul care să ofere funcţiile de care este nevoie la un moment dat, este posibilă crearea unuia nou, care să servească nevoilor personale;
- *popular*: în acest moment, serverele Apache acoperă aproximativ 60% din piaţa serverelor Web;
- *gratuit*: este distribuit în mod gratuit, ceea ce reprezintă un avantaj pentru Apache.

2.3.3. Dezvoltarea unei aplicaţii pentru gestionarea unui flux organizaţional

1. MOTIVAŢIA DEZVOLTĂRII APLICAŢIEI

Numărul mare de documente electronice din cadrul organizaţiilor, dublat de necesitatea colaborării şi accesului rapid, în timp real, la date şi informaţii, în condiţiile în care nevoia de automatizare a proceselor reprezintă o necesitate, implică utilizarea unor tehnologii diverse şi adoptarea unor măsuri de securitate atât la nivelul aplicaţiilor şi serviciilor, cât şi la nivelul sistemului de comunicaţii al organizaţiilor.

Dezvoltarea unor arhitecturi şi instrumente software performante, securizate, pentru unificarea datelor şi informaţiilor distribuite, constituie cerinţe de bază în procesul de proiectare şi implementare la nivel organizaţional a *sistemelor de management al documentelor* (DMS - *Document Management System*). Implementarea aplicaţiilor de tip management al documentelor permite dezvoltarea unui mediu coerent şi activ în procesul de colaborare cu alte entităţi, precum şi posibilitatea eficientizării fluxurilor de activităţi interne, a proceselor de analiză şi planificare.

Un sistem de management al documentelor poate fi asimilat la nivel conceptual cu procesul de gestionare şi evidenţă a documentelor unei organizaţii, prin conversia şi stocarea documentelor în format electronic şi administrarea lor, sub această formă, de la momentul creării/intrării până la arhivarea sau distrugerea lor.

Implementarea unui astfel de proces presupune aplicaţii şi instrumente software care asigură:

- gestionarea automată a fişierelor document şi a celor care realizează legături între documente;

- posibilitatea unui mod de lucru partajat (în colaborare) cu aceste documente, pe baza unor fluxuri de activităţi predefinite şi a unui sistem electronic care permite schimbul de informaţii/documente.

Prin implementarea unei aplicaţii de tip *sistem de management al documentelor* şi înregistrările asociate, organizaţiile beneficiază de o îmbunătăţire vizibilă a procesului de eficientizare a fluxurilor organizaţionale. Sistemele de management al documentelor permit organizaţiilor să-şi îmbunătăţească eficienţa şi productivitatea. Procesele de comunicare şi colaborare, permit automatizarea proceselor între departamente şi aduc un câştig financiar important.

2. ETAPE METODOLOGICE ALE DEZVOLTĂRII APLICAŢIEI

Activitatea de proiectare a unei aplicaţii presupune utilizarea unor elemente aflate într-o strânsă relaţie de interdependenţă, care asigură succesul oricărui proces de dezvoltare: limbajul de modelare, descrierea procesului şi instrumentul utilizat. Limbajul de modelare defineşte structura aplicaţiei, astfel încât să poată fi identificate diverse decizii tactice şi simulează modul de implementare a proceselor. Procesele privind dezvoltarea unei aplicaţii sunt structurate pe două dimensiuni:

- dimensiunea temporală - structurarea ciclului de viaţă în faze şi iteraţii, astfel:
  - lansarea - definirea succintă a proiectului;
  - elaborarea - planificarea activităţilor şi resurselor necesare, specificarea caracteristicilor şi proiectarea arhitecturii;
  - construcţia - realizarea produsului prin iteraţii incrementate;
  - tranziţia - furnizarea produsului (distribuire, instruire etc.).
- componentele procesului - producerea unei mulţimi specifice de elemente cu activităţi bine definite, care trebuie să conţină:
  - modelarea activităţii - identificarea nevoilor utilizatorilor şi a aşteptărilor acestora în ceea ce priveşte funcţionalitatea aplicaţiei;
  - identificarea cerinţelor - descrierea unei perspective asupra aplicaţiei, împreună cu un set de cerinţe funcţionale şi non-funcţionale;
  - analiza şi proiectarea - descrierea modului de realizare a aplicaţiei în faza de implementare;
  - implementarea - generarea efectivă a codului sursă;
  - testarea - verificarea aplicaţiei din punct de vedere tehnic şi funcţional.

În această etapă este descrisă modalitatea de implementare efectivă a proceselor, adică tehnologia care va fi utilizată în implementarea aplicaţiei conform cu

necesităţile aplicaţiei (rezultate în urma definirii obiectivelor, modelării arhitecturii şi în conformitate cu structura proceselor).

3. PROIECTAREA APLICAŢIEI

Pe baza cerinţelor formulate sunt dezvoltate etape metodologice privind dezvoltarea arhitecturii aplicaţiei, stabilirea componentelor, a diagramelor de activităţi şi a tehnologiei (platformei) care va fi adoptată pentru implementarea aplicaţiei.

Proiectarea aplicaţiei reprezintă una dintre etapele cele mai importante. Elaborarea corectă a cerinţelor va conduce definirea completă a funcţionalităţilor. În cadrul acestei faze sunt identificate o serie de acţiuni suplimentare care trebuie efectuate pentru a fi îndeplinite cerinţele formulate de beneficiar.

4. DESCRIEREA APLICAŢIEI. PREZENTARE GENERALĂ

Dezvoltarea unei aplicaţii care să realizeze o evidenţă completă a unor date specifice asociate pentru personalul din cadrul unei organizaţii. Aplicaţia va cuprinde un modul de evidenţă a persoanelor, care va conține informaţii relevante privind starea acestuia în raport cu procesul de evidenţă a documentelor.

Documentele asociate unei persoane vor fi stocate prin intermediul aplicaţiei, pe un mediu independent de utilizatorul aplicaţiei, în format .pdf (*Portable Document Format*) generat automat. Documentele trebuie să aibă asociat un număr unic de înregistrare (identificare) pe baza căruia se vor genera rapoarte, dovezi de depunere, borderouri de transmitere, registre. Toate aceste elemente ale aplicaţiei vor trebui să fie generate şi în format .pdf pentru uşurinţă la imprimare şi transmitere în format electronic, prin intermediul serviciului de poştă electronică, altor părţi interesate.

Modulul de evidenţă a persoanelor din cadrul sistemului şi cel de documente asociate trebuie să beneficieze de facilităţi de editare, modificare, actualizare şi arhivare. De asemenea, este necesară dezvoltarea unui modul de verificare şi alerte privind situaţia anumitor persoane care au depăşit anumite termene privind transmiterea documentelor, precum şi o avertizare a utilizatorilor referitor la intervalele de timp privind generarea rapoartelor obligatorii. Aplicaţia trebuie să fie scalabilă şi independentă de sistemul de operare.

5. ARHITECTURA APLICAŢIEI

Aplicaţiile de tip client/server sunt structurate pe trei niveluri (Fig.3.6): nivelul de prezentare, nivelul de logică a aplicaţiei (*business*) şi nivelul de date.

Nivelul de prezentare, numit şi interfaţă, reprezintă nivelul care asigură prezentarea datelor primite de la nivelul de logică a aplicaţiei într-un format prietenos pentru utilizator. Separarea serviciilor de prezentare de cele care ţin de

logica aplicaţiei permite modificarea interfeţei cu utilizatorul cu eforturi minime. La acest nivel se realizează o prelucrare a datelor introduse de utilizator astfel încât ele să fie trimise mai departe nivelului de logică a aplicaţiei într-un format recunoscut de acesta.

Nivelul de logică a aplicaţiei reprezintă nivelul dinamic al unei aplicaţii, deoarece conţine regulile de logică şi de funcţionalitate ale aplicaţiei. De asemenea, acest nivel joacă rolul de intermediar între baza de date şi client, fiind responsabil de transferul datelor. La acest nivel, prin scripturi PHP organizate în librării se stabilesc regulile de funcţionare a aplicaţiei. Aceste scripturi efectuează o serie de operaţii precum validarea datelor introduse de utilizator, construirea interogărilor SQL care vor fi trimise spre execuţie nivelului de date, luarea deciziilor în ceea ce priveşte informaţiile care vor fi trimise spre afişare nivelului de prezentare.

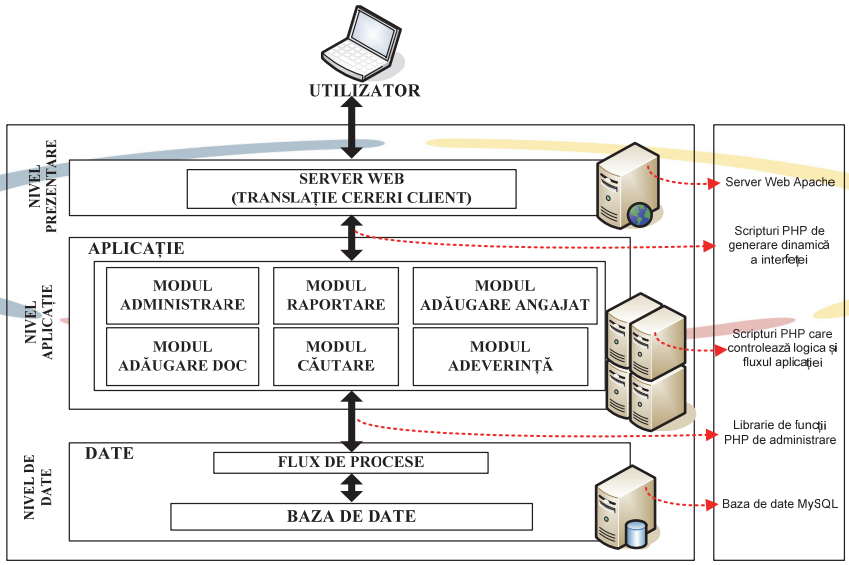


Fig. 3.6. Arhitectura 3-tier a aplicaţiei

Nivelul de date este nivelul static al aplicaţiei, la care se stochează datele care sunt furnizate nivelului logic pentru prelucrări şi eventual nivelului de prezentare, pentru a putea fi accesate de utilizator. De la acest nivel, datele sunt trimise pentru prelucrări către nivelul de logică al aplicaţiei sau sunt stocate informaţiile provenite de la utilizatori, după ce au fost validate şi prelucrate la nivelul de logică al aplicaţiei.

Principalul avantaj al unei arhitecturi pe 3 niveluri faţă de o arhitectură client/server tradiţională (pe două niveluri) este reprezentat de faptul că majoritatea procesărilor

se fac pe serverul de aplicaţie şi baza de date, nu pe sistemul de calcul client şi baza de date. Aceasta permite o scalabilitate mult mai bună a aplicaţiei în condiţiile unui volum de tranzacţii în creştere, prin adăugarea de servere suplimentare pentru creşterea capacităţii de procesare.

6. COMPONENTELE APLICAŢIEI

Diagrama de componente (Fig.3.7) oferă vederi structurale asupra aplicaţiei, prin evidenţierea componentelor funcţionale care interacţionează în timpul execuţiei. Modelul rezultat din aceste vederi are ca obiectiv delimitarea modulelor aplicaţiei, asupra cărora trebuie să se concentreze activitatea de implementare, precum şi a dependenţelor dintre acestea. Această diagramă are rolul de a evidenţia cele patru componente ale aplicaţiei şi pachetele de librării care susţin funcţionalitatea acestora. Am delimitat cele patru componente din tipul de arhitectură ales pentru aplicaţie ţinând, totodată, cont de caracterul public al mediului Web.

Componenta de **securitate** are un rol bine definit în asigurarea bunei funcţionări a aplicaţiei protejând-o împotriva ameninţărilor, inclusiv împotriva utilizării necorespunzătoare de către beneficiarii săi. Funcţia de *autentificare, autorizare şi verificare date trimise de utilizator* asigură cerinţa aplicaţiei de a controla accesul la funcţionalităţi prin intermediul conturilor şi al sesiunilor de lucru, respectiv oferă protecţie împotriva executării de operaţii neautorizate asupra bazei de date.

Componenta de **interfaţă** reprezintă spaţiul de exprimare a elementelor utilizate la comunicarea între utilizator şi aplicaţie, văzută ca un schimb bidirecţional de informaţie. Prin urmare, funcţionează ca parte vizibilă a aplicaţiei, fiind modalitatea prin care utilizatorul îşi comunică opţiunile, alegerile, deciziile în raport cu funcţionalităţile aplicaţiei.

Componenta de **procesare** este responsabilă cu implementarea logicii de funcţionare a aplicaţiei şi deţine responsabilitatea interfaţării cu componenta de *date*, realizată prin *interfaţa cu MySQL*.

Componenta de **date** execută la cererea explicită a componentei *procesare* acţiuni asupra bazei de date, îndeplinind rolul nivelului de date din arhitectura 3-tier.

Un aspect important al relaţiilor dintre componentele arhitecturii este dat de faptul că toate utilizează componenta de *securitate* datorită necesităţii de a valida comunicarea utilizator-aplicaţie conform unor reguli bine stabilite. Arhitectura 3-tier a aplicaţiei impune existenţa a două interfeţe care, transpuse în contextul componentelor delimitate, asigură comunicarea între:

- componenta de *interfaţă* şi *procesare* (operaţiuni): această interfaţă asigură transformările necesare între formatele de date cu care lucrează cele două componente;

- componenta de *date* şi *procesare* (modificare/extragere): funcţionalitatea acestei interfeţe rezidă în pachetul *Interfaţa cu MySQL* şi specifică modalitatea prin care componenta de *procesare* modifică datele din baza de date administrată de componenta de *date*.

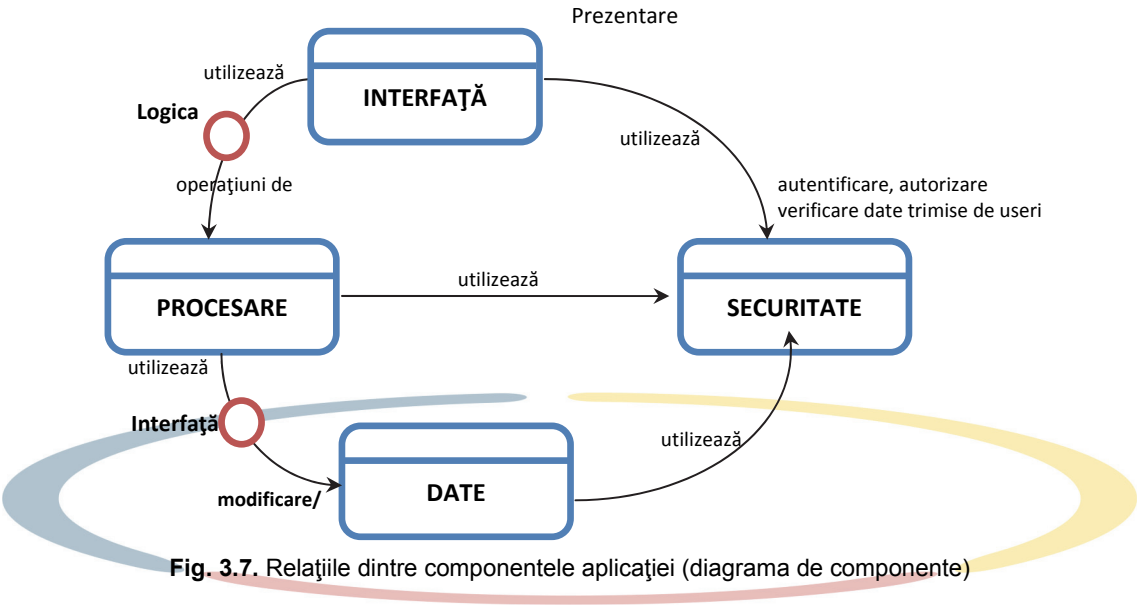


Fig. 3.7. Relaţiile dintre componentele aplicaţiei (diagrama de componente)

7. DIAGRAMELE DE ACTIVITATE

Diagramele de activitate (Fig.3.8) sunt utilizate pentru modelarea aspectelor dinamice ale aplicaţiei, prin asocierea proceselor unei activităţi folosind decizii şi condiţii. Obiectivele diagramelor de activitate constau în prezentarea fluxului secvenţial de activităţi şi cuprinde acţiunile efectuate şi rezultatele acestora prin:

- reprezentarea acţiunilor care vor fi realizate;
- modul de utilizare al unei instanţe în termenii acţiunilor;
- modul de organizare al aplicaţiei.

Una dintre cele mai reprezentative diagrame de activitate este reprezentată de introducerea unei noi persoane în sistem. Acţiunile parcurse pentru realizarea activităţii de introducere a unui nou utilizator în sistem sunt (tabela *date_identificare*):

1. utilizatorul se conectează pe baza unui user şi a unei parole la aplicaţie;
2. se verifică dacă persoana este introdusă în sistem;
3. dacă sunt respectate restricţiile privind introducerea caracterelor, se introduc datele de identificare ale persoanei;

4. se verifică dacă îndeplineşte condiţiile impuse în aplicaţie privind corectitudinea formatului datelor asociate;
5. se verifică operaţionalitatea identităţii prin posibilitatea de adăugare a unui document corespondent în cadrul sistemului.

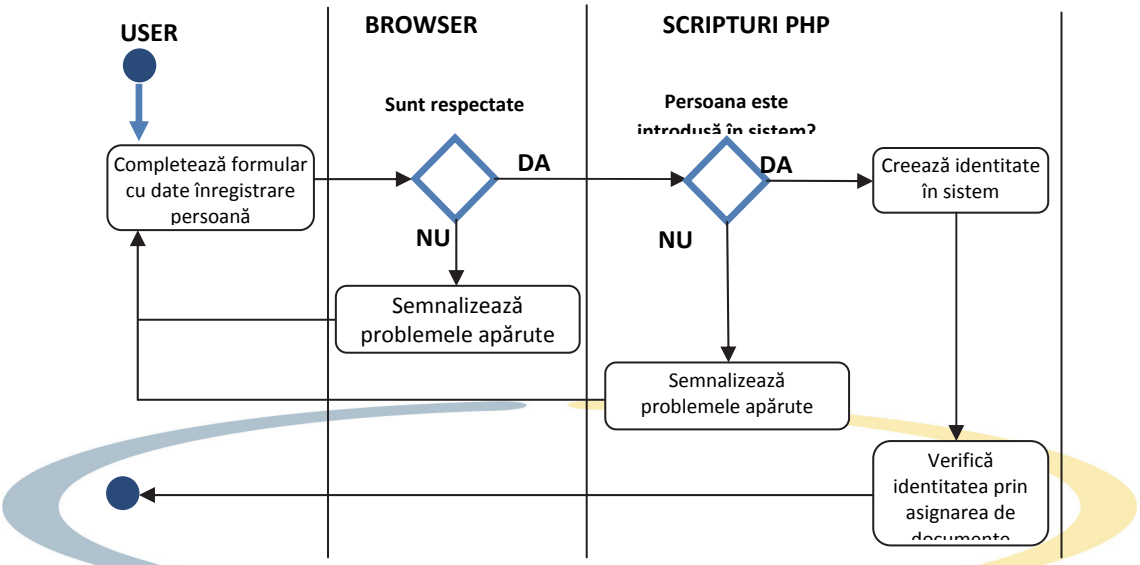


Fig. 3.8. Diagrama de activitate pentru introducerea unei noi persoane în sistem

8. IMPLEMENTAREA APLICAŢIEI

În dezvoltarea aplicaţiei a fost utilizat limbajul de programare PHP, având ca suport un server Web Apache şi un sistem de gestiune a bazelor de date MySQL. Structura de fişiere componente ale aplicaţiei este una intuitivă, fiind grupate pe directoare şi tipuri de acţiuni (administrare şi utilizare).

Astfel, directorul ***images*** conţine toate imaginile incluse în paginile aplicaţiei, directorul ***styles*** conţine fişierele .css (*Cascading Style Sheet*) folosite pentru formatarea aspectului, directorul ***declaratii*** conţine fişierele .pdf (generate de aplicaţie), directorul ***phppdf*** conţine clase PHP utilizate pentru generarea de fişiere în format .pdf şi directorul ***javascripts*** conţine fişierele de Java Script.

Componenta de interfaţă

Orice aplicaţie presupune dezvoltarea unei pagini de start, o pagină de index care trebuie să conţină opţiuni şi informaţii utile pentru utilizator, să aibă aspect plăcut, să fie intuitivă şi să se încarce rapid. Aplicaţia este structurată pe 2 module principale: modulul administrare şi modulul utilizator.

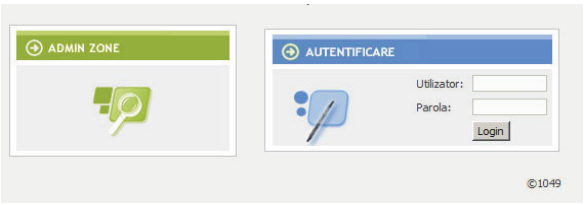


Fig. 3.9. Interfaţa de autentificare pentru conectare la aplicaţie

Modulul de administrare conţine secţiunea de adăugare utilizatori, care pot utiliza aplicaţia şi este rezervat administratorilor aplicaţiei. Modulul utilizator (autentificare) conţine aplicaţia propriu-zisă, accesibilă doar pe baza unui nume de utilizator şi a unei parole. După desfăşurarea operaţiunii de autentificare cu succes, utilizatorii au la dispoziţie o pagină de index care conţine un *meniu* în care se regăsesc toate opţiunile specifice de care beneficiază un utilizator în cadrul acestei aplicaţii. Opţiunile de meniu sunt grupate pe categorii şi subcategorii de acţiuni în funcţie de operaţiunea pe care o realizează.

Fig. 3.10. Structura meniului din aplicaţie

Dezvoltarea pe secţiuni, semnalizate sub formă vizuală, are rolul de a asigura o interfaţă prietenoasă cu utilizatorul şi un mod coerent de lucru conform analizelor proceselor aplicaţiei. Astfel, aplicaţia are primele 2 meniuri (*Adăugare angajat* şi *Editare angajat*) prin care se introduc sau modifică informaţii legate de datele de identificare ale persoanelor din sistemul aplicaţiei. Următoarele două (*Adăugare declaraţii* şi *Editare declaraţii*) se referă la acţiuni care sunt efectuate pentru introducerea în sistem a documentelor asociate persoanelor.

Fereastra de conţinut reprezintă spaţiul unde sunt afişate acţiunile pe care le vor efectua utilizatorii sistemului. Modul de organizare a paginilor impune un stil de utilizare a aplicaţiei ce se caracterizează prin simplitate şi care permite, prin modelul de afişare, o uşurinţă în utilizare.

Componenta de date

Pentru stocarea informaţiilor prelucrate în cadrul aplicaţiei pentru bazele de date, tipul de format este MyISAM, un format gratuit, neproprietar, simplu, lipsit de facilităţi precum: suport pentru tranzacţii, proceduri stocate sau triggere. Cerinţele pentru păstrarea integrităţii referenţiale sau a consistenţei datelor sunt realizate prin intermediul scripturilor de PHP.

Versiuni mai noi de MySQL 5.5 folosesc InnoDB care asigură păstrarea integrităţii referenţiale, a consistenţei datelor şi un suport pentru o mai mare concurenţă (număr mare de utilizatori simultan). Conectarea la baza de date se realizează cu un utilizator unic cu drepturi depline asupra bazelor de date, limitările impuse fiecărui tip de utilizator realizându-se prin intermediul scripturilor PHP.

Designul conceptual al bazei de date

Analiza, proiectarea şi implementarea structurii bazei de date se realizează utilizând un *model de date*. Modelele utilizate pentru bazele de date sunt clasificate în trei categorii: modele bazate pe obiect, modele bazate pe înregistrări şi modele fizice. În prezent, cel mai răspândit model de baze de date este cel relaţional (entitate-relaţie), obiectivul său fiind acela de a simplifica accesul la bazele de date pentru utilizatorii finali. Răspândirea acestui model se datorează faptului că SGBD-urile relaţionale dispun de un limbaj simplu pentru manipularea datelor şi de o interfaţă prietenoasă, care permite utilizarea bazelor de date relaţionale de către o categorie foarte largă de utilizatori. Aplicaţia utilizează un sistem de gestiune a bazelor de date MySQL, structura bazei de date fiind următoarea:

Baza de date a aplicaţiei cuprinde un număr de 5 tabele: *admin*, *arh_date_identificare*, *date_declaratie*, *date_declaratie_demnitari*, *date_identificare* şi 2 tabele de sistem ale SGDB: *files* şi *session*. Structura tabelelor este descrisă mai jos:

- tabela *admin* - conţine administratorii aplicaţiei care pot efectua activităţi de administrare şi management al datelor.
- tabela *date_identificare* - conţine datele de identificare ale persoanelor care transmit documente pentru a fi introduse în sistem.
- tabelele *date_declaratie* şi *date_declaratie_demnitari* - conţin datele de identificare ale documentelor depuse de persoanele din tabela anterioară, precum şi o serie de date administrative (cine a introdus documentul, adresa IP de la care fost introdus etc.). Tabelele au o structură comună, diferenţa dintre ele constă în câmpul categ_funcţie care diferenţiază persoanele din sistem în funcţionari şi demnitari.

	Table	Action	Records	Type	Collation	Size	Overhead
☐	admin		5	MyISAM	utf8_general_ci	2.3 KB	-
☐	arh_date_identificare		0	MyISAM	utf8_general_ci	1.0 KB	-
☐	date_declaratie		3,597	MyISAM	utf8_general_ci	370.7 KB	-
☐	date_declaratie_demnitari		1,583	MyISAM	utf8_general_ci	165.3 KB	-
☐	date_identificare		1,147	MyISAM	utf8_general_ci	211.4 KB	-
☐	files		0	MyISAM	utf8_general_ci	1.0 KB	-
☐	session		0	MyISAM	utf8_general_ci	1.0 KB	-
	7 table(s)	Sum	6,332	InnoDB	utf8_general_ci	752.7 KB	0 Bytes

Check All / Uncheck All With selected:

Fig. 3.11. Structura bazei de date a aplicaţiei

Modelul conceptual al bazei de date şi legăturile dintre tabele bazei de date sunt prezentate mai jos:

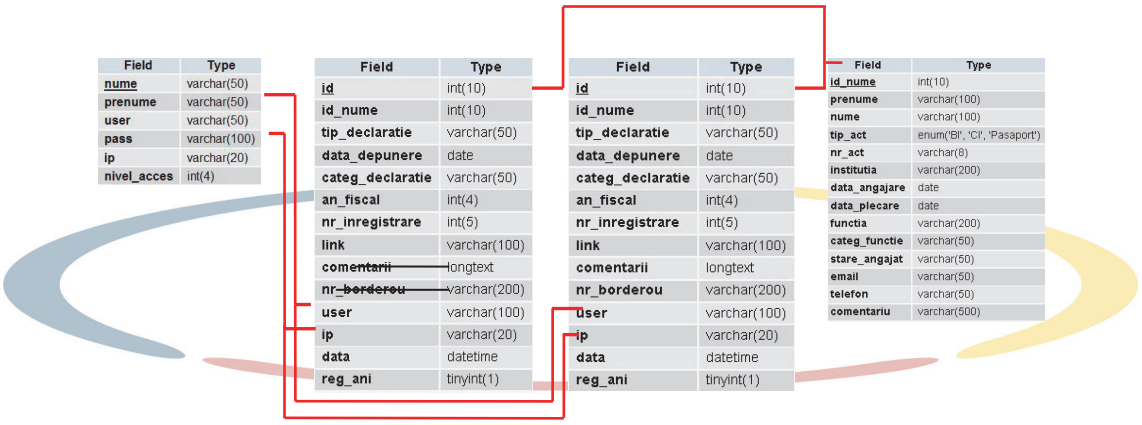


Fig. 3.12. Modelul conceptual al bazei de date

Componenta de procesare

Componenta de procesare conţine o librărie de funcţii necesare pentru administrarea bazei de date, prin intermediul scripturilor PHP, asigurând independenţa implementării aplicaţiei de tipul bazei de date administrate prin componenta de date**.** Mecanismul utilizat se bazează pe delimitarea unei interfeţe minimale de acces la o bază de date de orice tip, prin operaţii simple şi generale precum: conectarea la server, selectarea unei baze de date, executarea unei comenzi SQL etc.

Dacă datele au fost completate corect, formularul este transmis spre procesare cu ajutorul fişierului *form_add.php,* care verifică corectitudinea datelor şi transmite câmpurile respective către baza de date în tabela *date_identificare*. Pentru documente se realizează un proces similar de introducere a datelor asociate.

Fig. 3.13. Formular de adăugare / introducere persoane în baza de date

Pentru căutarea facilă a persoanelor în baza de date se utilizează un script Javascript care preia automat informaţii din baza de date, în funcţie de caracterele introduse în cadrul formularului.

Fig. 3.14. Căutarea automată a persoanelor în baza de date

După ce a fost introdusă persoana în baza de date, se introduc documentele asociate conform regulilor prestabilite, folosindu-se formularul de mai jos. La adăugarea unui document este utilizată selecţia, prin câmpuri predefinite - *drop-down* (au fost utilizate pentru limitarea introducerii de date eronate sau incomplete),a tipului de document, numărului de înregistrare în sistem, datei depunerii, precum şi a eventualelor informaţii suplimentare introduse de utilizator.

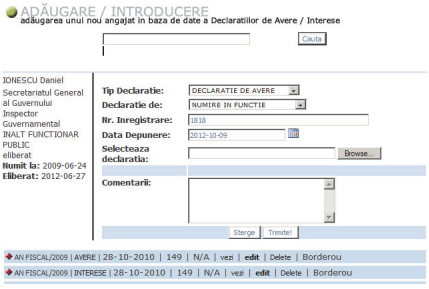


Fig. 3.15. Formularul de adăugare / introducere a documentelor asociate unei persoane

Câmpul "***selectează declaraţia***" realizează transmiterea fişierului scanat în format .pdf într-un director dedicat pe server sub forma id.persoană_tip.doc_nr.inreg.pdf. folosind librăriile phppdf.

Aplicaţia are proiectată o secţiune de raportare în care au fost dezvoltate diferite tipuri de rapoarte generate în format .pdf. Informaţiile sunt afişate şi direct în browser, prin interogări predefinite asupra bazei de date pentru diferite activităţi administrative privind procesul de gestionare a funcţionalităţilor implementate.

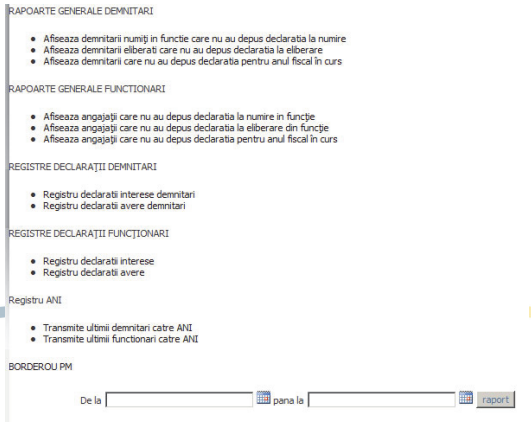


Fig. 3.16. Secţiunea de instrumente utilitare a aplicaţiei

Componenta de securitate

Principala problemă este reprezentată de accesul autorizat la funcţionalităţile aplicaţiei, care se realizează prin identificatori de acces (user şi parolă) şi printr-un mecanism de conectare şi validare la aplicaţie. Pentru toţi utilizatorii sistemului, parola se reţine criptat în formatul algoritmului MD5.

Mecanismul de conectare se bazează pe autentificarea utilizatorilor şi autorizarea accesului la paginile aplicaţiei. Autentificarea unui utilizator al aplicaţiei presupune verificarea dacă perechea nume de utilizator - parolă prezentată de el identifică un utilizator înregistrat în aplicaţie.

Această verificare este făcută de fişierul *autentificare.php* care validează corectitudinea datelor şi, în funcţie de rezultatul pe care îl returnează, va realiza autentificarea sau nu. Mecanismul de acces controlat la pagini asigură faptul că accesul la paginile destinate celor înregistraţi necesită operaţiunea de autentificare şi nu funcţionează fără acest pas obligatoriu. În acest mod, aplicaţia este protejată, de exemplu, împotriva eventualilor utilizatori fără cont care încearcă accesarea indexului de client din bara de adrese a browser-ului. Aceştia vor fi direcţionaţi către pagina de conectare.

2.4. Securitate şi confidenţialitate în internet

Conceptul de securitate a informaţiilor este complex şi are ca trăsătură principală asigurarea integrităţii, confidenţialităţii şi disponibilităţii informaţiei şi datelor. În contextul unei dinamici accelerate a dezvoltării tehnologice, diversificarea ameninţărilor asupra securităţii datelor a impus necesitatea implementării unor soluţii de securizare a echipamentelor şi aplicaţiilor utilizate în cadrul organizaţiei prin metode şi sisteme de protecţie din ce în ce mai complexe.

La nivelul organizaţiilor, securitatea şi protecţia informaţiilor confidenţiale sunt o cerinţă obligatorie în procesul de desfăşurare a activităţii, iar la nivel individual securitatea informaţiilor are un impact semnificativ asupra vieţii private şi modului în care aceasta este percepută.

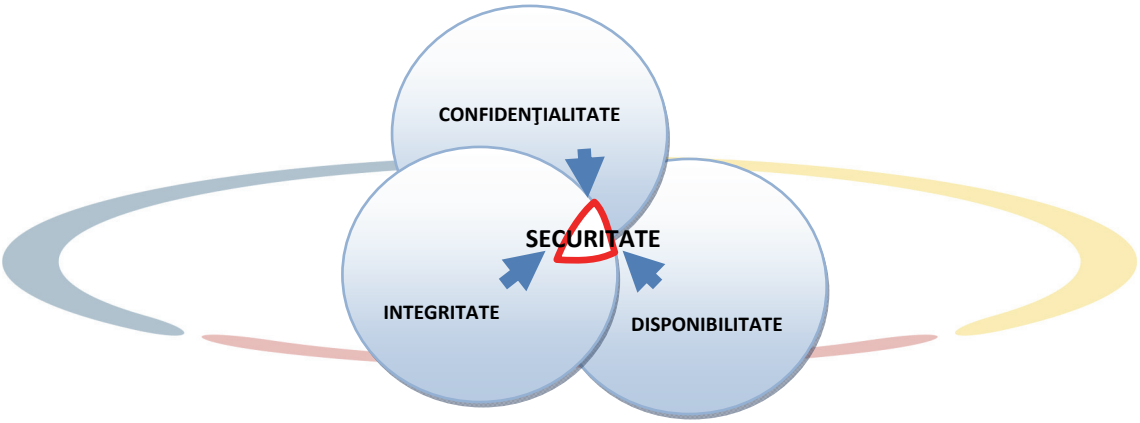


Fig. 4. 1. Concepte de bază ale securităţii informatice

Necesitatea accesului la informaţii şi comunicare fără implementarea unor măsuri minime de securitate poate conduce la urmări nedorite în cazurile de furt, modificare sau distrugere a informaţiei, precum şi la încetinirea sau întreruperea canalelor de comunicaţie. Sistemele informatice, indiferent de natura acestora, s-au dovedit de-a lungul timpului vulnerabile la accesări neautorizate ale informaţiilor, la modificarea sau distrugerea (accidentală sau voită) datelor unei organizaţii. Scopul implementării unor mecanisme de securitate într-un sistem de calcul sau reţea de calculatoare îl reprezintă protejarea informaţiilor şi serviciilor, astfel încât acestea să nu poată fi:

- interceptate (citite sau decodificate) de persoane neautorizate (fie din curiozitate, fie cu scop maliţios);
- modificate (falsificate) sau blocate la transmisie;
- inutilizabile (blocarea accesului pentru anumite categorii de utilizatori).

2.4.1. Model de securitate pentru un sistem

În definirea securităţii unui sistem informatic sunt frecvent întâlniţi termeni din mai multe domenii interdependente care realizează o descriere aproximativă a structurii departamentale specifice unei organizaţii şi care cuprind următoarele categorii:

- securitatea fizică - controlul intrărilor şi ieşirilor privind personalul şi echipamentele; asigurarea protecţiei împotriva dezastrelor naturale;
- securitatea operaţională/procedurală - acoperă modul de desfăşurarea a activităţilor, de la politica decizională managerială până la stabilirea ierarhiilor de raportare;
- securitatea personalului - formare profesională, pregătire pentru securitate, monitorizare;
- securitatea sistemului informatic - controlul accesului şi al autentificării utilizatorilor în sistemul informatic, acordarea drepturilor de acces, menţinerea integrităţii fişierelor şi a sistemului de fişiere, realizarea de backup-uri, monitorizarea proceselor şi auditare, păstrarea şi arhivarea fişierelor jurnal de evenimente (log-urilor);
- securitatea reţelei - protecţia echipamentelor active şi pasive componente ale reţelei şi a transferurilor din reţea, combaterea efectuării de interceptări, controlul accesului la conectări din alte reţele, utilizarea tehnologiilor de protecţie (firewall-uri şi detecţia intruziunilor).

Tipul de securitate pentru un sistem (un calculator sau o reţea de calculatoare) poate fi structurat folosind modelul OSI, pe mai multe straturi, fiecare strat reprezentând un nivel de securitate care protejează respectivul sistem. Fiecare nivel izolează sistemul şi îi asigură protecţie împotriva unei anumite forme de ameninţare, devenind mai dificil de accesat de către persoane neautorizate.

Securizarea unei reţele presupune implementarea unor metode şi tehnologii hardware şi/sau software pentru protecţia împotriva:

- interceptării datelor de către persoane neautorizate;
- modificării (alterării, falsificării) sau ştergerii datelor dintr-o reţea;
- realizării de conexiuni ilegale la reţea, prin folosirea identităţii unor utilizatori autorizaţi sau a unor sisteme de calcul din cadrul reţelei;
- utilizării neautorizate a serviciilor destinate unor categorii specifice de utilizatori ai reţelei.

Asigurarea securităţii unei reţele constituie un succes competiţional: încrederea în securitatea datelor stocate sau transferate reprezintă un punct forte pentru câştigarea încrederii partenerilor şi a clienţilor. Sistemul de securitate trebuie să fie obiectul unei permanente mentenanţe şi îmbunătăţiri. Un sistem sigur poate deveni nesigur la un moment dat, de aceea trebuie luate în calcul:

- apariţia permanentă a noi pericole şi vulnerabilităţi;
- implementarea unui mecanism de supraveghere continuă a sistemului, pentru repararea eventualelor breşe de securitate apărute (punctele slabe ale sistemului să fie acoperite).

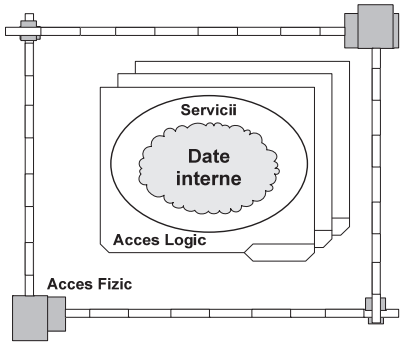


Fig. 4.2. Model de securitate

SECURITATEA LA NIVEL FIZIC

Securitatea fizică reprezintă nivelul exterior al modelului de securitate şi constă, în general, în amplasarea echipamentelor informatice sau a mediilor de stocare a datelor în spaţii special amenajate, având un control strict al accesului la acestea.

Implementarea securităţii la nivel fizic pentru un server, sistem de calcul sau pentru stocarea datelor de siguranţă (*backup*) presupune:

- asigurarea unui mediu potrivit de funcţionare, cu referire la parametrii specifici de temperatură, umiditate, presiune, vibraţii, şocuri mecanice, unde electromagnetice, praf;
- măsuri de protecţie în cazul unor calamităţi naturale (cutremure) sau incidente nedorite (incendii);
- protecţia sistemului de calcul (server) la căderi sau fluctuaţii ale tensiunii de alimentare folosind surse neîntreruptibile de putere (UPS);
- restricţionarea accesului fizic prin amplasarea echipamentelor în zone dotate cu sisteme de supraveghere, acces monitorizat şi autentificare (cartele magnetice, recunoaştere vocală, date biometrice - amprentă digitală, scanare iris);
- protecţia mediului de transmisie (montarea de canale pentru cablurile reţelei).

SECURITATEA LA NIVEL LOGIC

Securitatea logică cuprinde metodele implementate la nivel software prin care se asigură controlul accesului la resursele şi serviciile sistemului. Împărţirea pe niveluri se realizează în funcţie de tipul securităţii:

- nivel de securitate a accesului;
- nivel de securitate a serviciilor.

Securitatea accesului cuprinde:

- accesul la sistem - responsabil de condiţiile în care reţeaua este accesibilă utilizatorilor şi de evidenţa accesului. Accesul la sistem poate efectua operaţiuni de deconectare automată a utilizatorului în anumite condiţii prestabilite (expirarea intervalului orar alocat, activităţi ilegale);
- accesul la cont - verifică dacă utilizatorul care se conectează deţine un username şi o parolă valide;
- drepturile de acces (la fişiere, resurse, servicii) - determină privilegiile asociate unui utilizator sau grup de utilizatori.

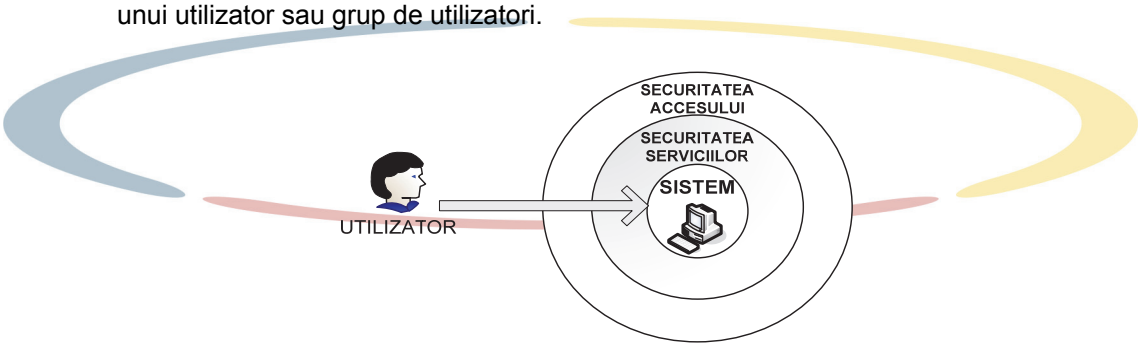


Fig. 4.3. Securitatea la nivel logic

Securitatea serviciilor controlează accesul la serviciile unui sistem (staţie de lucru sau reţea). Din acest nivel fac parte:

- controlul serviciilor - responsabil cu funcţiile de avertizare şi de raportare a stării serviciilor, precum şi cu activarea/dezactivarea serviciilor oferite de sistemul respectiv;
- drepturile la servicii - determină modul în care un serviciu este utilizat de un anumit cont (acces la fişiere, resurse, nivel de prioritate).

Odată stabilită conexiunea logică, subsistemul de securitate a accesului validează contul de acces. Subsistemul de securitate a serviciilor monitorizează activitatea

utilizatorului şi asigură măsuri de protecţie în cazul în care cererile acestuia depăşesc drepturile specificate în profilul utilizatorului (sau grupului de utilizatori).

Securitatea accesului într-un sistem se realizează prin implementarea obligatorie a nivelurilor de securitate descrise mai sus, nerespectarea acestora conducând la apariţia breşelor de securitate pentru sistem.

Astfel, în cazul unui server Web se identifică:

- entităţile cu acces local la acea maşină (utilizatori, programe server, agenţi locali), precum şi drepturile acestora (ce poate face un utilizator, privilegiile şi prioritatea cu care rulează un proces, drepturile asupra fişierelor, resursele pe care le poate accesa);
- serviciile oferite către exterior (servicii publice sau dedicate unei anumite categorii de utilizatori; autentificare, monitorizare);
- sistemul de operare (tipul, distribuţia, serviciile oferite).

Implementarea securităţii la nivel logic se realizează prin:

- instalarea programelor firewall (pentru securizarea sistemului la atacuri software din exterior);
- criptarea datelor;
- salvări regulate de date (*Backup*);
- limitarea accesului prin:
  - drepturi de scriere, citire, execuţie particularizată pe grupuri de utilizatori;
  - blocarea/limitarea accesului din exterior şi din interior pentru anumiţi utilizatori:
    - din exterior: prin mecanisme hard de autentificare:
      - cititor de amprentă digitală;
      - eToken - dispozitiv USB pentru generarea şi stocarea sigură a parolelor şi certificatelor digitale, pentru autentificare, semnătură digitală şi criptare;
      - USB Computer Lock - cheie USB prin care se limitează accesul la anumite informaţii.
    - din interior (login):
      - gestionarea accesului unui utilizator la o anumită staţie de lucru, într-un anumit interval orar;
      - monitorizarea accesului şi a activităţii.

2.4.2. Politica de securitate a unei organizaţii

Adoptarea unei strategii organizaţionale în domeniul securităţii informaţiei se realizează prin implementarea unor seturi de măsuri de control care implică politici, procese, proceduri, structuri organizaţionale care trebuie definite, implementate, monitorizate, revizuite şi îmbunătăţite atunci când acest lucru se impune, astfel încât să fie îndeplinite obiectivele specifice de securitate la nivelul organizaţiei.

Dezvoltarea unei strategii în domeniul securităţii informaţiei presupune şase activităţi principale:

1. dezvoltarea unei politici de securitate (*policy development*) - pornind de la obiectivele şi principiile de bază de securitate definite;
2. stabilirea/alocarea de roluri şi responsabilităţi (*roles and responsibilities*) – prin atribuirea rolurilor individuale, iar responsabilităţile şi modul de relaţionare trebuie să fie clar comunicate şi înţelese de toţi membrii organizaţiei;
3. proiectarea sistemului de securitate (*design*) - prin dezvoltarea unei structuri de control şi securitate care cuprinde standarde, măsuri, practici şi proceduri;
4. implementarea (*implementation*) - soluţiei şi întreţinerea acesteia;
5. monitorizarea (*monitoring*) - prin măsuri menite să detecteze şi să asigure corecţii ale problemelor de securitate, astfel încât toate breşele existente sau suspectate să fie prompt identificate, investigate şi rezolvate, pentru a asigura conformitatea permanentă cu politicile, standardele şi practicile de securitate minim acceptabile;
6. conştientizarea, formarea profesională şi educaţia (*awareness, training and education*) - necesitatea protecţiei informaţiei, pregătirea profesională pentru dobândirea abilităţilor şi cunoştinţelor necesare, în vederea securizării sistemelor informatice; educaţia privind bunele practici şi măsurile existente în domeniu.

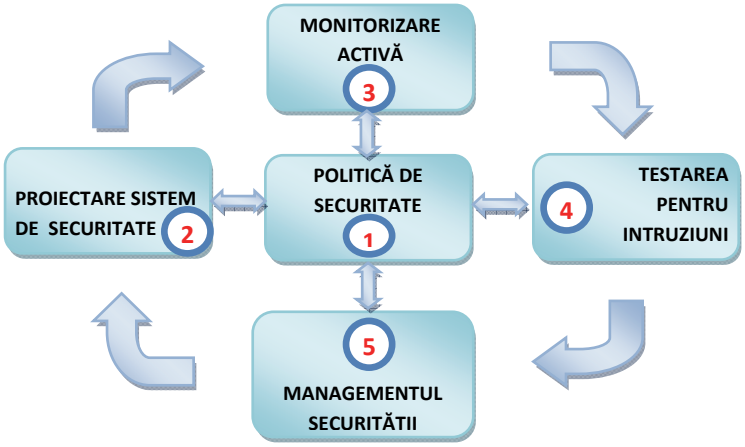


Fig. 4. 4. Model de strategie privind securitatea informaţiilor într-o organizaţie

ETAPELE PROCESULUI DE SECURIZARE

Procesul de asigurare a securităţii sistemelor informatice a impus dezvoltarea unui cadru etapizat de abordare a domeniului pe baza identificării elementelor componente. Modelarea procesului de asigurare a securităţii are la bază componenta funcţională a unui sistem şi presupune 4 etape (Figura 4.5.):

a. evaluare (*assessment*) - presupune activităţi manageriale (politici de securitate, proceduri, reglementări, bune practici, experienţă post-incident) şi o serie de acţiuni tehnice de inventariere a componentelor sistemului;

1. protecţie (*protection*) - dezvoltarea şi implementarea unor măsuri de prevenire şi protecţie pe baza estimărilor realizate în prima etapă (securizare infrastructură, mecanisme criptografice, management patch-uri, management configuraţii, controlul accesului);

2. detecţie (*detection*) - când măsurile de prevenire nu şi-au atins scopul, intervine detecţia pentru identificarea incidentelor (intruziunilor), scopul principal fiind acela de a oferi suficient timp pentru a opri compromiterea (prin activităţi de colectare, monitorizare şi audit al fişierelor de tip jurnal);

3. răspuns la atacuri (*response*) - adoptarea măsurilor pentru restaurarea funcţionalităţii şi alegerea remediilor legale (validare, izolare sau eradicare incident, refacere sau investigaţii post-incident).

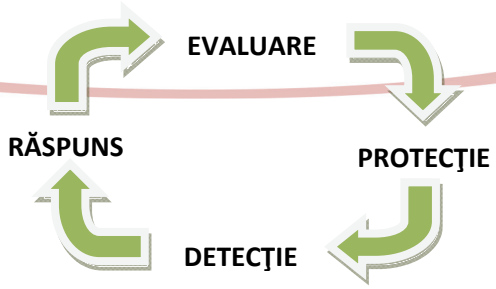


Fig. 4. 5. Etapele procesului de asigurare a securităţii conform ISO 27001

STANDARDE PRIVIND SECURITATEA INFORMAŢIEI

Adoptarea standardelor la nivel internaţional conferă un cadru organizat de implementare a măsurilor de securitate ale căror avantaje principale sunt:

- abordarea securităţii informaţiei în contextul general al activităţii specifice organizaţionale;

- proiectarea securităţii informaţiei în contextul strategiei, tehnologiei şi comportamentului uman, cu efectul adoptării unor decizii mai bune privind politica şi implementarea soluţiilor de securitate.

Printre cele mai importante standarde şi documente publicate privind controlul securităţii informaţiei pot fi enumerate: COBIT, COBIT Security Baseline, Guidelines for the Security of Information Systems, Guide for Assessing the Security Controls in Federal Information Systems NIST 800-53A, IT Infrastructure Library - ITIL, Standardele ISO/IEC 17799 şi ISO/IEC 27001 (BS 7799-2), Standard of Good Practice for Information Security.

POLITICI, STANDARDE, NORME ŞI PROCEDURI DE SECURITATE

Pentru a asigura protecţia informaţiilor, organizaţiile trebuie să implementeze reguli şi controale atât pentru date şi informaţii, cât şi pentru sistemele care stochează şi procesează aceste informaţii. De obicei, acest lucru se realizează prin dezvoltarea şi aplicarea unor politici de securitate, standarde, norme şi proceduri.

Fiecare dintre documentele enumerate mai sus are un public-ţintă bine definit şi diferit în cadrul organizaţiei şi, prin urmare, politicile nu trebuie să fie reunite într-un singur document sau să fie combinate, deoarece:

- fiecare politică îndeplineşte o funcţie diferită şi are propria audienţă;
- controalele securităţii pe linia confidenţialităţii sunt diferite pentru fiecare tip de politică;
- actualizarea şi întreţinerea politicii ar deveni extrem de dificilă.

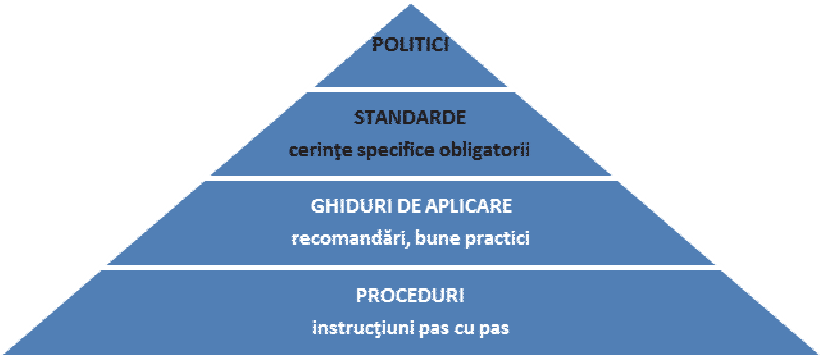


Fig. 4.6. Relaţiile dintre politici, standarde, norme şi proceduri

Aceste documente formează împreună conceptul de **securitate a informaţiei** şi asigură dezvoltarea unui cadru de securitate la nivel organizaţional:

- **politici de securitate** - constau în declaraţii de intenţie la cel mai înalt nivel cu privire la protecţia informaţiilor în cadrul unei organizaţii;
- **standarde** - constau în controale specifice, obligatorii, de nivel inferior, care ajută la aplicarea politicii şi securitatea informaţiilor;
- **norme** - constau în controale recomandate, non-obligatorii, care sunt suport pentru standarde sau sunt referinţe când un standard nu este aplicabil;
- **proceduri** - constau în instrucţiuni de tip pas cu pas pentru a ajuta utilizatorii la punerea în aplicare a diferitelor politici, standarde şi norme.

În conformitate cu RFC 2196, o **politică de securitate** "reprezintă o specificare formală a regulilor ce trebuie urmate de către persoanele ce au acces la bunurile tehnologice şi informaţionale ale unei organizaţii". O politică de securitate poate fi extrem de simplă (o scurtă prezentare) sau poate fi constituită dintr-o descriere detaliată a fiecărui element al sistemului, cu politicile de securitate asociate.

O definiţie explicită a politicii de securitate în domeniul tehnologiei informaţiei a fost sintetizată de ITSEC (*Information Technology Security Evaluation Criteria*): "un set de legi, reguli şi practici care reglementează prelucrarea de informaţii sensibile şi utilizarea resurselor hardware şi software ale unui sistem IT (tehnologia informaţiei) sau produs". În standardul SR ISO/CEI 17799:2006, politica de securitate constă dintr-un set de măsuri susţinute de factorii decizionali dintr-o organizaţie, care prevede reguli clare, dar flexibile, pentru a determina operaţiunile şi tehnologiile necesare pentru asigurarea securităţii.

Plecând de la modul de abordare a securităţii, politicile de securitate sunt împărţite în două mari categorii: militare şi comerciale. Cele militare au ca principal obiectiv necesitatea asigurării confidenţialităţii prin identificarea acelor stări care pot produce scurgeri de informaţii. Politicile de securitate comerciale au ca principal obiectiv asigurarea integrităţii prin identificarea entităţilor autorizate şi a modalităţilor de modificare a informaţiilor.

Toate aceste aspecte ale securităţii informaţiilor sunt abordate prin intermediul unor modele de securitate, grupate în: *multinivel* şi *multilaterale*.

Elementele fundamentale ale unui model de securitate informaţională sunt **resursele** (denumite generic *obiecte*), **utilizatorii** (numiţi *subiecte*) şi **relaţiile** dintre resurse şi utilizatori.

Modelele de securitate multinivel au ca principal obiectiv asigurarea diferitelor niveluri de securitate pentru resurse, în timp ce modelul de securitate multilateral are în vedere protecţia între entităţi interconectate la acelaşi nivel. Există două motive principale pentru studierea modelelor de securitate ale sistemelor:

- în primul rând, modelele sunt importante pentru determinarea politicilor care ar trebui să fie puse în aplicare pentru ca un sistem să fie securizat;

- în al doilea rând, studiul unor modele abstracte poate duce la o înţelegere a proprietăţilor sistemelor de securitate.

2.4.3. Vulnerabilităţi şi ameninţări în sistemul informatic

Vulnerabilitatea reprezintă slăbiciunea unui sistem (la nivel hardware sau software), care poate permite unui utilizator neautorizat să obţină acces asupra uneia sau mai multor componente ale sale. De cele mai multe ori, anumite particularităţi ale sistemelor informatice care devin cunoscute utilizatorilor neautorizaţi, pot deveni vulnerabilităţi, prezente în orice platformă software (nu există un sistem absolut sigur).

Securitatea unui sistem sau a unei reţele este ameninţată de:

- erori de programare, de cele mai multe ori neintenţionate;
- ignorarea bug-urilor cunoscute sau lipsa documentării în legătură cu vulnerabilităţile cunoscute (securitatea prin obscuritate);
- configurarea necorespunzătoare a serverelor şi a reţelelor (politici de securitate inadecvate);
- lipsa soluţiilor imediate (rezolvarea întârziată a problemelor din partea producătorilor);
- comoditatea sau necunoaşterea diferitelor probleme de securitate din partea administratorilor de sistem sau a companiilor (personal insuficient calificat);
- lipsa unei informări corecte a utilizatorilor asupra acţiunilor pe care le pot efectua în cadrul sistemelor;
- legislaţia tolerantă cu infracţiunile cibernetice şi deficienţele în aplicarea acesteia.

Vulnerabilităţile sunt clasificate în funcţie de tipul accesului şi al operaţiilor efectuate:

- care duc la refuzul unor servicii (DoS - *Denial of Service*);
- care permit utilizatorilor locali cu privilegii limitate să-şi mărească aceste avantaje fără a avea dreptul;
- care permit unor utilizatori externi (de pe calculatoare din alte reţele, aflate eventual la distanţă) să acceseze reţeaua sau sistemul local în mod neautorizat.

O etapă în implementarea securităţii datelor o reprezintă identificarea tuturor ameninţărilor şi, în special, a celor care pot afecta direct reţeaua sau sistemul vizat. Ameninţările pot fi clasificate după mai multe criterii:

- din punctul de vedere al intenţiei de atac:
  - neintenţionate: dezastre, calamităţi naturale, defectări ale echipamentelor, întreruperi ale alimentării cu energie electrică, erori umane în operarea datelor (introducere, prelucrare);
  - intenţionate: furtul echipamentelor, distrugerea echipamentelor, acces software neautorizat (din curiozitate, pentru testarea sistemelor de securitate, pentru furtul sau distrugerea unor informaţii, pentru spionarea activităţii).
- după tipul atacului (pentru atacurile software):
  - pasive: intrusul observă informaţia transmisă fără a interveni asupra ei şi fără a-i cunoaşte conţinutul. Persoana neautorizată poate face doar analiza traficului de pachete prin reţea (surse, destinaţii, volum de date transmis, frecvenţa), încălcând principiul confidenţialităţii.
  - active: intrusul intervine în fluxul de date pentru:
    - obţinerea în mod clandestin a unor informaţii (furt) - angajaţi care accesează servicii la care nu sunt autorizaţi, manageri care doresc acces la strategiile concurenţei, persoane care realizează fraude financiare (furtul numerelor de identificare a cărţilor de credit, transferuri bancare ilegale etc.);
    - distrugerea parţială (modificare, inserare), totală (ştergere) sau întârzierea unor mesaje - foşti angajaţi care urmăresc să distrugă informaţii, hackeri, viruşi, alte programe malware.
- după locaţia de provenienţă a atacului:
  - din exteriorul organizaţiei: hackeri, spam, malware, acţiuni DoS. Soluţii: instalare şi configurare firewall, programe anti-virus şi anti-malware.
  - din interiorul organizaţiei (*insider threat*):
    - angajaţi cu sau fără drepturi sporite de acces, cu diverse nemulţumiri referitoare la companie (post ocupat, salariu) pot sustrage în diverse scopuri informaţii sau pot crea/utiliza intenţionat breşe de securitate pentru exploatarea vulnerabilităţilor descoperite, sau pot instala malware etc.). Soluţii: monitorizarea activităţii angajaţilor, controlul accesului fizic, politica drepturilor de acces logic;
    - angajaţi insuficient instruiţi care pot instala, involuntar, programe nedorite atunci când navighează pe pagini nesigure sau accesează fişiere primite prin poşta electronică. Soluţii: instalare programe anti-virus

şi anti-malware pe serverul de e-mail, dar şi pe staţiile locale; instruirea angajaţilor în legătură cu pericolele existente şi modurile de evitare a lor.

Modelarea vulnerabilităţilor pe arhitectura funcţională a unui sistem informatic sau reţea presupune şi structurarea, după modelul de organizare şi comunicare al reţelei Internet.

VULNERABILITĂŢI LA NIVELUL PROTOCOALELOR

Vulnerabilităţile tehnologice sunt datorate, în special, deficienţelor structurale de funcţionalitate şi securitate de la nivelul suitei de protocoale de comunicaţie TCP/IP (*Transport Control Protocol/Internet Protocol*) sau implementărilor acestora, deficienţelor de securitate în sistemele de operare sau ale echipamentelor de reţea. Aceste vulnerabilități vizează, in special:

- **protocoalele de transport TCP şi UDP (*User Datagram Protocol*)** - utilizarea maliţioasă a tehnicilor de verificare şi identificare a serviciilor care rulează pe o altă reţea.
- **protocolul IP** - manipularea conţinutului datagramelor din pachetul de date IP.
- **protocoale de aplicaţie** - vulnerabilităţi în protocoalele native de poştă electronică (SMTP, IMAP şi POP) sau Web (HTTP), transmiterea traficului de date şi autentificarea în clar, lipsa unui mecanism nativ de autentificare pentru SMTP, existenţa pe scară largă a multor servere SMTP configurate să accepte mesaje de la orice utilizator (*open relay*) şi, nu în ultimul rând, o suită de bug-uri în diferitele implementări ale acestor protocoale.

VULNERABILITĂŢI LA NIVELUL SISTEMELOR DE OPERARE

În sistemele de operare de tip Windows sunt dezvoltate o gamă diversificată de servicii şi tehnologii de lucru în reţea. Vulnerabilităţile în aceste servicii care implementează funcţionalităţi ale sistemului de operare reprezintă una din cele mai uzuale posibilităţi de atac a echipamentelor care rulează sisteme Windows. Aceste servicii pot fi exploatate prin iniţierea unor sesiuni de tip anonim (sesiuni cu nume utilizator şi parolă implicite sau nule) pentru a executa şi modifica sistemul de privilegii.

VULNERABILITĂŢI LA NIVELUL SERVICIILOR

Majoritatea serviciilor de bază utilizate în reţeaua Internet au fost dezvoltate în perioada în care securitatea şi protecţia informaţiilor aveau la bază modelul de încredere reciprocă între parteneri. Astfel, servicii importante utilizate pentru funcţionarea aplicaţiilor şi comunicaţiilor pot fi compromise prin atacuri de tip: *cache poisoning*, *domain hijacking* şi *man-in-the-middle*.

VULNERABILITĂŢI LA NIVELUL APLICAŢIILOR

La nivelul aplicaţiilor, datorită domeniilor diverse de utilizare şi tehnologiilor utilizate (PHP, JavaScript, ASP etc.) au fost identificate, de-a lungul timpului, vulnerabilităţi care conduc în special la preluarea controlului şi la diverse acţiuni mai mult sau mai puţin distructive. Ţinta preferată este reprezentată de browserele Web (*Internet Explorer, Firefox, Chrome, Opera* etc.), acestea fiind principala "poartă" de acces pentru elementele maliţioase. Principala vulnerabilitate a aplicaţiilor este considerată a fi utilizarea de configuraţii, date de identificare şi administrare implicite, fără a personaliza şi realiza propriul sistem de lucru şi administrare.

De-a lungul timpului, au fost identificate vulnerabilităţi afectând mai toate categoriile reprezentative de aplicaţii utilizate în Internet, cum ar fi: acces la conţinut media (*Adobe Flash*), transmitere mesaje instant (*Yahoo Messenger, AOL Instant Messenger, MSN Messenger, Jabber, Trillian, Skype, Google Talk* sau *IRC*) şi chiar aplicaţiile antivirus (*AhnLab, Avast!, AVIRA, BitDefender, ClamAV, Computer Associates, F-Secure, Kaspersky, Mcafee, Sophos, Symantec, Trend Micro* sau *ZoneAlarm*), majoritatea exploatând slăbiciuni ale tehnologiei sau lipsa unor elemente de securitate în procesul de proiectare.

VULNERABILITĂŢI LA NIVELUL BAZELOR DE DATE

Bazele de date constituie una dintre cele mai importante componente ale unui sistem informatic, aici fiind păstrate şi prelucrate automat diverse informaţii. Datele reprezintă baza sistemelor de gestiune a documentelor şi evidenţelor contabile, sistemelor de colectare a taxelor şi impozitelor, sistemelor de facturare şi management al conţinutului (*Content Management Systems* - CMS), a sistemelor de gestiune a proceselor tehnologice industriale etc.

De asemenea, în procesul de evaluare a riscurilor trebuie luată în considerare şi fiabilitatea sistemelor, a sistemelor de gestiune a bazelor de date (SGBD) sau a mijloacelor tehnice care pot fi supuse unor factori de mediu, cum ar fi: incendiile, calamităţile naturale etc.

2.4.4. Programe dăunătoare (malware)

Termenul **malware** (***Mal****icious* ***Software***) defineşte, în general, orice program cu efecte dăunătoare asupra sistemului de calcul, cum ar fi:

- preluarea totală sau parţială a controlului asupra calculatorului;
- spionarea activităţii (parole, informaţii transmise, adrese vizitate);
- sustragerea unor informaţii confidenţiale (conturi bancare, documente);
- producerea unor daune sau situaţii neplăcute (blocarea sistemului, îngreunarea lucrului).

Principalele acţiuni realizate de un program de tip malware sunt:

- multiplicare prin sistemul de fişiere al calculatorului sau propagare în reţeaua locală fără cunoştinţa utilizatorului;
- permite preluarea controlului asupra calculatorului de către o persoană neautorizată;
- furnizează informaţii sau trimite fişiere la o anumită destinaţie fără ştirea utilizatorului;
- întrerupe activitatea normală a sistemului.

Modalităţile de multiplicare a programelor malware sunt diverse şi exploatează atât vulnerabilităţi software ale sistemelor de operare sau ale programelor utilitare folosite, cât şi credulitatea utilizatorilor, dar şi lipsa unei informări în ceea ce priveşte posibilele pericole atunci când navighează pe Internet sau îşi citesc poşta electronică. Propagarea programelor malware se poate realiza prin:

- utilizarea serviciului de poştă electronică;
- propriul motor SMTP, codat într-o librărie API inclusă în program;
- clientul e-mail utilizat (de obicei Microsoft Outlook sau Outlook Express);
- funcţia MAPI implementată în Windows (programul malware identifică adrese e-mail stocate în Address Book sau în alte fişiere de pe disc şi se auto-trimite folosind mecanismele prezentate mai sus);
- fişiere stocate pe unităţi fixe şi mobile partajate, infectând întreaga reţea locală;
- programe de mesagerie instant sau IRC, prin transmiterea unor link-uri către site-uri infectate. Paginile Web infectează apoi calculatoarele utilizatorilor care accesează acele site-uri.
- programe de partajare fişiere (Peer-to-Peer), prin auto-copierea în folderele partajate, ajungând astfel pe calculatoarele altor utilizatori care descarcă respectivele foldere.

Principalele categorii de programe de tip malware sunt:

- viruşii informatici (*Computer Viruses*); un program cu efect distructiv, proiectat pentru a infecta sistemele de calcul prin multiplicare şi constă într-o secvenţă de cod ataşată unui fişier (de obicei executabil) care se activează în momentul în care acest fişier este executat (în caz contrar, virusul este inactiv, dar "în aşteptare");
- viermii (*Worms*); o sub-clasă a viruşilor, cu mecanisme proprii de răspândire, fără a fi necesară acţiunea utilizatorului (executarea unui program infectat de

exemplu), fiind aplicaţii independente care au capacitatea de a infecta un computer la nivelul sistemului de operare, de a se auto-multiplica şi auto-propaga prin reţeaua locală;

- troienii (*Trojans*) - programe malware mascate în interiorul unor programe aparent utile şi bine intenţionate, provenite din surse ilegitime de software.

ALTE TIPURI DE MALWARE

Alte tipuri de programe din categoria malware sunt:

- **Downloader/Dropper** - aplicaţie care instalează în sistem un cod maliţios provenit fie din programe, fie de pe Internet.
- **Security Software Disabler** - program care dezactivează alte programe de securitate instalate pe calculator (anti-virus, anti-malware).
- **Trojan Server** (proxy, FTP, IRC, e-mail, HTTP/HTTPS) - tip de troian care transformă maşina victimă într-un server, fără ştirea utilizatorului. Atacatorul infectează o maşină şi o poate utiliza atât pentru a răspândi programul malware, cât şi pentru a ataca alte sisteme (atacatorul real îşi ascunde identitatea în spatele maşinii infectate).
- **Clicker, Startpage, Link Injector** - programe care acţionează la nivelul browserului Web (în special Internet Explorer) şi modifică diverse setări ale acestuia: deschid pagini Web fără consimţământul utilizatorului, schimbă diverşi parametrii, suprascriu link-urile cu adrese ale unor site-uri afiliate sau pot instala un cod maliţios.
- **Dialer** - formează automat anumite numere de telefon (în general cu supratarxă) şi se conectează prin modem-ul ataşat computerului.
- **Rootkit** - troian care înlocuieşte fişierele vitale ale unui sistem de operare, ceea ce permite ascunderea unor eventuale programe maliţioase instalate în sistem. Programele tip rootkit au fost iniţial create în scopuri legitime (pentru administrarea şi controlul la distanţă al unui calculator), însă acum sunt recunoscute şi pentru modul lor maliţios de utilizare.

SPYWARE

Spyware (Spy Soft**ware)** este un tip de aplicaţie care se instalează automat, fără acceptul utilizatorului şi transmite la o anumită destinaţie diverse informaţii, mai mult sau mai puţin confidenţiale, ori de câte ori utilizatorul se conectează la Internet.

ADWARE

Adware (***Ad**vertising-Supported Soft**ware***) este la origine o aplicaţie care afişează reclame pe calculatorul utilizatorului, dar care poate conţine şi o componentă de spyware prin care se transmit informaţii despre activitatea utilizatorului. Practic, un program adware poate veni ca modul inclus într-o aplicaţie mai mare sau ca program de sine stătător, rolul său declarat fiind acela de a scădea costurile programului principal oferit, prin afişarea unor reclame.

Diferenţa faţă de programele spyware este că utilizatorul a fost informat de existenţa unui astfel de modul şi a fost de acord cu condiţiile de utilizare ale acestuia şi cu instalarea lui, odată cu programul principal.

Malware prin telefonia mobilă

În ultimul timp, datorită dezvoltării fără precedent pe care a înregistrat-o telefonia mobilă, a apărut o nouă formă de aplicaţii de tip malware care atacă dispozitivele portabile (PDA, telefoane mobile, tablete PC). Primul troian pentru Palm OS a apărut în septembrie 2000, iar primul virus pentru Pocket PC în iulie 2004. Pentru telefoanele smartphone care rulează sistemul de operare Symbian, primul virus a apărut în iunie 2004. Transmiterea se face prin MMS (*Multimedia Messaging Service*) - de exemplu viermele Commwarrior - sau prin conexiunea Bluetooth.

E-MAIL MALIŢIOS

Programele malware prezentate anterior se pot propaga atât direct de la un utilizator la altul, prin reţeaua locală sau prin descărcare de pe Internet, cât şi prin e-mail, unul dintre cele mai solicitate servicii. În continuare, vor fi prezentate câteva ameninţări fără impact direct şi imediat asupra utilizatorului, ameninţări localizate în general (dar nu numai) la nivelul serviciului de poştă electronică.

Formele nocive ale unui e-mail maliţios prezentate mai jos se bazează pe înşelarea utilizatorului neinformat, încercându-se obţinerea unor informaţii (mai mult sau mai puţin confidenţiale) nu prin furt, ci prin înşelare, victima transmiţând de bună voie aceste date.

Spam şi Scam

Termenul *spam* se referă la mesaje e-mail (de obicei cu conţinut comercial) trimise în bloc unui număr mare de utilizatori, fără ca aceştia să le fi solicitat. Pe lângă poştă electronică, autorii mesajelor spam dezvoltă noi căi de atac folosind, de exemplu, mesageria instant (*Messaging Spam* sau *spim*), blog-urile Web sau mesajele SMS pe telefonul mobil. Scopul mesajelor spam este în general informativ (reclame), urmărindu-se:

- promovarea în masă a unor mărci, servicii, evenimente sau concepte;
- vânzarea unor produse sau prestarea unor servicii.

O variantă a spam-ului, cu posibile pagube (materiale, morale etc.), o reprezintă ***scam***-ul. Un e-mail scam (pentru că de obicei se propagă prin e-mail, însă nu e singura modalitate de răspândire) reprezintă o încercare de fraudare a unei persoane prin câştigarea încrederii ei. Câteva din consecinţele fenomenului spam/scam sunt:

- costuri mai mari pentru furnizorii de servicii în ceea ce priveşte timpul şi viteza de procesare a mesajelor e-mail, lăţimea de bandă, suprasolicitarea serverelor;
- creşterea volumului de date stocate şi transferate;
- necesitatea implementării unor scheme de filtrare a mesajelor nedorite;
- pagube materiale dacă utilizatorul dă curs cererilor din mesajele phishing.

HOAX ŞI CHAIN LETTERS

Hoax reprezintă o încercare intenţionată de a înşela publicul, de a-l face să creadă că o anumită idee sau întâmplare neobişnuită este reală, când autorul ştie că este falsă. Iniţial, mediul de propagare a acestor hoax-uri a fost mass-media (ziare, radio, televiziune), însă mediul electronic oferă orizonturi mai largi acestui tip de activitate. Aceste mesaje inutile pot colecta o mulţime de adrese e-mail, folosite ulterior de autorii de spam pentru trimiterea de mesaje nesolicitate. Ele nu provoacă altceva decât risipă de timp şi pierderi de bani (dacă utilizatorul răspunde unor eventuale solicitări financiare).

Chain letters (scrisori în lanţ) sunt mesaje nedorite care conţin, de obicei, fie text simplu, fie apeluri emoţionante, cu impact direct asupra sensibilităţii utilizatorului. Aceste scrisori solicită retrimiterea mesajului la cât mai mulţi destinatari, eventual după îndeplinirea unor condiţii (trimiterea unei sume de bani, exprimarea unei dorinţe etc.).

Phishing - Conceptul de phishing înglobează mai multe tehnici, cu scopul final de a sustrage date confidenţiale. Un termen corelat este **brand spoofing** (imitarea imaginii). Cele două noţiuni descriu o serie de metode elaborate prin care clienţii diverselor companii (în special bancare) sunt înşelaţi să-şi divulge anumite date confidenţiale (de obicei numărul cardului bancar).

Mecanismul presupune realizarea unor pagini Web contrafăcute, care imită într-o măsură cât mai mare paginile legitime ale furnizorilor de servicii (pentru a inspira încredere victimelor). Folosind diverse metode (în general adrese e-mail colectate sau cumpărate) şi un mod de acţiune cu impact emoţional, este lansată invitaţia de a completa sau actualiza unele informaţii confidenţiale folosind site-ul clonă.

2.4.5. Atacuri cibernetice de impact asupra instituţiilor publice

În general domeniul securităţii tratează un incident de securitate ca fiind o activitate care implică încălcarea elementelor fundamentale ale securităţii, iar în domeniul tehnologiei informaţiei poate fi asociat cu orice activitate desfăşurată în cadrul unui sistem.

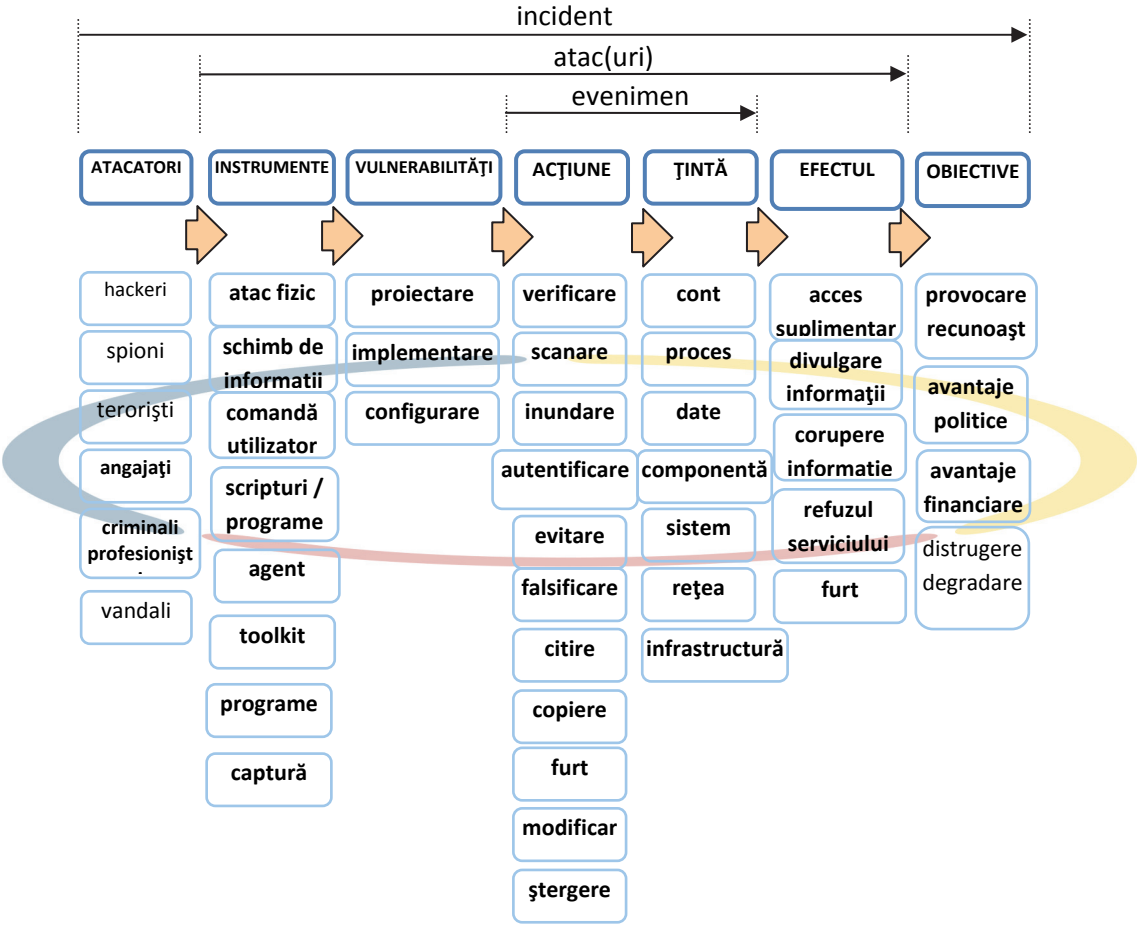


Fig. 4. 7. Clasificarea incidentelor de securitate informatică (conform CERT US)

Un cadru general de clasificare a incidentelor de securitate din domeniul tehnologiei informaţiei reprezintă o modalitate eficientă de gestionare a acestora şi permite strângerea de informaţii relevante despre incidentele cu impact major asupra sistemelor. Ierarhizarea incidentelor şi clasificarea pe domenii de interes

permit, în primul rând, o reacţie mai rapidă la incidente, precum şi o posibilitate de analiză elaborată.
Un model de clasificare generală a incidentelor de securitate este modelul dezvoltat de *Sandia National Laboratories* şi adoptat de CERT US ca model standard de organizare în raportarea incidentelor informatice şi dezvoltarea unei baze de date a acestora.
Un aspect important este reprezentat de faptul că nu toate evenimentele posibile (combinaţiile acţiune - ţintă) descrise în Figura 4.7. se realizează.
De exemplu, acţiunea de autentificare este, în general, asociată cu un cont sau un proces şi nu cu o ţintă diferită precum datele sau componentele. Alte exemple se referă la citire şi copiere (care au în general ca ţintă datele), inundarea (*flood*) care este, în general, îndreptată asupra unui cont, proces sau sistem sau furtul care are ca ţintă, în general, datele, o componentă sau un sistem de calcul.

Modul de relaţionare între evenimente, atacuri şi incidente, sugerează că prevenirea atingerii obiectivelor de către atacatori poate fi realizată prin faptul că aceştia nu pot parcurge complet toate etapele asociate procesului de desfăşurare a unui incident informatic.

De exemplu, pot fi realizate verificări periodice (controale) asupra unui sistem cu privire la noi modalităţi şi mijloace de atac, corectarea vulnerabilităţilor, întărirea politicii de control al accesului, criptarea fişierelor şi iniţierea unui program educaţional pentru angajaţi, în vederea asigurării protecţiei datelor personale şi a activelor din domeniul IT.

Combinaţia oferită de multitudinea de vulnerabilităţi, diversitatea tehnologică, zona politică şi socială dintre diverse state au dezvoltat un nou domeniu, cel al *infrastructurilor critice*. Deoarece statele sunt tot mai dependente de funcţionarea sistemelor de comunicaţii (reţele, servicii, aplicaţii), infrastructurile critice reprezintă acele sisteme absolut esenţiale pentru buna funcţionare a unei societăţi în momentul producerii unui dezastru (natural, social etc.).

Un număr tot mai mare de ţări consideră că securitatea cibernetică este una dintre cele mai importante probleme de securitate. Astfel, la nivelul statelor s-a dezvoltat o nouă clasificare ce are la bază nivelul de atac şi pe cel al intenţiilor:

- activism clasic în spaţiul virtual (*hacktivism*);
- criminalitate cibernetică (*cyber crime*);
- spionaj cibernetic (*cyber espionage*);
- sabotaj cibernetic (*cyber sabotage*);
- război cibernetic (*cyber warfare*);
- terorism cibernetic (*cyber terrorism*).

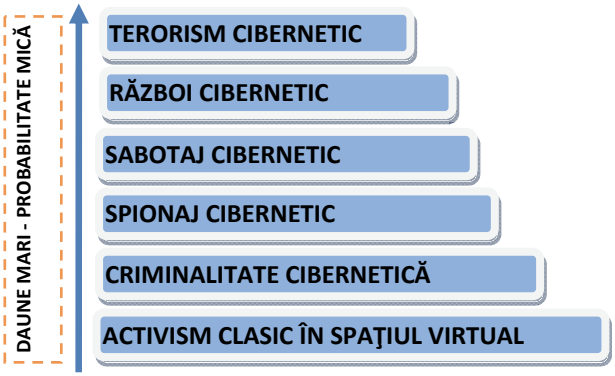


Fig. 4. 8. Tipuri de acţiuni ilegale în mediul virtual

ATAC INFORMATIC - definiţie, clasificare

Dezvoltarea reţelelor şi tehnologiilor a permis o extindere rapidă a mediului Internet, fără a lua în calcul posibilele ameninţări şi vulnerabilităţi ale sistemelor informatice şi ale tehnologiilor. Este recunoscut faptul că datele şi informaţiile pot fi pierdute, furate, modificate, utilizate în mod necorespunzător şi neautorizat, situaţii care conduc la pierderea integrităţii, confidenţialităţii şi disponibilităţii, elemente de bază ale asigurării securităţii.

O **resursă** (din punct de vedere fizic sau logic), numită un activ, poate avea una sau mai multe vulnerabilităţi care pot fi exploatate de către un agent de ameninţare într-o acţiune de compromitere. Potenţialul acţiunii poate compromite proprietăţile confidenţialităţii, integrităţii sau ale disponibilităţii resurselor organizaţiei şi ale altor părţi implicate (clienţi, furnizori).

Pe lângă vulnerabilităţile clasice din domeniul tehnologiei informaţiei, o formă importantă de incident informatic este **atacul informatic**, acesta reprezentând materializarea unei ameninţări, o acţiune dăunătoare cu scopul de a găsi şi exploata o vulnerabilitate a sistemului. Creşterea exponenţială a incidentelor având ca sursă atacul informatic, involuntar sau provocat, a condus la dezvoltarea unor politici de securitate şi strategii de combatere, astfel încât vulnerabilităţile sistemelor şi reţelelor să fie minimizate.

ATACURI LA NIVELUL REŢELELOR DE COMUNICAŢII

Cele mai cunoscute atacuri la nivelul reţelelor de comunicaţii şi al sistemelor de operare, cu efecte catastrofale la nivelul aplicaţiilor, serviciilor şi datelor, sunt atacurile de tip *refuzul serviciilor* (DoS), în care o entitate poate suspenda toate serviciile direcţionate la o destinaţie particulară.

O formă a acestui atac este reprezentată de supraîncărcarea reţelei cu pachete pentru blocarea sistemului sau scăderea performanţelor. Scopul acestui atac este constituit de generarea şi transmiterea unui volum semnificativ de date (sau solicitări) spre un anumit sistem de calcul, care are ca efect blocarea sau indisponibilizarea acestuia. Pentru ca atacul să reuşească este, însă, necesar ca atacatorul să dispună de o conexiune mai rapidă (lăţime de bandă mai mare) decât cea a sistemului de calcul vizat.

Atacurile de tip refuzul serviciilor sunt clasificate în funcţie de mai mulţi factori dintre care cei mai importanţi sunt: gradul de automatizare, tipul de vulnerabilitate exploatată, modul de efectuare a atacului, mecanismele de comunicare utilizate de atacatori. În general, atacurile de tip refuzul serviciilor sunt împărţite în 5 mari categorii, după resursa pe care o compromit (Figura 4.9.).

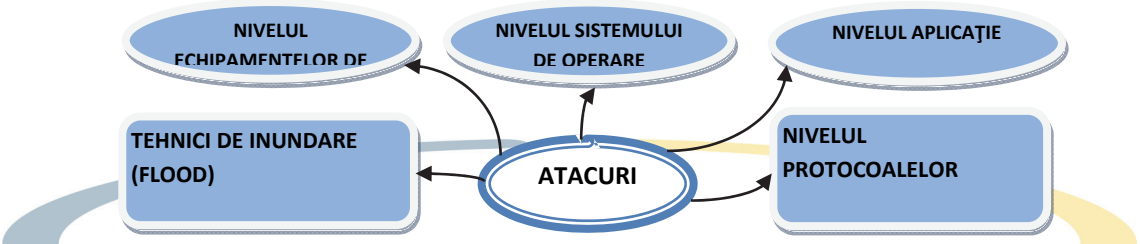


Fig. 4.9. Principalele categorii de atacuri de tip refuzul serviciului (DoS)

După modul cum poate fi efectuat, atacurile de tip DoS pot fi:

Atacuri DoS directe

Atacurile de tip DoS, directe, reprezintă cea mai simplă formă de efectuare a unui atac prin care un atacator transmite cu o frecvenţă foarte mare către ţintă, o serie de cereri de serviciu astfel încât, pentru a răspunde, ţinta utilizează toate resursele de bază (memorie, bandă) pe care le are la dispoziţie, ceea ce conduce la o blocare a serviciului pentru utilizatorii legitimi ai serviciilor sistemului de calcul "ţintă".

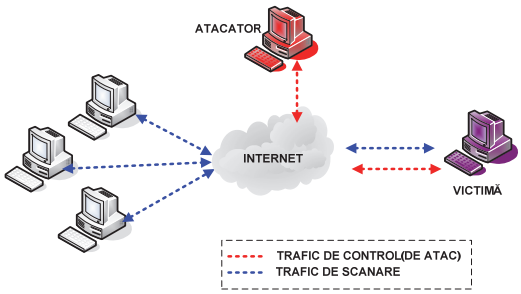


Fig. 4. 10. Model de atac DoS direct

Atacuri DoS distribuite (DDoS)

Atacul de tip DoS distribuit (DDoS) este un atac coordonat asupra disponibilităţii serviciilor oferite de resursele unui sistem "ţintă", lansat indirect prin intermediul mai multor sisteme compromise numite "agenţi". Un program "*zombie*" este instalat "pe ascuns" de către atacator pe calculatoarele agenţi, care pot fi localizate oriunde în spaţiul Internet. Atacatorul activează sistemele "zombie" pentru a ataca simultan "ţinta", mascând adevărata origine a atacului.

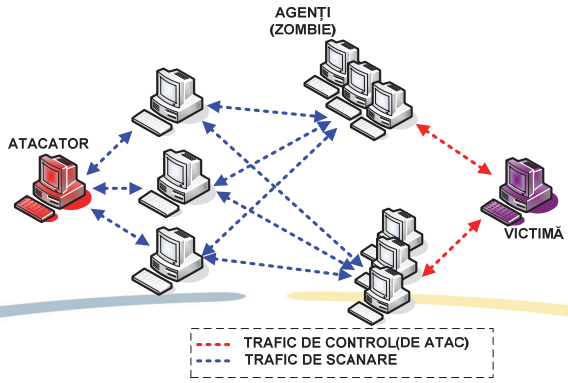


Fig. 4. 11. Model de atac DDoS

Modelul de atac DDoS prin utilizarea de sisteme intermediare de tip "agenţi" oferă atacatorului posibilitatea de a realiza un atac pe scară largă şi cu efecte distructive mult mai mari, operaţiile de identificare a atacatorului iniţial fiind mult mai dificile. După tipul resursei exploatate şi, în funcţie de gradul de elaborare, atacurile tip refuzul serviciilor pot fi clasificate după cum urmează:

- atacuri asupra echipamentelor de reţea;
- atacuri asupra sistemelor de operare:
  - atacuri la nivelul protocoalelor prin modificarea de pachete;
  - atacuri la nivelul sistemului de operare prin exploatarea vulnerabilităţilor locale.

ATACURI LA NIVELUL APLICAŢIILOR ŞI SERVICIILOR

Datorită dezvoltării fără precedent a mediului Internet, prin posibilităţile de conectare rapidă atât între diferite părţi ale unei organizaţii aflate la mare distanţă, cât şi cu clienţii sau potenţialii clienţi, a apărut necesitatea implementării unor aplicaţii complexe şi expunerea în mediul online a datelor şi informaţiilor utilizate în mod uzual în desfăşurarea activităţii. Scopul principal al unui atac la nivelul aplicaţiilor şi serviciilor este reprezentat de preluarea controlului asupra serviciilor

sau de accesul neautorizat la date şi informaţii, prin exploatarea unor vulnerabilităţi atât ale sistemului de operare, cât şi ale aplicaţiilor respective.

Securitatea aplicaţiilor reprezintă, în acest moment, una dintre cele mai mari provocări la adresa securităţii, în special pe Web, prin multitudinea posibilităţilor de efectuare a atacurilor, exploatarea vulnerabilităţilor limbajelor de programare şi ale sistemelor de gestionare a bazelor de date.

Atacurile asupra aplicaţiilor Web sunt atacuri de reţea îndreptate împotriva aplicaţiilor care rulează prin intermediul unui browser. De cele mai multe ori, acestea sunt conectate la o bază de date sau conţin programe sau scripturi care controlează aplicaţia Web. Atacurile asupra aplicaţiilor Web sunt diferite de atacurile care vizează aplicaţiile obişnuite, deoarece aplicaţiile Web se bazează şi pe utilizarea pe scară largă a protocoalelor de reţea. În conformitate cu *OWASP* (*Open Web Application Security Project*), cele mai reprezentative tipuri de atacuri asupra aplicaţiilor sunt:

- **Injectare (*Injection*)** - programele Web generate dinamic folosesc informaţii stocate în baze de date. Afişarea acestor date se realizează prin limbaje specifice de interogare, unul dintre cele mai folosite astfel de limbaje fiind SQL (*Structured Query Language*). *SQL Injections* reprezintă un tip de vulnerabilitate frecvent întâlnită în aplicaţiile din Internet care folosesc baze de date şi constă în posibilitatea ca interogările SQL să poată fi modificate extern. *Direct SQL Command Injection* este o tehnică prin care un atacator creează sau modifică o interogare SQL existentă pentru a afla informaţii confidenţiale, pentru a suprascrie informaţii sau chiar pentru a crea noi administratori (*superusers*). Atacul se realizează prin introducerea unor comenzi SQL în casetele de preluare a datelor din formularele Web.
- **Cross-Site Scripting (*XSS*)** - este una dintre cele mai comune vulnerabilităţi prezentă la aplicaţiile Web şi implică încorporarea unui script în cadrul acestora, cu un scop rău intenţionat. De exemplu, scriptul poate solicita altor utilizatori care navighează în acea aplicaţie Web numele de utilizator şi parola. Alte ameninţări specifice acestui tip de atac includ deturnarea sesiunii sau a conturilor utilizatorilor, preluarea şi intoxicarea cookie-urilor etc. Există două tipuri de vulnerabilităţi XSS:
    - XSS nepersistent (cunoscut şi ca XSS reflectat sau XSS temporar) - este un XSS ce afectează utilizatorul doar dacă acesta accesează pagina infectată, fiind cel mai întâlnit tip de vulnerabilitate;
    - XSS persistent (XSS permanent) este un XSS memorat de către o aplicaţie Web. Acest tip de XSS este cel mai periculos deoarece codul este introdus o dată şi afectează utilizatorii cât timp scriptul rămâne pe pagină.

ATACURI ASUPRA BAZELOR DE DATE

Aplicaţiile care au ca suport bazele de date au devenit componente esenţiale ale sistemelor complexe. Modelele tradiţionale de securitate implementează sisteme de control prin izolarea componentelor de bază ale sistemului şi concentrarea eforturilor de securitate împotriva ameninţărilor specifice îndreptate asupra sistemelor de calcul sau a componentelor software.

Securitatea bazelor de date urmează, în general, modelele tradiţionale prin utilizarea unor sisteme interdependente, care se bazează unul pe altul pentru o funcţionalitate corectă. Nivelul ridicat de încredere între cele două sisteme dezvoltă o extindere a posibilităţilor de ameninţare.

Bazele de date sunt adesea conectate la alte baze de date sau alte aplicaţii Web, aplicaţii situate în cadrul aceleiaşi reţele. Practic, aplicaţiile care folosesc colecţii organizate de date au dezvoltate baze de date asociate. La nivelul aplicaţiilor pot exista unele vulnerabilităţi care permit exploatarea directă prin utilizarea maliţioasă a instrucţiunilor SQL (atacuri *XSS* sau *SQL Injection*).

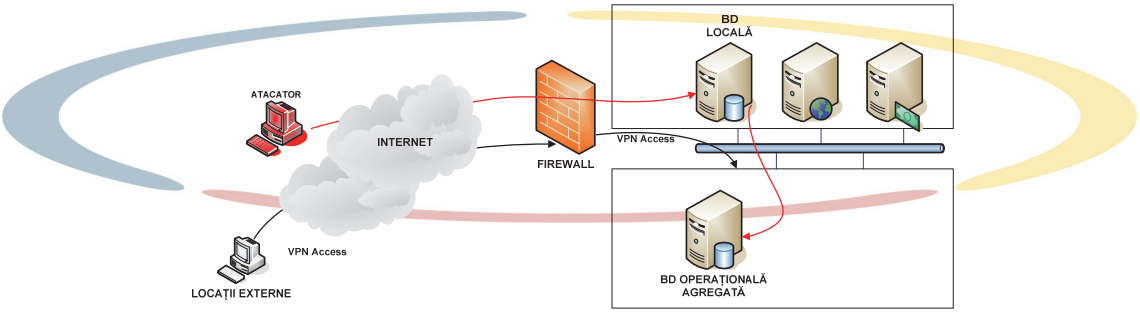


Fig. 4.12. Model de conectivitate între bazele de date

Figura 4.12. prezintă un exemplu de conectivitate deschisă între bazele de date ale unei organizaţii: o cale de comunicare între servere, de care un atacator ar putea să abuzeze pentru a avea acces în reţea. Injectarea de informaţii eronate într-o bază de date critică poate avea efecte majore, mai ales pentru domeniile în care integritatea şi disponibilitatea datelor reprezintă atribute esenţiale în procesul operaţional de luare a deciziilor.

Prin operaţiuni de replicare şi sincronizare între bazele de date se declanşează o propagare a datelor corupte, care poate avea un impact sever asupra proceselor operaţionale şi poate conduce la blocarea activităţii. Sisteme de tip *e-commerce* (*banking*) sunt cele mai afectate de injectarea SQL, în comparaţie cu alte domenii de utilizare a bazelor de date, deoarece sunt dependente critic de disponibilitatea şi integritatea datelor.

Importanţa datelor şi informaţiilor conţinute în baze de date face din acestea o ţintă preferată pentru orice atacator. Atunci când bazele de date conţin informaţii despre stadiul unor acţiuni, date financiare, ştiinţifice, militare etc. şi sunt accesate prin intermediul unor aplicaţii, atacatorii pot exploata canalul de comunicare între cele două reţele şi pot evita mecanismele de securitate utilizate în protecţia bazelor de date. Mai mult decât atât, compromiterea securităţii unei baze de date oferă unui atacator resurse suplimentare care pot fi utilizate atât pentru efectuarea de acţiuni de recunoaştere, cât şi la executarea de cod maliţios destinat altor baze de date.

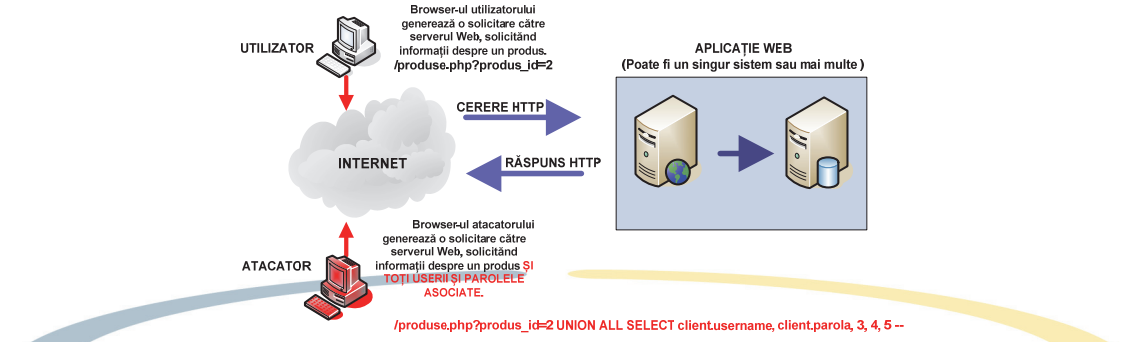


Fig. 4. 13. Model de atac SQL Injection

Având în vedere dependenţa din ce în ce mai mare a sistemelor privind capacitatea de stocare, acurateţea şi accesibilitatea datelor din sistem, precum şi extinderea domeniilor de utilizare a bazelor de date SQL, este necesară dezvoltarea unor modele standardizate de combatere a injectării SQL.

ATACURI LA NIVELUL SISTEMULUI DE OPERARE

RFI *(Remote File Inclusion)* este un tip de vulnerabilitate destul de întâlnită, care constă în mutarea unui fişier de pe serverul Web atacat pe alt server, prin utilizarea unui script. Vulnerabilitatea apare când nu se verifică integral datele de intrare, ceea ce poate conduce, în cel mai bun caz, la afişarea conţinutului fişierului inclus. De obicei, această vulnerabilitate are ca urmări:

- executare cod pe serverul Web;
- executare cod pe maşina clientului (de exemplu, coduri Javascript care pot duce la atacuri de tip XSS);
- Denial-of-Service;
- furt sau modificare a datelor.

Validarea incompletă a unor variabile externe (de exemplu, $_GET, $_POST, $_COOKIE din limbajul PHP) poate permite transmiterea ca parametru a unui fişier extern care injectează astfel cod maliţios. Un utilizator poate folosi o sintaxă de tipul:

http://example.com/script.php?pagina=pag1.php

Un atacator care exploatează o vulnerabilitate de tip RFI poate apela:

http://example.com/script.php?pagina=http://site.com/script.txt

Metodele de prevenire a Remote File Inclusion constau în:

- filtrarea şirurilor "http://" şi "ftp://";
- includerea unor fişiere prin folosirea comenzilor de tip switch, care conţin o listă explicită cu paginile care pot fi incluse.

Dezvoltarea fără precedent a aplicaţiilor Web şi extinderea utilizării bazelor de date în mediul Internet au condus la apariţia unor multiple tipuri de vulnerabilităţi, toate acestea exploatând în special lipsa unor minime configurări de securitate la nivelul sistemelor din cadrul aplicaţiei. Un clasament al celor mai periculoase vulnerabilităţi de securitate pentru aplicaţiile Web în anul 2010, conform OWASP (*Open Web Application Security Project*) este prezentat în tabelul următor.

Tabel .... Top 10 vulnerabilităţi Web în 2010

Loc	Tip vulnerabilitate Web
1	Injection
2	Cross-Site Scripting (XSS)
3	Broken Authentication and Session Management
4	Insecure Direct Object References
5	Cross-Site Request Forgery (CSRF)
6	Security Misconfiguration
7	Insecure Cryptographic Storage
8	Failure to Restrict URL Access
9	Insufficient Transport Layer Protection
10	Unvalidated Redirects and Forwards

3. Content Management Systems

3.1. Introducere în CMS

3.1.1. Noțiunea de Content Management System

Domeniul CMS (Content Management System - Sistem de Administrare a Conţinutului) este relativ nou şi s-a dezvoltat ca un mecanism care se adresează problemelor de care se lovesc instituţiile pentru a-şi menţine prezenţa pe web.

Confruntându-se cu informaţii şi materiale neactualizate, un design si o navigaţie cu un control deficitar, o lipsă a supervizării de către o autoritate în domeniu (a unui webmaster competent), instituţiile au recurs la dezvoltarea de procese şi instrumente customizate pentru a rezolva această situaţie dificilă.

În trecut, web-ul era caracterizat mai degrabă de o abordare mai complexă, "manuală" în privinţa menţinerii, dar în ziua de azi, web-ul se axează mai mult pe o întreţinere "automată", iar Content Management System (CMS) constituie instrumentul major în această automatizare.

Tranziția la societatea informaţională implică creșterea volumului de informaţii şi a nevoilor de comunicare, iar problema managementului eficient al conţinutului devine tot mai importantă. Sistemele de management al conţinutului (CMS) facilitează elaborarea şi mentenanţa site-urilor Web, indiferent de complexitatea acestora.

Un CMS este un sistem software de management al conţinutului care este destinat celor ce vor să creeze şi să administreze site-uri web. Scopul folosirii unui CMS este acela de a elimina intervenţia programatorilor în editarea sau administrarea site-urilor. Content (conţinutul) reprezintă, în esenţă, orice tip sau unitate de informaţie digitală folosită pentru a popula o pagină de web sau alte medii asemănătoare. Conţinutul poate fi text, imagine grafică, video, sunet. Cu alte cuvinte, este tot ceea ce poate fi publicat pe Internet, intranet şi/sau extranet.

Content Management (administrarea conţinutului) contribuie la managementul efectiv al diverselor tipuri de conţinut prin combinarea de reguli, procese şi fluxuri de lucru, în aşa fel încât webmasterii centralizaţi şi editorii web descentralizaţi să poată crea, edita, administra şi publica tot conţinutul unei pagini de web, în conformitate cu un anumit context sau cu anumite cerinţe.

Content Management reprezintă o strategie şi o tehnologie de stocare şi de indexare a informaţiei din şi despre media digitală şi analogică. Un produs de Web Content Management permite oamenilor nu numai să preia controlul asupra conţinutului web, ci şi să-şi atingă obiectivele afacerii prin colectarea, administrarea eficientă şi distribuirea informaţiei în publicaţiile targetate.

Noțiunea de CMS:

- se intersectează cu cea a sistemelor de gestiune a documentelor, sistemelor de gestiune a cunoştinţelor, sistemelor de integrare a aplicaţiilor industriale, sistemelor e-commerce şi portalurilor.

Termenul de CMS:

- este folosit pentru descrierea softului care asistă oamenii în crearea, managementul, transmiterea şi navigarea conţinutului paginilor web.

Sistemul de management al conținutului:

- este un produs software implementat ca o aplicaţie web şi este folosit la crearea şi utilizarea unui conţinut HTML;
- se utilizează pentru a putea controla o gamă largă şi dinamică de materiale web (documente HTML precum şi imaginile asociate acestora);
- facilitează crearea conţinutului, controlarea lui, editarea şi multe alte funcţii web de întreţinere.

De obicei, produsul software furnizează instrumente pe care utilizatorii, deloc cunoscători ai limbajelor de programare, le pot folosi pentru crearea şi întreţinerea conţinutului, aceasta realizându-se cu o oarecare uşurinţă în practică.

Cele mai multe sisteme utilizează o bază de date pentru stocarea conţinuturilor, iar învelişul prezentării poate expune aceste conţinuturi vizitatorilor fideli ai site-ului, la baza acestui procedeu stând un set de template-uri. Crearea şi administrarea de conţinut se face, de obicei, printr-o aplicaţie web, însă un CMS poate fi modificat în felurite moduri.

Un CMS e diferit de alţi realizatori de web site-uri ca Microsoft FrontPage sau Macromedia Dreamweaver. Un CMS permite utilizatorilor să realizeze anumite schimbări asupra unui site dat, fără a fi nevoie de o pregătire tehnică specială, prealabilă. CMS-ul solicită, de obicei, un programator experimentat pentru a-l instala şi a-i adăuga diferite particularităţi, detalii, dar el este, în primul rând, o unealtă de întreţinere web ce se adresează utilizatorilor non-tehnici.

1. Caracteristici

Un CMS este un produs software implementat ca o aplicaţie web şi este folosit la crearea şi utilizarea unui conţinut HTML. Este utilizat pentru a putea controla o gamă largă, dinamică de materiale web (documente HTML şi imaginile asociate acestora). Un CMS facilitează controlul documentului, revizia, editarea şi inclusiv optimizarea timpului de realizare a lui. CMS-ul are următoarele proprietăţi-cheie care îl diferențiază de alte soluții software:

Template-uri automatizate

Crearea unor template-uri standardizare ce respectă o identitate vizuală unitară și care pot fi aplicate în mod automat unui conţinut nou, realizându-se astfel, o poziţie esenţială pentru a schimba, în mod nemijlocit, imaginea unui grup de conţinuturi ce aparţin unei sau mai multor instituții.

Conţinuturi uşor editabile

Separarea conținutului în raport cu prezentarea vizuală a site-ului, permite ca editarea şi administrarea să devină mult mai uşoare şi rapide. Cele mai multe soft-uri CMS includ instrumente de editare WYSIWYG (what you see is what you get), ceea ce face ca utilizatorii non-tehnici să poată crea, edita și vizualiza forma finală a conţinutului.

Usurința în dezvoltarea soluțiilor personalizate

Cele mai multe CMS-uri au conectori sau module (plugin) uşor instalabile, care permit extinderea funcţionalităţilor unui site.

Actualizarea continuă la cele mai recente standarde web

Soluţiile CMS active primesc update-uri regulate, care includ seturi noi de proprietăţi, păstrând astfel sistemul la un nivel ridicat, coincident standardelor web (exemplu HTML 5).

Administrare fluxuri de lucru

Fluxurile de lucru reprezintă procesul de creare a sarcinilor secvenţiale şi paralele ce trebuie îndeplinite în cadrul unui CMS. De exemplu, un realizator de conţinut formulează un text, dar nu îl publică pe website, până când responsabilul cu drepturile de publicare nu îl verifică, iar editorul-şef îl aprobă spre publicare.

Administrarea documentului

Soluţiile CMS pot să asigure o modalitate de supraveghere a ciclului de viaţă al unui document, începând de la momentul iniţial al realizării acestuia, continuând cu reviziile, publicarea, arhivarea, până la momentul final al distrugerii documentului. Un sistem de tip CMS permite actualizarea unui site în absenţa oricăror cunoştinţe privind tehnologiile Internet, direct de către utilizator – cel care iniţiază informaţia în cadrul firmei. Componentele majore ale unui editor de conţinut sunt:

a. interfaţa web;

b. sistemul de management al fluxului de documente.

Este important ca administratorul să poată aloca drepturi de acces distincte, în funcţie de diferitele funcţii îndeplinite de către utilizatori.

Sistemul CMS simplifică procesul de modificare și afisare a conținutului prin faptul că, odată textul aprobat, editorul îl poate afișa direct, fără acordul sau ajutorul webmasterului. Dintr-un singur click, prin intefața web, folosind, de cele mai multe ori, șabloane pentru eficientizare, conținutul este postat.

2. Principalele beneficii ale CMS-urilor:

- usurinţa în utilizare, atât pentru cel care publică,cât şi pentru cititor;
- informaţie de actualitate, consistentă şi de calitate;
- refolosirea conţinutului;
- crearea descentralizată a conţinutului, crearea şi transferul de documente;
- centralizarea fluxului de activitate, a procesului de aprobare şi a regulilor, precum şi atribuirea de roluri şi responsabilităţi pentru diferitele categorii de conţinut;
- publicarea conţinutului într-un mod unitar pentru a sprijini accesul la informaţii;
- posibilitatea contribuirii unui număr mare de persoane la conținut, prin împărţirea pe grupuri sau în funcție de rolul pe care îl îndeplineşte fiecare.

3.1.2. Tipuri de CMS

După domeniul de aplicare, sistemele de management al conţinutului pot fi împărţite în două mari categorii: WCMS (Web CMS) şi ECMS (Entreprise CMS). Următoarele abrevieri reprezintă subseturi ale ECMS:

- Enterprise Resource Planning Systems (sisteme ERP - sisteme de administrare a datelor corporatiste);
- Customer Relationship Management Systems (sisteme CRM - Sisteme de administrare şi menţinere a contractelor clientului);
- Document Management Systems (sisteme DMS - sisteme de administrare a documentelor);
- Human Resource Management Systems (sisteme HRM - sisteme de management a resurselor umane), şi multe altele.

În funcție de modul de dezvoltare, există două tipuri principale de CMS-uri:

- Software as a service (SaaS);
- CMS bazat pe web (Open source software).

În funcţie de tehnologiile în care sunt dezvoltate, CMS-urile sunt bazate pe Java, Microsoft ASP.NET, Perl, Phyton şi PHP.

Exemple de CMS bazate pe PHP: AdaptCMS Lite, ATutor, b2evolution, BEdita, CivicSpace, CMS Made Simple, Concrete5, Cotonti, Dotclear, **Drupal**, DynPG,

Exponent CMS, eZ Publish, **Joomla**, System, Midgard CMS, Nucleus CMS, Ocportal, papaya CMS, Phire CMS, PHP-Fusion, PHP-Nuke, PHPSlash, phpWarmSky, phpWebSite, pimcore, PivotX, Pixie (CMS), P, RavenNuke CMS, RenovatioCMS, Serendipity, SilverStripe, SPIP, TangoCMS,Textpattern, Tribiq, TYPO3, whCMS, WolfCMS, **WordPress**, Wuzly, Xaraya, XOOPS, Zext. Cele mai populare CMS-uri bazate pe PHP sunt: **Drupal, Joomla, WordPress.**

Tipuri de CMS bazate pe tehnologii			
Alfresco	ASP.NET	Blosxom	Django-cms
dotCMS	Composite C1	Bricolage	Merengue
DSpace	DotNetNuke Community Edition	Foswiki	MoinMoin
Fedora	Kentico CMS	Ikiwiki	Plone
Hippo CMS	mojoPortal	Movable Type	CKAN
jAPS	Orchard Project	TWiki	
Liferay	Umbraco	Scoop	
LogicalDOC		Slash	
Magnolia		WebGUI	
Nuxeo EP			
OpenCms			
OpenWGA			
VosaoCMS			
Yanel			
Java	**Microsoft**	**Perl**	**Python**

Drupal - este un software open-source de management al conținutului (CMS) scris în PHP și distribuit sub GNU General Public License. Este folosit de cel puțin 2,1 % din toate site-urile web la nivel mondial, de la blog-uri personale, la magazine online, site-uri guvernamentale, site-uri de prezentare sau chiar rețele sociale. Drupal poate fi folosit ca un site web de prezentare, cu un singur sau mulți useri, un blog, un forum pe internet sau un site de comunitate pentru conținutul generat de utilizator.

Joomla - este un sistem de management al conținutului Open Source, destinat publicării de conținut pe inter și intra net, prin intermediul bazelor de date SQL. Joomla! include funcționalități precum cache-ingul paginilor pentru îmbunătățirea performanțelor, RSS, știri de ultimă oră, bloguri, sondaje, căutare web și localizare internațională.

WordPress - este o platformă de tip Open Source care dispune de un sistem de șabloane scrise în limbajele HTML și CSS. Avantajele majore prezentate de WordPress sunt simplitatea și numeroasele plugin-uri create de către comunitate

care pot modifica funcționalitatea WordPress-ului, tranformându-l în aproape orice tip de site web. De asemenea, interfața poate fi schimbată foarte ușor cu ajutorul multitudinii de teme gratuite sau premium, cu doar un click.

Comparatie			
Funționalitate	**Drupal**	**Joomla**	**Wordpress**
Instalare	Relativ ușoară necesita cunostinte tehnice minime	Ușoară	Ușoaraă
Usurința în utilizare	Este mai mult destinat dezvoltatorilor web	Ușor de folosit	Ușor de folosit
Optimizare pentru motoarele de căutare			
Structura URL prietenoasă	Da	Da	Da
Taguri Meta	Standard SEO	Standard SEO	Standard SEO
Rescriere URL	Ușor de rescris	Ușor de rescris	Ușor de rescris
Harta Site	Modul suplimentar	Modul suplimentar	Modul suplimentar
Sindicalizare RSS	Da	Da	Da
Publicare multiuser			
Personalizare pe categorie, tipuri de conținut și structură organizațională	Da	Limitat	Da
Creare de pagini din front end	Da, interfață unitară	Da	Depinde de temă
Sistem de gestionare a sarcinilor	Simplu, extensibil	Simplu, extensibil	Simplu, extensibil
Aspect și design			
Teme	Suficient	Multitudine de teme	Un număr excelent de teme disponibile
Modificare aspect din interfața de administrare	Nu	Da	Da
Folosirea mai multor tipuri de aspect	Limitat	Da	Limitat
Alocarea modulelor de tip plugin din interfața de administrare	Da	Da	Da
Crearea și administrarea meniurilor din interfața backend	Da	Da	Da
Necesități sistem			
Costuri aproximative	Gratuit	Gratuit	Gratuit
Limbaj de programare	Php	Php	Php 4 si 5
Particularități			
Securitate	Bună	Bună	Bună
Bloguri	Da	Da	Da
Forumuri	Decent funcțional	Da, pe bază de plugin	Da, pe bază de plugin
Comerț electronic	Da	Da	Da, pe bază de plugin

Video	Da	Nu	Da, pe bază de plugin
Audio	Da	Da	Da, pe bază de plugin
Functionalități web 2.0	Da	Da	Da
Viteză	Rapid	Rapid	Rapid
Statistici integrate	Da	Da	Da
Abonare	Da	Nu	Da
Comentarii	Da	Da	da

3.1.3. Conceptul Open Source

Termenul „**sursă deschisă**” (en: *open source*) descrie practica de a produce sau dezvolta anumite produse finite, permițând accesul utilizatorilor să acționeze liber asupra procesului de producție sau dezvoltare. Unii specialiști definesc „sursa deschisă” ca un concept filozofic; alții consideră că este o metodologie pragmatică.

Fiind foarte frecvent utilizat în dezvoltarea de programe software, anumite tipuri de CMS se încadrează în această categorie (Wordpress, Joomla, Drupal). Mulți specialiști în elaborarea de programe au consideră că "open source" este o noțiune specifică acestei activități. În realitate, "open source" se poate aplica în orice domeniu în care se produce sau dezvoltă un produs. Există exemple de asemenea aplicații și în tehnologie, medicină, învățământ, cultură și altele, unde dezoltatorul sau inventatorul renunță practic la dreptul de a fi remunerat atunci când aplicația sa este utilizată chiar și în scopuri comerciale.

Wikipedia este un exemplu tipic de aplicație a principiului „cu sursă deschisă”, prin faptul că permite contribuția oricui la elaborarea sau îmbunătățirea produsului final, adică a enciclopediei. Mai mult decât atât, acoperind o gamă deosebit de largă de preocupări și nefiind limitată la o anumită specialitate, Wikipedia se adresează unui număr mult mai larg de utilizatori decât orice altă aplicație "open source" și poate atrage un număr mult mai mare de contributori decât alte aplicații. În plus, adresându-se unui public extrem de larg, Wikipedia, mai mult decât orice altă aplicație, poate permite unor nespecialiști să înțeleagă ce este și cum se aplică conceptul „sursei deschise”.

WordPress este, la rândul său, un proiect Open Source, ceea ce înseamnă că sunt mii de oameni din întreaga lume care lucrează la dezvoltarea lui (mai multe persoane decât lucrează la orice platformă comercială). Aceasta înseamnă, de asemenea, că atunci cand folosiți Wordpress sunteți liber să-l utilizați pentru orice, de la pagină personală la un site web din topul Fortune 500, fără a plăti o taxă de licență și a renunța la alte libertăți importante.

3.2. Administrarea platformei Wordpress

3.2.1. Instalarea și configurarea platformei

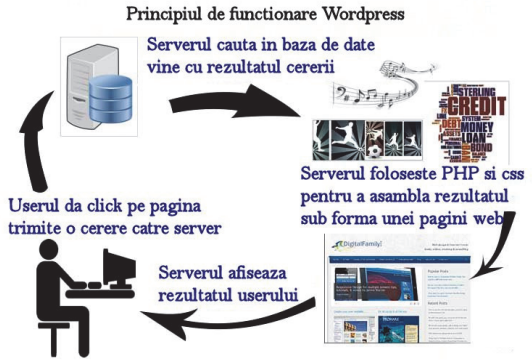
WordPress este binecunoscut pentru instalarea sa foarte uşoară. În majoritatea cazurilor, instalarea Wordpress este un proces foarte simplu şi durează mai puţin de cinci minute. Caracteristici ale WordPress-ului:

- Este perceput ca o aplicaţie de blogging, dar în realitate a devenit un adevărat CMS, un instrument de publicare în mediul online. Poate fi orice, de la blog, la o platformă avansată de comunicare, la un magazin virtual;
- Este gratuit şi open-source, are 10 ani de experienţă, fiind înbunătăţit de peste 80 de ori.
- Este poate cel mai utilizat CMS la nivel mondial, aproximativ 80% din paginile publicate pe web sunt publicate cu wordpress, iar 1 din 4 pagini nou create folosește această platformă.
- Câteva site-uri care rulează Wordpress sau derivate din acesta : realitatea.net, kmkz.ro, timesnewroman.ro, gandul.info.
- Este una dintre cele mai uşor de învăţat platforme de management al conţinutului.
- Este într-o continuă dezvoltare, având în spate o comunitate de 50.000 de dezvoltatori.
- Dispune de un editor propriu pentru previzualizarea paginilor înainte de publicare.
- Există o multitudine de unelte (plugin) gratuite şi uşor de instalat (dezvoltate deja de comunitate), care rezolvă marea majoritate a nevoilor utilizatorilor.
- Dispune de funcţii de automatizare completă, ce permit actualizarea, crearea de back-up şi programarea publicării.
- Este printre cele mai sigure platforme.

Principiul de funcţionare al Wordpress este următorul :

- Atunci când accesăm o pagină web, solicităm informaţii din baza de date, prin intermediul funcţiilor PHP şi le afisăm sub forma unei pagini HTML.
- Aspectul paginii HTML este dat de valorile prezente în fișierul CSS.
- Funcţiile PHP ale platformei sunt deja definite, ele trebuind doar apelate. (exemplu <?php wp_title ;?> va afişa titlul unei pagini)
- Aspectul vizual, este deja definit în fişierul CSS al plaformei, acesta putând fi modificat cu usurinţă.
- PHP este un acronim recursiv pentru PHP: Hypertext Preprocessor. Este un popular server-side, scripting, limbaj special conceput pentru integrarea cu

HTML şi este folosit (de multe ori în colaborare cu MySQL) în Content Management Systems şi alte aplicaţii web. Este disponibil pe mai multe platforme, inclusiv Windows, Unix / Linux şi Mac OS X şi este un software open source. WordPress este scris folosind PHP şi necesită existenţa suportului de PHP şi MySQL pe hosting-ul dumneavoastră, pentru a fi operaţional acest script. Mai multe informaţii despre PHP găsiți pe PHP Net, PHP pentru designeri - aparţine leaderului de dezvoltare Matthew Mullenweg.



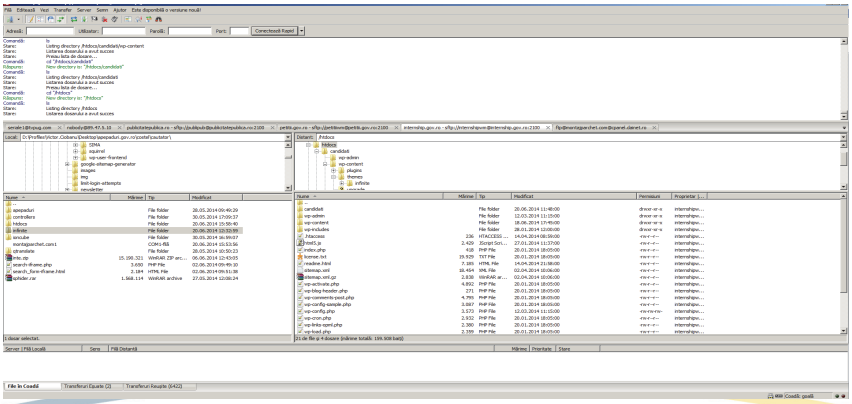
- HTML sau Hyper Text Markup Language, foloseşte limbajul standard WC3, cu toate paginile web care sunt construite. Este???, de la predecesorul său XHTML, HTML, dar de multe ori este încă folosit pentru a descrie o funcţie. Ea este deseori utilizată în combinație cu CSS şi/sau JavaScript. WordPress, se străduieşte să se conformeze cu standardul XHTML. Mai multe informaţii despre HTML găsim pe W3C org.
- CSS este acronimul pentru Cascading Style Sheets. CSS este un limbaj (style language) care defineşte "aspectul" pentru documentele HTML. CSS acoperă culori, font-uri, margini (borders), linii, înălţime, lăţime, imagini de fundal, poziţii avansate şi multe alte opţiuni.

Instalarea se va face pe un server Apache, cu baze de date MySQL. Copierea fișierelor pe domeniul web și în directorul dorit se va face folosind aplicația de transfer de fișiere FileZilla.

Pentru început, voi downloada arhiva WP de pe site-ul WordPress.org. Dacă se dorește instalarea versiunii în limba română trebuie accesat site-ul ro.wordpress.org. Localizarea în limba română se poate face și ulterior. După download, se dezarhivează arhiva și se copiază pe server în directorul dorit, cu ajutorul aplicației FileZilla, folosind protocolul FTP.

Observaţie: în funcție de server pot fi necesare setări mai detaliate pentru a face transferul fișierelor. Citiți cu atenție instrucțiunile oferite de administratorul serverului.

Odată transferate fișierele pe server am încheiat primul pas important în instalarea WordPress-ului pe serverul nostru.



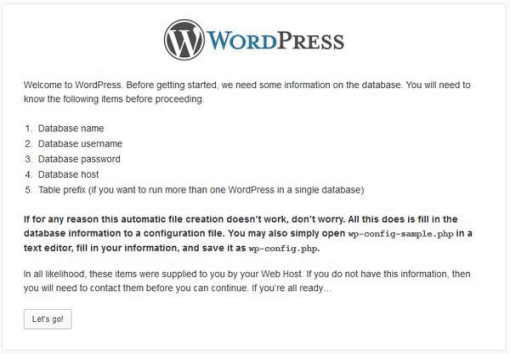
FTP sau File Transfer Protocol este destul de utilizat, fiind un protocol client-server pentru transferul de fişiere. Este un mod de a descărca fişierele şi cea mai comună metodă de a încărca fişiere pe un server. Un client de FTP este un program care să poate descărca fişiere sau încărca fişiere, pe un server FTP. Este posibil să fie nevoie să folosiți un client de FTP, pentru a vă încărca fişiere de WordPress pe serverul dvs. Web, în special în cazul în care utilizaţi un furnizor de hosting.

Programe tip client FTP sunt:

- Filezilla
- FlashFXP
- Total Commander

Pentru a finaliza instalarea, deschidem un browser și în adressbar introducem calea completă spre directorul în care am copiat fișierele WP. Enter și, în următoarea fereastră, este un mesaj prin care suntem atenționați că se va crea fișierul *config.php* în care se vor păstra setările site-ului.

Pentru a continua instalarea automată, facem click pe butonul "**Create a configuration file**". În următoarea fereastră sunt prezentate informațiile necesare instalării precum și câteva cuvinte despre ce trebuie făcut dacă fișierul config.php nu poate fi creat automat.



După cum vedeți, lista conține informațiile necesare conectării la baza de date și creării tabelelor wordpress-ului.

Ceea ce înainte era ca o listă informațională acum este un formular. Introduceți în formular datele notate la crearea bazei de date.

- Database Name (numele bazei de date)
- User Name (numele de utilizator bază de date)
- Password (parolă bază de date)
- Database Host (numele hostului, a serverului de baze de date de obicei localhost)

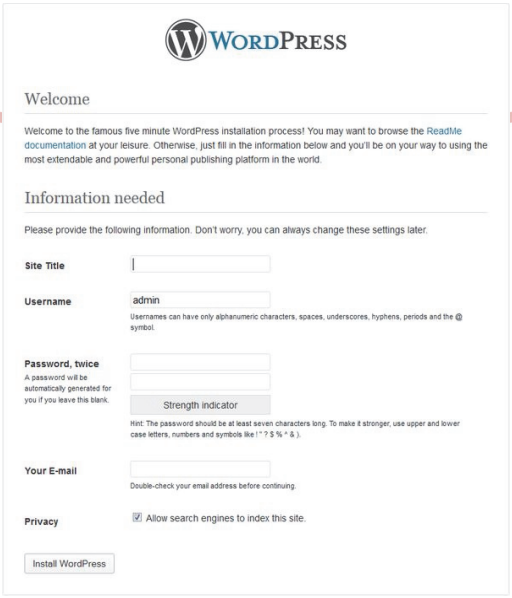
- Table Prefix (prefixul tabelelor wordpress, în cazul în care există mai multe instanţe Wordpress în aceiaşi bază de date)

Dacă nu se specifică nicăieri altfel, Database Host este localhost, ceea ce înseamnă că serverul MySQL de baze de date este pe aceeași mașină cu serverul de web. Dacă aveți un alt nume pentru server, introduceți-l pe acesta.

Ultimul câmp din acest formular este Table Prefix completat implicit cu wp_. Din motive de securitate schimbați acest prefix cu unul personalizat. Modificându-l, puteți instala în aceeași bază de date mai multe wordpress-uri.

O dată completat acest formular, click pe Submit și trecem la următoarea etapă în care ni se va cere să rulăm instalarea.

Run the install (click pe buton) și ni se va deschide ultimul formular din procesul de instalare.



În acest formular vor trebui introduse informațiile de identificare a site-ului și a administratorului. Toate aceste informații vor putea fi modificate ulterior!

- *Site Title* (numele site-ului)
- *Username* (numele de utilizator al administratorului). Implicit acest nume este admin. Din motive de securitate, schimbați acest username cu unul personal.
- *Password* (parola asociată utilizatorului administrator). Din motive de securitate este indicat ca parola să conțină litere mici, litere mari, cifre și simboluri ca: !, ?, $, &, % și altele. De asemenea, este indicat ca în parolă să nu repetați numele de utilizator. Puterea parolei este arătată într-un indicator de putere. Cu cât este mai puternică cu atât mai bine!
- *Your E-mail* (e-mailul tău) este e-mailul oficial al site-ului, e-mail pe care vor veni mesajele generate automat de WordPress sau de plugin-urile instalate. De, asemenea cu ajutorul acestui e-mail puteți genera o nouă parolă dacă pe cea veche ați uitat-o.
- *Privacy*. Această opțiune va permite motoarelor de căutare să indexeze site-ul. Aici se impune o observație. Dacă site-ul este de test sau este în dezvoltate, debifați această opțiune. Nu are rost ca, din greșeală, site-ul să fie indexat în stadiul de dezvoltare sau de testare. Ca și restul informațiilor și aceasta poate fi modificată ulterior instalării.

O dată finalizat și acest formular, click pe Install WordPress și succes!

WordPress este instalat și funcțional!

Acum puteți accesa interfața de administrare pentru a adăuga conținut și pentru a face alte setări folosind numele de utilizator și parola setate anterior.

3.2.2. Structura ierarhică a nivelurilor de acces

- *Administratorul* are acces la toate facilităţile din secţiunea de administrare
- *Editorul* poate publica şi administra materialele publicate – ale lui dar şi ale altora. Acesta poate edita și publica și pagini.
- *Autorul* poate să publice şi să îşi administreze propriile materiale publicate.

- *Contributorul* poate să scrie şi să îşi administreze propriile materiale, dar nu le poate publica.
- *Abonatul* poate să scrie comentarii (dacă acest drept nu este deschis tuturor) şi eventual alte mici facilităţi (tinzând spre zero dacă nu se folosesc plugin-uri specifice).

DREPTURILE UTILIZATORILOR

DREPTURILE UTILIZATORULUI	Administrator	Editor	Autor	Contribuitor	Abonat
Modifică tema	X				
Modifică widgeturi, bara laterală şi footerul	X				
Activează şi dezactivează plugin-uri	X				
Adaugă şi elimină alţi utilizatori	X				
Schimbă rolul utilizatorilor	X	X			
Editează, aprobă sau şterge comentarii	X	X			
Adaugă/şterge eticheta	X	X			
Adaugă/şterge categorii	X	X			
Editează sau şterge articole publicate de orice utilizator	X	X			
Publică pagini	X	X			
Încarcă fişiere media	X	X	X		
Vizionează comentarii	X	X	X	X	
Scrie articole	X	X	X	X**	
Editează articole	X	X	X	X	
Editează profilul personal	X	X	X	X	X

** Contribuitorul are posibilitatea de a publica articole, dar are nevoie de acceptul unui Admin sau Editor.

3.2.3. Adăugarea și editarea conținutului - Tutorial publicare articole în Wordpress

Ghid scriere articole în WordPress:

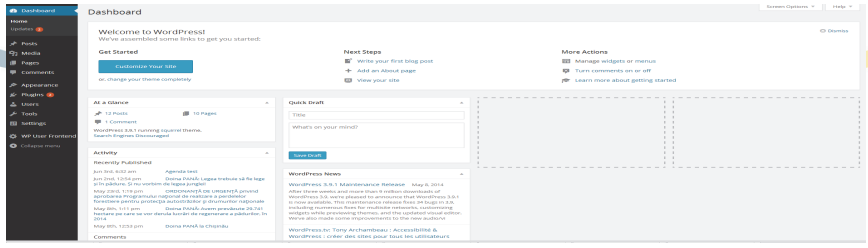
1. Logare

- accesaţi pagina de logare a blogului pe care doriţi să scrieţi (http://blog.com/wp-admin/index.php)

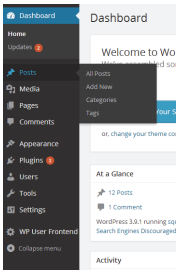
- introduceţi datele de logare şi apasaţi butonul LOGIN

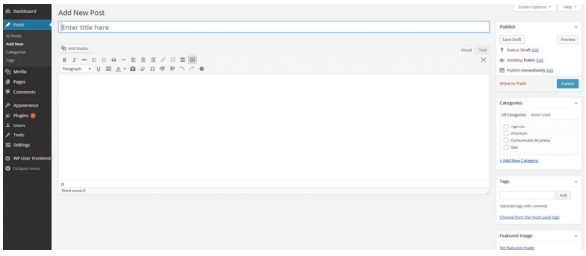
2. Începerea unui articol nou

- după logare veţi vedea panoul de administrare – Dashboard (în imagine, mai jos)



- apăsaţi în partea dreaptă butonul Posts şi apoi Add New.





- în partea de sus, adăugaţi titlul articolului aşa cum doriţi să apară afişat pe blog

• în partea de jos, aveţi secţiunea de adăugare a conţinutului articolului. Acest lucru se poate realiza atât în modul *vizual* (Visual), cât şi *html* (HTML).

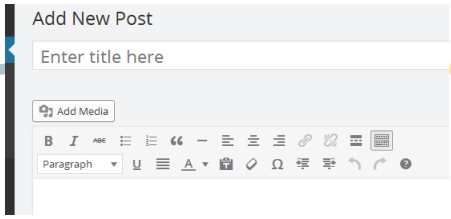
3. Adăugare TEXT

• Modul Visual seamănă foarte mult cu un editor clasic de text (Word/Wordpad). Puteţi îngroşa, înclina, tăia textul. Puteţi crea liste numerotate sau nenumerotate şi puteţi alinia textul (la stânga, la dreapta şi centrare).

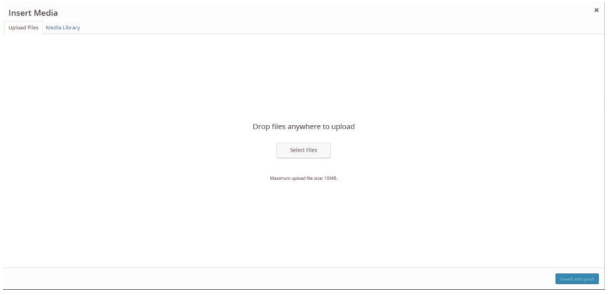
• Modificările menţionate la modul Visual pot fi realizate şi în modul HTML doar că sunt folosite anumite tag-uri (, , etc.)

4. Adăugare IMAGINI

• Pentru a adăuga imagini, apăsaţi primul buton pătrat de deasupra casetei de adăugare text (Add media)

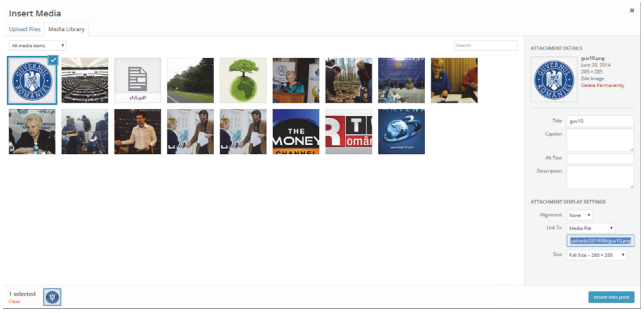


• Acum apăsaţi butonul Upload Files şi alegeţi directorul din care doriţi să includeţi imaginile (puteţi selecta una sau mai multe)

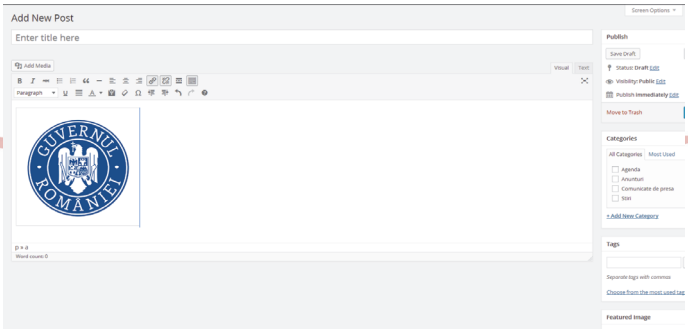


• După introducerea imaginilor, le puteţi edita pe fiecare în parte (dimensiune: Thumbnail, Medium, Large, Full size) şi le puteţi alinia (None, Left, Center, Right)

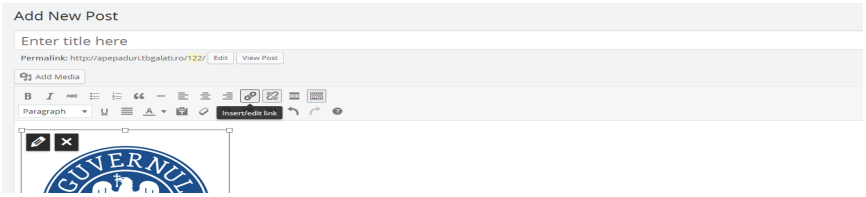
• Pentru a introduce imaginea în articol apăsaţi butonul: Insert into Post



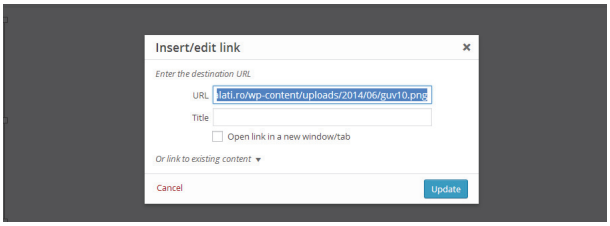
- Vă recomand ca înainte să introduceţi imaginea, să poziţionaţi cursorul în locaţia în care doriţi să apară aceasta
- Dacă vreţi să adăugaţi o nouă imagine trebuie să mergeţi din nou pe butonul pătrat (add media) să selectaţi Gallery şi apoi să apăsaţi butonul Show pentru a vedea detaliile imaginii dorite
- Cam aşa arată imaginea introdusă în articol în modul Visual (în HTML este afişat doar codul):



5. Adăugare LINK-uri

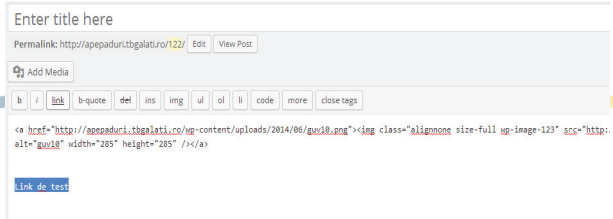


- Pentru a adăuga un link, trebuie mai intâi să selectaţi cuvântul sau adresa (scrisă manual) pe care doriţi să aplicaţi legătura (link-ul) şi apoi să apăsaţi butonul LINK (primul patrăţel roşu), iar apoi să completaţi adresa dorită:



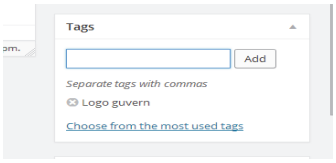
- Pentru a şterge link-ul de pe un text, apăsaţi butonul Remove Link (în dreapta butonului LINK)
- În modul HTML, trebuie tot să selectaţi textul şi apoi să apăsaţi butonul “link”, dar ştergerea legăturii trebuie efectuată manual

După finalizarea articolului mai sunt câteva lucruri care trebuie realizate:



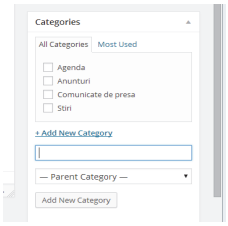
6. Adăugarea de TAG-uri

- Tag-urile reprezină cuvinte cheie din textul articolului sau cuvinte descriptive pentru acesta. Pot avea unul sau mai multe cuvinte, iar fiecare tag trebuie separat prin virgulă de următorul (Ex: tag1, tag 2 cuvinte, tag 3, tag 4). Tag-urile acestea pot fi folosite pentru a grupa diverse articole (o altfel de categorisire, diferită de “categories”) sau pentru a completa meta-keywords
- Optim ar fi să adăugaţi minim 5 tag-uri



7. Adăugarea de CATEGORII

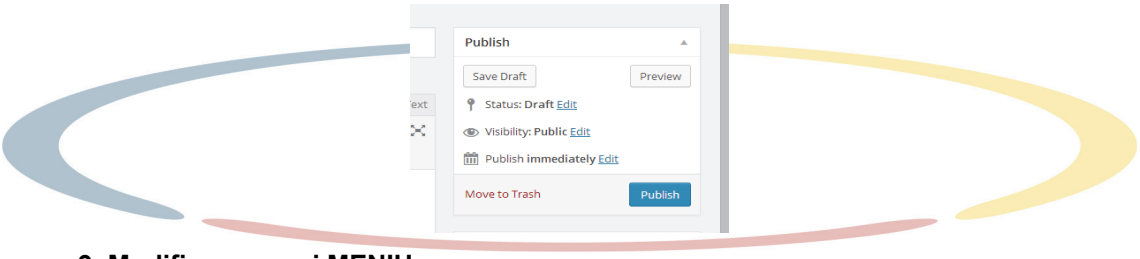
- Articolul trebuie încadrat în categoriile corespunzătoare. Le găsiţi imediat sub secţiunea de tag-uri. De obicei, un articol se încadrează într-o categorie. (nu este nici o problemă dacă articolul se încadrează în mai multe, însă acesta va fi afişat în mai multe secţiuni ale site-ului)



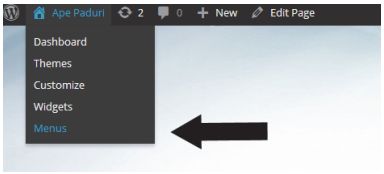
8. Salvarea şi publicarea ARTICOLULUI

- Pentru salvarea stadiului în care se află un articol, apăsaţi butonul Save Draft din colţul dreapta sus. Nu uitaţi să salvaţi articolul din când în când.
- După finalizarea unui articol, apăsaţi butonul Submit for Review, în cazul în care acesta va trebui aprobat de administrator şi apoi va fi publicat sau direct Publish, dacă aveţi acest drept.

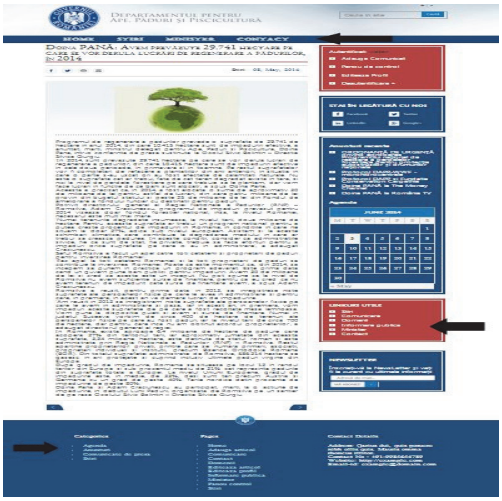
Aceştia sunt paşii de bază pentru scrierea unui articol în WordPress.



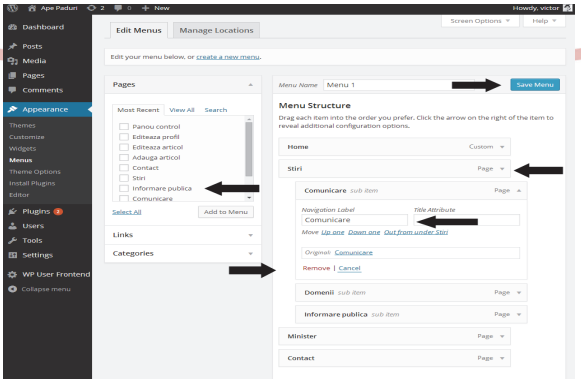
9. Modificarea unui MENIU



Un meniu este o ierarhizare logică a paginilor statice conţinute de un web-site. Meniurile se pot regăsi în diferite secţiuni ale unei pagini web. De obicei, meniul superior conţine trimiteri către paginile ce aparţin platformei, iar cel inferior conţine trimiteri către pagini web ale altor instituţii. Pot exista şi meniuri laterale ce ajută în navigarea sau structurarea informaţiei. Meniul trebuie, obligatoriu, să conţină o pagină de “acasă” sau “home” şi una de contact.



Pentru a modifica un meniu se accesează din bara superioară numele paginii web, apoi secţiunea “Menus”. În secţiunea meniu, putem modifica ordinea afişării paginilor, modifica denumirea elementelor din meniu, adauga sau şterge pagini din meniu. Tot în această secţiune putem crea un nou meniu pe care să îl folosim fie în bara laterală (sidebar), fie în partea inferioară a paginii (footer).



10. Modificarea unei PAGINI STATICE

Există o multitudine de asemănări între o pagină şi un articol. Articolele conţin, de obicei, informaţii de ultimă oră legate de ştiri, agendă, comunicate de presă sau anunţuri, adică informaţii ce se modifică în mod curent. Articolele se regăsesc pe prima pagină şi sunt ierarhizate în funcţie de dată (cronologic), cele mai recente, de obicei, fiind afişate în secţiunea superioară iar cele mai vechi în cea inferioară,

dar pot fi organizate şi în funcţie de categorie, etichete, autor sau taxonomie adiţională.

De obicei, paginile conţin informaţii permanente despre pagina web. Acestea sunt disponibile prin intermediul meniurilor (superior, inferior sau lateral). Paginile nu conţin, de obicei, data la care au fost publicate şi nu sunt ierarhizate cronologic sau în funcţie de categorii, ci prin intermediul meniurilor. Un exemplu ar fi organigrama unei instituţii sau informaţii legate de legislaţie. Chiar dacă paginile conţin informaţii statice, acestea pot fi modificate cu usurinţă.

- Pentru a modifica o pagină se merge la pagina pe care dorim să o modificăm şi se apasă butonul “edit” situat în partea superioară a paginii
- Se poate modifica/completa titlul paginii
- Se poate modifica/completa conţinutul text al paginii
- Se poate adăuga o imagine reprezentativă a paginii
- Se poate crea o galerie compusă din mai multe imagini şi afişa pe pagină
- La final se apasă “Update”

4. BIBLIOGRAFIE

Abric, J. C. – *Psihologia comunicării*, Iaşi, 2002

Alexandru, Ioan – *Drept Administrativ European*, Editura Universul Juridic, Bucureşti, ISBN 978–973–127–081–4, 2008;

Bacivarov A., Ciuchi C., Petrică G., *Servicii Internet*, Editura Matrix Rom, Bucureşti, 197 pag., ISBN 978-973-755-743-8, 2011

Badea-Dincă, N., Păunescu, F., Stăicuț, E. - *Informatizarea societăţii: un fenomen inevitabil?*, Editura Ştiinţifică şi Enciclopedică, Bucureşti,1985

Bird, L. - *Internet - Ghid complet de utilizare*, Editura Corint, Bucureşti, 2004

Bishop, G., Fuchs, H. (co-chairs) - *Research Directions in Virtual Environments*, ACM Computer Graphics, vol. 26, 3, pp. 153-177, 1992

Buckley, P., Clark, D. - *Ghid complet Internet*, Editura Litera Internaţional, Bucureşti, 2009

Buraga, S.C. - *Manipularea obiectelor multimedia in Internet*, lucrare de doctorat, 1998

Chiru , I. – *Comunicare interpersonală*, Editura Tritonic, Bucureşti, 2003

Cristea, V., Patriciu, V. V., Pietroșanu, M., Petculescu, C. - *Mai multe despre Internet*, Editura Teora, Bucureşti, 1996

Cristea, V., Ţăruş, N., Moisa, T., Damian, V. - *Reţele de calculatoare. Proiectare şi utilizare cu programe în limbajul C*, Editura Teora, Bucureşti, 1992

Coman-Kund , F.– *Politica de comunicare externă a colectivităţilor locale*, Editura Economică, Bucureşti, 2000

Dobel, Patrick J. – *Public Integrity* (2001), Johns Hopkins University Press, Maryland, ISBN 978–080–186–916–7, 2001

Dubois , F. – *Les politiques de communication externe des collectivités territoriales*, Université de Lille III, Lille, 1994

Edwards, Michael; Hulme, David – *Beyond the Magic Bullet: NGO Performance and Accountability in the Post-Cold War World* (1996), Kumarian Press, Connecticut, ISBN 978–156–549–051–2, 1996

Florian, G. - *Dicţionar explicativ IT&C*, Editura All, Bucureşti, 2009

Gralla, P. - *Cum funcţionează Internetul*, Editura All, Bucureşti, 2007

Howard J. D. and Longstaff T. A., *A Common Language for Computer Security Incidents*, Sandia Report: SAND98-8667, Sandia National Laboratories.

Ionescu, F. - *Baze de Date Relaţionale şi Aplicaţii*, Editura Tehnică, Bucureşti, 2004

ISO/IEC GUIDE 73:2009

Kaufman, Herbert – *Emerging Conflicts in the Doctrines of Public Administration* American Political Science Review (Vol. 50), Cambridge Univ. Press, ISSN 0003–0554, 1956

Lungu, I. - *Integrarea sistemelor informatice*, Editura ASE, Bucureşti, 2007

Marteau, A. – *Communication publique territoriale*, Les editions de C.N.F.P.T, Paris, 1996

Matei, Lucica – *Managment public, Editura Economică, 2006*

Bacivarov, Mihai I.C., , I. - *E-learning Systems Security*, Quality and Dependability Proceedings of the 12th International Conference on Quality and Dependability Sinaia, Romania, September 22nd-24th, 2010

Marinescu, Ion Alexandru, Antonio Cohal, Valentin Radut, Dezvoltarea şi administrarea aplicaţiilor web folosind instrumente software "open source" de "Content Management System". Studiu comparativ între sistemele JOOMLA şi CMS made simple, Revista Română de Informatică 70 şi Automatică, vol. 20, nr. 4, 2010

Mirkovic J., Prier G., Reiher P., *Attacking DDoS at the Source*, Technical Report, UCLA, 2002
Mirkovic J., Dietrich S., Dittrich D., Reiher P., *Internet Denial of Service: Attack and Defense Mechanisms*, Prentice Hall, 2004
Muller, N.J. - *Enciclopedia Internet*, Editura Tehnică, Bucureşti, 2002
Munteanu, V. A. – *Marketing public*, Editura Sedcom Libris, Iaşi, 2006
Nedelea, Alexandru – *Marketing în Administraţia publică,* 2006
Norton, P., Goodman, J. - *PC - Totul despre calculatoare personale*, Editura Teora, Bucureşti, 2001
Norton, P., Kearns, D. - *Reţele de calculatoare*, Editura Teora, Bucureşti, 2000
Odom, W. - *Primii paşi în reţele de calculatoare*, Editura Corint, 2004
Ogletree, T.W. - *Firewalls. Protecţia reţelelor conectate la Internet*, Editura Teora, Bucureşti, 2001
Patriciu, V.V., Ene-Pietroșanu, M., Bica, I., Priescu, J. - *Semnături electronice şi securitate informatică*, Editura All, Bucureşti, 2006
Patriciu, V.V., Ene-Pietroșanu, M., Bica, I., Văduva, C., Voicu, N. - *Securitatea comerţului electronic*, Editura All, Bucureşti, 2001
Patriciu V.V., Priescu I., Nicolaescu S., *Internet Worms - Propagation Modeling and Analysis*, The 4th ROEDUNET International Conference "Education/Training and Information/Communication Technologies" - ROEDUNET '05, Targu-Mures, Romania, pp. 218-224, ISBN 973-7794-26-5.
Parker D. B., *Computer Security Management*, Reston, VA: Reston Publishing Company Inc., 1981.
Priescu I., Neagu R., Nicolaescu S., *Research Results of a Network Security Perimeter for Romanian E-Commerce Companies*, UTM Megabyte Magazine, Vol. 6, No. 2, pp. 2010, Bucharest, Romania, ISSN: 1841-7361
Popescu D. E., Vladu E., *A genetic Algorithm Approach for Optimizing the File Availability in PeertoPeer Content Distribution*, Journal of Computer Scioence and Control Systems, vol.2, no.1, 2009, pp. 4146.
Random House Webster - *Calculatoare şi Internet*, Editura Corint, Bucureşti, 2003
Roșca, I.Gh., Ţăpuș, N., Cristea, V. ş.a. - *Intranet*, Editura ASE, Bucureşti, 1999
Russell D.and Gangemi G. T. Sr. *Computer Security Basics*, O'Reilly & Associates, Inc.,
Simon , H. A. – *Comportamentul administrativ*
Simon, H. A. . V. A. Thompson, D. W. Smithburg – *Administraţia publică*
Smart, J., Paffendorf, J., and Cascio, J. - *Metaverse Roadmap Overview Project,* 2007
Schneider G. P., *Electronic Commerce*, Third Annual Edition, Thomson Learning, 2002
Shinder D., *Examining intrusion and nonintrusion network attacks*, 2001.
Snell, N., TEMPLE, B., CLARK, M.T. - *Internet şi Web. Ghid complet*, Editura All, Bucureşti, 2004
Sraicut, E. - *".RO" Top Level Domain Registrations,* Proceedings of the NATO Advanced Networking Workshop on Creative and Innovative Network Management, Ohrid, Macedonia, Computer and Systems Sciences, vol. 189, IOS Press, 2003
Tanenbaum, A.S. - *Reţele de calculatoare*, ediţia a 4-a, Editura Byblos, Bucureşti, 2003
Thomas, T. - *Primii paşi în securitatea reţelelor*, Editura Corint, 2005
Vinţan, L.N. - *Maeştri ai ingineriei calculatoarelor - Pagini de istorie (Compilaţie)*, www.agir.ro, 2007

Caruseanu, Vlad Avantajele şi dezavantajele utilizarii unui CMS, www.editorialweb.ro
Vorzsak , A. (coord.) – *Marketingul serviciilor*, Presa Universitară Clujeană, Cluj-Napoca, 2004
Zemor, P. – *La communication Publique,* Presses Universitaires de France, Paris, 1995

RESURSE ONLINE

gs.statcounter.com
www.chip.ro
www.cisco.com
The Cross Site Scripting FAQ, http://www.cgisecurity.com/, 2003
www.drupal.ro
RFC 2196, http://www.ietf.org/rfc/rfc2196.txt
www.joomla.ro
Software Architecture and Design, www.msdn.microsoft.com
Using a Three-Tier Architecture Model, www.msdn.microsoft.com
Web Server Survey, news.netcraft.com
Open Web Application Security Project, https://www.owasp.org
www.pcworld.ro
www.securitatea-informatiilor.ro
US Homeland Security Department - CERT Cyber Security Bulletins - http://www.uscert.gov/
www.w3.org
W3Techs, w3techs.com
www.wikipedia.org
www.wordpress.ro

5. ANEXE

ANEXA 1. DOMENII DE NIVEL SUPERIOR (TOP-LEVEL DOMAIN)

- **ccTLD (*Country-Code Top-Level Domain*)** - secvenţă formată din 2 litere

Tabel A1.1. ccTLD pentru Europa

Ţara (teritoriul)	ccTLD	Ţara (teritoriul)	ccTLD
Albania	**.al**	Isle Of Man	**.im**
Andorra	**.ad**	Italy	**.it**
Armenia	**.am**	Jersey	**.je**
Ascension Island	**.ac**	Latvia	**.lv**
Austria	**.at**	Liechtenstein	**.li**
Azerbaijan	**.az**	Lithuania	**.lt**
Belarus	**.by**	Luxembourg	**.lu**
Belgium	**.be**	Macedonia	**.mk**
Bosnia	**.ba**	Malta	**.mt**
Bouvet Island	**.bv**	Moldova	**.md**
British Indian Ocean	**.io**	Monaco	**.mc**
British Virgin Islands	**.vg**	Montenegro	**.me**
Bulgaria	**.bg**	Netherlands	**.nl**
Croatia/Hrvatska	**.hr**	Norway	**.no**
Cyprus	**cy**	Poland	**.pl**
Czech Republic	**.cz**	Portugal	**.pt**
Denmark	**.dk**	Romania	**.ro**
Estonia	**.ee**	Russia	**.ru**
Europe	**.eu**	San Marino	**.sm**
Faroe Island	**.fo**	Serbia	**.rs**
Finland	**.fi**	Slovakia	**.sk**
France	**.fr**	Slovenia	**.si**
French Southern	**.tf**	South Georgia	**.gs**
Georgia	**.ge**	Spain	**.es**
Germany	**.de**	Svalbard Island	**.sj**
Great Britain	**.gb**	Sweden	**.se**
Greece	**.gr**	Switzerland	**.ch**
Greenland	**.gl**	Turkey	**.tr**
Guernsy	**.gg**	Ucraina	**.ua**
Hungary	**.hu**	United Kingdom	**.uk**
Iceland	**.is**	Vatican City	**.va**
Ireland	**.ie**		

- **gTLD (*Generic Top-Level Domain*)** - secvenţă formată din 3 sau mai multe litere

Tabel A1.2. gTLD generale

Acronim	Descriere	Exemple
.biz	domeniul afacerilor (*business*)	businessseek.biz

Acronim	Descriere	Exemple
.com	societăţi şi companii comerciale	google.com
.info	site-uri informaţionale	worldometers.info
.name	familii, nume de persoane, porecle	nic.name

Acronim	Descriere	Exemple
.net	diverse resurse pentru reţeaua Internet	php.net
.org	alte organizaţii	gentoo.org
.pro	unele profesii	registry.pro

Tabel A1.3. gTLD referitoare la infrastructura reţelei Internet

Acronim	Descriere
.arpa	rezervat în exclusivitate pentru infrastructura reţelei Internet (*Address and Routing Parameter Area*)

Tabel A1.4. gTLD rezervate

Acronim	Descriere
.example	pentru utilizare în exemple; www.example.com
.invalid	pentru utilizare în nume de domenii inexistente
.localhost	pentru a se evita confuzia cu localhost (calculatorul local)
.test	pentru utilizare în teste

Tabel A1.5. gTLD sponsorizate

Acronim	Descriere	Exemple
.aero	industria transporturilor aeriene	sita.aero
.asia	organizaţii şi companii din zona Asia-Pacific	domains.asia
.cat	limba şi cultura catalană	domini.cat
.coop	cooperative	wedge.coop
.edu	organizaţii educaţionale (universităţi, colegii)	harvard.edu
.gov	entităţi guvernamentale americane (federale, statale sau locale)	fbi.gov, cia.gov
.int	organizaţii internaţionale inter-guvernamentale	nato.int
.jobs	site-uri legate de forţa de muncă	goto.jobs
.mil	organizaţii militare americane (armată, marină)	nic.mil
.mobi	site-uri cu referinţă la dispozitive mobile	mtld.mobi
.museum	Muzee	about.museum
.tel	servicii referitoare la conexiuni între reţele telefonice şi Internet	app.tel
.travel	site-uri legate de turism şi călătorii: agenţii de turism, linii aeriene, hoteluri	whl.travel
.xxx	industria divertismentului pentru adulţi	about.xxx

ANEXA 2 – GOV.RO - Evoluţia www.gov.ro – 2000 – 2014

Înregistrarea domeniului - 1996-01-01.

2001 - 2002

Primele teste – 23 octombrie 2000, OPERAŢIONAL – 28 noiembrie 2001

- Site de prezentare;
- Tehnologie – HTML;
- Informaţie multă;
- Căutarea informaţiei greoaie;
- Organizarea conţinutului;
- Actualizare cu întârzieri mari a conţinutului;

VIZITATORI (media zilnică cf. trafic.ro):

- 7.125 vizitatori/zi;
- 177.761 afişări.

2003 - 2004

- Frecvenţă mare de actualizare;
- Reorganizare conţinut;
- Adoptarea unei noi tehnologii - PHP (o parte din pagini rămân statice în HTML);
- Implementarea de baze de date;
- Dezvoltarea unui modul de tip CMS pentru actualizarea conţinutului.

VIZITATORI (media lunară cf. trafic.ro):

- 78.858 vizitatori;
- 387.622 afişări.

2005

- Modificare layout & design;
- Adăugarea de noi secţiuni (declaraţii de avere)
- Îmbunătăţirea modulului de CMS (Backend) pentru automatizarea introducerii de conţinut;
- Reproiectarea bazei de date asociate.

VIZITATORI (media lunară cf. trafic.ro):

- 156.974 vizitatori;
- 701.389 afişări.

2006 – 2007 – Îmbunătăţiri la nivel de conţinut, apariţia de noi secţiuni, reorganizare content, apariţia newsletterului ca alternativă de contact pentru vizitatorii www.gov.ro, secţiuni dedicate pentru transparenţă (acte normative supuse consultării publice), implementarea serviciului de ştiri în format RSS.

2008

- Modificare design & layout
- Îmbunătăţire modul introducere content (backend - editor de text WYSIWYG, utilizare sisteme de templaturi “Smarty”),
- Realizarea unui model standardizat de lucru privind introducerea informaţiei.
- CMS bazat pe roluri (admini şi editori),
- Transferul introducerii de content către cei care produc contentul.
- Diversificarea materialelor multimedia (audio / video)
- Realizarea unui manual de administrare şi utilizare
- Tehnologie - cerinţe tehnice (Apache 2.2.8, PHP 5.2.5, MySql 5.0.45)

VIZITATORI (media lunară):

- 221.424 vizitatori
- 801.389 afişări

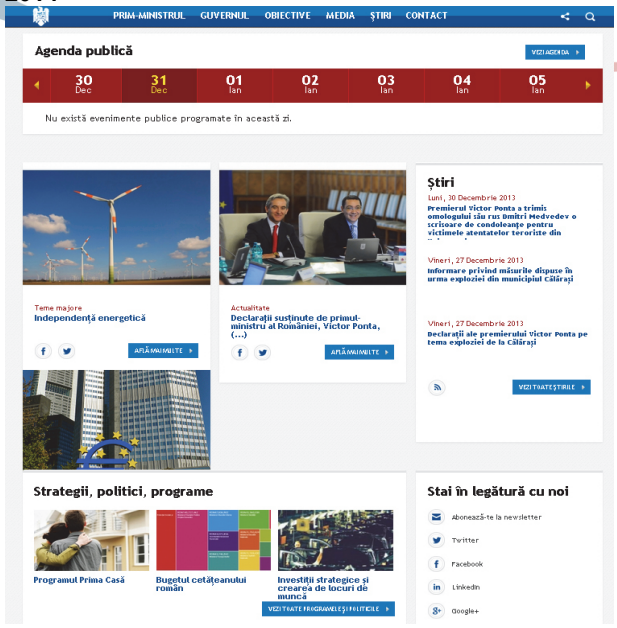
2008 – 2013 - au fost realizate îmbunătăţiri la nivel de structurare conţinut, reorganizare secţiuni şi modificare de template-uri, conţinutul fiind elementul cel mai important în raport cu design-ul şi tehnologia adoptată, noi modalităţi de comunicare media: Youtube, Twitter, Facebook, Newsletter, implementarea de capacităţi de streaming live.

2013

- Modificare design la nivel CSS;
- Dimensiunea bazei de date şi a conţinutului foarte mari (bd - 500Mb, conţinut – 12Gb);
- timp de răspuns mare.

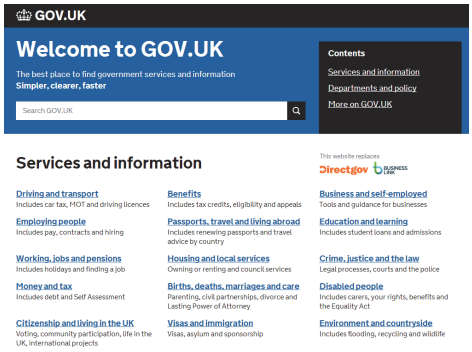
VIZITATORI (media lunară):
- 177.258 vizitatori
- 814.100 afişări

2014

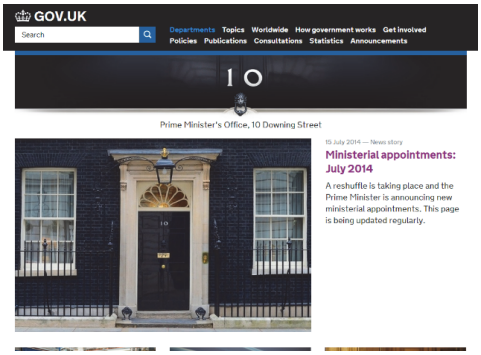


- Modificare arhitectura aplicaţiei, design şi template;
- Arhitectura bazelor de date;
- Diversificarea canalelor de comunicare (Linkedin, Google+);
- Introducerea de proprietăţi pentru device-uri mobile (responsive etc)

ANEXA 3 – Identitatea vizuală unică în comunicarea online

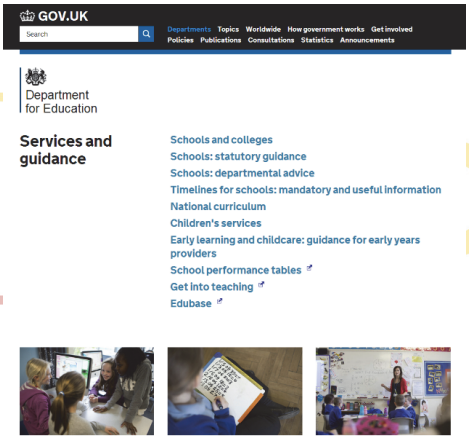


Imaginea 1: Portalul GOV.UK



Imaginea 2: Biroul Premierului

Imaginea 3: Departamentul pentru Inovare în Business



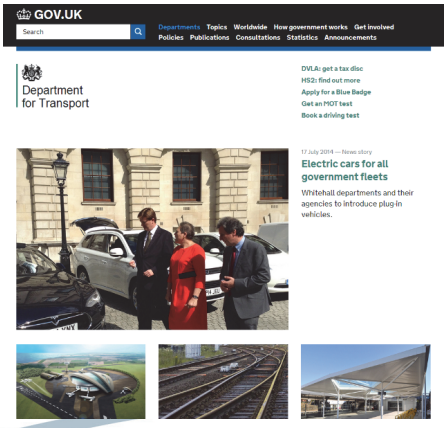
Imaginea 4: Departamentul pentru Educație

Conceptul „Digital by default" a fost propus inițial în cadrul raportului Directgov 2010 and beyond: revolution not evolution, elaborat pentru Guvernul britanic de către Martha Lane Fox, fondatoarea portalului lastminute.com. Conceptul a reprezentat ulterior fundamentul Strategiei Digitale Guvernamentale[22], adoptate în noiembrie 2012, strategia prin care s-a estimat o economisire sistematică anuală în ceea ce privește cheltuielile din domeniul IT de 1,7 miliarde de lire sterline.

Principalul organism instituțional creat în vederea implementării Strategiei este Serviciul Digital Guvernamental (*Government Digital Service*), aflat în subordinea Secretariatului General al Guvernului Regatului Unit. Acest organism s-a ocupat de tranziția platformelor

[22] A se vedea https://www.gov.uk/government/publications/government-digital-strategy (accesat 17 iulie 2014)

online ale administrației publice centrale către o interfață unică, dezideratul final fiind accesul prin intermediul spectrului online la orice serviciu public ce poate fi obținut în mod tradițional numai prin deplasarea fizică la sediul instituțiilor. Totodată, Strategia prevede realizarea unei identități online standardizate atât din perspectiva reprezentării grafice, cât și din cea a structurării informațiilor prezentate pe paginile instituționale.



Imaginea 5: Departamentul pentru Transporturi

Imaginea 6: Departamentul pentru Sănătate

Standardizarea a fost planificată pe un calendar de acțiuni având anul 2014 ca termen limită pentru tranziția către noul format. La acest moment, toate ministerele și departamentele centrale au fost transpuse pentru a respecta principiile trasate din perspectiva layout-ului, a tipografiei, a culorilor, imaginilor, iconițelor, butoanelor și a datelor[23].

Analizând comparativ, dacă în Regatul Unit a fost aleasă decizia de a centraliza informațiile și de a standardiza conținutul și designul prin intermediul unui portal unic (gov.uk), în România ministerele și instituțiile își gestionează în mod individual paginile de internet, ceea ce duce la cheltuieli ridicate pentru realizare, mentenanță și actualizare.

[23] A se vedea https://www.gov.uk/service-manual/user-centred-design/resources/elements/index.html (accesat 17 iulie 2014)

ANEXA 4 – SEO

SEO, Optimizarea poziționării la (motoare de) căutare, este un proces de perfecționare (favorizare) a vizibilității paginilor web site sau web page în cadrul ordonării rezultatelor căutării în lista făcută de motorul de căutare. "Search Engine Optimization" (SEO, în română optimizare pentru motoare de căutare) este o subcategorie a marketing-ului online SEM, practică apărută în anul 1990, odată cu apariția primelor site-uri pe Internet și care reprezintă totalitatea tehnicilor prin care un site web este adus la o formă în care este propulsat mai sus în lista de rezultate date de un motor de căutare pentru diverse căutări. Cu timpul, optimizarea unei pagini web a unui site a devenit un serviciu oferit de unele companii și/sau corporații.

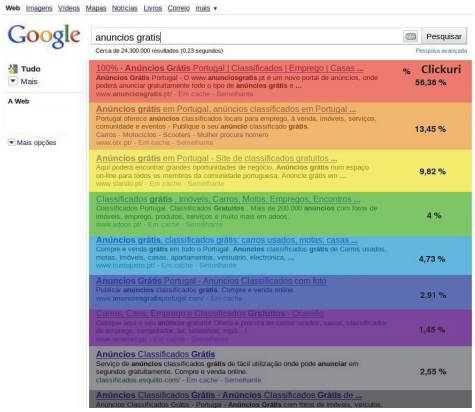
La începuturile Internetului, motoarele de căutare afișau în urma unei căutari, pagini în a căror descriere se afla cuvântul de cautare. Deoarece webmaster-ii (proprietarii de site-uri) au făcut abuz de acest factor pentru a atrage mai mult trafic, motoarele de căutare au alcătuit algoritme mult mai complexe, care includ:

- Textul cuprins între etichetele <title> și </title>
- Nume de domeniu
- Elementele HTML
- Etichetele HTML
- Frecvența unui cuvânt cheie, atât în pagină cât și global
- Sinonime ale cuvântului cheie
- Atributele ALT pentru imagini
- Titlul link-urilor
- Numărul total de hyperlink-uri de la și spre o pagină
- Calitatea site-urilor de la care pleacă link-uri spre o pagină
- Vechimea unui site

CE ESTE SEO

În sens larg, SEO reprezintă o componentă a Marketing-ului prin faptul că necesită înţelegerea modului în care funcționează algoritmii de căutare și ce ar căuta vizitatorii, pentru a stabili o corespondență cu site-urile care oferă ceea ce aceștia caută. Anumite tehnici SEO pot implica optimizarea codării unui site, fără a face modificări vizibile pentru vizitatori, precum ierarhizarea structurii site-ului, evitarea sau rezolvarea unor probleme care ar putea impiedica motoarele de căutare să indexeze complet site-ul. Alte eforturi mai vizibile ar fi includerea de conținut unic care este ușor indexat şi extras de pe site-uri web.

Acum că am stabilit ce înseamnă SEO şi la ce serveşte – haideţi să vedem cine are nevoie de aceste servicii. În principiu – orice entitate prezentă pe web. Dar, aici apare o problemă – e clar că două site-uri diferite nu pot fi în acelaşi timp pe primul loc în pagina de rezultate Google.



Marea majoritate a celor care folosesc Google sau alte motoare de cautare, se opresc asupra primelor rezultate returnate la cautarea lor, de aceea, pentru ca un site să primească mulţi vizitatori, el trebuie să se afle pe prima pagina de rezultate returnate de Google, la căutările legate de domeniul de care ţine şi pe o poziţie superioară.

Se spune că Google are peste 300 de factori în componența algoritmului de afișare a rezultatelor, ceea ce a creat numeroase polemici legate de tacticile folosite pentru SEO, în randul webmasterilor. Iar, într-un sondaj de opinie, peste 120 de experți în SEO au oferit opinii despre importanţa a peste 80 de factori de ranking.

Optimizarea corectă a unui site conduce la o mai bună prezenţă în motoarele de căutare, la căutări relevante efectuate de utilizatori, legate de informaţiile, serviciile sau produsele prezentate pe site. Acest lucru conduce la mai mulţi vizitatori, mai multe persoane interesate şi mai multe vânzări. Insă, asta nu este tot ceea ce face SEO, impactul lui fiind unul mult mai vast şi mai benefic.

SEO AJUTĂ

- motoarele de cautare să afle informaţii despre pagina dvs. mai rapid şi mai eficient
- oamenii să găsească informaţiile, imaginile, produsele sau serviciile de care au nevoie
- instituţiile să furnizeze cetăţeanului informaţii actualizate
- adevarata industrie de specialişti şi traineri să aibă locuri de muncă
- la reducerea cheltuielilor cu promovarea online

CARE SUNT FACTORII PRINCIPALI

În ceea ce priveşte SEO făcut unei pagini web, trebuie să avem în considerare o serie de activităţi:

- Crearea unui design SEO prietenos, care să capteze utilizatorii şi să îi ţină cât mai mult pe site, urmând să îi facă să revină
- Domeniul web - vârsta şi relevanţa acestuia
- Vârsta fiecărui link din site şi redirectul linkurilor vechi către cele noi, pentru a transmite din autoritatea acestora

- Scrierea codului pentru un site web optimizat
  - Scrierea codului cât mai eficient posibil, astfel încât citirea şi implicit, încarcarea paginii, să fie cât mai rapidă
  - Dimensiunea totală a codului să nu fie foarte mare
  - Existenţa atributelor alt şi title pentru imagini
  - Folosirea tag-urilor heading: h1, h2, h3, h4, h5, h6
  - Ideal ar fi să existe un singur fişier CSS
  - Evitarea linkurilor către alte site-uri, întrucât daţi din autoritatea site-ului dumneavoastră către aceste site-uri
  - Nu folosiţi prea multe linkuri interne pe o singură pagină
  - O singură intrare în site: www.site.ro sau site.ro; redirectul unuia dintre ele în celălalt
  - Redirectarea paginilor care nu mai există către homepage-ul site-ului; veţi transfera astfel şi din autoritatea paginilor care nu mai există şi evitaţi situaţiile neplăcute de a trimite utilizatorul către o pagină inexistentă
  - Scrierea META Titlurilor (60-70 caractere), a META Descrierilor (150-160 de caractere) şi definirea cuvintelor cheie pentru fiecare pagină – acestea trebuie să fie cât mai relevante şi să se regăsească în pagină
  - Rescrierea linkurilor care să conţină cuvintele cheie alese (dar care să aibă legatură cu tot conţinutul paginii)
  - Redirectarea linkurilor vechi către cele noi (redirect 301) pentru a transefera autoritatea
  - Implementarea tool-urilor Google Analytics şi Google Webmaster pentru monitorizarea site-ului
  - Existenţa faviconului (logo-ul dumneavoastră trebuie să se regăsească sus în bara de browser
  - Existenţa fişierului robots.txt
  - Existenţa sitemap.xml şi a sitemap.html
- Conţinutul site-ului
  - Scrierea unui continut relevant pentru utilizator, folosind cuvintele cheie dupa care dorim să se facă indexarea
  - Nu folosiţi conţinut duplicat
  - Pagina trebuie să aibă cât mai mult conţinut şi să fie updatată frecvent
- Imaginile
  - Imaginile trebuie să aibă o dimensiune cât mai mică, să fie facute special pentru web, astfel încât să se încarce cât mai rapid de pe server
  - Imaginile trebuie denumite conform cuvintelor cheie alese
  - Marimea site-ului
  - Cu cât este mai mare, cu atât un site este mai important. Trebuie sa ne concentram în permanenţă asupra adaugării unor pagini noi şi a unui conţinut nou pe paginile existente.
- Reţele Sociale
  - Existenţa reţelelor sociale în site este foarte importantă; încercaţi să postaţi cât mai mult pe reţelele de socializare şi să atrageţi cât mai mulţi utilizatori către site
- Găzduirea

- Site-ul trebuie gazduit pe servere de încredere, astfel încât să se încarce repede, sa nu intrăm în blacklist şi să fie în permanenţă activ
- Cu cât obţinem o notă mai mare în tabelul de mai jos, cu atât şansele de a fi bine poziţionat pe pagina de rezultate, cresc.

Content - conţinut	Html - Html	Architecture - arhitectură site	Links - legături	Trust - încredere	Social - interacţiuni social media	Personal - factori personali
Cq - calitate	Ht - titlu	Ac - indexabil	Lq - calitate articol	Ta - autoritar	Sr - reputaţie	Pc - ţara
Cr - cercetare	Hd - descriere	Ad - articol unic	Lt - calitate explirare	Th - vechime	SS - număr de partajări	Pl - localitate
Cw - cuvinte folosite	Hh - antet	As - viteză	Ln - corectitudine cifre	Ti - identitate		Ph - istoric
Ce - angrenare	Hs - structură	Au – URL clar	Vp - articol plătit	Vd - piraterie		Ps - interacţiuni sociale
Cf - noutate	Vs - repetiţii	Am - funcţionabil pe mobil	VL - spam			
Vt – nedocumentat	Vh - text ascuns	Vc - link ascuns				
Va - reclamă platită						